TARTU ÜLIKOOL

Ülo Kaasik, Uno Kaljulaid

KOMBINATOORIKA

analüütilisi ja algebralisi meetodeid

TARTU 1993

TARTU ÜLIKOOL

ARVUTITEADUSE INSTITUUT

Ülo Kaasik, Uno Kaljulaid

KOMBINATOORIKA

analüütilisi ja algebralisi meetodeid

Tartu 1993

Arvutiteaduse instituudi kolleegiumi koosolekul 23. veebruaril 1993. a. kinnitatud õppevahendiks aines "Diskreetne matemaatika III"

Sisukord

Sissejuhatus kombinatoorikasse

1. Permutatsioonid

Kombinatoorikal on diskreetses matemaatikas mõnevõrra keskne koht selles mõttes, et ta ühendab nimetatud matemaatikaharu mitmeid näiliselt erinevaid suundi. *Kombinatoorika* eesmärgiks on luua ning uurida meetodeid niisuguste ülesannete lahendamiseks, mis seostuvad teatava diskreetse (eeskätt just lõpliku) hulga elementide mingeid lisatingimusi rahuldavate nn. paigutuste (näiteks valikute või järjestuste) leidmisega. Põhiprobleemideks osutuvad sealjuures just nõutud liiki paigutuste olemasolu selgitamine, olemasolu korral aga eristatavate paigutuste koguarvu loendamine ja vastavate moodustamisalgoritmide konstrueerimine.

Kuigi mõningad kombinatoorika-alased teadmised pärinevad juba antiikajast (näiteks hulknurkarvud esinesid Pythagorasel), võib selle matemaatikaharu tekkimise siiski seostada XVII sajandiga, mil eeskätt just hasartmängudest tulenevate tõenäosusteoreetiliste ülesannete lahendamiseks tuletati esimesed kombinatoorikavalemid (P. de Fermat, Chr. Huygens, B. Pascal). Esimese katse saadud tulemuste üldistavaks kokkuvõtmiseks tegi juba 1666. aastal vaevu kahekümneaastane G. W. Leibniz (kellelt muide pärineb ka kombinatoorika nimetus). Kuigi lihtsaimate kombinatoorikaülesannete lahendamiseks vajalikkude meetodite põhiosa kujundati tegelikult välja juba XVIII sajandil (Jak. Bernoulli, L. Euler, J. Stirling), on nende meetodite loomine ja täiustamine jätkunud ka XX sajandil.

Mitmesuguste kombinatoorikaprobleemide käsitlemisel, aga samuti ka vastavate lahendamismeetodite tuletamisel tuginetakse enamasti kas nii või teisiti järgmisele kahele postulaadile, mis võibki võtta kogu edasise käsitluse aluseks.

Korrutamisreegel. Kui objekti A saab valida m erineval viisil ja pärast iga sellist valikut saab objekti B valida n erineval viisil, siis nii A kui ka B valimiseks leidub täpselt $m \cdot n$ erinevat võimalust.

Liitmisreegel. Kui objekti A saab valida m erineval viisil, objekti B aga n erineval viisil, kusjuures A ja B valikud on teineteist välistavad (s.t. pole võimalik valida nii A kui ka B samal viisil), siis kas A või B valimiseks leidub täpselt $m + n$ erinevat võimalust.

Loomulikult saab samad reeglid täiesti vahetult üldistada kahelt objektilt ka objektide suvalise lõpliku hulga juhule. Mõnevõrra kompaktsemateks osutuvad niiviisi tekkivate üldistuste sõnastused aga hulgateooria terminites, sest need reeglid on tõlgendatavad vastavalt lõplike hulkade otsekorrutise ja ühendi võimsuste ehk elementide arvude leidmise järgmiste eeskirjadena.

Korrutamisreegel. Suvaliste lõplike hulkade $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$ korral avaldub nende otsekorrutise elementide arv korrutisena

$$|\mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_n| = |\mathcal{H}_1| \cdot |\mathcal{H}_2| \cdots |\mathcal{H}_n|.$$

Liitmisreegel. Paarikaupa ühisosata lõplike hulkade $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$ korral avaldub nende ühendi elementide arv summana

$$|\mathcal{H}_1 \cup \mathcal{H}_2 \cup \ldots \cup \mathcal{H}_n| = |\mathcal{H}_1| + |\mathcal{H}_2| + \cdots + |\mathcal{H}_n|.$$

Kombinatoorika klassikalisteks ülesanneteks võib lugeda teatava suvalise struktuuriga põhihulga mingis mõttes eristatavate alamhulkade (kombinatoorikas nimetatakse neid mõnikord ka *ühenditeks*) moodustamisvõimaluste arvu leidmise ülesanded. Sõltuvalt põhihulga struktuuri ja alamhulkade eristamisviisi täpsustamisest saab siit mitu erinevat ühendiliiki.

Eristamisviisi poolest jagunevad ühendid kahte põhiklassi. Võtame nendest kõigepealt vaatlusele just selle klassi, kus hulkade eristamise aluseks on võetud neis määratud *lineaarne järjestus*.

Põhihulga m-elemendilisi lineaarselt järjestatud alamhulkasid nimetatakse *m-permutatsioonideks*. Alamhulkade eristamine toimub permutatsioonide korral seega nii nende koosseisu kui ka järjestuse järgi. Konkreetseid permutatsioone esitame järgnevas kas vektoritena $(a_1, a_2, \dots, a_m)$ või võimaluse korral sõnedena $a_1a_2\dots a_m$.

Vaatleme kõigepealt juhtu, mil põhihulk on n.-ö. tavaline hulk, mis koosneb n erinevast elemendist. Niisuguse põhihulga erinevate m-permutatsioonide arvu tähistatakse enamasti sümboliga $P(n, m)$. Selle arvu (mida koolikirjanduses on nimetatud ka "*variatsioonide arvuks n elemendist m kaupa*" ja tähistatud kas sümboliga V_n^m või A_n^m) võib leida järgmise täiesti vahetu aruteluga. Alamhulga esimese elemendi valimiseks on ilmselt n võimalust, teise elemendi valimiseks $n-1$ võimalust (sest põhihulga üks element on juba valitud) jne., nii et korrutamisreegli rakendamine annab otsitava arvu jaoks kokkuvõttes valemi

$$P(n, m) = n(n-1)\dots(n-m+1), \tag{1.1}$$

mis kehtib iga $m = 1, 2, \dots, n$ korral. Nii näiteks põhihulga $\{a, b, c, d\}$ korral saab moodustada kokku $P(4, 3) = 24$ erinevat 3-permutatsiooni, mis kolmetäheliste sõnede kujul esitatuna on järgmised:

abc abd acb acd adb adc bac bad bca bcd bda bdc

cab cad cba cbd cda cdb dab dac dba dbc dca dcb.

Valemist (1.1) järeldub tegelikult ka asjaolu, et $m > n$ korral $P(n, m) = 0$ (s. t. põhihulgast võimsamaid alamhulki ei ole võimalik moodustada). Selle valemi täiendamiseks aga defineeritakse tavaliselt veel juurde, et tühja alamhulka saab moodustada ainult ühel viisil: iga n korral $P(n, 0) = 1$.

Erijuhul $m = n$ annab valem (1.1) n-permutatsioonide (ehk lihtsalt *permutatsioonide*) arvu, mis avaldub *faktoriaalina*

$$P(n,n) = n(n-1)\dots 1 = n!.$$

Seda arvu on sageli otstarbekohane tõlgendada n-elemendilises hulgas defineeritavate erinevate lineaarsete *järjestuste arvuna*. Teisiti öeldes annab faktoriaal seega n-elemendilise hulga kõikide erinevate teisenduste (s. t. üksüheste iseendalekujutuste) ehk substitutsioonide arvu.

Võrduse (1.1) parem pool kujutab endast diskreetses matemaatikas sageli esinevat avaldiseliiki, milleni tihti jõutakse isegi siis, kui probleemil ei näi olevat üldse mingisugust seost permutatsioonidega. Seetõttu nimetatakse niisugust järjestikuste täisarvude korrutist matemaatikas enamasti arvu n *kahanevaks m-faktoriaaliks* ning kasutatakse tema tähistamiseks sümbolit

$$(n)_m = n(n-1)\dots(n-m+1) \tag{1.2}$$

(paneme ühtlasi tähele, et tavalist faktoriaali $n!$ võib seega soovi korral tõlgendada arvu n kahaneva n-faktoriaalina).

Tegelikult kujutab võrdus (1.2) endast erijuhtu mõnevõrra üldisemast definitsioonist. Nimelt võib iga fikseeritud naturaalarvu m jaoks defineerida suvalise reaalarvu $x \in \mathbb{R}$ korral määratud funktsiooni

$$(x)_m = x(x-1)\dots(x-m+1), \tag{1.3}$$

mida nimetatakse arvu x *kahanevaks m-faktoriaaliks*. Täiendavalt võib selle funktsiooni defineerida veel ka mittepositiivse m tarvis: iga x korral $(x)_0 = 1$ ning

$$(x)_{-m} = \frac{1}{(x+1)(x+2)\dots(x+m)}.$$

Viimane üldistus tuleneb soovist säilitada kahaneva faktoriaali põhiomadus

$$(x)_{m+n} = (x)_m(x-m)_n.$$

Analoogiliselt defineeritakse iga naturaalarvu m jaoks veel teine suvalise reaalarvu $x \in \mathbb{R}$ korral määratud funktsioon, arvu x *kasvav m-faktoriaal*:

$$x^{(m)} = x(x+1)\dots(x+m-1) = (x+m-1)_m. \tag{1.4}$$

Peale selles võrduses näidatu saab kahe äsjadefineeritud funktsiooni tarvis kergesti põhjendada veel seosed

$$x^{(m)} = (-1)^m(-x)_m = \frac{1}{(x-1)_{-m}}. \tag{1.5}$$

Erinevate m-permutatsioonide arvu ülalkirjeldatud vahetu leidmisviis pole rakendatav kõikide ühendiliikide korral. Osutame seetõttu ka üldisema meetodi arvude $P(n,m)$ leidmiseks.

Fikseerime põhihulgas mingi ühe elemendi ja jaotame permutatsioonid selle järgi kahte klassi. Fikseeritud elementi mitte sisaldavate m-permutatsioonide arvu saab esitada kujul $P(n-1,m)$, s. t. kui m-permutatsioonide arvu ülejäänud elementidest moodustatud põhihulga korral.

Fikseeritud elementi sisaldavad m-permutatsioonid võime saada sel teel, et lisame fikseeritud elemendi mistahes $(m-1)$-permutatsioonile ülejäänud elementidest. Kuid nimetatud permutatsioonide arv on $P(n-1,m-1)$ ja fikseeritud elemendi lisamisel $(m-1)$-elemendilisse järjendisse saab valida m positsiooni vahel. Seega kokkuvõttes annavad korrutamis- ja liitmisreegel võrduse

$$P(n,m) = P(n-1,m) + m\,P(n-1,m-1). \tag{1.6}$$

See kujutab endast *rekurrentset võrrandit*, mis tuleb lahendada ülalnimetatud *rajatingimustel* $P(n,0) = 1$ ja iga $m > n$ korral $P(n,m) = 0$. Lahendamine võib toimuda näiteks induktsiooniga m järgi, milleks võrdust (1.6) korduvalt rakendades avaldame m-permutatsioonide arvu $(m-1)$-permutatsioonide arvude kaudu:

$$\begin{aligned} P(n,m) &= P(n-1,m) + m\,P(n-1,m-1) = \\ &= P(n-2,m) + m\,P(n-2,m-1) + m\,P(n-1,m-1) = \dots \\ \dots &= P(m-1,m) + m\sum_{i=1}^{n-m+1} P(n-i,m-1) = \\ &= m\sum_{i=1}^{n-m+1} P(n-i,m-1). \end{aligned}$$

Juhul $m = 1$ omandab see võrdus kuju

$$P(n,1) = 1\cdot\sum_{i=1}^{n} P(n-i,0) = \sum_{i=1}^{n} 1 = n$$

ja juhul $m = 2$ kuju

$$P(n,2) = 2\cdot\sum_{i=1}^{n-1} P(n-i,1) = 2\cdot\sum_{i=1}^{n-1}(n-i) = n(n-1).$$

Need erijuhud võimaldavad nähtavasti juba oletada lahendi üldkuju (1.1) ning jääb veel vaid tulemuse põhjendamine induktsioonimeetodil (jätame põhjendamise siin siiski esitamata, pealegi võiks kasutada ka induktsiooni n järgi).

Permutatsioonide teise klassikalise juhu annab niisugune põhihulk, milles on samuti n erinevat elementi, kuid igaühte neist võib permutatsioonide moodustamisel võtta suvaline arv korda (öeldakse ka, et põhihulk sisaldab iga elementi suvalises arvus eksemplarides). Erinevate m-permutatsioonide arvud $W(n,m)$ saab nüüd leida täiesti vahetu mõttekäiguga täpselt samuti, nagu me ülal leidsime arvud $P(n,m)$:

$$W(n,m) = n^m.$$

Näiteks eesti tähestiku tähti kasutades saab moodustada kokku $23^3 = 12\,167$ erinevat kolmetähelist sõnet.

Vaatleme lõpuks veel niisugust juhtu, mil põhihulgas on küll kokku n elementi, kuid nende seas leidub vaid k erinevat, kus $k < n$. Esinegu nimelt esimene element m_1 eksemplaris, teine element m_2 eksemplaris jne., kusjuures peab muidugi kehtima seos $m_1 + m_2 + \cdots + m_k = n$.

Hulga mõiste niisugust üldistust nimetatakse tavaliselt multihulgaks. Täpsemalt, ***multihulk*** defineeritakse kui paar $(\mathcal{H}, s)$, kus $\mathcal{H}$ (multihulga *baas*) on tavaline hulk ja s (multihulga *spetsifikatsioon*) funktsioon baasist $\mathcal{H}$ kõikide *naturaalarvude hulka* $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Näiteks kui multihulga baas on $\mathcal{H} = \{h_1, h_2, \ldots, h_k\}$, siis esitab funktsiooni $s : \mathcal{H} \to \mathbb{N}$ vektor $s = (m_1, m_2, \ldots, m_k)$, kus $m_i = s(h_i)$ on elemendi h_i esinemise *kordsus* multihulgas. Öeldakse, et multihulk on n-elemendiline, kui

$$m_1 + m_2 + \cdots + m_k = n$$

ja mõnikord isegi tähistatakse teda tavalise n-elemendilise hulgana, kirjutades baasi iga elementi kordsusega võrdne arv korda. Näiteks baasiga $\mathcal{H} = \{a, b, c\}$ ning spetsifikatsiooniga $s = (2, 4, 4)$ määratud 10-elemendilise multihulga võib soovi korral kirjutada kujul $\{a, a, b, b, b, b, c, c, c, c\}$ või isegi kujul $\{a^2, b^4, c^4\}$.

Piirdume üldise multihulga juhul üksnes erinevate n-permutatsioonide arvu $K(m_1, m_2, \ldots, m_k)$ leidmisega. Seda arvu on loomulik tõlgendada vaadeldava spetsifikatsiooniga multihulgas defineeritavate lineaarsete *järjestuste arvuna*.

Oletame, et põhihulga esimese elemendi kõik m_1 eksemplari on omavahel eristatud näiteks järjekorranumbritega varustamise teel. Mistahes n-permutatsioonis saab neid elemente siis veel $m_1!$ viisil omavahel permuteerida ning kõikide eristatavate n-permutatsioonide arv on seega juba $K(m_1, m_2, \ldots, m_k)m_1!$. Samasugusel viisil toimime ka kõigi ülejäänud elemendiliikide korral, millega saame juba n erinevast elemendist koosneva põhihulga ja seega

$$K(m_1, m_2, \ldots, m_k)\, m_1!\, m_2! \ldots m_k! = n!$$

ehk

$$K(m_1, m_2, \ldots, m_k) = \frac{n!}{m_1!\, m_2! \ldots m_k!} \tag{1.7}$$

Nii näiteks numbritest 2, 4, 4, 4 ning 6 on seega võimalik moodustada kokku $K(1,3,1) = 20$ erinevat viiekohalist naturaalarvu ja nimelt suuruse järjekorras:

24446 24464 24644 26444 42446 42464 42644 44246 44264 44426
44462 44624 44642 46244 46424 46442 62444 64244 64424 64442.

Valemi (1.7) parem pool tuli täpselt sama kujuga nagu seda on üldliikme kordaja nn. *polünoomvalemis* ehk *multinoomvalemis*, mis esitab hulkliikme astme tema liikmete astmete kaudu kujul

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{\Sigma m_i = n} \frac{n!}{m_1!\, m_2! \ldots m_k!} a_1^{m_1} a_2^{m_2} \ldots a_k^{m_k}, \tag{1.8}$$

kus summa võetakse üle kõikide võimaluste, kuidas arvu n saab esitada mittenegatiivsete täisarvuliste liidetavate $m_1, m_2, \ldots, m_k$ summana (nagu hilisemas käsitluses selgub, pole see ühekujulisus muidugi juhuslik).

Valemis (1.8) esinevat nn. *polünoomkordajat* ehk *multinoomkordajat* on matemaatilises kirjanduses enamasti kombeks tähistada kujul

$$\binom{n}{m_1, m_2, \ldots, m_k} = \frac{n!}{m_1!\, m_2! \ldots m_k!}.$$

Olgu märgitud, et eelmise klassikalise juhu korral oleksime m-permutatsioonide arvu leidmisel seega võinud põhihulgaks lugeda multihulga n-elemendilise baasiga ning spetsifikatsiooniga näiteks $(m, m, ..., m)$. Niisuguse multihulga m-permutatsioone nimetatakse mõnikord ka *kordumistega m-permutatsioonideks*, kasutades tavalise hulga m-permutatsioonide jaoks sel juhul *kordumisteta m-permutatsioonide* nimetust. Vastavalt siis $W(n, m)$ on kordumistega m-permutatsioonide arv ja $P(n, m)$ on kordumisteta m-permutatsioonide arv.

Kordumistega m-permutatsiooni võib vajaduse korral tõlgendada ka kui *funktsiooni f* mingist m-elemendilisest hulgast mingisse n-elemendilisse hulka, näiteks $f\colon \mathcal{M} \to \mathcal{N}$, kus $\mathcal{M} = \overline{1,m} = \{1, 2, \ldots, m\}$ ja $\mathcal{N} = \overline{1,n} = \{1, 2, \ldots, n\}$. Tõepoolest, selleks tarvitseb vaid suvalist m-permutatsiooni kui m-elemendilist lineaarselt järjestatud hulka $(a_1, a_2, \ldots, a_m)$ tõlgendada näiteks vastava funktsiooni f kõikide võimalikkude väärtuste järjendina, s. t.

$$a_1 = f(1),\ a_2 = f(2),\ \ldots,\ a_m = f(m).$$

Analoogiliselt võib kordumisteta m-permutatsiooni tõlgendada sellise funktsioonina, mille väärtused on määramispiirkonna erinevates punktides alati erinevad, ehk funktsioonina, mis määrab *injektiivse kujutuse* hulgast $\mathcal{M}$ hulka $\mathcal{N}$ (injektiivseid kujutusi leidub muidugi vaid siis, kui $m \leqslant n$).

2. Kombinatsioonid

Kombinatoorika klassikaliste ülesannete teine põhiklass seostub selliste alamhulkade moodustamisega, kus järjestust ei arvestata või kus see pole üldse defineeritud. Põhihulga m-elemendilisi alamhulkasid on sel juhul nimelt kombeks nimetada *m-kombinatsioonideks*. Alamhulkade eristamine toimub kombinatsioonide korral seega üksnes nende koosseisu järgi. Konkreetseid kombinatsioone esitame järgnevas nii, nagu matemaatikas ikka hulki tähistatakse, näiteks $\{a_1, a_2, \ldots, a_m\}$.

Vaatleme ka nüüd kõigepealt juhtu, mil põhihulk on tavaline hulk, koosnedes n erinevast elemendist (igaüks ühes eksemplaris). Erinevate m-kombinatsioonide arvu $C(n, m)$ leidmiseks võib kasutada ülal kord juba tutvustatud mõttekäiku.

Põhihulga mingit üht fikseeritud elementi sisaldavate m-kombinatsioonide arv on $C(n-1, m-1)$, s.t. $(m-1)$-kombinatsioonide arv ülejäänud elementidest. Seda elementi mitte sisaldavate kombinatsioonide arv on aga $C(n-1, m)$ ja liitmisreegli kasutamine annab seega iga $m = 1, 2, \ldots, n$ korral

$$C(n, m) = C(n-1, m-1) + C(n-1, m), \tag{2.1}$$

kusjuures rajatingimustena on jälle loomulik nõuda, et iga n korral oleks $C(n, 0) = 1$ ning $m > n$ korral $C(n, m) = 0$.

Võrduse (2.1) abil saab juba rida-realt moodustada arvude $C(n, m)$ kolmnurkse tabeli, mida nimetatakse *Pascali kolmnurgaks*. Selle tabeli esimene rida sisaldab vaid ühe nullist erineva arvu $C(0, 0) = 1$ ja edasi iga järjekordne arv võrdub eelmises reas tema kohal paikneva kahe arvu summaga.

Arvude $C(n, m)$ üldavaldise saamiseks võib võrduse (2.1) korduva rakendamise teel kõigepealt tuletada võrduse

$$\begin{aligned} C(n, m) &= C(n-1, m-1) + C(n-1, m) = \\ &= C(n-1, m-1) + C(n-2, m-1) + C(n-2, m) = \ldots \\ \ldots &= \sum_{i=1}^{n-m+1} C(n-i, m-1) + C(m-1, m) = \sum_{i=1}^{n-m+1} C(n-i, m-1). \end{aligned}$$

Juhul $m = 1$ omandab see võrdus kuju

$$C(n, 1) = \sum_{i=1}^{n} C(n-i, 0) = n,$$

juhul $m = 2$ aga kuju

$$C(n,2) = \sum_{i=1}^{n-1} C(n-i,1) = \sum_{i=1}^{n-1}(n-i) = \frac{n(n-1)}{2}.$$

Nendele kahele tulemusele toetudes peaks juba kerge olema oletada, et üldiselt

$$C(n,m) = \frac{(n)_m}{m!}, \tag{2.2}$$

kuigi selle võrduse põhjendamine näiteks induktsioonimeetodiga võib tekitada mõningaid tehnilisi raskusi.

Sama tulemuseni võib aga jõuda ka veel näiteks järgmise täiesti vahetu arutelu teel. Igat m-kombinatsiooni saab teatavasti järjestada $m!$ viisil, s. t. temast saab moodustada $m!$ erinevat m-permutatsiooni. Et aga niiviisi toimides saame kõik võimalikud m-permutatsioonid, siis järelikult

$$m!\,C(n,m) = P(n,m),$$

mis annabki valemi (2.2).

Näiteks põhihulga $\{a,b,c,d\}$ korral saab seega moodustada $C(4,3) = 4$ erinevat 3-kombinatsiooni ja nimelt:

$$\{a,b,c\} \quad \{a,b,d\} \quad \{a,c,d\} \quad \{b,c,d\}.$$

Saadud avaldis (2.2) m-kombinatsioonide koguarvu leidmiseks kujutab endast nn. *binoomkordajat*

$$\binom{n}{m} = \frac{(n)_m}{m!} = \frac{n!}{m!(n-m)!},$$

s. t. üldliikme kordajat binoomi astme esituses tema liikmete astmete kaudu ehk nn. *binoomvalemis*

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}. \tag{2.3}$$

Selle üpris sageli vajaliku valemi põhjendamiseks kombinatoorikale tüüpilise mõttekäigu abil tarvitseb vaid jälgida astme ehk võrdsete tegurite korrutise

$$(a+b)^n = (a+b)(a+b)\ldots(a+b)$$

liikmete kujunemist siin esinevate sulgude vahetu avamise ning sarnaste liikmete järgneva koondamise käigus.

Paneme nimelt tähele, et korrutis $a^m b^{n-m}$ esineb sulgude täielikul avamisel tekkiva 2^n liikme hulgas nii mitu korda, kui mitmel viisil on võimalik vaadeldava korrutise n teguri hulgast täpselt m teguris välja valida just esimene liidetav a (ülejäänud

$n-m$ tegurist valitakse siis loomulikult teine liidetav b). Et aga selliste võimaluste arv on $C(n,m)$, siis sarnaste liikmete koondamisel kujunebki valem (2.3) ja liikmete koguarvu silmas pidades on ühtlasi põhjendatud võrdus

$$\sum_{m=0}^{n}\binom{n}{m}=2^n.$$

Kombinatoorne sisu on binoomkordaja mõistel üksnes naturaalarvuliste n ja m korral, kuid binoomvalem on üldistatav ka mistahes reaalarvulise (võiks aga isegi kompleksarvulise) astendaja $\lambda \in \mathbb{R}$ juhule. Valemis (2.3) tuleb sel juhul üksnes lõplik summa asendada reaga, nii et binoomvalem omandab üldkuju

$$(a+b)^\lambda=\sum_{m=0}^{\infty}\binom{\lambda}{m}a^m\,b^{\lambda-m},$$

kus binoomkordaja on nagu varemgi ikka defineeritud kahaneva faktoriaali kaudu võrdusega

$$\binom{\lambda}{m}=\frac{(\lambda)_m}{m!}.$$

Näiteks negatiivse täisarvulise astendaja olulisel erijuhul, s. t. $\lambda=-n$ korral saame binoomkordaja tähenduseks

$$\binom{-n}{m}=\frac{(-n)_m}{m!}=(-1)^m\frac{(n+m-1)_m}{m!}=(-1)^m\binom{n+m-1}{m},$$

millega vastav binoomvalem omandab kuju

$$(a+b)^{-n}=\sum_{m=0}^{\infty}\binom{n+m-1}{m}(-a)^m b^{-n-m}.$$

Valides $a=-x$, $b=1$ saame siit järgnevas tihti vajalikuks osutuva erijuhu

$$(1-x)^{-n}=\sum_{m=0}^{\infty}\binom{n+m-1}{m}x^m. \tag{2.4}$$

Kõrvalmärkusena olgu siinkohal veel nimetatud, et suvalise m-kombinatsiooni moodustamisel moodustavad ülejäänud elemendid ühe konkreetse $(n-m)$-kombinatsiooni. Selline üksühene vastavus tähendab, et m- ja $(n-m)$-kombinatsioonide arvud on võrdsed, mis annab binoomkordaja põhiomaduse

$$\binom{n}{m}=\binom{n}{n-m}.$$

Sellele omadusele tuginemine võimaldab juhul $m \geqslant n$ (m ja n on naturaalarvud) anda sisu isegi näiteks järgmisele kirjutisele:

$$\binom{-n}{-m}=\binom{-n}{m-n}=(-1)^{m-n}\binom{m-1}{m-n}=(-1)^{m+n}\binom{m-1}{n-1}$$

Binoomvalemi korral kasutatuga täiesti analoogilist mõttekäiku saab muide kasutada ka *multinoomvalemi* (1.8) põhjendamisel. Selleks tuleb jälgida liikmete kujunemist sulgude avamisel astme ehk n ühesuguse teguri korrutises

$$(a_1 + a_2 + \dots + a_k)(a_1 + a_2 + \dots + a_k)\dots(a_1 + a_2 + \dots + a_k).$$

Kui naturaalarvud $m_1, m_2, \dots, m_k \in \mathbb{N}$ on fikseeritud nii, et

$$m_1 + m_2 + \dots + m_k = n,$$

siis toodud n tegurist saab täpselt m_1 korral esimese liikme a_1 valida $C(n, m_1)$ viisil, seejärel ülejäänud $n-m_1$ tegurist täpselt m_2 korral teise liikme a_2 valida $C(n-m_1, m_2)$ viisil jne. Kokkuvõttes seega korrutis $a_1^{m_1} a_2^{m_2} \dots a_k^{m_k}$ esineb tekkiva k^n liikme hulgas täpselt

$$\binom{n}{m_1}\binom{n-m_1}{m_2}\dots\binom{n-m_1-m_2-\dots-m_{k-1}}{m_k} =$$

$$= \frac{n!}{m_1!(n-m_1)!} \cdot \frac{(n-m_1)!}{m_2!(n-m_1-m_2)!} \dots \frac{(n-m_1-\dots-m_{k-1})!}{m_k!(n-m_1-\dots-m_k)!} =$$

$$= \frac{n!}{m_1!m_2!\dots m_k!} = \binom{n}{m_1, m_2, \dots, m_k}$$

korda, millega valem (1.8) ongi põhjendatud. Ühtlasi on aga niiviisi põhjendatud veel ka võrdus

$$\sum_{\Sigma m_i = n} \binom{n}{m_1, m_2, \dots, m_k} = k^n.$$

Kombinatsioonide teise klassikalise erijuhu saame siis, kui põhihulgaks on multihulk, milles leidub kokku n erinevat elementi, neist igaüks suvalises arvus eksemplarides (jätkub kui vähemalt m eksemplaris). Tähistame erinevate m-kombinatsioonide arvu sel juhul sümboliga $F(n, m)$. Olgu ühtlasi veel märgitud, et sellise multihulga m-kombinatsioone nimetatakse vastavas kirjanduses sageli ka *kordumistega m-kombinatsioonideks*, kusjuures tavalise hulga m-kombinatsioonide korral kasutatakse vastavalt *kordumisteta m-kombinatsioonide* nimetust.

Arvu $F(n, m)$ leidmiseks iga naturaalarvulise m ja n tarvis paneme tähele, et põhihulga mingit fikseeritud elementi mitte sisaldavate m-kombinatsioonide arv on $F(n-1, m)$, seda elementi vähemalt üks kord sisaldavate m-kombinatsioonide arv aga $F(n, m-1)$. Järelikult liitmisreegli kasutamine annab iga $m = 1, 2, \dots$ korral

$$F(n, m) = F(n, m-1) + F(n-1, m), \tag{2.5}$$

kusjuures rajatingimusteks on nüüd loomulik võtta juba tuntud $F(n, 0) = 1$ ning lisaks veel täiesti vahetu mõttekäiguga kergesti kontrollitav $F(1, m) = 1$ (tuleb nimelt tähele panna, et erinevalt mõnedest varem vaadeldud juhtudest arv $F(n, m)$ enam $m > n$ korral ilmselt null ei ole).

Rekurrentse seose (2.5) korduva rakendamisega on $F(n,m)$ avaldatav kujul

$$\begin{aligned} F(n,m) &= F(n,m-1) + F(n-1,m) = \\ &= F(n,m-1) + F(n-1,m-1) + F(n-2,m) = \\ \cdots &= \sum_{i=2}^{n} F(i,m-1) + F(1,m) = \sum_{i=1}^{n} F(i,m-1). \end{aligned}$$

Juhul $m = 1$ omandab see võrdus kuju

$$F(n,1) = \sum_{i=1}^{n} F(i,0) = \sum_{i=1}^{n} 1 = n = \binom{n}{1},$$

juhul $m = 2$ kuju

$$F(n,2) = \sum_{i=1}^{n} F(i,1) = \sum_{i=1}^{n} i = \binom{n+1}{2}$$

ja juhul $m = 3$ kuju

$$F(n,3) = \sum_{i=1}^{n} F(i,2) = \sum_{i=1}^{n} \binom{i+1}{2} = \binom{n+2}{3}.$$

Nendele erijuhtudele tuginedes pole enam vist raske oletada, et üldvalem peaks nähtavasti tulema

$$F(n,m) = \binom{n+m-1}{m} = \frac{n^{(m)}}{m!}, \tag{2.6}$$

kuid saadud valemi põhjendamine näiteks induktsioonimeetodil on seotud mõningate tehniliste raskustega. Seetõttu võtamegi valemi (2.6) esialgu teadmiseks ilma vastavat tõestust lõpuni esitamata ning pöördume tõestuse puuduva osa juurde tagasi mõnevõrra hiljem (seitsmendas jaotises).

Näiteks elemente a, b, c ja d suvalises arvus eksemplarides (ehk igaüht vähemalt kolmes eksemplaris) sisaldava põhihulga korral saab valemi (2.6) kohaselt seega moodustada kokku $F(4,3) = 20$ erinevat 3-kombinatsiooni ja nimelt:

$\{a,a,a\}$	$\{a,a,b\}$	$\{a,a,c\}$	$\{a,a,d\}$	$\{a,b,b\}$
$\{a,b,c\}$	$\{a,b,d\}$	$\{a,c,c\}$	$\{a,c,d\}$	$\{a,d,d\}$
$\{b,b,b\}$	$\{b,b,c\}$	$\{b,b,d\}$	$\{b,c,c\}$	$\{b,c,d\}$
$\{b,d,d\}$	$\{c,c,c\}$	$\{c,c,d\}$	$\{c,d,d\}$	$\{d,d,d\}$

Osutub, et vaadeldavat liiki kombinatsioonide arvu leidmisega tuleb tegemist muuhulgas näiteks sel juhul, kui on vaja selgitada liikmete arvu multinoomvalemis (1.8), s.t. leida võrrandi

$$m_1 + m_2 + \cdots + m_k = n$$

mittenegatiivsete täisarvuliste lahendite arvu. Üsna lihtsa mõttekäiguga võib nimelt tõestada, et selleks arvuks osutub $F(k,n)$. Nii näiteks hulkliikmes $(a_1 + a_2 + a_3 + a_4)^3$ on järelikult $F(4,3) = 20$ liiget.

3. Kombinatsioonide arvusid genereerivad funktsioonid

Rekurrentsete võrrandite kasutamine mitmesuguste ühendite arvude leidmiseks on küll üpris universaalne meetod, kuid praktikas tihti seotud mõningate tehniliste raskustega. Seetõttu võtamegi vaatlusele kombinatoorikale iseloomulikuma meetodi, mis pealegi võimaldab nimetatud tehnilisi raskusi enamasti lihtsamini ületada. Alustame selle meetodi tutvustamist kombinatsioonide arvu leidmisega juhul, kui põhihulgaks on valitud harilik n-elemendiline hulk.

Olgu põhihulga elemendid varustatud järjekorranumbritega ($i = 1, 2, \ldots, n$) ja x_i selline *indikaator* (muutuja), mille astendaja näitab, kui mitu korda element number i vaadeldavasse kombinatsiooni kuulub. Siis iga i puhul vastav element kas ei kuulu sellesse kombinatsiooni (seda iseloomustab x_i^0) või ta kuulub sinna täpselt üks kord (seda iseloomustab x_i^1). Et need on üheaegselt mitte esineda saavad võimalused, siis analoogia liitmisreegliga lubab oletada, et elemendi number i kuulumist kombinatsiooni peaks iseloomustama summa

$$x_i^0 + x_i^1 = 1 + x_i.$$

Sellise indikaatori astmete summa saame muidugi iga järjekorranumbri i korral, kusjuures mingisse kombinatsiooni alati esimene element ($i = 1$) kas kuulub või mitte ja ka teine element ($i = 2$) kas kuulub või mitte jne. Analoogia korrutamisreegliga võimaldab nüüd oletada, et kõigi n elemendi kuulumist või mittekuulumist kombinatsiooni iseloomustab avaldis

$$(1 + x_1)(1 + x_2)\ldots(1 + x_n).$$

Niisugune analoogiatele tuginenud mõttekäik leiab kinnitust selle korrutise esitamisel hulkliikmena. Sulgude avamisel näeme nimelt, et iga tekkiv liige vastab tegurite liikmete ühele valimismoodusele, mis aga tähendab põhihulga iga elemendi korral otsustamist, kas lülitada teda konkreetsesse kombinatsiooni null või üks korda.

Nii näiteks konkreetsel erijuhul $n = 4$ (s. t. neljast erinevast elemendist koosneva põhihulga korral) saame

$$\begin{aligned}(1 + x_1)(1 + x_2)(1 + x_3)(1 + x_4) = 1 + (x_1 + x_2 + x_3 + x_4) +{}\\ + (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) +{}\\ + (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) + x_1x_2x_3x_4.\end{aligned}$$

Igaüks selle avaldise $2^4 = 16$ liikmest vastab mingile konkreetsele kombinatsioonile neljast elemendist. Näiteks liige 1 vastab 0-kombinatsioonile (tühjale alamhulgale), liige $x_1x_2x_3$ aga 3-kombinatsioonile, mille moodustavad põhihulga esimesed kolm elementi. Sulgudega on viimases avaldises ühendatud võrdse astmega liikmed, s. t. need m-kombinatsioonid, kus elementide arv m osutub ühesuguseks.

Kui konkreetseid kombinatsioone pole tarvis eraldi esile tuua (näiteks kui meid huvitab vaid mingi fikseeritud võimsusega kombinatsioonide arv), siis võime ühesuguse astmega liikmed ühendada sel teel, et samastame kõikide elementide indikaatorid, s. t. võtame iga i korral $x_i \equiv x$. Näiteks äsjavaadeldud juhul $n = 4$ omandab viimane võrdus niiviisi toimides kuju

$$(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4,$$

kus x^m kordaja annab erinevate m-kombinatsioonide arvu.

Täpselt samal viisil iseloomustab kombinatsioonide arvusid üldjuhul (s. t. kui n on suvaline) seega avaldis

$$(1+x)^n = \sum_{m=0}^{n} \binom{n}{m} x^m = \sum_{m=0}^{n} C(n,m)x^m. \tag{3.1}$$

Seost (3.1) võib soovi korral tõlgendada ka nii, et funktsioon $(1+x)^n$ genereerib jada $\{C(n,m)\}_m$ ehk teisiti öeldes on jada *genereeriv funktsioon* selles mõttes, et funktsiooni kirjutamisel astmereana (või erijuhul polünoomina) saame argumendi astmete kordajateks nimetatud jada elemendid. Seega võrduse (3.1) võib sõnastada ka nii, et kordumisteta kombinatsioonide arvude jada genereerivaks funktsiooniks on binoomi $1 + x$ nii mitmes aste, kui palju on põhihulgas elemente.

Kirjeldatud lähenemisviisi saab kombinatsioonide arvude leidmiseks kasutada ka teistsuguse struktuuriga põhihulkade või isegi mõningate kombinatsioonidele seatavate täiendavate nõuete korral. Teistsuguse struktuuriga põhihulkade vaatlemine tähendab seejuures muidugi üleminekut multihulkade vaatlemisele, kus elementide kordsused üldiselt erinevad ühest.

Samuti nagu binoom $1 + x_i$ iseloomustab elemendi number i mittekuulumist või ühekordset kuulumist kombinatsiooni, võib selle elemendi $0, 1, 2, \ldots, m_i$-kordset kuulumist kombinatsiooni iseloomustada teguriga

$$1 + x_i + x_i^2 + \cdots + x_i^{m_i}.$$

Ülalkirjeldatuga analoogiliselt näeme nüüd, et kui põhihulga spetsifikatsioon on $s = (m_1, m_2, \ldots, m_k)$, siis kõikide võimalikkude kombinatsioonide moodustamist niisugusest hulgast saab iseloomustada funktsiooniga

$$(1 + x_1 + \cdots + x_1^{m_1})(1 + x_2 + \cdots + x_2^{m_2}) \ldots (1 + x_k + \cdots + x_k^{m_k}).$$

See iseloomustamine tähendab, et sulgude avamisel saadava k muutuja polünoomi iga liige vastab ühele konkreetsele võimalikule kombinatsioonile, kusjuures polünoomi liikmete arvuks osutub muidugi kombinatsioonide koguarv

$$(m_1+1)(m_2+1)\dots(m_k+1).$$

Kui meid ka nüüd huvitab mitte kõikide konkreetsete kombinatsioonide esiletoomine, vaid üksnes nende arvude loendamine võimsuste järgi, siis indikaatorite samastamisega saame viimasele funktsioonile kuju

$$(1+x+\cdots+x^{m_1})(1+x+\cdots+x^{m_2})\dots(1+x+\cdots+x^{m_k}).$$

Sulgude avamisel annab see korrutis ühe muutuja polünoomi, milles x^m kordajaks osutub loomulikult ikka kõikide vaadeldava põhihulga korral võimalikkude m-kombinatsioonide koguarv.

Nii näiteks põhihulga $\{a,a,b,b,b,b,c,c,c,c\}$ puhul tuleb meil erinevate 4-kombinatsioonide arvu saamiseks leida x^4 kordaja korrutise

$$(1+x+x^2)(1+x+x^2+x^3+x^4)^2$$

arendises (sulgusid vaid osaliselt avades on lihtne kontrollida, et see kordaja tuleb 12). Antud juhul pole selline ühe kordaja leidmine küll oluliselt vähem töömahukas, kui nõutud kombinatsioonide vahetu väljakirjutamine, näiteks kujul

$$\begin{array}{cccc}
\{a,a,b,b\} & \{a,a,b,c\} & \{a,a,c,c\} & \{a,b,b,b\} \\
\{a,b,b,c\} & \{a,b,c,c\} & \{a,c,c,c\} & \{b,b,b,b\} \\
\{b,b,b,c\} & \{b,b,c,c\} & \{b,c,c,c\} & \{c,c,c,c\},
\end{array}$$

kuid viimati esitatud korrutises sulgusid täielikult avades leiame polünoomi

$$1+3x+6x^2+9x^3+12x^4+13x^5+12x^6+9x^7+6x^8+3x^9+x^{10},$$

mis annab vahetust ülelugemisest märgatavalt lihtsamini korraga kõigi m-kombinatsioonide arvud (kus $m=0,1,\dots,10$).

Ülalvaadeldutega analoogiline tegur iseloomustab elemendi kuulumist kombinatsiooni ka sel juhul, kui elemendi kordsus põhihulgas pole piiratud. Nimelt kombinatsioonides piiramata arv korda esineda võiva elemendi number i tarvis saame nüüd lõpliku summa asemel geomeetrilise rea

$$1+x_i+x_i^2+\cdots=(1-x_i)^{-1}.$$

Vaatleme näiteks kordumistega kombinatsioonide juhtumit, mil põhihulga n erinevat elementi võivad kõik kombinatsioonides esineda piiramata arv korda. Pärast kõigi indikaatorite samastamist ($x_i\equiv x$) saame vastava jada $\{F(n,m)\}_m$ genereerivaks funktsiooniks seega astme

$$(1+x+x^2+\cdots)^n.$$

Kui arendada see aste binoomvalemit (2.4) kasutades astmereaks, siis oleme valemi (2.6) põhjendanud tunduvalt lihtsamini, kui seda oleks võimaldanud näiteks rekurrentse võrrandi (2.5) vahetu lahendamine:

$$(1+x+x^2+\cdots)^n=(1-x)^{-n}=\sum_{m=0}^{\infty}\binom{n+m-1}{m}x^m.$$

Kasutame vaadeldud metoodikat lõpuks ka mõne sellise tulemuse saamiseks, kus kombinatsioonidele on seatud mingisuguseid täiendavaid nõudeid või kitsendusi.

Koosnegu põhihulk n erinevast elemendist, mis kõik tohivad kombinatsioonides esineda mistahes positiivne arv korda. Järelikult igas m-kombinatsioonis peab iga element vähemalt üks kord esinema ja ilmselt on mõtet vaadelda vaid juhtu $m \geqslant n$ (täpsemalt, juhul $m < n$ tuleb niisuguste m-kombinatsioonide arv võrdne nulliga).

Neid kitsendusi rahuldavate kombinatsioonide arvude jada genereeriv funktsioon on nüüd aste $(x+x^2+x^3+\cdots)^n$, mille reaksarendus omandab kuju

$$(x+x^2+\cdots)^n=x^n(1-x)^{-n}=x^n\sum_{m=0}^{\infty}\binom{n+m-1}{m}x^m=$$
$$=\sum_{m=0}^{\infty}\binom{m-1}{m-n}x^m=\sum_{m=n}^{\infty}\binom{m-1}{n-1}x^m.$$

Seega vaadeldavate m-kombinatsioonide arvuks osutub x^m kordaja selles reas, s. t. $m < n$ korral null ning $m \geqslant n$ korral binoomkordaja

$$\binom{m-1}{n-1}.$$

Lisatingimuste teise näitena vaatleme veel olukorda, kus põhihulk on sama, kuid kombinatsioonidesse tohib iga element kuuluda üksnes paarisarv $(0,2,4,\ldots)$ korda. Vastava genereeriva funktsiooni reaksarendus annab nüüd

$$(1+x^2+x^4+\cdots)^n=(1-x^2)^{-n}=\sum_{m=0}^{\infty}\binom{n+m-1}{m}x^{2m},$$

s. t. $(2m+1)$-kombinatsioonide arv tuleb iga naturaalarvu m korral null (nagu nähtub vastavate liikmete puudumisest selles reas), aga $2m$-kombinatsioonide arvuks osutub

$$\binom{n+m-1}{m}=F(n,m).$$

Püüame lõpuks veel veidi täpsustada genereeriva funktsiooni äsjases käsitluses enam-vähem heuristiliselt kasutusele võetud mõistet. Vastava traditsioonilise definitsiooni võib nimelt esitada näiteks järgmises sõnastuses.

Arvjada $\{a_k\} \equiv a_0, a_1, a_2, \ldots$ (polünomiaalseks ehk harilikuks) *genereerivaks funktsiooniks* nimetatakse niisugust funktsiooni $a(x)$, mille arendamisel astmeritta argumendi x astmete kordajateks osutuvad jada $\{a_k\}$ elemendid, s. t. kehtib võrdus

$$a(x) = \sum_{k=0}^{\infty} a_k x^k. \tag{3.2}$$

Selles definitsioonis on küll tegelikult jäetud täpsustamata nii funktsiooni argumendi x kui ka astmeritta arendamise (ehk võrduses (3.2) esineva võrdusmärgi) tähendus, kuid meie hilisemas käsitluses selgub, et niisuguseks täpsustamiseks ei olegi erilist vajadust. Suuremat konkreetsust taotledes võime aga esitatud võrdust esialgu mõista näiteks selliselt, et $a(x)$ on vastava rea summa koondumise mõttes, kusjuures x tähendab selle rea koonduvusringi kuuluvat kompleksmuutujat.

Mõningate kõige sagedamini vajalike jadade genereerivad funktsioonid võib nähtavasti üldtuntuteks lugeda. Neli sellist on esitatud näiteks järgmises tabelis:

a_k	c^k	k	$\binom{n}{k}$	$\binom{n+k-1}{k}$
$a(x)$	$(1-cx)^{-1}$	$x(1-x)^{-2}$	$(1+x)^n$	$(1-x)^{-n}$

Paneme siinjuures tähele, et tooduist esimese funktsiooni astmerida koondub üksnes ringis $|x| < |c|^{-1}$, teise ja neljanda funktsiooni astmeread aga ringis $|x| < 1$ ning kolmanda funktsiooni astmerida osutub lõplikuks summaks, s. t. polünoomiks.

Genereerivate funktsioonide kasutamisel on sageli oluline osata tehteid funktsioonidega üle kanda vastavatele jadadele ning vastupidi. Niisuguste üleminekureeglite sõnastamise lihtsustamiseks tähistame jadade $\{a_k\}$, $\{b_k\}$ ja $\{c_k\}$ genereerivaid funktsioone vastavalt $a(x)$, $b(x)$ ja $c(x)$. Jadade ja neid genereerivate funktsioonidega sooritatavad tehted võib siis seostada järgmiselt.

Funktsioonide vaheline võrdus $c(x) = a(x)$ tähendab, et vastavates jadades peab iga k korral olema $c_k = a_k$.

Funktsioonide vaheline võrdus $c(x) = \lambda\, a(x)$ tähendab, et vastavates jadades peab iga k korral olema $c_k = \lambda\, a_k$, kus λ on näiteks reaal- või kompleksarv.

Funktsioonide vaheline võrdus $c(x) = a(x) + b(x)$ tähendab, et vastavates jadades peab iga k korral olema $c_k = a_k + b_k$.

Funktsioonide vaheline võrdus $c(x) = a(x) \cdot b(x)$ tähendab, et vastavates jadades peab iga k korral olema

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \tag{3.3}$$

(see valem tagab kooskõla polünoomide korrutamise üldtuntud eeskirjaga).

4. Permutatsioonide arvusid genereerivad funktsioonid

Kombinatsioonide tarvis kirjeldatud meetodi ülekandmisel permutatsioonide arvude juhule ei õnnestu jadade ja funktsioonide vahelist seost kahjuks enam niivõrd otseselt tuletada sulgude avamise reeglitest. Vastava idee saamise lihtsaimaks mooduseks osutub nüüd nähtavasti tuginemine permutatsioonide arvude jaoks juba ülal tuletatud valemitele ning võimaluste otsimine nende seostamiseks ridadega.

Näiteks tavalise hulga kombinatsioonide ning permutatsioonide arvude vahelist seost $C(n,m) = P(n,m)/m!$ arvestades võib binoomvalemi (3.1) esitada kujul

$$(1+x)^n = \sum_{m=0}^{n} P(n,m)\frac{x^m}{m!}. \tag{4.1}$$

Võrdust (4.1) võib tõlgendada ka nii, et astme $(1+x)^n$ arendamisel ritta funktsioonide $x^m/m!$ järgi tulevad vastavateks kordajateks just kordumisteta m-permutatsioonide arvud. Niisugune tähelepanek võimaldabki teha järgmise oletuse.

Kui põhihulga mingi element number i tohib permutatsioonis esineda null kuni k_i korda (ehk: seda elementi on olemas k_i eksemplari), siis selle elemendi kuuluvuse iseloomustamiseks tuleb nähtavasti kasutada summat

$$1 + x_i + \frac{x_i^2}{2!} + \cdots + \frac{x_i^{k_i}}{k_i!}$$

ja kõikide elementide kuulumise iseloomustamiseks korrutist

$$\prod_{i=1}^{k}\left(1 + x_i + \frac{x_i^2}{2!} + \cdots + \frac{x_i^{k_i}}{k_i!}\right), \tag{4.2}$$

kus k on põhihulga erinevate elementide arv. Niisugust valikut õigustab muuhulgas ka asjaolu, et sulgude avamine korrutises (4.2) annab üldliikme

$$\frac{x_1^{m_1}}{m_1!}\cdot\frac{x_2^{m_2}}{m_2!}\cdots\frac{x_k^{m_k}}{m_k!}.$$

Kui siin samastada indikaatorid ($x_i \equiv x$) ja ühtlasi tähistada nende astendajate summa $m_1 + m_2 + \cdots + m_k = n$, siis

$$\frac{x^{m_1}}{m_1!}\cdot\frac{x^{m_2}}{m_2!}\cdots\frac{x^{m_k}}{m_k!} = \frac{n!}{m_1!\,m_2!\ldots m_k!}\cdot\frac{x^n}{n!}.$$

Saadud kordaja on aga valemi (1.7) kohaselt tõepoolest vastava spetsifikatsiooniga n-permutatsioonide koguarv.

Täiendavalt paneme tähele, et kui element number i tohib permutatsioonis esineda piiramata arv korda, siis tuleb selle elemendi kuuluvuse iseloomustamiseks nähtavasti kasutada funktsiooniteooriast tuntud astmerida

$$1 + x_i + \frac{x_i^2}{2!} + \cdots = e^{x_i}. \tag{4.3}$$

Indikaatorite x_i samastamine valemis (4.2) tähendab ikka loobumist konkreetsete sama liiki permutatsioonide eristamisest ning üleminekut vaid nende koguarvude loendamisele. Nii näiteks põhihulga korral, milles leidub n erinevat elementi, igaüht piiramata arv eksemplare, saame indikaatorite samastamise tulemusel korrutise (4.2) asemele hoopis astme

$$\left(1 + x + \frac{x^2}{2!} + \cdots\right)^n = e^{nx} = \sum_{m=0}^{\infty} n^m \frac{x^m}{m!},$$

millest võib kohe välja lugeda erinevate m-permutatsioonide arvu $W(n,m) = n^m$, kui liikme $x^m/m!$ kordaja.

Võrdust (4.3) arvestades kasutatakse saadud liiki reaksarendustest kõneledes enamasti eksponentsiaalsete genereerivate funktsioonide nimetust. Vaatleme selliste funktsioonide kasutamist konkreetset tüüpi permutatsioonide arvude leidmisel veel paari näite varal.

Kõigepealt leiame m-permutatsioonide arvu sellise põhihulga korral, kus igaüht n erinevast elemendist saab permutatsiooni võtta kas mitte üheski või siis kahes eksemplaris. Vajalik genereeriv funktsioon tuleb nüüd

$$\left(1 + \frac{x^2}{2!}\right)^n = \sum_{m=0}^{n} \binom{n}{m} \frac{x^{2m}}{2^m} = \sum_{m=0}^{n} \binom{n}{m} \frac{(2m)!}{2^m} \cdot \frac{x^{2m}}{(2m)!}.$$

Siit näeme, et $(2m+1)$-permutatsioonide arv on loomulikult null, $2m$-permutatsioonide arvuks saame aga

$$\binom{n}{m} \frac{(2m)!}{2^m} = \binom{n}{m} \frac{(2m)!!(2m-1)!!}{2^m} = (n)_m \cdot (2m-1)!!,$$

kus kasutasime *poolfaktoriaalide* omadust $2^m \cdot m! = (2m)!!$.

Leiame nüüd selliste m-permutatsioonide arvu, milles põhihulga kõik n erinevat elementi peavad esinema vähemalt üks kord. Niisugust kordumistega m-permutatsiooni võib vajaduse korral tõlgendada funktsioonina, mis määrab *sürjektiivse kujutuse* hulgast $\mathcal{M} = \overline{1,m} = \{1, 2, \ldots, m\}$ hulgale $\mathcal{N} = \overline{1,n} = \{1, 2, \ldots, n\}$ (loomulikult on nende kujutuste arv $m < n$ korral võrdne nulliga).

Nõutud liiki permutatsioonide koguarvude jada eksponentsiaalse genereeriva funktsiooni võime nüüd esitada kujul

$$\left(x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^n=(e^x-1)^n=\sum_{j=0}^{n}(-1)^j\binom{n}{j}e^{x(n-j)}=$$

$$=\sum_{j=0}^{n}(-1)^j\binom{n}{j}\sum_{m=0}^{\infty}\frac{x^m(n-j)^m}{m!}=\sum_{m=0}^{\infty}\frac{x^m}{m!}\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^m,$$

millest vaadeldavat liiki m-permutatsioonide arvu saame muidugi ikka $x^m/m!$ kordajana, s. t. see arv tuleb

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^m. \tag{4.4}$$

Sellele avaldisele veidi kompaktsema kuju andmiseks võib kasutada näiteks diferentsarvutuse standardsümboolikat. Seal defineeritakse täisarvulise argumendiga funktsioonide f vallas nn. *nihutamisoperaator*

$$Ef(k)=f(k+1)$$

ja *diferentsimisoperaator*

$$\Delta f(k)=f(k+1)-f(k)=(E-1)f(k). \tag{4.5}$$

Pole raske märgata, et nihutamisoperaatori korduval rakendamisel astmefunktsioonile $f(k)=k^m$ (kus m on fikseeritud naturaalarv) saame

$$Ek^m=(k+1)^m,\quad E^2k^m=(k+2)^m,\ldots,\quad E^{n-j}k^m=(k+n-j)^m.$$

Argumendi väärtusel $k=0$ võime seega kirjutada

$$(n-j)^m=E^{n-j}0^m,$$

kus viimane kirjutis on tavaline lühend tähenduses

$$E^p0^m=E^pk^m|_{k=0}.$$

Binoomvalemi ilmset üldistust operaatorite valda kasutades võime summa (4.4), s. t. sürjektiivseid kujutusi määravate funktsioonide arvu nüüd esitada kujul

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^m=\sum_{j=0}^{n}\binom{n}{j}(-1)^jE^{n-j}0^m=$$
$$=(E-1)^n0^m=\Delta^n0^m.$$

Loomulikult on sama lähenemisviis rakendatav üldse suvalise spetsifikatsiooniga põhihulga korral. Nii näiteks põhihulga $\{a, a, b, b, b, b, c, c, c, c\}$ erinevate 4-permutatsioonide arvu saamiseks tuleb leida $x^4/24$ kordaja korrutise

$$\left(1+x+\frac{x^2}{2!}\right)\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}\right)^2$$

esituses hulkliikmena (sulgusid üksnes osaliselt avades on lihtne kontrollida, et see kordaja tuleb 72).

Siinesitatud heuristilise käsitluse seos kombinatsioonide korral kasutatud analoogilise metoodikaga tugineb tegelikult järgmisele üldisele definitsioonile. Selles definitsioonis loetakse fikseerituks *baas* ehk funktsionaaljada $\{g_k(x)\}$, mille elementidelt nõuatakse *lineaarset sõltumatust*, s. t. jada iga lõplik lõige $\{g_0(x), g_1(x), \dots, g_n(x)\}$ peab koosnema lineaarselt sõltumatutest funktsioonidest.

Arvjada $\{a_k\}$ *genereerivaks funktsiooniks* baasil $\{g_k(x)\}$ nimetatakse niisugust funktsiooni $a(x)$, mille reaksarenduses baasi funktsioonide järgi osutuvad kordajateks sellesama jada $\{a_k\}$ elemendid, s. t. kehtib võrdus

$$a(x) = \sum_{k=0}^{\infty} a_k g_k(x). \tag{4.6}$$

Juhul $g_k(x) \equiv x^k$ saame siit eelmises jaotises vaadeldud *harilikud* ehk *polünomiaalsed genereerivad funktsioonid*, teisel tähtsal erijuhul $g_k(x) \equiv x^k/k!$ aga nn. *eksponentsiaalsed genereerivad funktsioonid*.

Mõningate kõige sagedamini tarvis minevate jadade eksponentsiaalsed genereerivad funktsioonid võib üldtuntuteks lugeda. Viis neist on esitatud järgmises tabelis:

a_k	c^k	k	$k!$	$(n)_k$	$n^{(k)}$
$a(x)$	e^{cx}	$x\,e^x$	$(1-x)^{-1}$	$(1+x)^n$	$(1-x)^{-n}$

Genereerivate funktsioonide võrdumise, skalaariga korrutamise ning liitmise tähendus defineeritakse iga baasi korral täpselt niisamuti, nagu polünomiaalsete genereerivate funktsioonide tarvis näidatud. Oluliselt sõltub baasist aga genereerivate funktsioonide korrutamise tõlgendus vastavate jadade kaudu.

Kui jadade $\{a_k\}$, $\{b_k\}$ ning $\{c_k\}$ eksponentsiaalseid genereerivaid funktsioone tähistada vastavalt sümbolitega $a(x), b(x)$ ning $c(x)$, siis võrdus $c(x) = a(x) \cdot b(x)$ tähendab, et vastavates jadades peab iga k korral olema

$$c_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}. \tag{4.7}$$

See võrdus tuleneb ikka nõudest tagada kooskõla polünoomide korrutamise eeskirjaga. Kui arvestada, et vaadeldavaid funktsioone $a(x)$, $b(x)$, $c(x)$ võib soovi korral tõlgendada ka jadade $\{a_k/k!\}$, $\{b_k/k!\}$, $\{c_k/k!\}$ polünomiaalsete genereerivate funktsioonidena, siis järeldub võrdus (4.7) täiesti vahetult võrdusest (3.3):

$$\frac{c_k}{k!} = \sum_{i=0}^{k} \frac{a_i}{i!} \cdot \frac{b_{k-i}}{(k-i)!} = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}.$$

Võrdus (4.7) erineb binoomvalemist

$$(a+b)^k = \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i}$$

üksnes selle poolest, et parema poole astendajate asemele on kirjutatud indeksid. Jadade elementidega opereerimisel kasutataksegi diskreetses matemaatikas mõnikord sellist puhtformaalset võtet, mis seisneb jada $a_0, a_1, \ldots, a_k, \ldots$ asendamises jadaga $a^0, a^1, \ldots, a^k, \ldots$, kusjuures kõikides tehetes tõlgendatakse indekseid astendajatena ja alles lõpptulemuses kirjutatakse indeksid jälle oma tavalisele kohale.

Niisuguse formaalse arvutusvõtte (nn. *sümbolarvutuse*) kasutamisel tuleb aga võimalikkude eksituste vältimiseks astmetega opereerimisel silmas pidada, et näiteks $a^i a^j$ ei tarvitse üldiselt olla sama mis a^{i+j} ja a^0 pole enamasti võrdne ühega.

Võtte lihtsaima illustratsioonina nimetame, et eksponentsiaalsete genereerivate funktsioonide korrutamise reegli (4.7) võib selle kohaselt kirjutada võrdusena

$$c_k = (a+b)^k, \tag{4.8}$$

kus tuleb muidugi arvestada, et $a^k \equiv a_k$, $b^k \equiv b_k$ ja erijuhul $k = 0$ saame $c_0 = a_0 b_0$.

Sama formaalse võtte järjekindla kasutamise korral võime jada $\{a_k\}$ eksponentsiaalse genereeriva funktsiooni vajaduse korral üldse esitada kujul

$$a(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!} = e^{ax}, \tag{4.9}$$

kus vastavas astmereas loeme ikka $a^k \equiv a_k$. Niisuguse kirjutusviisi kasutamise korral jõuame genereerivate funktsioonide korrutamise eeskirja (4.7) juurde täiesti vahetult: kui võrdus $c(x) = a(x) \cdot b(x)$ esitada kujul

$$e^{cx} = e^{ax} \cdot e^{bx} = e^{(a+b)x},$$

siis ülaltoodud seos (4.8) järeldub $x^k/k!$ kordajate võrdlemisest otsekohe.

Mõningaid näiteid sümbolarvutuse kasulikkusest esineb ka järgnevas käsitluses, kuigi enamasti esitatakse jadasid edaspidi ikka traditsioonilisel kujul.

5. Jadad ja nende genereerivad funktsioonid

Mitmesuguseid (diskreetses) matemaatikas olulisi arvusid saab enamasti kõige mugavamini defineerida sobivate genereerivate funktsioonide kaudu. Järgnevalt ongi esitatud mõned edasise käsitlusega seostuvad näited.

Euleri esimest liiki arvudeks nimetatakse niisuguseid täisarvusid E_k, milledest moodustatud jada $\{E_k\}$ eksponentsiaalseks genereerivaks funktsiooniks osutub hüperboolse koosinuse pöördväärtus $1/\operatorname{ch} x$:

$$\frac{1}{\operatorname{ch} x} = \sum_{k=0}^{\infty} E_k \frac{x^k}{k!}. \tag{5.1}$$

Bernoulli arvudeks nimetatakse niisuguseid ratsionaalarvusid B_k, milledest moodustatud jada $\{B_k\}$ eksponentsiaalseks genereerivaks funktsiooniks osutub jagatis $x/(e^x - 1)$:

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}. \tag{5.2}$$

Stirlingi esimest liiki arvudeks nimetatakse niisuguseid täisarvusid $s(n,k)$, milledest moodustatud jada $\{s(n,k)\}_k$ polünomiaalseks genereerivaks funktsiooniks osutub argumendi kahanev n-faktoriaal:

$$(x)_n = \sum_{k=0}^{n} s(n,k) x^k. \tag{5.3}$$

Stirlingi teist liiki arvudeks nimetatakse niisuguseid naturaalarvusid $S(n,k)$, milledest moodustatud jada $\{S(n,k)\}_k$ genereerivaks funktsiooniks kahanevatest faktoriaalidest koosneval baasil $\{(x)_k\}$ osutub argumendi n-es aste:

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k. \tag{5.4}$$

Euleri teist liiki arvudeks nimetatakse niisuguseid naturaalarvusid $E(n,k)$, milledest moodustatud jada $\{E(n,k)\}_k$ genereerivaks funktsiooniks binoomkordajatest koosneval baasil $\{\binom{x+k}{n}\}$ osutub argumendi n-es aste:

$$x^n = \sum_{k=0}^{n-1} E(n,k) \binom{x+k}{n}. \tag{5.5}$$

Niisugused definitsioonid pole enamasti küll sobivad vastavate arvude vahetuks arvutamiseks, kuid neile on loomulik toetuda nii arvude mitmesuguste omaduste põhjendamisel kui ka tegelike arvutamiseeskirjade tuletamisel. Illustreerime selliseid võimalusi mõne näitega.

Et *Euleri esimest liiki arvude* genereeriv funktsioon ehk definitsiooni (5.1) vasak pool kujutab endast paarisfunktsiooni:

$$\frac{1}{\operatorname{ch} x} = \frac{2}{e^x + e^{-x}},$$

siis peab muidugi iga $k > 0$ korral olema $E_{2k-1} = 0$. Seega $\operatorname{ch} x$ reaksarendust

$$\operatorname{ch} x = \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!}$$

arvestades võib definitsiooni (5.1) esitada ka kujul

$$\sum_{k=0}^{\infty} E_{2k} \frac{x^{2k}}{(2k)!} = \left(\sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!} \right)^{-1}.$$

Kui siin x asemele kirjutada $\imath x$ (kus $\imath \equiv \sqrt{-1}$), siis

$$\sum_{k=0}^{\infty} (-1)^k E_{2k} \frac{x^{2k}}{(2k)!} = \left(\sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!} \right)^{-1} = (\cos x)^{-1} = \sec x,$$

s. t. saame valemi

$$\sec x = \sum_{k=0}^{\infty} (-1)^k E_{2k} \frac{x^{2k}}{(2k)!},$$

mille tõttu arvusid $(-1)^k E_{2k}$ nimetatakse mõnikord ka *seekansarvudeks*.

Sümbolarvutuse meetodeid kasutades võime definitsiooni (5.1) kirjutada kujul

$$2 = e^{Ex} (e^x + e^{-x}) = e^{(E+1)x} + e^{(E-1)x}.$$

Kui nüüd võrrelda $x^n/n!$ kordajaid selle võrduse vasakus ja paremas pooles, siis saame iga $n > 0$ korral

$$(E+1)^n + (E-1)^n = 0 \tag{5.6}$$

ja $n = 0$ korral

$$E_0 + E_0 = 2 \qquad \text{ehk} \qquad E_0 = 1.$$

Võrdusi $E_{2k-1} = 0$ arvestades järeldub seosest (5.6), et iga $n > 0$ korral

$$\sum_{k=0}^{n} \binom{2n}{2k} E_{2n-2k} = 0,$$

mis väärtusest $E_0 = 1$ lähtudes võimaldab arvutada

$$E_2 = -1, \quad E_4 = 5, \quad E_6 = -61, \quad E_8 = 1385, \quad E_{10} = -50521, \ \ldots$$

Analoogilist lähenemisviisi kasutades võime ka *Bernoulli arvude* definitsiooni (5.2) kirjutada sümbolkujul

$$x = e^{Bx} \cdot (e^x - 1) = e^{(1+B)x} - e^{Bx},$$

milles $x^n/n!$ kordajaid võrreldes saame $n > 1$ korral

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0 \tag{5.7}$$

ja $n = 1$ korral

$$(1 + B)^1 - B^1 = 1 \quad \text{ehk} \quad 1^0 \cdot B_1 + 1^1 \cdot B_0 - B_1 = 1 \quad \text{ehk} \quad B_0 = 1.$$

Algväärtusele $B_0 = 1$ toetudes leiame valemist (5.7):

$$B_1 = -\frac{1}{2}, \ B_2 = \frac{1}{6}, \ B_4 = -\frac{1}{30}, \ B_6 = \frac{1}{42}, \ B_8 = -\frac{1}{30}, \ B_{10} = \frac{5}{66},$$

$$B_{12} = -\frac{691}{2730}, \ B_{14} = \frac{7}{6}, \ B_{16} = -\frac{3617}{510}, \ B_{18} = \frac{43867}{798}, \ B_{20} = -\frac{174611}{330}, \ \ldots,$$

kusjuures iga $k > 0$ korral selgub, et $B_{2k+1} = 0$. Selle fakti saab aga tuletada ka peaaegu vahetu järeldusena definitsioonist. Tõepoolest, äsjaleitud väärtusi $B_0 = 1$ ja $B_1 = -\frac{1}{2}$ arvestades võime seose (5.2) kirjutada kujul

$$b(x) \equiv \frac{x}{e^x - 1} + \frac{x}{2} = 1 + \sum_{n=2}^{\infty} B_n \frac{x^n}{n!},$$

kus täiesti vahetu kontrollimise teel pole raske veenduda, et vasak pool kujutab endast paarisfunktsiooni, s. t. iga x korral $b(-x) = b(x)$.

Olgu veel nimetatud, et ilmsete võrduste

$$\frac{e^x - 1}{x} = \sum_{n=1}^{\infty} \frac{x^{n-1}}{n!} = \sum_{n=0}^{\infty} \frac{1}{n+1} \cdot \frac{x^n}{n!}$$

tõttu saame eksponentsiaalse genereeriva funktsiooni (5.2) soovi korral esitada ka kujul

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \left(\sum_{n=0}^{\infty} \frac{1}{n+1} \cdot \frac{x^n}{n!} \right)^{-1},$$

s. t. Bernoulli arvude jada $\{B_n\}$ eksponentsiaalne genereeriv funktsioon on võrdne nn. *harmoonilise jada*

$$\left(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n+1}, \ldots\right)$$

eksponentsiaalse genereeriva funktsiooni pöördväärtusega.

Eksponentsiaalse genereeriva funktsiooni viimati toodud kujust järeldub korrutamise eeskirja (4.7) arvestades veel, et iga $n > 0$ korral kehtib seos

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} B_{n-k} = 0.$$

Olgu märgitud, et Bernoulli võttis oma arvud vaatlusele seoses *astmesummade*

$$P_n(m) = \sum_{k=0}^{m-1} k^n$$

arvutamisega. Ta nimelt näitas, et kehtib seos

$$P_n(m) = \frac{1}{n+1} \sum_{i=0}^{n} \binom{n+1}{i} B_i m^{n+1-i}. \tag{5.8}$$

Selle seose põhjendamiseks moodustame fikseeritud m korral jada $\{P_n(m)\}$ eksponentsiaalse genereeriva funktsiooni:

$$\begin{aligned} e^{P(m)x} &= \sum_{n=0}^{\infty} P_n(m) \frac{x^n}{n!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{m-1} k^n = \\ &= \sum_{k=0}^{m-1} \sum_{n=0}^{\infty} \frac{(kx)^n}{n!} = \sum_{k=0}^{m-1} e^{kx} = \frac{e^{mx}-1}{e^x-1} = \\ &= x^{-1} \cdot e^{Bx} \cdot (e^{mx}-1) = x^{-1}\left(e^{(B+m)x} - e^{Bx}\right). \end{aligned}$$

Kui selles astmeridade vahelises võrduses

$$x\, e^{P(m)x} = e^{(B+m)x} - e^{Bx}$$

võrrelda $x^{n+1}/(n+1)!$ kordajaid, siis saamegi valemi (5.8):

$$(n+1)P_n(m) = (B+m)^{n+1} - B^{n+1} =$$

$$= \sum_{i=0}^{n+1} \binom{n+1}{i} B_i m^{n+1-i} - B_{n+1} = \sum_{i=0}^{n} \binom{n+1}{i} B_i m^{n+1-i}.$$

Stirlingi arvude omaduste selgitamisel paneme kõigepealt tähele, et kasvava faktoriaali definitsiooni (1.4) kohaselt on $x^{(n)} = x(x+1)\ldots(x+n-1)$ mittenegatiivsete kordajatega polünoom. Võrdust (1.5) arvestades saame aga selle kergesti siduda kahaneva faktoriaali ja seega *Stirlingi esimest liiki arvudega*:

$$x^{(n)} = (-1)^n(-x)_n = (-1)^n \sum_{k=0}^{n} s(n,k)(-1)^k x^k.$$

Siit järeldub kohe kordajate $(-1)^{n+k}s(n,k)$ positiivsus iga $k = 1,2,\ldots,n$ korral. Seega on Stirlingi esimest liiki arvud vahelduvate märkidega (mõlema argumendi suhtes) ja viimase võrduse saab kirjutada ka kujul

$$x^{(n)} = \sum_{k=0}^{n} |s(n,k)|\, x^k,$$

s. t. x-i kasvavat n-faktoriaali võib vajaduse korral tõlgendada jada $\{|s(n,k)|\}_k$ polünomiaalse genereeriva funktsioonina.

Stirlingi esimest liiki arvude leidmine otse definitsioonist osutub üsna töömahukaks (sest tülikaks kujuneb sulgude avamine kahanevat faktoriaali määravas korrutises). Seetõttu on tegelikkudes arvutustes lihtsam kasutada ilmsest seosest

$$(x)_{n+1} = (x-n)(x)_n$$

ja Stirlingi esimest liiki arvude definitsioonist (5.3) tulenevat võrdust

$$\sum_{k=0}^{n+1} s(n+1,k)x^k = \sum_{k=0}^{n} s(n,k)x^{k+1} - n\sum_{k=0}^{n} s(n,k)x^k.$$

Võrreldes siin suvalise k korral x^k kordajaid saame rekurrentse võrrandi

$$s(n+1,k) = s(n,k-1) - n\, s(n,k), \tag{5.9}$$

mis kehtib iga n ja $k = 1, 2, \ldots, n$ korral.

Analoogiliselt tuleneb võrdusest $x^{n+1} = x \cdot x^n$ ja *Stirlingi teist liiki arvude* definitsioonist (5.4) võrdus

$$\sum_{k=0}^{n+1} S(n+1,k)(x)_k = x \cdot \sum_{k=0}^{n} S(n,k)(x)_k = \sum_{k=0}^{n} S(n,k)((x)_{k+1} + k\,(x)_k),$$

milles x^k kordajate võrdlemine annab rekurrentse võrrandi

$$S(n+1,k) = S(n,k-1) + k\,S(n,k). \tag{5.10}$$

Võrrandite (5.9) ja (5.10) abil saab kergesti koostada arvude $s(n,k)$ ja $S(n,k)$ tabelid. Sealjuures tuleb lähteks võtta vahetult definitsioonidest tulenevad algtingimused $S(1,1) = s(1,1) = 1$ ja $S(n,0) = s(n,0) = 0$ (viimane järeldub iga $n > 0$ korral näiteks sellest, et kahanevas faktoriaalis puudub vabaliige). Niisuguste tabelite algus tuleb järgmine (koondtabeli iga lahtri loodenurgas on antud $s(n,k)$ ja kagunurgas $S(n,k)$ väärtus; nulle ei ole tabelisse kantud):

n \ k	1	2	3	4	5	6
2	−1 = s(1,2) S(1,2) = 1	1 1				
3	2 1	−3 3	1 1			
4	−6 1	11 7	−6 6	1 1		
5	24 1	−50 15	35 25	−10 10	1 1	
6	−120 1	274 31	−225 90	85 65	−15 15	1 1
7	720 1	−1764 63	1624 301	−735 350	175 140	−21 21

Stirlingi teist liiki arvud on muide lihtsalt avaldatavad *diferentsimisoperaatori* (4.5) kaudu. Kui võtta aluseks eelmises jaotises tuletatud valemi $m^n = E^m 0^n$ formaalne üldistus $x^n = E^x 0^n$, siis binoomkordaja definitsiooni arvestades

$$x^n = (1+\Delta)^x = \sum_{m=0}^{x} \binom{x}{m} \Delta^m 0^n = \sum_{m=0}^{x} \frac{(x)_m}{m!} \Delta^m 0^n.$$

Selle tulemuse võrdlemine definitsiooniga (5.4) annab

$$S(n,m) = \frac{\Delta^m 0^n}{m!}.$$

Seega eelmise jaotise vastavat tulemust arvestades näeme, et $m!\,S(n,m)$ võrdub niisuguste n-permutatsioonide arvuga, kus põhihulga m erinevat elementi peavad kõik esinema vähemalt ühes eksemplaris (ehk kõikide *sürjektiivsete kujutuste* arvuga hulgast $\overline{1,n} = \{1, 2, \ldots, n\}$ hulgale $\overline{1,m} = \{1, 2, \ldots, m\}$).

Euleri teist liiki arvude tegeliku arvutamise jaoks vajaliku rekurrentse seose leidmiseks lähtume jälle ilmsest võrdusest $x^{n+1} = x \cdot x^n$. Asendades siin astmed definitsioonist (5.5) saame:

$$\sum_{k=0}^{n} E(n+1,k)\binom{x+k}{n+1} = \sum_{k=0}^{n-1} E(n,k)\cdot x \cdot \binom{x+k}{n} =$$

$$= \sum_{k=0}^{n-1} E(n,k)\frac{(k+1)(x+k-n)+(n-k)(x+k+1)}{n+1}\binom{x+k}{n} =$$

$$= \sum_{k=0}^{n-1} E(n,k)\left((k+1)\binom{x+k}{n+1} + (n-k)\binom{x+k+1}{n+1}\right) =$$

$$= \sum_{k=0}^{n-1}(k+1)E(n,k)\binom{x+k}{n+1} + \sum_{k=1}^{n}(n+1-k)E(n,k-1)\binom{x+k}{n+1},$$

kus $\binom{x+k}{n+1}$ kordajate võrdlemine annab rekurrentse võrrandi

$$E(n+1,k) = (k+1)E(n,k) + (n+1-k)E(n,k-1), \tag{5.11}$$

mis kehtib iga $n > 0$ ja $k = 1, 2, \ldots, n$ korral.

Selle võrrandi kasutamisel võib toetuda kergesti kontrollitavatele rajatingimustele: iga $n > 0$ korral on $E(n,0) = 1$ ja $E(n,k) = 0$ siis, kui $k \geqslant n$ (kuid täiendavalt defineeritakse tavaliselt $E(0,0) = 1$). Võrrandist (5.11) saame Euleri teist liiki arvude tabelile järgmise alguse:

n \ k	0	1	2	3	4	5	6
2	1	1					
3	1	4	1				
4	1	11	11	1			
5	1	26	66	26	1		
6	1	57	302	302	57	1	
7	1	120	1191	2416	1191	120	1

6. Rekurrentsed võrrandid

Nagu me eelmises jaotises nägime, tuleb genereerivate funktsioonide abil defineeritavate jadade elementide tegelikuks arvutamiseks enamasti konstrueerida ka vastav rekurrentne võrrand koos sobivate rajatingimustega. Mõnikord on aga jada lihtsaimini defineeritav just oma rekurrentse võrrandi kaudu. Niisuguse olukorraga puutusime kokku juba permutatsioonide ja kombinatsioonide arvude vaatlemisel, kuid lisame siin veel ühe kombinatoorset laadi näite.

Olgu F_n järjestatud hulga $\overline{1,n} = \{1, 2, \ldots, n\}$ niisuguste mittetühjade alamhulkade arv, mis ei sisalda kaht järjestikust elementi. Ilmselt on $F_1 = 1$ ja täiendavalt osutub mugavaks laiendada vaadeldavat definitsiooni veel võrdusega $F_0 = 1$.

Jada $\{F_n\}$ elementide vahelise seose leidmiseks paneme tähele, et vaadeldava F_n alamhulga seas on F_{n-1} sellist, mis ei sisalda viimast elementi n. Seda elementi sisaldavad alamhulgad ei saa aga sisaldada eelviimast elementi $n-1$ ja nende arv on järelikult F_{n-2}. Seega kehtib iga $n \geqslant 2$ korral teist järku rekurrentne võrrand

$$F_n = F_{n-1} + F_{n-2}. \tag{6.1}$$

Arvude F_n leidmiseks tuleb rekurrentne võrrand (6.1) lahendada ülalnimetatud rajatingimustel $F_0 = F_1 = 1$. Lahendamise lihtsustamiseks võime näiteks defineerida jada $\{F_n\}$ genereeriva funktsiooni

$$F(x) = \sum_{n=0}^{\infty} F_n x^n. \tag{6.2}$$

Rajatingimusi ja võrdusi (6.1) definitsioonis (6.2) arvestades võime selle kirjutada ka kujul

$$\begin{aligned}
F(x) &= F_0 + F_1x + F_2x^2 + F_3x^3 + \cdots = \\
&= 1 + x + (F_0 + F_1)x^2 + (F_1 + F_2)x^3 + \cdots = \\
&= 1 + x + x^2 \cdot (F_0 + F_1x + \cdots) + x \cdot (F_1x + F_2x^2 + \cdots) = \\
&= 1 + x + x^2 \cdot F(x) + x \cdot (F(x) - 1).
\end{aligned}$$

Kui nüüd tähistada

$$\xi = \frac{-1+\sqrt{5}}{2} \quad \text{ja} \quad \eta = \frac{-1-\sqrt{5}}{2},$$

siis saame $x^2 + x - 1 = (x-\xi)(x-\eta)$ ning seega

$$F(x) = \frac{1}{1-x-x^2} = \frac{-1}{(x-\xi)(x-\eta)} = \frac{1}{\sqrt{5}(\xi - x)} - \frac{1}{\sqrt{5}(\eta - x)} =$$
$$= \frac{1}{\xi\sqrt{5}}\sum_{n=0}^{\infty}\left(\frac{x}{\xi}\right)^n - \frac{1}{\eta\sqrt{5}}\sum_{n=0}^{\infty}\left(\frac{x}{\eta}\right)^n.$$

Saadud tulemuse võrdlemine definitsiooniga (6.2) annab

$$F_n = \frac{1}{\sqrt{5}\,\xi^{n+1}} - \frac{1}{\sqrt{5}\,\eta^{n+1}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}. \tag{6.3}$$

Sellest nn. *Binet' valemist* (6.3) vahetult leitavaid naturaalarvusid F_n nimetatakse tavaliselt *Fibonacci arvudeks.*

Et võrrandi (6.1) lahendamisel kasutatud veidi kunstlikku meetodit täpsustada, vaatleme nüüd üldist metoodikat genereerivate funktsioonide kasutamiseks *rekurrentsete võrrandite* lahendamisel, tutvustades seda ühe konkreetse näite varal. Meenutame nimelt (vt. (2.5)), et *kordumistega m-kombinatsioonide* arvud $F(n, m)$ rahuldavad kõikide $n = 1, 2, \ldots$ ja $m = 1, 2, \ldots$ väärtuste korral teatavasti võrrandit

$$F(n, m) = F(n, m-1) + F(n-1, m). \tag{6.4}$$

Selle võrrandi lahendamiseks teises jaotises nimetatud rajatingimustel $F(n, 0) = = F(1, m) = 1$ võtame iga fikseeritud n korral vaatlusele jada $\{F(n, m)\}_m$ polünomiaalse genereeriva funktsiooni

$$f_n(x) = \sum_{m=0}^{\infty} F(n, m)x^m. \tag{6.5}$$

Kui nüüd võrrandi (6.4) mõlemaid pooli korrutada argumendi astmega x^m ja tulemused liita üle kõigi $m = 1, 2, \ldots,$ siis saame võrduse

$$\sum_{m=1}^{\infty} F(n, m)x^m = \sum_{m=1}^{\infty} F(n, m-1)x^m + \sum_{m=1}^{\infty} F(n-1, m)x^m.$$

Lisame selles võrduses esinevale esimesele ja viimasele summale veel rajatingimuse kohaselt võrdsed liidetavad $F(n, 0)x^0$ ja $F(n-1, 0)x^0$ ning muudame teises summas summeerimisindeksit:

$$\sum_{m=0}^{\infty} F(n, m)x^m = \sum_{m=0}^{\infty} F(n, m)x^{m+1} + \sum_{m=0}^{\infty} F(n-1, m)x^m.$$

Selle võrduse võib aga tähistuse (6.5) tõttu kirjutada kujul

$$f_n(x) = x\,f_n(x) + f_{n-1}(x) \qquad \text{ehk} \qquad f_n(x) = (1-x)^{-1} f_{n-1}(x).$$

Viimase võrduse korduva rakendamise teel saame nüüd

$$f_n(x) = (1-x)^{-1} f_{n-1}(x) = \ldots = (1-x)^{-n+1} f_1(x) =$$

$$= (1-x)^{-n} = \sum_{m=0}^{\infty} \binom{n+m-1}{m} x^m,$$

kus on arvestatud veel rajatingimuse $F(1,m) = 1$ vahetut järeldust $f_1(x) = (1-x)^{-1}$. Saadud tulemuse võrdlemine definitsiooniga (6.5) näitab, et x^m kordajad peavad võrdsed olema, s. t. valem (2.6) osutub tõestatuks.

Analoogilist metoodikat saab kasutada ka jada genereeriva funktsiooni leidmiseks juhul, mil on teada vastav rekurrentne võrrand. Illustreerime seda kõigepealt *Stirlingi esimest liiki arvude* korral, leides fikseeritud k tarvis jada $\{s(n,k)\}_n$ eksponentsiaalse genereeriva funktsiooni. Selle funktsiooni

$$s_k(x) = \sum_{n=0}^{\infty} s(n,k) \frac{x^n}{n!}$$

leidmiseks paneme tähele, et eelmises jaotises tuletatud võrrandi (5.9) tõttu võime välja kirjutada võrdused

$$\frac{d}{dx} s_k(x) = \sum_{n=1}^{\infty} s(n,k) \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} s(n+1,k) \frac{x^n}{n!} =$$

$$= \sum_{n=0}^{\infty} s(n,k-1) \frac{x^n}{n!} - \sum_{n=1}^{\infty} n\, s(n,k) \frac{x^n}{n!} = s_{k-1}(x) - x \frac{d}{dx} s_k(x).$$

Saadud diferentsiaalvõrrandite rekurrentse süsteemi

$$\frac{d}{dx} s_k(x) = (1+x)^{-1} s_{k-1}(x) \tag{6.6}$$

lahendamine toimub põhimõtteliselt sama meetodiga, lähtuda tuleb seejuures rajatingimusest $s_0(x) = 1$ (sest kahaneva 0-faktoriaali definitsiooni kohaselt $s(0,0) = 1$). Aluseks võtame nüüd funktsionaaljada $\{s_k(x)\}$ polünomiaalse genereeriva funktsiooni

$$s(x,y) = \sum_{k=0}^{\infty} s_k(x) y^k.$$

Selle võrduse diferentseerimine x järgi koos võrrandi (6.6) arvestamisega annab (hariliku) diferentsiaalvõrrandi

$$\frac{\partial}{\partial x}s(x,y) = \sum_{k=1}^{\infty} \frac{d}{dx}s_k(x)\,y^k = (1+x)^{-1}\sum_{k=1}^{\infty} s_{k-1}(x)\,y^k = \frac{y\,s(x,y)}{1+x},$$

mille lahendiks rajatingimusel $s(x,0) = s_0(x) = 1$ on

$$s(x,y) = e^{y\ln(1+x)} = \sum_{k=0}^{\infty} \frac{y^k\,(\ln(1+x))^k}{k!}.$$

Saadud tulemuse võrdlemine funktsiooni $s(x,y)$ definitsiooniga annabki otsitava funktsiooni avaldise

$$s_k(x) = \frac{(\ln(1+x))^k}{k!}.$$

Üsna analoogilise mõttekäiguga võib võrrandile (5.10) tuginedes *Stirlingi teist liiki arvude* eksponentsiaalse genereeriva funktsiooni leida kujul

$$S_k(x) = \sum_{n=0}^{\infty} S(n,k)\,\frac{x^n}{n!} = \frac{(e^x-1)^k}{k!}. \tag{6.7}$$

Seda funktsiooni kasutades võib näiteks tõestada seose *Bernoulli arvude* ja Stirlingi teist liiki arvude vahel. Nimelt kehtib iga $n \in \mathbb{N}$ korral valem

$$B_n = \sum_{k=0}^{n}(-1)^k\,\frac{k!\,S(n,k)}{k+1}. \tag{6.8}$$

Lähtudes definitsioonist (5.2) ja meenutades logaritmrea summat leiame:

$$\begin{aligned}
\sum_{n=0}^{\infty} B_n\,\frac{x^n}{n!} &= x(e^x-1)^{-1} = \ln(1+(e^x-1))\cdot(e^x-1)^{-1} = \\
&= \left(\sum_{n=1}^{\infty}(-1)^{n-1}\frac{(e^x-1)^n}{n}\right)\cdot(e^x-1)^{-1} = \\
&= \sum_{k=0}^{\infty}(-1)^k\,\frac{(e^x-1)^k}{k+1} = \sum_{k=0}^{\infty}(-1)^k\,\frac{k!}{k+1}\cdot\frac{(e^x-1)^k}{k!} = \\
&= \sum_{k=0}^{\infty}(-1)^k\frac{k!}{k+1}\cdot\sum_{n=0}^{\infty}S(n,k)\frac{x^k}{n!} = \\
&= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{\infty}(-1)^k\,\frac{k!\,S(n,k)}{k+1}\right)\cdot\frac{x^n}{n!}.
\end{aligned}$$

Valemi (6.8) saamiseks võrdleme nüüd $x^n/n!$ kordajaid seda võrduste järjendit alustavas ja lõpetavas astmereas ning arvestame, et $k > n$ korral on $S(n,k) = 0$.

Ülalnäidatuga analoogiliselt võib fikseeritud n korral tuletada ka *Euleri teist liiki arvude* jada $\{E(n,k)\}_k$ jaoks polünomiaalse genereeriva funktsiooni

$$E_n(x) = \sum_{k=0}^{n-1} E(n,k)x^k. \tag{6.9}$$

Kui rekurrentse võrrandi (5.11) pooli korrutada teguriga x^k ja summeerida üle kõikide $k = 1, 2, \ldots, n$, siis saame võrrandi

$$\sum_{k=1}^{n} E(n+1,k)x^k = \sum_{k=1}^{n-1}(k+1)E(n,k)x^k + \sum_{k=1}^{n}(n+1-k)E(n,k-1)x^k,$$

mis tähistust (6.9) arvestades on kirjutatav kujul

$$E_{n+1}(x) - 1 = \left(x\frac{d}{dx}E_n(x) + E_n(x) - 1\right) + \left(n\,x\,E_n(x) - x^2\frac{d}{dx}E_n(x)\right).$$

Seega peavad funktsioonid (6.9) rahuldama rekurrentset diferentsiaalvõrrandit

$$E_{n+1}(x) = x(1-x)\frac{d}{dx}E_n(x) + (1+n\,x)E_n(x)$$

loomulikul rajatingimusel $E_0(x) = 1$. Vahetu kontrollimise teel võib veenduda, et selle võrrandi lahendiks osutub

$$E_n(x) = (1-x)^{n+1}\sum_{k=0}^{\infty}(k+1)^n x^k, \tag{6.10}$$

mille võrdlemine definitsiooniga (6.9) annab

$$E(n,k) = \sum_{j=0}^{k}(-1)^j\binom{n+1}{j}(k-j+1)^n.$$

Tulemust (6.10) kasutades saab nüüd kergesti leida genereerivate funktsioonide jada $\{E_n(x)\}$ eksponentsiaalse genereeriva funktsiooni:

$$\begin{aligned}
e^{E(x)z} &= \sum_{n=0}^{\infty} E_n(x)\frac{z^n}{n!} = \sum_{n=0}^{\infty}\frac{(1-x)^{n+1}z^n}{n!}\sum_{k=0}^{\infty}(k+1)^n x^k = \\
&= (1-x)\sum_{k=0}^{\infty} x^k \sum_{n=0}^{\infty}\frac{((k+1)(1-x)z)^n}{n!} = (1-x)\sum_{k=0}^{\infty} x^k e^{(k+1)(1-x)z} = \\
&= (1-x)\sum_{k=0}^{\infty} x^k\left(e^{(1-x)z}\right)^{k+1} = \frac{(1-x)e^{(1-x)z}}{1-x\,e^{(1-x)z}}.
\end{aligned}$$

5*

Kirjeldatud lähenemisviis on rakendatav ka üldjuhul, kui moodustatava jada $\{u_n\}$ elementide vaheline seos on õnnestunud esitada iga $n \geqslant 0$ korral kehtiva k-järku lineaarse homogeense *rekurrentse võrrandina*

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = 0, \tag{6.11}$$

mis tuleb lahendada *rajatingimustel* $u_0 = c_0$, $u_1 = c_1$, $\ldots$, $u_{k-1} = c_{k-1}$. Näitame, et selle jada polünomiaalse genereeriva funktsiooni $u(x)$ saab esitada kujul

$$u(x) \equiv \sum_{n=0}^{\infty} u_n x^n = \frac{P(x)}{1 + a_1 x + \cdots + a_k x^k}, \tag{6.12}$$

kus $P(x)$ on ülimalt $(k-1)$-astme polünoom. Tõepoolest, korrutises

$$(1 + a_1 x + \cdots + a_k x^k)(u_0 + u_1 x + u_2 x^2 + \cdots)$$

on x^{n+k} kordaja $u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n$ seose (6.11) kohaselt iga $n \geqslant 0$ korral null, nullist erineda võivad kordajad aga annavad

$$P(x) = c_0 + (c_1 + a_1 c_0)x + \cdots + (c_{k-1} + a_1 c_{k-2} + \cdots + a_{k-1} c_0) x^{k-1}.$$

Ratsionaalfunktsiooni (6.12) arendame astmeritta traditsioonilisel viisil. Selleks tuleb teatavasti leida abivõrrandi

$$y^k + a_1 y^{k-1} + \cdots + a_{k-1} y + a_k = 0$$

lahendid $\xi_1, \xi_2, \ldots, \xi_s$ ja nende kordsused $m_1, m_2, \ldots, m_s$ (kus $\Sigma m_i = k$), esitada $u(x)$ osamurdude summana ning kasutada binoomvalemit:

$$\begin{aligned}
u(x) &= \frac{P(x)}{(1-\xi_1 x)^{m_1}(1-\xi_2 x)^{m_2}\ldots(1-\xi_s x)^{m_s}} = \\
&= \sum_{i=1}^{s}\left(\frac{\alpha_{i1}}{1-\xi_i x} + \frac{\alpha_{i2}}{(1-\xi_i x)^2} + \cdots + \frac{\alpha_{im_i}}{(1-\xi_i x)^{m_i}}\right) = \\
&= \sum_{n=0}^{\infty} x^n \sum_{i=1}^{s}\left(\alpha_{i1}\binom{n}{0} + \alpha_{i2}\binom{n+1}{1} + \cdots + \alpha_{im_i}\binom{n+m_i-1}{m_i-1}\right)\xi_i^n.
\end{aligned}$$

Näiteks kolmandat järku võrrandi $u_{n+3} - 6u_{n+2} + 11u_{n+1} - 6u_n = 0$ ja rajatingimuste $u_0 = 2$, $u_1 = 0$, $u_2 = -2$ korral saame kergesti

$$u(x) = \frac{2 - 12x + 20x^2}{1 - 6x + 11x^2 - 6x^3} = \frac{5}{1-x} - \frac{4}{1-2x} + \frac{1}{1-3x},$$

mille reaksarenduses x^n kordaja tuleb $u_n = 5 - 2^{n+2} + 3^n$.

7. Summade arvutamine

Genereerivate funktsioonide veel ühe rakendusvaldkonnana vaatleme nende kasutamist mitmesuguste lõplike või lõpmatute *summade arvutamisel*. Vastavatest rohketest võtetest piirdume siin vaid polünomiaalsete genereerivate funktsioonidega ning nendegi korral üksnes mõne kõige olulisema võtte demonstreerimisega.

Sageli saab lõpliku või lõpmatu summa

$$s = \sum_{i \in I} a_i$$

arvutada sel teel, et konstrueeritakse jada $\{a_i\}$ polünomiaalne genereeriv funktsioon

$$a(x) = \sum_{i \in I} a_i x^i$$

ja leitakse siis selle funktsiooni väärtus kohal $x = 1$ (või piirväärtus, kui $x \to 1 - 0$), sest ilmselt $s = a(1)$ (või $s = \lim_{x \to 1-0} a(x)$). Näiteks summa

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i}$$

arvutamiseks moodustame kõigepealt genereeriva funktsiooni

$$a(x) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} x^i = (1-x)^n,$$

millest saamegi vaadeldava summa väärtuse

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = a(1) = 0. \tag{7.1}$$

Lõpmatute summade korral tuleb muidugi täiendavalt kontrollida, kas vaadeldav rida on üldse koonduv, sest kirjeldatud moodus (mis tegelikult pole midagi muud kui nn. *Abeli summeerimismenetlus*) summeerib ka mõningaid hajuvaid ridu. Nii näiteks hajuva rea

$$\sum_{m=0}^{\infty} (-1)^m \binom{n+m}{m}$$

korral saame binoomvalemist $a(x) = (1+x)^{-n-1}$, mis annab "summa" $a(1) = 2^{-n-1}$.

Mõnikord tuleb summade arvutamiseks vajalikkude genereerivate funktsioonide konstrueerimisel kasutada ka mitmesuguseid täiendavaid, enam või vähem kunstlikke võtteid. Nimetame neist siinkohal üksnes kaht.

Näiteks lõpmatu summaga

$$\sum_{k=0}^{\infty} \frac{1}{(2k)!}$$

loomulikult seostuva genereeriva funktsiooni

$$a(x) = \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!}$$

avaldise saamiseks on kasulik võtta vaatlusele veel teine funktsioon

$$b(x) = \sum_{k=0}^{\infty} \frac{x^{2k+1}}{(2k+1)!}.$$

Nüüd on lihtne veenduda, et neid ridu liites saame

$$a(x) + b(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x$$

ja lahutades

$$a(x) - b(x) = \sum_{k=0}^{\infty} \frac{(-x)^k}{k!} = e^{-x}.$$

Viimaste võrduste liitmise teel leiamegi otsitava funktsiooni

$$a(x) = \frac{e^x + e^{-x}}{2}$$

ning vaadeldava summa väärtus tuleb järelikult

$$\sum_{k=0}^{\infty} \frac{1}{(2k)!} = a(1) = \frac{e + e^{-1}}{2} = \operatorname{ch} 1.$$

Soovi korral võime aga avaldada ka abifunktsiooni

$$b(x) = \frac{e^x - e^{-x}}{2},$$

millega oleme "kõrvaltulemusena" arvutanud veel summa

$$\sum_{k=0}^{\infty} \frac{1}{(2k+1)!} = b(1) = \frac{e - e^{-1}}{2} = \operatorname{sh} 1.$$

Teist Abeli menetlusega seostuvat kunstlikku võtet läheb tarvis näiteks summa

$$\sum_{i=1}^{n} i\binom{n}{i}$$

arvutamisel. Nimelt otsides vastavat genereerivat funktsiooni kujul

$$a(x) = \sum_{i=0}^{n} i\binom{n}{i}x^{i-1},$$

on kerge veenduda, et funktsiooni $a(x)$ võib saada näiteks funktsiooni

$$b(x) = \sum_{i=0}^{n} \binom{n}{i}x^{i} = (1+x)^{n}$$

diferentseerimise teel. Seega

$$a(x) = \frac{d}{dx}b(x) = n(1+x)^{n-1}$$

ja

$$\sum_{i=1}^{n} i\binom{n}{i} = a(1) = n\,2^{n-1}.$$

Niisuguste lõplikkude summade arvutamisel, kus summeerimisindeks muutub nullist mingi konstandini, osutub efektiivseks järgmine näiliselt kunstlik võte.

Nimelt kujuneb summa

$$s = \sum_{i=0}^{k} s_i$$

arvutamine üsna lihtsaks sel juhul, kui summa üldliiget s_i õnnestub esitada kujul $s_i = a_i b_{k-i}$ ning jadadele $\{a_k\}$ ja $\{b_k\}$ vastavad polünomiaalsed genereerivad funktsioonid $a(x)$ ja $b(x)$ on kergesti leitavad. Tõepoolest, valemi (3.3) kohaselt osutub otsitav summa s siis x^k kordajaks nende funktsioonide korrutisele $a(x)b(x)$ vastavas astmereas. Kogu küsimus taandub seega üheainsa liikme leidmisele kahe tuntud funktsiooni $a(x)$ ja $b(x)$ korrutise reaksarenduses.

Rohkesti rakendusi leiab see meetod just binoomkordajaid sisaldavate seoste põhjendamisel. Nii näiteks summa

$$\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$$

arvutamiseks tarvitseb vaid tähistada

$$a_i = \binom{n}{i} \qquad \text{ja} \qquad b_{k-i} = \binom{m}{k-i}.$$

Binoomvalemit kasutades leiame kohe nende abijadade genereerivad funktsioonid

$$a(x) = (1+x)^n,$$
$$b(x) = (1+x)^m$$

ja järelikult

$$a(x)b(x) = (1+x)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i.$$

Otsitava summa leiame siit kui x^k kordaja:

$$\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{n+m}{k}.$$

Veel ühe näitena selle meetodi kasutamise kohta meenutame, et *kordumistega kombinatsioonide* arvu $F(n,m)$ määramisel jäi meil ülal lõpetamata valemi (2.6) tuletamine. Nimelt jäi induktsioonimeetodi kasutamisel põhjendamata, et võrrandi

$$F(n,m) = \sum_{i=1}^{n} F(i, m-1) \tag{7.2}$$

lahendiks on iga m korral

$$F(n,m) = \binom{n+m-1}{m}.$$

Kui oletada selle võrduse kehtimist mingi m korral, siis võrrandist (7.2) järeldub otsekohe, et

$$F(n,m+1) = \sum_{i=1}^{n} F(i,m) = \sum_{i=1}^{n} \binom{i+m-1}{m} = \sum_{i=0}^{n-1} \binom{i+m}{m}.$$

Selle summa arvutamiseks tähistame

$$a_i = \binom{i+m}{m} \qquad \text{ja} \qquad b_{(n-1)-i} = 1.$$

Siis täiesti vahetult saame:

$$a(x) = \sum_{i=0}^{\infty} \binom{i+m}{m} x^i = (1-x)^{-m-1},$$

$$b(x) = \sum_{i=0}^{\infty} x^i = (1-x)^{-1},$$

$$a(x)b(x) = (1-x)^{-m-2} = \sum_{i=0}^{\infty} \binom{m+1+i}{i} x^i,$$

kus x^{n-1} kordaja annab otsitava summa väärtuse:

$$\sum_{i=0}^{n-1} \binom{i+m}{m} = \binom{m+n}{n-1} = \binom{n+m}{m+1}.$$

Vaatleme lõpuks veel üht efektiivset, kuigi eelmistest enamasti tunduvalt töömahukamaks osutuvat võtet, mille korral (kas lõpliku või lõpmatu) summa

$$s = \sum_{i \in \mathcal{I}} a_i$$

üldliige a_i püütakse teisendada niisugusele kujule, et ta võrduks argumendi x teatava i-st sõltumatu astendajaga astme x^k kordajaga mingi tuntud genereeriva funktsiooni $A_i(x)$ astmereas. Otsitava summa s saamiseks tuleb siis leida argumendi sellesama astme x^k kordaja funktsiooni

$$A(x) = \sum_{i \in \mathcal{I}} A_i(x)$$

arendamisel saadavas astmereas.

Paneme tähele, et vaadeldava meetodi korral pole põhiliseks momendiks enam astmereana antud genereeriva funktsiooni kompaktse avaldise leidmine, vaid teatavate funktsioonide lõpliku või lõpmatu summa arendamine astmereaks (täpsemalt, saadava reaksarenduse ühe konkreetse kordaja leidmine).

Meetodi illustreerimiseks arvutame näitena lõpliku summa

$$\sum_{i=0}^{n} (-1)^i \binom{2n-i}{i} 2^{2n-2i}.$$

Kui selle summa üldliige kirjutada kujul

$$\binom{2n-i}{2n-2i} 2^{2n-2i} \cdot (-1)^i,$$

siis märkame, et tegemist on x^{2n} kordajaga funktsiooni

$$A_i(x) \equiv (1+2x)^{2n-i} \cdot (-x^2)^i$$

reaksarenduses. Geomeetrilise progressiooni summa valemit

$$\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q}$$

kasutades leiame nüüd üsna kompaktse avaldise $A(x)$ jaoks:

$$A(x) = \sum_{i=0}^{n} (1+2x)^{2n-i}(-x^2)^i = (1+2x)^n \frac{(1+2x)^{n+1} - (-x^2)^{n+1}}{(1+x)^2} =$$

$$= \frac{(1+2x)^{2n+1}}{(1+x)^2} - \frac{(-1)^{n+1} x^{2n+2} (1+2x)^n}{(1+x)^2}.$$

Saadud avaldis kujutab endast muidugi polünoomi, kuid selle polünoomi esitamine kanoonilisel kujul osutub nähtavasti üpris raskeks ülesandeks. Sellepärast unustame, et tegemist on polünoomiga ja arendame ta reaks nagu ikka ratsionaalfunktsiooni.

Siinjuures näeme, et selle funktsiooni avaldise teise liikme arendamisel saadavas astmereas on x^{2n} kordaja null, sest argumendi madalaimaks astmeks tuleb x^{2n+2}. Järelikult piisab vaid funktsiooni avaldise esimese liikme vaatlemisest, s. t. peame arendama astmereaks jagatise

$$\frac{(1+2x)^{2n+1}}{(1+x)^2}.$$

Selle jagatise täisosaks tuleb mingi $(2n-1)$-astme polünoom, jäägiks aga esimese astme polünoom. Meid huvitava jäägi leidmiseks võime kasutada *Bezout' teoreemi* tuntud üldistust, mille kohaselt iga (vähemalt teise astme) polünoomi $P(x)$ ja mistahes arvu a korral

$$\frac{P(x)}{(x-a)^2} = Q(x) + \frac{(x-a)P'(a) + P(a)}{(x-a)^2},$$

kus $Q(x)$ on teatav kahe võrra madalama astme polünoom kui $P(x)$.

Et antud juhul $P(x) = (1+2x)^{2n+1}$ ja $a = -1$, siis saame jäägi

$$(x-a)P'(a) + P(a) =$$

$$= (1+x)(2n+1)\cdot 2\cdot(-1)^{2n} + (-1)^{2n+1} = -1 + (4n+2)(1+x)$$

ning küsimus taandub järelikult x^{2n} kordaja leidmisele jagatise

$$\frac{-1+(4n+2)(1+x)}{(1+x)^2} = \frac{-1}{(1+x)^2} + \frac{4n+2}{1+x}$$

arendamisel saadavas astmereas. Selle astmerea leidmiseks saame aga juba vahetult kasutada binoomvalemit (2.4), mis annab

$$\frac{-1}{(1+x)^2} = -\sum_{i=0}^{\infty}(-1)^i\binom{i+1}{i}x^i = \sum_{i=0}^{\infty}(-1)^{i+1}(i+1)x^i,$$

$$\frac{4n+2}{1+x} = (4n+2)\sum_{i=0}^{\infty}(-1)^i\binom{i}{i}x^i = (4n+2)\sum_{i=0}^{\infty}(-1)^i x^i.$$

Järelikult x^{2n} kordajaks tuleb

$$(-1)^{2n+1}(2n+1) + (4n+2)(-1)^{2n} = -2n-1+4n+2 = 2n+1$$

ja vaadeldava summa väärtuseks saame seega

$$\sum_{i=0}^{n}(-1)^i\binom{2n-i}{i}2^{2n-2i} = 2n+1.$$

8. Formaalsed read

24 Genereeriva funktsiooni idee on tuntud juba Euleri ja Laplace'i aegadest, kuid esimesed katsed selle mõiste matemaatiliselt rangeks käsitlemiseks tehti alles XIX sajandil (A. L. Cauchy). Meie senise heuristilise lähenemisviisi täpsustamiseks tutvumegi järgnevalt vastavate algebraliste põhjendustega. Konkreetsuse huvides võtame seejuures aluseks mitte suvalise korpuse, vaid kompleksarvude korpuse $\mathbb{C}$, s. t. piirdume üksnes arvjadade (ehk kompleksarvuliste jadade) vaatlemisega.

Arvjada $a \equiv (a_0, a_1, a_2, \ldots)$ defineerime ikka kui funktsiooni $a\colon \mathbb{N} \to \mathbb{C}$, kusjuures funktsiooni väärtusi ehk jada elemente tähistame siin traditsioonilise a_k kõrval sageli ka kujul $(a)_k$ (mitte aga kujul $a(k)$, sest niisugust tüüpi tähise reserveerime teise tähenduse tarvis). Kõikide jadade hulka tähistame sümboliga $\mathbb{C}^{\mathbb{N}}$.

Hulga $\mathbb{C}^{\mathbb{N}}$ võib kergesti muuta algebraks (mida nimetatakse enamasti *Cauchy algebraks*), kui defineerida temas operatsioonid järgmiselt:

$$
\begin{aligned}
(\lambda a)_k &= \lambda(a)_k \quad (\lambda \in \mathbb{C}),\\
(a+b)_k &= (a)_k + (b)_k,\\
(ab)_k &= \sum_{j=0}^{k} (a)_j (b)_{k-j}.
\end{aligned}
$$

Algebra aksioomide täidetuse kontrollimine nende operatsioonide korral osutub triviaalseks, nimetamist väärib siin vast ainult *korrutamise* assotsiatiivsuse kontrollimine. Nimelt saame iga k korral:

$$
\begin{aligned}
((ab)c)_k &= \sum_{i=0}^{k} (ab)_i c_{k-i} = \sum_{i=0}^{k} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) c_{k-i} =\\
&= \sum_{i=0}^{k} \sum_{j=0}^{i} a_j b_{i-j} c_{k-i} = \sum_{j=0}^{k} \sum_{i=j}^{k} a_j b_{i-j} c_{k-i} =\\
&= \sum_{j=0}^{k} a_j \sum_{i=0}^{k-j} b_i c_{k-j-i} = \sum_{j=0}^{k} a_j (bc)_{k-j} = (a(bc))_k.
\end{aligned}
$$

Lisame, et jadade korrutamine on kommutatiivne, jada $\mathbf{0} = (0, 0, 0, \ldots)$ on algebras $\mathbb{C}^{\mathbb{N}}$ nullelemendiks, jada $\mathbf{1} = (1, 0, 0, \ldots)$ aga ühikelemendiks. Jada $a \in \mathbb{C}^{\mathbb{N}}$ *järk* $o(a)$ defineeritakse kui tema esimese nullist erineva elemendi indeks:

$$o(a) = \min\{k : a_k \neq 0\}.$$

Kasulikkudeks osutuvad veel järgmised tähelepanekud algebra $\mathbb{C}^{\mathbb{N}}$ kohta.

Esiteks, Cauchy algebras puuduvad nullitegurid. Tõepoolest, nullelemendist $\mathbf{0}$ erinevate jadade a ja b korral ei saa olla $ab = \mathbf{0}$, sest kui $m = o(a)$, $n = o(b)$, siis

$$(ab)_{m+n} = \sum_{j=0}^{m+n} a_j b_{m+n-j} = a_m b_n \neq 0.$$

Teiseks, kui $(a)_0 \neq 0$, siis jada a on pööratav. See tähendab, et leidub üheselt määratud jada b, mille korral $ab = \mathbf{1}$. Jada a jaoks niiviisi saadavat *pöördjada* b tähistatakse tavaliselt kujul a^{-1}. Pöördjada elemendid saab määrata võrranditest

$$a_0 b_0 = 1, \quad a_0 b_1 + a_1 b_0 = 0, \quad \ldots, \quad a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = 0, \quad \ldots$$

Kui tavalisel viisil defineerida *jada aste* (s. t. $a^0 \equiv \mathbf{1}$ ning iga $n > 0$ korral $a^n \equiv a^{n-1}a$), siis on kerge veenduda, et ka $a^n(a^{-1})^n = \mathbf{1}$. Seega pöördjada ühesuse tõttu $(a^n)^{-1} = (a^{-1})^n$, mis annab aluse kasutada tähistust $a^{-n} \equiv (a^n)^{-1}$.

Kolmandaks, fikseeritud jada $a \in \mathbb{C}^{\mathbb{N}}$ ja naturaalarvu n korral leidub tingimust $a = b^n$ rahuldav jada $b \in \mathbb{C}^{\mathbb{N}}$ parajasti siis, kui jada a järk on arvu n kordne, s. t. kui $o(a) = k \cdot n$. Selle väite põhjendusel siinkohal peatumata märgime, et iga niisugust jada b nimetatakse n-astme *juureks* jadast a ja tähistatakse $b = a^{\frac{1}{n}}$.

Meie edasises käsitluses omandab erilise koha jada

$$x \equiv (0, 1, 0, 0, \ldots),$$

mille astmed avalduvad kujul $x^2 = (0,0,1,0,\ldots)$, $x^3 = (0,0,0,1,\ldots)$ ning üldiselt $x^n = (\underbrace{0,0,\ldots,0}_{n},1,0,\ldots)$, kuhu võib veel lisada võrduse $x^0 = (1,0,0,\ldots) = \mathbf{1}$.

Arvestades operatsioonide definitsioone Cauchy algebras saame suvalise jada $a = (a_0, a_1, a_2, \ldots) \in \mathbb{C}^{\mathbb{N}}$ korral võrduse

$$a_n x^n = (a_n, 0, 0, \ldots)(\underbrace{0, 0, \ldots, 0}_{n}, 1, 0, \ldots) = (\underbrace{0, 0, \ldots, 0}_{n}, a_n, ,0, \ldots)$$

ja terve selle jada a võime formaalselt üles kirjutada reana

$$a \equiv a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n \geqslant 0} a_n x^n.$$

Siinkohal on oluline rõhutada, et jada niisugune esitus on puhtformaalne ega ole seotud matemaatilises analüüsis vaadeldavate astmeridadega või üldse piirprotsessiga. Seepärast kasutataksegi nende kirjutiste korral *formaalsete ridade* nimetust ega räägita ridade summadest (kas koondumise või mõnes muus mõttes). Edaspidi kasutame a asemel sageli tähist $a(x)$ selle asjaolu allakriipsutamiseks, et jada a vaadeldakse formaalse rea kujul.

25

Vaadeldavas uues tõlgenduses võib jadade (siitpeale küll juba ridade!) korrutamise definitsiooni üles kirjutada võrdusena

$$a(x)b(x) = \sum_{k \geqslant 0} \Big(\sum_{j=0}^{k} a_j b_{k-j} \Big) x^k.$$

Nii näiteks jadade korrutise

$$(1, -1, 0, \ldots)(1, 1, 1, \ldots) = \mathbf{1}$$

saab vastavaid ridu kasutades seega esitada kujul

$$(1 - x)(1 + x + x^2 + \cdots) = \mathbf{1}(x) \equiv 1,$$

millega oleme põhjendanud võrduse

$$(1 - x)^{-1} = 1 + x + x^2 + \cdots .$$

Kõikide (formaalsete) ridade hulka tähistame edaspidi sümboliga $\mathcal{R}^{\#}$. Ühtlasi võtame iga $m \in \mathrm{N}$ korral kasutusele veel tähistuse

$$\mathcal{R}^{\#}_m = \{a \colon a(x) = \sum_{k \geqslant 0} a_k x^k, \ a_0 = \ldots = a_{m-1} = 0\}.$$

Ilmselt $a \in \mathcal{R}^{\#}_m \setminus \mathcal{R}^{\#}_{m+1}$ tähendab, et rea a järk on m, s. t. $o(a) = m$. Seevastu aga $a \in \mathcal{R}^{\#}_m$ on samaväärne väitega $o(a) \geqslant m$, samuti nagu näiteks $a \in \mathcal{R}^{\#} \setminus \mathcal{R}^{\#}_1$ on samaväärne väitega $o(a) = 0$.

Ridade hulka $\{a^{(i)} \colon i \in \mathcal{I}\}$ nimetatakse *summeeruvaks*, kui iga naturaalarvu n korral leidub vaid lõplik alamhulk selliseid ridu

$$a^{(i)}(x) = \sum_{k \geqslant 0} (a^{(i)})_k x^k,$$

kus $(a^{(i)})_n \neq 0$. Ridade summeeruva hulga $\{a^{(i)} \colon i \in \mathcal{I}\}$ *summaks* nimetatakse rida $a(x) = \sum_{n \geqslant 0} a_n x^n$, mille kordajad on määratud valemiga

$$a_n = \sum_{i \in \mathcal{I}} (a^{(i)})_n,$$

kus nullist erinevate liidetavate hulk tuleb iga n korral muidugi lõplik. Ilmselt ridade sellise summeerimise operatsioon on kommutatiivne ning assotsiatiivne.

Summeeruvuse mõiste abil saab summamärgile formaalse rea avaldises anda uue tõlgenduse. Selleks paneme tähele, et iga monoomi $a_n x^n$ võib tõlgendada reana $\sum_{k \geqslant 0} a_k x^k$, tarvitseb vaid $k \neq n$ korral lugeda $a_k = 0$. Edaspidi arvestamegi, et vajaduse korral võib kirjutis $a_n x^n$ tähendada ka niisugust üheainsa nullist erineva liikmega rida.

Monoomide hulk $\{a_n x^n \colon n \in \mathrm{N}\}$ on kordajate $a_n \in \mathbb{C}$ igasuguse valiku korral ilmselt summeeruv, kusjuures summaks tuleb rida $\sum_{n \geqslant 0} a_n x^n$. Sellise tõlgenduse korral võib ka ridade $\sum_{n \geqslant 0} a_n x^n$ ja $\sum_{n \geqslant 0} b_n x^n$ korrutist vaadelda kui monoomide summeeruva hulga $\{a_n b_m x^{n+m} \colon (n, m) \in \mathrm{N}^2\}$ summat.

Formaalsete ridade kasutamisel kombinatoorikas osutuvad sageli vajalikkudeks operaatorid D: $\mathcal{R}^{\#} \to \mathcal{R}^{\#}$ (diferentseerimisoperaator ehk *tuletisrea* leidmise operaator) ja A: $\mathcal{R}^{\#} \to \mathcal{R}^{\#}$ (integreerimisoperaator ehk *algrea* leidmise operaator).

Diferentseerimisoperaator D seab reale $a(x) = \sum_{n \geqslant 0} a_n x^n$ vastavusse rea

$$D(a) = \sum_{n \geqslant 1} n\, a_n x^{n-1}. \tag{8.1}$$

Ridade kordajate vahetu võrdlemise teel võib veenduda, et suvaliste $a, b \in \mathcal{R}^{\#}$ korral kehtivad matemaatilisest analüüsist tuntutega analoogilised seosed

$$\left.\begin{aligned} D(a+b) &= D(a) + D(b), \\ D(ab) &= aD(b) + bD(a), \\ D(a^n) &= na^{n-1}D(a). \end{aligned}\right\} \tag{8.2}$$

Kui $o(a) = 0$, siis kehtib veel seos

$$D(a^{-n}) = -na^{-n-1}D(a).$$

Tõepoolest, rakendades seose $a\,a^{-1} = \mathbf{1}$ mõlemale poolele operaatorit D leiame $D(a^{-1}) = -a^{-2}D(a)$ ja võrdusi $a^{-n} = (a^n)^{-1} = (a^{-1})^n$ arvestades seega

$$\begin{aligned} D(a^{-n}) &= D((a^{-1})^n) = n(a^{-1})^{n-1}D(a^{-1}) = \\ &= n(a^{-1})^{n-1}(-a^{-2}D(a)) = -na^{-n-1}D(a). \end{aligned}$$

Veelgi üldisemalt, suvalise ratsionaalarvu $r \in \mathbb{Q}$ ja $o(a) = 0$ korral kehtib seos

$$D(a^r) = r\, a^{r-1}D(a).$$

Tõepoolest, kui $r = m/n$, kus $m, n \in \mathbb{Z}$, siis

$$D((a^r)^n) = n(a^r)^{n-1}D(a^r) \quad \text{ning} \quad D((a^r)^n) = D(a^m) = m\, a^{m-1}D(a),$$

millest

$$n(a^r)^{n-1}D(a^r) = m\, a^{m-1}D(a),$$

ehk

$$D(a^r) = \frac{m}{n}a^{m-1}\Big((a^r)^{n-1}\Big)^{-1}D(a) = r\, a^{r-1}D(a).$$

Diferentseerimisoperaatori definitsiooni (8.1) traditsioonilisel viisil induktiivselt jätkates tähistame $D^1(a) \equiv D(a)$, defineerime iga $k > 1$ korral

$$D^k(a) \equiv D(D^{k-1}(a))$$

ja kirjutiste ühtsuse huvides laiendame seda kirjutusviisi vajaduse esinemisel ka veel juhule $k = 0$, defineerides $D^0(a) \equiv a$.

Induktiivse arutlusega saab kergesti tõestada võrduse

$$D^k(a) = \sum_{n-k \geqslant 0} n(n-1)\dots(n-k+1)a_n x^{n-k} = \sum_{i \geqslant 0} \frac{(k+i)!}{i!} a_{k+i} x^i,$$

kust näeme, et $(D^k(a))_0 = k!\, a_k$, millega on põhjendatud *Maclaurini valemi* analoog

$$a = \sum_{k \geqslant 0} (D^k(a))_0 \frac{x^k}{k!}. \tag{8.3}$$

Induktsiooniga saab põhjendada veel *Leibnizi valemi* analoogi

$$D^k(ab) = D^k(a)b + \binom{k}{1} D^{k-1}(a)D(b) + \binom{k}{2} D^{k-2}(a)D^2(b) + \dots + a\,D^k(b)$$

ning suvaliste ratsionaalarvude r ja s korral kehtiva *binoomvalemi*

$$(1+sx)^r = \sum_{n \geqslant 0} \binom{r}{n} (sx)^n. \tag{8.4}$$

Näiteks viimase tõestamiseks lähtume võrdusest

$$D((1+sx)^r) = r(1+sx)^{r-1} D(1+sx) = rs(1+sx)^{r-1},$$

millest induktsiooniga n järgi tuleneb võrdus

$$D^n((1+sx)^r) = r(r-1)\dots(r-n+1)s^n(1+sx)^{r-n},$$

seega

$$\left(D^n(1+sx)^r\right)_0 = r(r-1)\dots(r-n+1)s^n.$$

Valem (8.4) järeldub nüüd rea $(1+sx)^r$ Maclaurini valemist (8.3):

$$(1+sx)^r = \sum_{n \geqslant 0} \frac{1}{n!}\left(D^n(1+sx)^r\right)_0 x^n =$$

$$= \sum_{n \geqslant 0} \frac{1}{n!} r(r-1)\dots(r-n+1)s^n x^n = \sum_{n \geqslant 0} \binom{r}{n} (sx)^n.$$

Märgime veel, et summeeruva hulga $\{a^{(i)}\colon i \in \mathcal{I}\}$ jaoks kehtib valem

$$D\Big(\sum_{i \in \mathcal{I}} a^{(i)}\Big) = \sum_{i \in \mathcal{I}} D(a^{(i)}).$$

Integreerimisoperaator defineeritakse valemiga

$$A\Big(\sum_{n \geqslant 0} a_n x^n\Big) = \sum_{n \geqslant 1} \frac{a_{n-1}}{n} x^n.$$

Vahetult definitsioonidest järelduvad seosed

$$D(A(a)) = a \qquad \text{ja} \qquad A(D(a)) = \sum_{n \geqslant 1} a_n x^n,$$

kusjuures $A(Da)) = a$ kehtib parajasti siis, kui $o(a) > 0$.

9. Operatsioonid formaalsete ridadega

Formaalsete ridade rakendustes kõige olulisemaks operatsiooniks osutub nähtavasti ühe formaalse rea superponeerimine teise ritta, mis on teostatav alati siis, kui superponeeritava rea "vabaliige" võrdub nulliga.

Lähtudes formaalsetest ridadest $a \in \mathcal{R}^{\#}$ ja $c \in \mathcal{R}_1^{\#}$, s. t.

$$a = \sum_{n\geqslant 0} a_n x^n \quad \text{ja} \quad c = \sum_{n\geqslant 1} c_n x^n$$

seame igale monoomile $a_n x^n$ vastavusse formaalse rea $a_n c^n$. Niiviisi saadava rea järk tuleb vähemalt n, sest $o(c) \geqslant 1$ tõttu

$$o(a_n c^n) = o(a_n) + \underbrace{o(c) + o(c) + \cdots + o(c)}_{n} = o(a_n) + n\, o(c) \geqslant n.$$

Sellest nähtub, et ridade hulk $\{a_n c^n : n \in \mathbb{N}\}$ osutub summeeruvaks ja järelikult leidub summa $\sum_{n\geqslant 0} a_n c^n$. Saadud rea liikmete korraldamine x astmete järgi annab formaalse rea, mida nimetatakse rea $c(x)$ *superpositsiooniks* ritta $a(x)$ ja tähistatakse $a(c(x))$ või lühemalt ka kujul $a \circ c$.

Märgime, et vastavalt äsjatoodud definitsioonile ja varasemale kokkuleppele $x^0 = \mathbf{1}$ kehtib iga $c \in \mathcal{R}_1^{\#}$ korral seos $\mathbf{1} \circ c = \mathbf{1}$. Samuti saab kergesti tõestada seosed

$$(a + b) \circ c = a \circ c + b \circ c, \tag{9.1}$$

$$(ab) \circ c = (a \circ c)(b \circ c), \tag{9.2}$$

millest järeldub, et rea $c \in \mathcal{R}_1^{\#}$ poolt määratud kujutus $a \mapsto a \circ c$ osutub ringi $\mathcal{R}^{\#}$ endomorfismiks.

Omadust (9.1) saab kergesti üldistada. Olgu nimelt $\{a^{(i)} : i \in \mathcal{I}\}$ ridade mingi summeeruv hulk ning $c \in \mathcal{R}_1^{\#}$. Sel korral osutub hulk $\{a^{(i)} \circ c : i \in \mathcal{I}\}$ samuti summeeruvaks ning kehtib võrdus

$$\Big(\sum_{i\in\mathcal{I}} a^{(i)}\Big) \circ c = \sum_{i\in\mathcal{I}} a^{(i)} \circ c.$$

Tõepoolest, kui $a^{(i)}(x) = \sum_{n\geqslant 0} a_n^{(i)} x^n$, siis

$$\sum_{i\in\mathcal{I}} a^{(i)} = \sum_{n\geqslant 0} \Big(\sum_{i\in\mathcal{I}} a_n^{(i)}\Big) x^n$$

ja järelikult

$$\Big(\sum_{i\in\mathcal{I}} a^{(i)}\Big) \circ c = \sum_{n\geqslant 0} \Big(\sum_{i\in\mathcal{I}} a_n^{(i)}\Big) c^n.$$

Teiselt poolt aga kehtib ka võrdus

$$\sum_{i\in\mathcal{I}} a^{(i)} \circ c = \sum_{i\in\mathcal{I}} \Big(\sum_{n\geqslant 0} a_n^{(i)} c^n\Big),$$

mille võrdlemine eelmise võrdusega annabki omaduse (9.1) nimetatud üldistuse (mõlemal juhul on x^k kordajaks arvude $a_n^{(i)}$ lõplik summa).

Ridade superpositsiooni oluliseks omaduseks on tema assotsiatiivsus, s. t. et suvaliste $c, d \in \mathcal{R}_1^\#$ korral kehtib võrdus

$$(a \circ c) \circ d = a \circ (c \circ d). \tag{9.3}$$

Väidetava omaduse põhjendamiseks vaatleme algul erijuhtu $a \equiv x^n$, mil (9.3) omandab kuju $c^n \circ d = (c \circ d)^n$. See võrdus tuleneb aga vahetult omadusest (9.2), kui seal võtta $a = b = c$ ning kasutada induktsiooni n järgi.

Üldjuhu taandamiseks sellele erijuhule tarvitseb vaid formaalset rida vaadelda tema monoomide summeeruva hulga summana. Võrdusele $a \circ c = \sum_{n\geqslant 0} a_n c^n$ ning äsjatõestatule toetudes saame võrduse (9.3) nüüd täiesti vahetult:

$$(a \circ c) \circ d = \Big(\sum_{n\geqslant 0} a_n c^n\Big) \circ d = \sum_{n\geqslant 0} a_n (c^n \circ d) = \sum_{n\geqslant 0} a_n (c \circ d)^n = a \circ (c \circ d).$$

Paneme tähele, et rida x käitub superpositsiooni suhtes ühikelemendina selles mõttes, et iga $a \in \mathcal{R}^\#$ korral kehtivad võrdused:

$$a \circ x = a = x \circ a$$

(tuleb rõhutada, et ritta x saab erandina superponeerida suvalist rida a). Siit tuleneb mingi fikseeritud rea $a \in \mathcal{R}^\#$ korral loomulik küsimus niisuguse *neutraliseeriva rea* c olemasolu kohta, mis annaks $a \circ c = x$.

Teoreem. Antud rea $a \in \mathcal{R}^\#$ korral leidub seost

$$a \circ c = x$$

rahuldav rida $c \in \mathcal{R}_1^\#$ parajasti siis, kui $o(a) = 1$; sel tingimusel kehtib ka $c \circ a = x$ ning rida c on üheselt määratud.

Tõestuseks kirjutame meid huvitava seose $a \circ c = x$ ridade $a(x) = \sum_{n\geqslant 0} a_n x^n$ ja $c(x) = \sum_{n\geqslant 1} c_n x^n$ vahel välja kujul

$$a_0 + a_1 c(x) + a_2 (c(x))^2 + \cdots = x.$$

See ridadevaheline võrdus tähendab, et iga $n \in \mathrm{N}$ korral peavad x^n kordajad mõlemas reas ühesugused olema. Nii näiteks võttes $n = 0$ ja $n = 1$ saame kõigepealt $a_0 = 0$ ja $a_1 c_1 = 1$, millest vahetult nähtub tingimuse $o(a) = 1$ tarvilikkus vaadeldava seose $a \circ c = x$ kehtimiseks.

Tingimuse piisavuse tõestamiseks näitame, et viimati välja kirjutatud võrduses x^n kordajaid võrreldes saab nüüd üheselt määrata kõik kordajad c_n. Kui $a_1 \neq 0$, siis juba nimetatud seosest $a_1c_1 = 1$ saame muidugi $c_1 = a_1^{-1}$. Niiviisi jätkates avaldub vastav seos suvalise n korral kujul

$$a_1c_n + P_n(a_2, a_3, \ldots, a_n, c_1, c_2, \ldots, c_{n-1}) = 0,$$

kus P_n tähistab naturaalarvuliste kordajatega polünoomi, mis on $a_2, a_3, \ldots .a_n$ suhtes lineaarne ning sõltub eelnevalt leitud kordajatest $c_1, c_2, \ldots, c_{n-1}$ (see järeldub täiesti vahetult korrutamise definitsioonist Cauchy algebras). Näiteks x^2 kordajate võrdlemine annab seose

$$a_1c_2 + P_2(a_2, c_1) = a_1c_2 + a_2c_1^2 = 0,$$

millest $c_2 = -a_1^{-1}a_2c_1^2$. Sel viisil jätkates saame järk-järgult määrata rea $c(x)$ kõik kordajad, kusjuures tuleb muidugi $o(c) = 1$.

Kui äsjakirjeldatud protseduuri rakendada reale c, siis saame rea d, mis rahuldab tingimusi $d_0 = 0$ ja $c \circ d = x$. Sellest näeme, et

$$d = x \circ d = (a \circ c) \circ d = a \circ (c \circ d) = a \circ x = a,$$

s. t. $x = c \circ d = c \circ a$ ja teoreem on tõestatud.

Diferentseerimisoperaatorit D seob superpositsiooniga iga $c \in \mathcal{R}_1^{\#}$ korral võrdus

$$D(a \circ c) = \big(D(a) \circ c\big)D(c).$$

Tõepoolest, kui $a = \sum_{n\geqslant 0} a_nx^n$, siis $D(a) = \sum_{n\geqslant 1} na_nx^{n-1}$ ja

$$D(a \circ c) = D\Big(\sum_{n\geqslant 0} a_nc^n\Big) = \sum_{n\geqslant 1} na_nc^{n-1}D(c) = \big(D(a) \circ c\big)D(c).$$

Vaatleme suvalist rida a, milles $(a)_0 = 1$. Sel korral leidub rida $b \in \mathcal{R}_1^{\#}$ nii, et $a = 1 + b$. *Formaalne logaritm* $L(a)$ defineeritakse kui rida

$$L(a) = L(1 + b) = \sum_{n\geqslant 1}(-1)^{n+1}\frac{b^n}{n}. \tag{9.4}$$

Diferentseerimisoperaatoriga seob formaalset logaritmi võrdus

$$D(L(a)) = a^{-1}D(a), \tag{9.5}$$

mis tuleneb järgmistest arvutustest:

$$D(L(a)) = D\Big(\sum_{n\geqslant 1}(-1)^{n+1}\frac{b^n}{n}\Big) = \sum_{n\geqslant 1}(-1)^{n+1}\frac{nb^{n-1}D(b)}{n} =$$
$$= D(b)\sum_{n\geqslant 1}(-1)^{n-1}b^{n-1} = D(b)(1 + b)^{-1} = a^{-1}D(a).$$

Kirjutiste lühendamiseks kasutame formaalse logaritmi võimalikkude argumentide hulga jaoks edaspidi tähistust $\mathcal{R}^{\#}(1) \equiv \{a\colon a \in \mathcal{R}^{\#},\ (a)_0 = 1\}$.

Formaalse logaritmi omaduste selgitamisel osutub kõigepealt, et suvaliste ridade $c, d \in \mathcal{R}^{\#}(1)$ korral on võrduse (9.5) otseseks järelduseks valem

$$L(cd) = L(c) + L(d). \tag{9.6}$$

Tõepoolest, esimest valemitest (8.2) arvestades saame

$$D(L(cd)) = (cd)^{-1}D(cd) = d^{-1}D(d) + c^{-1}D(c) = D(L(c) + L(d)).$$

Et aga nii $L(cd)$ kui ka $L(c) + L(d)$ kuuluvad hulka $\mathcal{R}_1^{\#}$, siis diferentseerimisoperaatori väärtuste võrdsusest nende argumentide korral järeldub ka argumentide eneste võrdsus ning valem (9.6) on tõestatud.

Märgime veel, et iga $a \in \mathcal{R}^{\#}(1)$ korral

$$L(a) = \mathbf{0} \iff a = \mathbf{1}. \tag{9.7}$$

Tõepoolest, kui $L(a) = \mathbf{0}$, siis võrdus (9.5) annab

$$a^{-1}D(a) = D(L(a)) = D(\mathbf{0}) = \mathbf{0}.$$

Et aga seejuures $a \in \mathcal{R}^{\#}(1)$, siis $D(a) = \mathbf{0}$ tähendab sama mis $a = \mathbf{1}$. Vastassuunaline implikatsioon järeldub definitsioonist (9.4) vahetult.

Iga ratsionaalarvu r ja rea $a \in \mathcal{R}^{\#}(1)$ korral kehtib ka võrdus

$$L(a^r) = rL(a), \tag{9.8}$$

mille põhjendamiseks paneme kõigepealt tähele, et

$$\mathbf{0} = L(\mathbf{1}) = L(aa^{-1}) = L(a) + L(a^{-1}).$$

Seega $L(a^{-1}) = -L(a)$. Nüüd pole induktsiooni kasutades raske veenduda, et iga täisarvu n korral $L(a^n) = nL(a)$. Esitades aga ratsionaalarvu r kujul $r = m/n$, kus $m, n \in \mathbb{Z}$, saamegi võrduse (9.8):

$$mL(a) = L(a^m) = L((a^r)^n) = nL(a^r).$$

Seosed (9.4) kuni (9.8) võimaldavad veel üsna kergesti näidata, et suvaliste $r \in \mathbb{Q}$ ja $b \in \mathcal{R}_1^{\#}$ korral kehtib *binoomvalem*

$$(1 + b)^r = \sum_{n \geqslant 0} \binom{r}{n} b^n.$$

7*

28

Suvalise rea $b \in \mathcal{R}_1^\#$ korral defineeritakse tema *formaalne eksponent* kui rida

$$E(b) = \sum_{n \geqslant 0} \frac{b^n}{n!} \tag{9.9}$$

(sellealases kirjanduses on küll kasutatud ka tähistust $\exp b$ või e^b). Definitsioonist (9.9) nähtub, et kujutus $b \mapsto E(b)$ toimib hulgast $\mathcal{R}_1^\#$ hulka $\mathcal{R}^\#(1)$.

Formaalse eksponendi omadustest märgime kõigepealt seost

$$D(E(b)) = D(b)E(b), \tag{9.10}$$

mille saab täiesti vahetu aruteluga põhjendada:

$$D(E(b)) = D\Big(\sum_{n \geqslant 0} \frac{b^n}{n!}\Big) = \sum_{n \geqslant 1} D(b)\frac{b^{n-1}}{(n-1)!} =$$
$$= D(b)\sum_{k \geqslant 0} \frac{b^k}{k!} = D(b)E(b).$$

Edasi tõestame implikatsiooni

$$E(b) = E(c) \implies b = c.$$

Võrduse $E(b) = E(c)$ pooltele diferentseerimisoperaatorit D rakendades ja ühtlasi seost (9.10) arvestades saame

$$D(b)E(b) = D(c)E(c).$$

Et seejuures $E(b) = E(c) \neq \mathbf{0}$ ning algebras $\mathcal{R}^\#$ puuduvad nullitegurid, siis saame $D(b) = D(c)$, millest $b, c \in \mathcal{R}_1^\#$ tõttu järeldubki $b = c$.

Seosed formaalse eksponendi ja formaalse logaritmi vahel on määratud järgmiste implikatsioonidega:

$$\begin{aligned} b \in \mathcal{R}_1^\# &\implies L(E(b)) = b, \\ a \in \mathcal{R}^\#(1) &\implies E(L(a)) = a. \end{aligned} \tag{9.11}$$

Neist esimene järeldub võrduste reast

$$D(L(E(b))) = (E(b))^{-1}D(E(b)) = (E(b))^{-1}D(b)E(b) = D(b).$$

Teise põhjendamiseks tähistame $c = E(L(a))$. Siis esimese implikatsiooni kohaselt $L(c) = L(E(L(a))) = L(a)$, millest

$$\mathbf{0} = L(c) - L(a) = L(c) + L(a^{-1}) = L(ca^{-1}),$$

mis (9.7) tõttu tähendab, et $ca^{-1} = \mathbf{1}$ ehk $c = a$.

Tõestatud seosed võimaldavad teha kaks olulist järeldust.

Esimese järeldusena selgub, et suvaliste ridade $b, c \in \mathcal{R}_1^{\#}$ korral jääb kehtima tavalise eksponentfunktsiooni tuntud omaduse analoog

$$E(b+c) = E(b)E(c), \tag{9.12}$$

mille saab põhjendada eksponendi leidmise teel võrduse

$$L(E(b)E(c)) = L(E(b)) + L(E(c)) = b + c$$

mõlemast poolest (arvestades, et $E(b), E(c) \in \mathcal{R}^{\#}(1)$):

$$E(b+c) = E(L(E(b)E(c))) = E(b)E(c).$$

Teise järeldusena näitame, et suvaliste $r \in \mathbb{Q}$ ja $a \in \mathcal{R}^{\#}(1)$ korral kehtib valem

$$a^r = E(rL(a)). \tag{9.13}$$

Põhjendamiseks esitame arvu r kujul $r = m/n$ (kus $m \in \mathbb{N}$, $n \in \mathbb{Z}$) ja kirjutame (9.12) ning (9.11) põhjal võrdused

$$E(mL(a)) = E(\underbrace{L(a) + L(a) + \cdots + L(a)}_{m}) = (E(L(a)))^m = a^m.$$

Valemi (9.13) saamiseks tuleb saadud võrduses $a^m = E(mL(a))$ nüüd ainult a asemele kirjutada $a^{\frac{1}{n}}$, mis annab:

$$a^r = \left(a^{\frac{1}{n}}\right)^m = E\left(mL\left(a^{\frac{1}{n}}\right)\right) = E\left(\frac{m}{n}L(a)\right).$$

29

Võttes eeskujuks astmeridade teooriast tuntud valemid võib kergesti defineerida ka trigonomeetriliste funktsioonide formaalsed analoogid. Nii näiteks suvalise rea $b \in \mathcal{R}_1^{\#}$ korral defineeritakse tema *formaalne siinus* kui rida

$$\sin b = \sum_{n \geqslant 0} (-1)^n \frac{b^{2n+1}}{(2n+1)!}.$$

Analoogiliselt saab defineerida ka *formaalse koosinuse*

$$\cos b = \sum_{n \geqslant 0} (-1)^n \frac{b^{2n}}{(2n)!}$$

ning ülejäänud formaalsed trigonomeetrilised (ja ka paljud muud traditsiooniliselt astmeridadega seotud) funktsioonid. Edasi võime aga äsjavaadeldud viisil juba üsna lihtsalt tõestada mitmesuguste tuntud seoste (näiteks trigonomeetria põhivalemite) formaalsed analoogid.

Definitsioonide ja põhivalemite niisuguse ülekandmise peamiseks eesmärgiks on näidata, et kombinatoorikas võime formaalsete ridadega (ehk *harilikkude genereerivate funktsioonidega*) opereerimisel kasutada praktiliselt muutusteta peaaegu kõiki astmeridade teooriast tuntud võtteid ilma näiteks vastavate ridade koonduvuse küsimusi tõstatamata. Formaalsete ridade algebraline teooria annab sellisele kasutamisviisile täiesti rahuldava aluse, kuigi suhteliselt levinud arvamuse kohaselt saavat astmeridadega opereerida üksnes nendel juhtudel, mil tegemist on Taylori ridade kaudu määratud analüütiliste funktsioonidega.

Loomulikult ei tohi aga kalduda ka teise äärmusse, jättes ridade koondumise mõiste diskreetses matemaatikas üldse kõrvale: mitmetes diskreetse iseloomuga ülesannetes võib vajalikkude genereerivate funktsioonide tõlgendamine analüütiliste funktsioonidena osutuda väga efektiivseks. Eriti sageli on niisugust lähenemisviisi siiani kasutatud just diskreetse matemaatika ühes kõige vanemas valdkonnas – arvuteoorias (aga ka näiteks tõenäosusteoorias).

Suhteliselt väikeste muutustega saab esitatud mõttekäigud kohaldada ka eksponentsiaalsete genereerivate funktsioonidega opereerimise traditsiooniliste eeskirjade põhjendamiseks. Tarvitseb vaid jada $a \equiv (a_0, a_1, a_2, \dots)$ *eksponentsiaalseks genereerivaks funktsiooniks* lugeda jadale

$$\left(\frac{a_0}{0!}, \frac{a_1}{1!}, \frac{a_2}{2!}, \dots\right)$$

vastavat formaalset rida, mida (4.9) eeskujul tähistame siin kujul e^{ax} või siis kujul $\exp(ax)$, s. t.

$$\exp(ax) \equiv e^{ax} \equiv \sum_{n\geqslant 0} a_n \frac{x^n}{n!}.$$

Vaadeldud skeemi mahuvad aga muide ka arvuteoorias laialdaselt rakendamist leidvad Dirichlet' read. Arvjada $a \equiv (a_1, a_2, a_3, \dots)$ *Dirichlet' reaks* nimetatakse nimelt "baasil" $g_k(x) \equiv k^x$ moodustatud genereerivat funktsiooni

$$a(x) = \sum_{n\geqslant 1} \frac{a_n}{n^x} = \frac{a_1}{1^x} + \frac{a_2}{2^x} + \frac{a_3}{3^x} + \cdots.$$

Siit saadavate Dirichlet' formaalsete ridade hulga võib muuta algebraks üldiselt tavalisel viisil, ainult ridade korrutamine (mida nimetatakse ka Dirichlet' konvolutsiooniks) tuleb nüüd defineerida eeskirjaga: võrdus $c(x) = a(x) \cdot b(x)$ tähendab, et vastavates jadades peab iga n korral olema

$$c_n = \sum_{i\,|\,n} a_i b_{n/i},$$

kus summa võetakse üle arvu n kõikide jagajate i.

10. Elimineerimismeetod

Kombinatoorika probleemid on tihti seotud mingil kaudsel teel defineeritavate alamhulkade elementide loendamisega kas ühtekokku või siis teatavate etteantud liikide järgi. Niisuguste loendamisülesannete lahendamisel osutub üsna otstarbekohaseks kasutada abivahendina hulga loendi mõistet.

Olgu põhihulga $\mathcal{R}$ elementidele omistatud kaalud, kui teatava fikseeritud integriteetkonna (või vähemalt kommutatiivse ringi) $\mathcal{W}$ elemendid. See tähendab, et on defineeritud funktsioon $w: \mathcal{R} \to \mathcal{W}$ ehk iga $r \in \mathcal{R}$ korral on ühesel viisil määratud tema *kaal* $w(r) \in \mathcal{W}$. Kaalude konkreetne valik sõltub muidugi lahendatavast ülesandest, kuid enamasti valitakse nad nii, et samasse liiki loendatavate elementide kaalud oleks ühesugused. Näiteks kui tarvis on leida alamhulkade elementide koguarvusid, siis sobivad *triviaalsed kaalud*: iga $r \in \mathcal{R}$ korral $w(r) = 1$.

Kaaludega varustatud hulga kõigi elementide kaalude summat nimetatakse selle hulga *loendiks* ning tähistatakse tähega ℓ, millele tarbe korral lisatakse hulga tähis (sulgudes). Näiteks kogu põhihulga $\mathcal{R}$ loend $\ell \equiv \ell(\mathcal{R})$ avaldub seega kujul

$$\ell = \sum_{r \in \mathcal{R}} w(r).$$

Paneme tähele, et triviaalsete kaalude $w(r) = 1$ kasutamise korral annab hulga loend lihtsalt selle hulga võimsuse ehk elementide arvu: $\ell = |\mathcal{R}|$.

Vaatleme suhteliselt üldist juhtu, mil põhihulga $\mathcal{R}$ alamhulgad defineeritakse mingite *binaarsete omaduste* abil (binaarsus tähendab, et iga elemendi korral saab tegemist olla ühega kahest alternatiivsest võimalusest: kas elemendil on vaadeldav omadus või tal pole seda). Kui a on üks hulgal $\mathcal{R}$ defineeritud binaarne omadus, siis sümbol $\bar{a}$ tähendagu omadust, mille sisuks on omaduse a puudumine. Kirjutis $\ell(a)$ (vastavalt $\ell(\bar{a})$) tähendagu kõikidest niisugustest elementidest moodustatud alamhulga loendit, millel on omadus a (vastavalt $\bar{a}$).

Nimetatud loendeid seob ilmne võrdus

$$\ell(\bar{a}) = \ell - \ell(a), \tag{10.1}$$

mida sageli nimetatakse *elimineerimisreegliks*: vajalik loend saadakse kogu vaadeldava põhihulga loendist selle osa elimineerimise teel, mis meid antud juhul ei huvita. Sellele triviaalsele võrdusele tuginebki üldine nn. *elimineerimismeetod* – meetod binaarsete omaduste abil defineeritud hulkade loendite leidmiseks teatavate hulkade loendite vahelduva lisamise ja eemaldamise teel.

Kui vaatlusel on kaks erinevat omadust a ja b, siis üsna lihtne kontroll näitab, et kõigi ilma mõlema nende omaduseta elementide hulga loend $\ell(\overline{a}\overline{b})$ avaldub kujul

$$\ell(\overline{a}\overline{b}) = \ell - \ell(a) - \ell(b) + \ell(ab), \tag{10.2}$$

kus $\ell(ab)$ tähendab kõikide niisuguste elementide hulga loendit, millel on nii omadus a kui ka omadus b.

Vaatleme nüüd üldjuhtu, eeldades, et põhihulgal $\mathcal{R}$ on defineeritud n omadust $a_1, a_2, \ldots, a_n$. Siis valemite (10.1) ja (10.2) üldistus kõikidele nendele omadustele peaks tulema nähtavasti kujul

$$\ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_n}) = \ell - \sum_{i=1}^{n} \ell(a_i) + \sum_{i<j} \ell(a_i a_j) - \cdots$$
$$\cdots + (-1)^n \ell(a_1 a_2 \ldots a_n). \tag{10.3}$$

Selle valemi põhjendamisel arvestame, et võrdus (10.1) on õige iga omaduse ja iga põhihulga korral. Kui omaduseks võtta a_n ja põhihulgaks nende elementide hulk, millel pole omadusi $a_1, a_2, \ldots, a_{n-1}$, siis võrdus (10.1) on kirjutatav kujul

$$\ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_{n-1}}\,\overline{a_n}) = \ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_{n-1}}) - \ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_{n-1}}a_n). \tag{10.4}$$

Valemi (10.3) tõestamiseks induktsioonimeetodil oletame nüüd tema kehtivust mistahes $n-1$ omaduse, sealhulgas näiteks esimese $n-1$ omaduse korral:

$$\ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_{n-1}}) = \ell - \sum_{i=1}^{n-1} \ell(a_i) + \cdots + (-1)^{n-1}\ell(a_1 a_2 \ldots a_{n-1}). \tag{10.5}$$

Kui põhihulgaks võtta siin $\mathcal{R}$ asemel omadusega a_n elementide hulk, siis võime valemi (10.5) kirjutada kujul

$$\ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_{n-1}}a_n) = \ell(a_n) - \sum_{i=1}^{n-1} \ell(a_i a_n) + \cdots + (-1)^{n-1}\ell(a_1 a_2 \ldots a_n).$$

Seose (10.4) tõttu annab viimase tulemuse lahutamine võrdusest (10.5) soovitud valemi (10.3).

Valemi (10.3) üsna kohmakat ja halvasti meeles peetavat kuju saab mõnevõrra lihtsustada, kui võtta kasutusele spetsiaalsed tähised temas esinevate liikmete tarvis. Tähistame nimelt iga $k = 1, 2, \ldots, n$ korral

$$L_k = \sum_{c(k)} \ell(a_{i_1} a_{i_2} \ldots a_{i_k}), \tag{10.6}$$

kus summa võetakse üle vaadeldavate omaduste $a_1, a_2, \ldots, a_n$ kõikide k-kombinatsioonide $c(k) = \{i_1, i_2, \ldots, i_k\}$ (tähe ℓ asemel kasutatakse selles sümbolis tähte L

rõhutamaks, et kuigi L_k on integriteetkonna $\mathcal{W}$ element, pole ta üldiselt ühegi hulga loend). Kui defineerida veel $L_0 = \ell$, siis võib valemi (10.3) esitada kujul

$$\ell(\overline{a_1}\,\overline{a_2}\ldots\overline{a_n}) = L_0 - L_1 + L_2 - \cdots + (-1)^n L_n.$$

Selle valemi vasak pool tähendab kõikide nende elementide hulga loendit, millel ei ole mitte ühtegi vaadeldavatest omadustest (ehk millel on vaadeldavast n omadusest null omadust). Tähistame seda loendit edaspidi veidi lühema sümboliga $D(n,0)$, mis annab viimasele valemile kuju

$$D(n,0) = \sum_{k=0}^{n} (-1)^k L_k. \qquad (10.7)$$

Loomulik on nüüd sümboliga $D(n,m)$ tähistada kõikide niisuguste elementide hulga loendit, millel vaadeldavast n omadusest on olemas täpselt m omadust. Osutub, et see loend avaldub nn. *Ryseri valemina*

$$D(n,m) = \sum_{k=m}^{n} (-1)^{k-m} \binom{k}{m} L_k. \qquad (10.8)$$

Valemi (10.8) põhjendamiseks fikseerime suvalise elemendi $r \in \mathcal{R}$, millel olgu täpselt p omadust. Kui $p < m$, siis ei sisaldu valemi (10.8) parema poole üheski liikmes definitsiooni (10.6) kohaselt liidetavat $w(r)$. Kui $p = m$, siis $w(r)$ esineb vaid liikmes L_m ning sealgi ühekordselt, sest leidub ainult üks omaduste m-kombinatsioon, mille korral r kuulub definitsiooni (10.6) paremas pooles vaadeldud hulkadesse. Kui aga $p > m$, siis $w(r)$ esineb valemi (10.8) paremas pooles vaid liikmete $L_m, L_{m+1}, \ldots, L_p$ koosseisus. Sealjuures liikmes L_k esineb ta liidetavana $\binom{p}{k}$ korda, sest nii mitmel viisil saab fikseeritud p omaduse hulgast välja valida k omadust. Järelikult valemi (10.8) paremas pooles tuleb $w(r)$ kordajaks valemi (7.1) kohaselt null:

$$\sum_{k=m}^{p} (-1)^{k-m} \binom{k}{m} \binom{p}{k} = \binom{p}{m} \sum_{k=0}^{p-m} (-1)^k \binom{p-m}{k} = 0.$$

Kokkuvõttes näeme, et valemi (10.8) paremas pooles säilib nende elementide kaalude summa, millel on täpselt m omadust.

Kui iga $k > n$ korral lugeda $L_k = 0$ (see on kaalude hulga $\mathcal{W}$ nullelement!), siis võime valemi (10.7) esitada kujul

$$D(n,0) = \sum_{k=0}^{\infty} (-1)^k L_k = (1+L)^{-1}, \qquad (10.9)$$

kus loeme, et iga k korral $L^k \equiv L_k$. Sama tähistusviisi kasutades on aga valem (10.8) kirjutatav kujul

$$D(n,m) = \sum_{k=m}^{\infty} (-1)^{k-m} \binom{k}{m} L_k = L^m (1+L)^{-m-1}, \qquad (10.10)$$

mis juhul $m = 0$ annab muidugi valemi (10.9).

Mõnedes rakendustes võivad veel vajalikuks osutuda jadade $\{D(n,m)\}_m$ ja $\{L_k\}$ polünomiaalsed genereerivad funktsioonid $D_n(x)$ ja $L_n(x)$ (x on muutuja, mille väärtused kuuluvad kaalude hulka $\mathcal{W}$):

$$D_n(x) = \sum_{m=0}^{\infty} D(n,m)x^m = \sum_{m=0}^{\infty} L^m(1+L)^{-m-1}x^m = (1+L-Lx)^{-1},$$

$$L_n(x) = \sum_{k=0}^{\infty} L_k x^k = (1-Lx)^{-1} = D_n(1+x).$$

Elimineerimismeetodi rohkete rakendusvaldkondade ühe näitena võib nimetada arvuteooriat, kus põhihulk on positiivsete täisarvude hulk $\mathcal{R} = \overline{1,n} = \{1,2,\ldots,n\}$ mingi kindla n korral, varustatult triviaalsete kaaludega $w(r) = 1$.

Vaatleme näiteks järgmist ülesannet. Olgu fikseeritud m paarikaupa ühisteguri-ta naturaalarvu $k_1, k_2, \ldots, k_m \in \mathcal{R}$. Vaja on selgitada, kui palju leidub hulgas $\mathcal{R}$ elemente, mis ei jagu ühegagi nendest arvudest k_i.

Ütleme, et naturaalarvul on omadus a_i siis, kui ta jagub arvuga k_i. Ilmselt $\ell(a_i) = [n/k_i]$ (kus nurksulgudega [ ] tähistatakse täisosa), sest nii palju leidub ju hulgas $\mathcal{R}$ arvusid, mis jaguvad arvuga k_i. Analoogiliselt $\ell(a_i a_j) = [n/k_i k_j]$ jne. Et meie eesmärgiks on leida niisuguste elementide arv, millel ei ole ühtegi omadust a_i, siis valemitest (10.6) ja (10.7) saame

$$D(m,0) = n - \sum_i \left[\frac{n}{k_i}\right] + \sum_{i<j}\left[\frac{n}{k_i k_j}\right] - \cdots + (-1)^m \left[\frac{n}{k_1 k_2 \ldots k_m}\right].$$

Näiteks juhul $n = 106$, $m = 3$, $k_1 = 3$, $k_2 = 5$, $k_3 = 7$ leiame:

$$D(3,0) = 106 - \left(\left[\frac{106}{3}\right] + \left[\frac{106}{5}\right] + \left[\frac{106}{7}\right]\right) +$$
$$+ \left(\left[\frac{106}{3\cdot 5}\right] + \left[\frac{106}{3\cdot 7}\right] + \left[\frac{106}{5\cdot 7}\right]\right) - \left[\frac{106}{3\cdot 5\cdot 7}\right] = 49.$$

Positiivsete naturaalarvude vallas $\{1,2,\ldots\}$ määratud *Euleri funktsiooni* $\varphi(n)$ väärtuseks on arvust n mitte suuremate ja temaga ühistegurita naturaalarvude arv. Näiteks $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$ jne. Selle funktsiooni väärtuste leidmine vahetult definitsioonist on üpris tülikas, kuid vastava analüütilise avaldise saame eelmisest tulemusest, valides arvudeks k_i argumendi n algtegurid $p_1, p_2, \ldots, p_m$. Seega kui argumendi lahutus algteguriteks on

$$n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m},$$

siis

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i<j}\frac{n}{p_i p_j} - \cdots + (-1)^m \frac{n}{p_1 p_2 \ldots p_m} = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right).$$

Teise illustreeriva näitena vaatleme elimineerimismeetodi kasutamist veel maatriksite permanentide arvutamisel. Olgu $A = (a_{ij})$ mingist kommutatiivsest ringist pärinevate elementidega $(m \times n)$-maatriks, kusjuures tavaliselt eeldatakse, et $m \leqslant n$. Selle maatriksi *permanent* defineeritakse teatavasti kui summa

$$\operatorname{per} A = \sum_{(j_1,\ldots,j_m)} a_{1j_1} a_{2j_2} \ldots a_{mj_m}, \tag{10.11}$$

kus summeerimine toimub üle kõigi kordumisteta m-permutatsioonide $(j_1, j_2, \ldots, j_m)$ indeksitest $1, 2, \ldots, n$. Näiteks

$$\operatorname{per} \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix} = 0 \cdot 4 + 0 \cdot 5 + 1 \cdot 3 + 1 \cdot 5 + 2 \cdot 3 + 2 \cdot 4 = 22.$$

Permanentidega tuleb tegemist näiteks järgmises kombinatoorset tüüpi ülesandes. Olgu $\mathcal{X}$ lõplik hulk ja $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_m$ tema alamhulgad. Nende alamhulkade süsteemi esindajatekoguks ehk *transversaaliks* nimetatakse m erinevast elemendist koosnevat lineaarselt järjestatud hulka $(x_1, x_2, \ldots, x_m)$, kus iga $i = 1, 2, \ldots, m$ korral $x_i \in \mathcal{X}_i$ (eeldatakse, et $|\mathcal{X}| = n \geqslant m$).

Kui moodustada kõikide vaadeldavate alamhulkade $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_m$ ning põhihulga $\mathcal{X} = \{y_1, y_2, \ldots, y_n\}$ *intsidentsusmaatriks* $A = (a_{ij})$, kus

$$a_{ij} = \begin{cases} 1, & \text{kui } y_j \in \mathcal{X}_i, \\ 0, & \text{kui } y_j \notin \mathcal{X}_i, \end{cases}$$

siis võib kohe veenduda, et vaadeldava süsteemi erinevate transversaalide arv on per A. Tõepoolest, erinevatest elementidest koosnev järjestatud hulk $(y_{j_1}, y_{j_2}, \ldots, y_{j_m})$ osutub transversaaliks parajasti siis, kui $a_{1j_1} a_{2j_2} \ldots a_{mj_m} = 1$. Seega summa (10.11) annabki erinevate transversaalide arvu.

Permanendi arvutamine definitsioonist (10.11) osutub suuremate maatriksite korral ebamugavaks. Veidi parema arvutuseeskirja saab anda elimineerimismeetodi põhivalemite kaudu, kui valida põhihulgaks $\mathcal{R}$ kõikide funktsioonide hulk hulgast $\overline{1,m} = \{1, 2, \ldots, m\}$ hulka $\overline{1,n} = \{1, 2, \ldots, n\}$. Elementi $r \in \mathcal{R}$ võib teatavasti tõlgendada kordumistega m-permutatsioonina

$$r = (j_1, j_2, \ldots, j_m) \tag{10.12}$$

n erinevast elemendist, millest igaüht on põhihulgas olemas suvaline arv eksemplare. Varustame veel hulga $\mathcal{R}$ elemendid maatriksi A abil kaaludega järgmiselt: kui r on m-permutatsioon (10.12), siis

$$w(r) = a_{1j_1} a_{2j_2} \ldots a_{mj_m}.$$

Täiesti vahetult võib nüüd veenduda, et selliste kaalude korral osutub hulga $\mathcal{R}$ loendiks maatriksi A reasummade korrutis (tähistame niisugust korrutist järgnevas sümboli $\sqcap$ abil):

$$\ell(\mathcal{R}) = \sum_{r \in \mathcal{R}} a_{1j_1} a_{2j_2} \ldots a_{mj_m} = \prod_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sqcap(A).$$

Elemendil $r \in \mathcal{R}$ olgu omadus a_j (kus $j = 1, 2, \ldots, n$) sel ja ainult sel juhul, kui vastavas permutatsioonis (10.12) arv j kordagi ei esine. Definitsiooni (10.11) arvestades on $\operatorname{per} A$ nüüd võrdne sellise alamhulga loendiga, mille elementidel on täpselt $n - m$ nendest omadustest: iga element r selles alamhulgas sisaldab täpselt m erinevat arvu ja osutub järelikult kordumisteta m-permutatsiooniks. Seega oleme tõestanud, et $\operatorname{per} A = D(n, n - m)$.

Valemi (10.8) rakendamiseks tuleb meil veel anda suuruste L_k leidmise eeskiri maatriksi A kaudu. Paneme nimelt tähele, et kui fikseerida mingid k omadust $a_{j_1}, a_{j_2}, \ldots, a_{j_k}$ (ehk indeksite k-kombinatsioon $c(k) = \{j_1, j_2, \ldots, j_k\}$), siis loend $\ell(a_{j_1} a_{j_2} \ldots a_{j_k})$ osutub võrdseks niisuguse maatriksi $A_{c(k)}$ reasummade korrutisega, mis on saadud maatriksist A veergude $j_1, j_2, \ldots, j_k$ kõrvaldamisel ehk asendamisel nullveergudega:

$$\ell(a_{j_1} a_{j_2} \ldots a_{j_k}) = \sqcap(A_{c(k)}).$$

Järelikult definitsiooni (10.6) kohaselt

$$L_k = \sum_{c(k)} \sqcap(A_{c(k)}),$$

kus summa võetakse üle kõikide k-kombinatsioonide $c(k)$ indeksitest $1, 2, \ldots, n$. Kui nüüd veel valemis (10.8) kirjutada m asemele $n - m$, siis saame permanendi arvutamiseks valemi

$$\operatorname{per} A = \sum_{k=n-m}^{n-1} (-1)^{k-n+m} \binom{k}{n-m} \sum_{c(k)} \sqcap(A_{c(k)}), \tag{10.13}$$

kus täiendava lihtsustusena on viimane liidetav ($k = n$) ära jäetud, sest $A_{c(n)}$ osutub ju nullmaatriksiks ja $\sqcap(A_{c(n)}) = 0$.

Vaatamata näiliselt keerulisemale kujule osutub valem (10.13) definitsioonist (10.11) arvutuslikult märksa lihtsamaks sellepärast, et summeerimine toimub siin üle kõikide kombinatsioonide, aga mitte üle kõikide permutatsioonide (arvutuste lihtsustumine avaldub muidugi seda enam, mida suuremateks osutuvad maatriksi mõõtmed m ja n). Valemi (10.13) kasutamise illustreerimiseks arvutame siinkohal veel kord varem juba näitena leitud permanendi:

$$\operatorname{per} \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix} = \sum_{k=1}^{2} (-1)^{k-1} \binom{k}{1} \sum_{c(k)} \sqcap(A_{c(k)}) =$$

$$= \left(\sqcap \begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix} + \sqcap \begin{pmatrix} 0 & 2 \\ 3 & 5 \end{pmatrix} + \sqcap \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \right) - 2 \cdot \left(\sqcap \begin{pmatrix} 0 \\ 3 \end{pmatrix} + \sqcap \begin{pmatrix} 1 \\ 4 \end{pmatrix} + \sqcap \begin{pmatrix} 2 \\ 5 \end{pmatrix} \right) =$$

$$= (1 \cdot 7 + 2 \cdot 8 + 3 \cdot 9) - 2 \cdot (0 \cdot 3 + 1 \cdot 4 + 2 \cdot 5) = 50 - 2 \cdot 14 = 22.$$

11. Substitutsioonitsüklid

Olgu S teatav fikseeritud n-elemendiline põhihulk, mille elemente mingis "loomulikus" järjekorras tähistame naturaalarvudega $1, 2, \ldots, n$. Selle hulga suvalist n-permutatsiooni võib tõlgendada kui loomulikus järjestuses teostatud muutuse ehk hulga S teisenduse tulemust. Et lõpliku hulga teisendust (s. t. üksühest kujutust iseendale) nimetatakse *substitutsiooniks*, siis võib n-permutatsiooni vajaduse korral lugeda n-elemendilise hulga substitutsiooni rakendamise tulemuseks.

Konkreetne substitutsioon g esitatakse $(2 \times n)$-maatriksina

$$g \equiv \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix},$$

mis tähendab, et $g(1) = j_1$, $g(2) = j_2$ jne. Kirjutiste lühendamiseks võib aga piirduda ka ainult selle maatriksi teise reaga:

$$g \equiv (j_1 \; j_2 \; \ldots \; j_n)$$

(komade ärajätmisega rõhutame, et tegemist on substitutsiooniga, mitte permutatsiooniga). Nii näiteks substitutsioonid

$$g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 7 & 8 & 9 & 2 & 5 & 4 & 1 \end{pmatrix} \quad \text{ja} \quad g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 3 & 7 & 2 & 5 & 9 & 8 & 4 \end{pmatrix}$$

võib lühemalt esitada kujul

$$g_1 = (3\;6\;7\;8\;9\;2\;5\;4\;1) \quad \text{ja} \quad g_2 = (6\;1\;3\;7\;2\;5\;9\;8\;4).$$

Substitutsioonide järjestrakendamist nimetatakse ka nende *korrutamiseks*. Näiteks vaadeldud substitutsioonide korral $g_1g_2(1) = g_1(g_2(1)) = g_1(6) = 2$. Niiviisi põhihulga kõiki elemente läbi vaadates leiame, et

$$g_1g_2 = (2\;3\;7\;5\;6\;9\;1\;4\;8),$$

seevastu aga

$$g_2g_1 = (3\;5\;9\;8\;4\;1\;2\;7\;6).$$

Juba sellestki ühestainsast näitest järeldub, et substitutsioonide korrutamine ei ole kommutatiivne.

Antud hulga S kõigi substitutsioonide seas leidub muidugi *ühiksubstitutsioon* $g_0 = (1\ 2\ \ldots\ n)$ ja samuti iga substitutsiooni g *pöördsubstitutsioon* g^{-1}, mis rahuldab tingimusi $gg^{-1} = g^{-1}g = g_0$. Näiteks ülalvaadeldud g_1 korral saame

$$g_1^{-1} = (9\ 6\ 1\ 8\ 7\ 2\ 3\ 4\ 5).$$

Et lihtne on veel veenduda vaadeldava korrutamise assotsiatiivsuses, siis moodustavad hulga S kõik $n!$ substitutsiooni rühma. Seda ($n > 2$ korral mittekommutatiivset) rühma nimetatakse hulga S *sümmeetriliseks rühmaks*.

Substitutsioonide mitmesugustes rakendustes osutub sageli oluliseks tunda nende n.-ö. tsüklilisuse omadusi. Substitutsiooni g *tsükliks* nimetatakse hulga S iga niisugust minimaalset alamhulka, mis on g suhtes kinnine (s. t. $T \subseteq S$ on g tsükkel parajasti siis, kui iga $s \in T$ korral ka $g(s) \in T$ ning ei leidu samasuguse omadusega pärisalamhulka $T' \subset T$). *Tsükli pikkuseks* nimetatakse elementide arvu temas. Tsüklit, mille pikkus on k, nimetatakse lühidalt *k-tsükliks*. Ilmselt leidub igal substitutsioonil vähemalt üks tsükkel: kui tsüklite arv võrdubki ühega, siis selleks ainsaks tsükliks on S ise.

Tsükli pikkusega üks (s. t. 1-tsükli) moodustab põhihulga iga niisugune element s, mis on vaadeldava substitutsiooni g suhtes *invariantne*, s. t. $g(s) = s$.

Kui substitutsiooni g vaadeldava tsükli T pikkus on k ja $s \in T$, siis see tsükkel koosneb elementidest

$$T = \{s, g(s), g^2(s), \ldots, g^{k-1}(s)\}, \tag{11.1}$$

kus substitutsiooni astendamine on ikka defineeritud tavalisel viisil: $g^1 = g$, $g^2 = gg$ ja üldiselt $g^i = g^{i-1}g$.

Iga fikseeritud substitutsioon g jaotab hulga S tsüklite kui ühisosata alamhulkade summaks (ühendiks), kusjuures liidetavate komplekt on üheselt määratud. Kui veel igas tsüklis järjestada elemendid eeskirja (11.1) kohaselt, siis on substitutsioon täielikult kirjeldatav oma tsüklite kaudu. Esituse ühesuse saavutamiseks lepitakse tavaliselt kokku alustada iga tsükli kirjutamist tema vähima elemendiga (hulgas S määratud "loomuliku" järjestuse mõttes), esitada tsüklid nende pikkuste mittekahanevas järjekorras ning ühepikkused tsüklid näiteks nende esimeste elementide kasvavas järjekorras. Nii võime ülalvaadeldud substitutsioone g_1 ja g_2 kirjeldada vastavalt tsüklite järjenditega $\{2,6\}, \{4,8\}, \{1,3,7,5,9\}$ ja $\{3\}, \{8\}, \{4,7,9\}, \{1,6,5,2\}$. Enamasti on aga niisuguse kohmaka kirjeldamisviisi asemel kombeks esitada substitutsioonid mitte tükeldustena vaid n.-ö. tsüklite korrutistena kujul

$$g_1 = (2\ 6)(4\ 8)(1\ 3\ 7\ 5\ 9), \quad g_2 = (3)(8)(4\ 7\ 9)(1\ 6\ 5\ 2).$$

Nende korrutiste tegureid võib tõlgendada ühetsükliliste substitutsioonidena, mis tsükliliselt muudavad näidatud elemente ja jätavad ülejäänud invariantseteks. Kokkuleppeliselt jäetakse siin pealegi 1-tsüklid enamasti hoopis kirjutamata, lisades need vaid siis, kui on tarvis põhihulga kõik elemendid otseselt ära näidata.

Diskreetses matemaatikas osutub sageli vajalikuks eristada substitutsioone just nende tsüklistruktuuri järgi. Öeldakse, et substitutsioon on (ehk kuulub) *tsüklitüüpi* $(k_1, k_2, k_3, \ldots, k_n)$, kui ta jaotab põhihulga k_1 1-tsükliks, k_2 2-tsükliks, k_3 3-tsükliks jne. Tsüklite mittelõikumise tõttu siinjuures muidugi

$$\sum_{i=1}^{n} i\, k_i = k_1 + 2\, k_2 + 3\, k_3 + \cdots + n\, k_n = n. \tag{11.2}$$

Konkreetsete substitutsioonide korral on tsüklitüüpi tavaliselt mugavam tähistada sümboliga

$$(1^{k_1} 2^{k_2} 3^{k_3} \ldots n^{k_n}),$$

kusjuures juhtudele $k_i = 0$ vastavad tegurid i^{k_i} jäetakse üldse kirjutamata. Nii näiteks ülalvaadeldud substitutsioonide g_1 ja g_2 tüüpe tähistame kujul $(2^2 5^1)$ ja $(1^2 3^1 4^1)$, mitte aga $(0, 2, 0, 0, 1, 0, 0, 0, 0)$ ja $(2, 0, 1, 1, 0, 0, 0, 0, 0)$.

Lihtsaimaks tsüklitüübiks on (1^n) ja selle tüübi ainsaks esindajaks ühiksubstitutsioon g_0. Lihtsuselt järgmiseks võib lugeda tüüpi $(1^{n-2} 2^1)$, millesse kuuluvaid substitutsioone nimetatakse *transpositsioonideks*. Kompaktsuse huvides kirjutatakse transpositsioon

$$(i_1)(i_2) \ldots (i_{n-2})(j_1\, j_2)$$

ülalnimetatud kokkuleppe kohaselt muidugi lihtsalt paarina $(j_1\, j_2)$.

Nagu algebrast teada, saab suvalise substitutsiooni esitada transpositsioonide korrutisena. Niisuguses esituses pole küll üheselt määratud ei tegurid ise ega nende täpne järjekord, kuid üheselt määratuks osutub tegurite arvu paarsus. Paarisarvu transpositsioonide korrutisena avalduvaid substitutsioone nimetatakse *paarissubstitutsioonideks*, ülejäänuid aga paarituteks. Ilmselt on nii paarissubstitutsioonide korrutis kui ka samuti ühiksubstitutsioon paaris. Seega kõikide paarissubstitutsioonide hulk moodustab sümmeetrilises rühmas alamrühma (mida algebras nimetatakse enamasti *märgivahetusrühmaks*).

Substitutsioonide liigitamisel on üheks eesmärgiks tavaliselt kas antud tüüpi või siis tüüpide teatud klassi kuuluvate substitutsioonide arvu määramine. Reeglina ei ole sealjuures aga vaatlusel mitte kogu sümmeetriline rühm, vaid ainult selle mingi alamrühm $\mathcal{G}$, s. t. vaadeldakse üksnes selliseid substitutsioone, mis peavad rahuldama veel mingeid lisatingimusi.

Olgu $\mathcal{G}$ hulga $\mathcal{S}$ sümmeetrilise rühma alamrühm. Alamrühma $\mathcal{G}$ *tsüklilisuse indikaatoriks* nimetatakse n muutuja (nn. isobaarset) polünoomi

$$P_{\mathcal{G}}(x_1, x_2, \ldots, x_n) = \sum_{g \in \mathcal{G}} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}, \tag{11.3}$$

kus iga substitutsiooni $g \in \mathcal{G}$ korral on astendajateks $k_1, k_2, \ldots, k_n \in \mathbb{N}$ valitud selle substitutsiooni tsüklitüübi komponendid.

Tsüklilisuse indikaatorit võib soovi korral tõlgendada ka kui tsüklitüüpidesse kuuluvate substitutsioonide arvude jada genereerivat funktsiooni. Tõepoolest, sarnaste liikmete koondamine summas (11.3) annab liikme $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ kordajaks tsüklitüüpi $(k_1, k_2, \dots, k_n)$ kuuluvate substitutsioonide arvu.

Demonstreerime tsüklilisuse indikaatori moodustamist kõigepealt ühe praktikas olulise alamrühma korral. Olgu nimelt g nn. *nihkesubstitutsioon*, mis sooritab põhihulga tsüklilise nihke: iga $s = 1, \dots, n-1$ korral $g(s) = s+1$ ja $g(n) = 1$. Siis moodustab substitutsioonide hulk $\mathcal{G} = \{g, g^2, g^3, \dots, g^n\}$ rühma (ilmselt $g^n = g_0$), mida nimetatakse *nihkerühmaks* või ka n-järku tsükliliseks rühmaks.

Nihkerühma tsüklilisuse indikaatori leidmisel on oluline tähele panna, et mistahes $m = 1, 2, \dots, n$ korral kuulub g^m tüüpi (i^d), kus d on m ja n suurim ühistegur ning $i = n/d$ (selles veendumiseks piisab mõne väiksema n väärtuse vaatlemisest). Seega kui fikseerida arvu n mingi jagaja i, siis kuuluvad tüüpi $(i^{n/i})$ kõik need substitutsioonid g^m, kus n/i on n ja m suurim ühistegur. See aga tähendab, et sobivad parajasti need m väärtused, kus $m = pn/i$, $p \leqslant i$ ning p ja i on ühistegurita. *Euleri funktsiooni* definitsiooni meenutades näeme, et nihkerühma tsüklilisuse indikaator avaldub summana üle arvu n kõikide jagajate i:

$$P_{\mathcal{G}}(x_1, x_2, \dots, x_n) = \sum_{i|n} \varphi(i) x_i^{n/i}. \tag{11.4}$$

Järgmisena vaatleme mõningate mängude uurimisel vajalikuks osutuvat näidet, mil põhihulga S elementideks on 3×3 ruudustiku üheksa lahtrit nummerdatult näiteks kõrvaloleval joonisel kujutatud viisil. Olgugi nüüd alamrühma $\mathcal{G}$ elementideks niisuguse ruudustiku pöördeid ja peegeldusi sooritavad substitutsioonid.

1	2	3
8	9	4
7	6	5

Järgmises tabelis on loetletud selle rühma kõik kaheksa teisendust tõlgendatult substitutsioonidena, kusjuures ühtlasi näidatakse igaühe jaoks neist veel ka tema tsüklitüüp:

	Teisendus	Substitutsioon	Tüüp
g_0	samasusteisendus	(1 2 3 4 5 6 7 8 9)	(1^9)
g_1	pööre 90° võrra	(7 8 1 2 3 4 5 6 9)	$(1^1 4^2)$
g_2	pööre 180° võrra	(5 6 7 8 1 2 3 4 9)	$(1^1 2^4)$
g_3	pööre 270° võrra	(3 4 5 6 7 8 1 2 9)	$(1^1 4^2)$
g_4	peegeldus horisontaaltelje suhtes	(7 6 5 4 3 2 1 8 9)	$(1^3 2^3)$
g_5	peegeldus vertikaaltelje suhtes	(3 2 1 8 7 6 5 4 9)	$(1^3 2^3)$
g_6	peegeldus peadiagonaali suhtes	(1 8 7 6 5 4 3 2 9)	$(1^3 2^3)$
g_7	peegeldus kõrvaldiagonaali suhtes	(5 4 3 2 1 8 7 6 9)	$(1^3 2^3)$

Rühma $\mathcal{G}$ tsüklilisuse indikaatori võib nüüd vahetult üles kirjutada selle tabeli viimase veeru järgi (esitades liikmed leksikograafilises järjestuses):

$$P_{\mathcal{G}}(x_1, x_2, \ldots, x_9) = x_1^9 + 4x_1^3x_2^3 + x_1x_2^4 + 2x_1x_4^2. \tag{11.5}$$

Viimase näitena vaatleme juhtu, mil hulga $\mathcal{S}$ elementideks on kuubi tahud (nende "loomulikku" järjestust pole siin tarvis täpsustada) ning rühmaks $\mathcal{G}$ kuubi pöörete rühm, kusjuures pöördeid tõlgendame kui kuubi tahkude substitutsioone.

Rühma $\mathcal{G}$ (nn. *heksaeedri rühma*) elemendid on nende tähenduse järgi loomulik jaotada järgmisse viide klassi:

1) samasusteisendus;

2) pööre 180° võrra ümber kuubi vastastahkude keskpunkte läbiva telje (selliseid telgi leidub kolm);

3) pööre 90° võrra ümber eelmises klassis nimetatud telje (iga telje korral saab sooritada kaks niisugust pööret);

4) pööre 180° võrra ümber kuubi vastaservade keskpunkte läbiva telje (selliseid telgi leidub kuus);

5) pööre 120° võrra ümber kuubi vastastippe läbiva telje (selliseid telgi leidub neli, iga telje korral saab aga sooritada kaks niisugust pööret).

Kokku sisaldab heksaeedri rühm $\mathcal{G}$ seega 24 substitutsiooni, kusjuures iga klassi korral saab üpris kergesti (näiteks kas vastavalt jooniselt või mudelilt) üle lugeda nende tsüklid. Nimelt kuulub esimese klassi ainus substitutsioon muidugi tüüpi (1^6), teise klassi kõik kolm substitutsiooni aga tüüpi $(1^2 2^2)$, kolmanda klassi kõik kuus substitutsiooni tüüpi $(1^2 4^1)$, neljanda klassi kõik kuus substitutsiooni tüüpi (2^3) ning viienda klassi kõik kaheksa substitutsiooni tüüpi (3^2). Seega vaadeldava rühma tsüklilisuse indikaatori võib esitada kujul

$$P_{\mathcal{G}} = x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2, \tag{11.6}$$

kus indikaatori tähise $P_{\mathcal{G}}$ taga on kirjutiste lihtsustamiseks argumendid $x_1, x_2, \ldots, x_6$ näitamata jäetud (kontrolliks paneme tähele, et polünoomi (11.6) kordajate summa tuleb ikka tõepoolest 24).

Kui sama rühma $\mathcal{G}$ elemente tõlgendada kuubi servade hulga substitutsioonidena (põhihulga $\mathcal{S}$ elementideks kuubi 12 serva) või kuubi tippude hulga substitutsioonidena (põhihulga $\mathcal{S}$ elementideks kuubi 8 tippu), siis vaadeldud klasside tsüklitüübid osutuvad teistsugusteks ja muutuvad ka tsüklilisuse indikaatorid, omandades vastavalt kuju

$$P_{\mathcal{G}} = x_1^{12} + 6x_1^2x_2^5 + 3x_2^6 + 8x_3^4 + 6x_4^3$$

või

$$P_{\mathcal{G}} = x_1^8 + 8x_1^2x_3^2 + 9x_2^4 + 6x_4^2.$$

12. Sümmeetriline rühm

Mitmesuguste praktikas vajalikkude substitutsioonirühmade hulgas on eriline koht sümmeetrilisel rühmal, mis sisaldab kõik $n!$ substitutsiooni. Leiamegi järgnevalt selle rühma tsüklilisuse indikaatori $P_n(x_1, x_2, \ldots, x_n)$ või lühidalt P_n.

Kui tüüpi $(k_1, k_2, \ldots, k_n)$ kuuluvate substitutsioonide koguarv tähistada sümboliga $c(k_1, k_2, \ldots, k_n)$, siis omandab sümmeetrilise rühma tsüklilisuse indikaator sarnaste liikmete koondamise tulemusel kuju

$$P_n \equiv P_n(x_1, x_2, \ldots, x_n) = \sum_{\Sigma i k_i = n} c(k_1, k_2, \ldots, k_n) x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

kus summa tuleb võtta üle kõikvõimalike tsüklitüüpide, ehk seose (11.2) kohaselt üle arvu n kõigi esituste kujul $k_1 + 2k_2 + \cdots + nk_n = n$.

Arvud $c(k_1, k_2, \ldots, k_n)$ saame leida täiesti vahetu arutelu teel. Võtame nimelt mingi vaadeldavasse tüüpi $(k_1, k_2, \ldots, k_n)$ kuuluva substitutsiooni

$$(i_1) \cdots (i_{k_1})(j_1\ j_1') \cdots (j_{k_2}\ j_{k_2}') \cdots$$

ja teostame selles elementidega kõik $n!$ permutatsiooni, jättes sulud sealjuures paigale. Niiviisi saadud $n!$ substitutsiooni on sulgude paigalejäämise tõttu muidugi sedasama tüüpi, kuid nad pole kõik erinevad. Kokkulangemine saab olla tingitud kas sellest, et mingi tsükli sees on elementide järjekord tsükliliselt muutunud, või siis sellest, et sama pikkusega tsüklite järjekord on muutunud.

Paneme tähele, et m-tsükli saab üles kirjutada m ekvivalentsel kujul, sest alustada võib ükskõik millisega sellesse tsüklisse kuuluvast m elemendist. Et m-tsükleid on vaadeldava tüübi korral k_m tükki, siis saame nende jaoks m^{k_m} erinevat kirjutusviisi ja kokku üle kõigi esinevate tsüklite seega $1^{k_1} 2^{k_2} \ldots n^{k_n}$ väliselt erinevat kirjutusviisi.

Vaadeldava tsüklitüübi k_m erinevat m-tsüklit on $k_m!$ viisil järjestatavad. Kokku üle kõigi tsüklipikkuste annab see $k_1!\, k_2! \ldots k_n!$ väliselt erinevat järjestamisviisi.

Sellega aga olemegi kõik kokkulangemised üles lugenud ja vaadeldavat tüüpi erinevate substitutsioonide arvuks osutub

$$c(k_1, k_2, \ldots, k_n) = \frac{n!}{1^{k_1} k_1!\, 2^{k_2} k_2! \ldots n^{k_n} k_n!}.$$

Selle väärtuse asendamisel *sümmeetrilise rühma* tsüklilisuse indikaatori ülaltoodud avaldisse saame

$$P_n = \sum_{\Sigma i k_i = n} \frac{n!}{1^{k_1} k_1!\, 2^{k_2} k_2! \dots n^{k_n} k_n!} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n},$$

ehk pärast sama astendajaga astmete ühendamist

$$P_n = \sum_{\Sigma i k_i = n} \frac{n!}{k_1!\, k_2! \dots k_n!} \left(\frac{x_1}{1}\right)^{k_1} \left(\frac{x_2}{2}\right)^{k_2} \cdots \left(\frac{x_n}{n}\right)^{k_n}. \tag{12.1}$$

Saadud üldvalem on muidugi kasutatav iga põhihulga, s. t. iga $n = 1, 2, \dots$ korral, kuid n väärtuse suurenemisel muutub kõikide võrrandit (11.2) rahuldavate tsüklitüüpide $(k_1, k_2, \dots, k_n)$ vahetu väljakirjutamine kiiresti üha töömahukamaks. Suhteliselt lihtsa vaevaga võib veel näiteks leida

$$\begin{aligned}
&P_1 = x_1, \qquad P_2 = x_1^2 + x_2, \qquad P_3 = x_1^3 + 3x_1x_2 + 2x_3,\\
&P_4 = x_1^4 + 6x_1^2x_2 + 8x_1x_3 + 3x_2^2 + 6x_4,\\
&P_5 = x_1^5 + 10x_1^3x_2 + 20x_1^2x_3 + 15x_1x_2^2 + 30x_1x_4 + 20x_2x_3 + 24x_5,\\
&P_6 = x_1^6 + 15x_1^4x_2 + 40x_1^3x_3 + 45x_1^2x_2^2 + 90x_1^2x_4 + 120x_1x_2x_3 +\\
&\qquad + 144x_1x_5 + 15x_2^3 + 90x_2x_4 + 40x_3^2 + 120x_6.
\end{aligned}$$

Arvutuslike raskuste ületamiseks kasutame standardmetoodikat: täiendame saadud üldvalemit veel loomuliku definitsiooniga $P_0 = 1$ ning leiame kõigi sümmeetriliste rühmade tsüklilisuse indikaatorite niiviisi saadava jada $\{P_n\}$ eksponentsiaalse genereeriva funktsiooni e^{Px}. Selle funktsiooni moodustamisel toetume tähelepanekule, et leitud üldvalemi (12.1) parem pool erineb multinoomvalemi

$$\left(\frac{x_1}{1} + \frac{x_2}{2} + \dots + \frac{x_n}{n}\right)^n = \sum_{\Sigma k_i = n} \frac{n!}{k_1!\, k_2! \dots k_n!} \left(\frac{x_1}{1}\right)^{k_1} \left(\frac{x_2}{2}\right)^{k_2} \cdots \left(\frac{x_n}{n}\right)^{k_n}$$

paremast poolest ainult oma summeerimisviisilt.

Kui eksponentsiaalse genereeriva funktsiooni e^{Px} üldliikmes argumendi aste x^n selle kordajaks oleva summa liikmetes esinevate astmete vahel loomulikul viisil (tsüklitüüpi iseloomustavat seost (11.2) arvestades) ära jaotada, siis võime moodustatava genereeriva funktsiooni esitada kujul

$$\begin{aligned}
e^{Px} &= \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{\Sigma i k_i = n} \frac{n!}{k_1!\, k_2! \dots k_n!} \left(\frac{x_1}{1}\right)^{k_1} \left(\frac{x_2}{2}\right)^{k_2} \cdots \left(\frac{x_n}{n}\right)^{k_n} =\\
&= \sum_{n=0}^{\infty} \sum_{\Sigma i k_i = n} \frac{1}{k_1!\, k_2! \dots k_n!} \left(\frac{x\,x_1}{1}\right)^{k_1} \left(\frac{x^2 x_2}{2}\right)^{k_2} \cdots \left(\frac{x^n x_n}{n}\right)^{k_n}.
\end{aligned}$$

Rühmitame nüüd selles kahekordses summas liikmed ümber nii, et kõigepealt võetakse kokku ühesuguse astendajate summaga liikmed ja saadud tulemused liidetakse seejärel üle astendajate summa k kõikide võimalikkude väärtuste:

$$e^{Pz} = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{\Sigma k_i = k} \frac{k!}{k_1!\, k_2! \ldots} \left(\frac{z x_1}{1}\right)^{k_1} \left(\frac{z^2 x_2}{2}\right)^{k_2} \cdots \left(\frac{z^i x_i}{i}\right)^{k_i} \cdots =$$

$$= \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{z x_1}{1} + \frac{z^2 x_2}{2} + \cdots\right)^k = e^{\left(\frac{z x_1}{1} + \frac{z^2 x_2}{2} + \cdots\right)}.$$

Saadud (arvutusteks näiliselt üpris ebamugava) tulemuse tegelike kasutusvõimaluste demonstreerimiseks lahendame kõigepealt järgmise lihtsa ülesande: leida n-elemendilise hulga niisuguste substitutsioonide arv, millel on täpselt k tsüklit (tsüklite pikkusi sealjuures arvestamata).

Tähistame otsitava arvu sümboliga $c(n,k)$ ja leiame niiviisi defineeritud arvude jada $\{c(n,k)\}_k$ polünomiaalse genereeriva funktsiooni

$$c_n(x) = \sum_{k=0}^{n} c(n,k) x^k.$$

Selle polünoomi võib aga saada vahetult sümmeetrilise rühma tsüklilisuse indikaatorist $P_n(x_1, x_2, \ldots, x_n)$, kui seal iga $k = 0, 1, \ldots, n$ korral ühendada kõik need liikmed, kus muutujate x_i astendajate summa (ehk tsüklite koguarv) on k. Liikmete niisuguseks ühendamiseks tarvitseb vaid samastada kõik tsüklilisuse indikaatori P_n argumendid: iga i korral $x_i \equiv x$. Seega

$$c_n(x) = P_n(x, x, \ldots, x)$$

ja nende polünoomide jada $\{c_n(x)\}$ eksponentsiaalse genereeriva funktsiooni (mille muutujat tähistame sümboliga z) saame kohe e^{Pz} avaldisest:

$$e^{c(x)z} = e^{x\left(\frac{z}{1} + \frac{z^2}{2} + \cdots\right)} = e^{x \ln(1-z)^{-1}} = (1-z)^{-x} = \sum_{n=0}^{\infty} \binom{x+n-1}{n} z^n.$$

Et siin $z^n/n!$ kordaja peab olema $c_n(x)$, siis

$$c_n(x) = n! \binom{x+n-1}{n} = x^{(n)}$$

(juhul $n = 0$ muidugi $c_0(x) = 1$) ja järelikult

$$x^{(n)} = \sum_{k=0}^{n} c(n,k) x^k. \tag{12.2}$$

Kui meenutada *Stirlingi esimest liiki arvude* seost kasvava faktoriaaliga

$$x^{(n)} = (-1)^n \sum_{k=0}^{n} s(n,k)(-1)^k x^k,$$

siis olemegi saanud, et

$$c(n,k) = (-1)^{n+k} s(n,k) = |s(n,k)|.$$

Teise analoogilise näitena genereeriva funktsiooni e^{Pz} kasutamise kohta leiame veel n-elemendilise hulga niisuguste substitutsioonide arvu $d(n,k)$, millel on täpselt k tsüklit, sealjuures kõik ühest suurema pikkusega.

Jada $\{d(n,k)\}_k$ polünomiaalne genereeriv funktsioon $d_n(x)$ avaldub seekord tsüklilisuse indikaatori P_n kaudu kujul

$$d_n(x) = \sum_{k=0}^{n} d(n,k)x^k = P_n(0, x, \dots, x).$$

Nende funktsioonide jada $\{d_n(x)\}$ eksponentsiaalse genereeriva funktsiooni (kus muutuja tähiseks võtame jälle z) saame eelmise näite tulemusi arvestades:

$$e^{d(x)z} = e^{x\left(\frac{z^2}{2}+\frac{z^3}{3}+\cdots\right)} = e^{x(\ln(1-z)^{-1}-z)} =$$
$$= e^{-xz}(1-z)^{-x} = \left(\sum_{n=0}^{\infty}(-x)^n \frac{z^n}{n!}\right) \cdot \left(\sum_{n=0}^{\infty} c_n(x)\frac{z^n}{n!}\right).$$

Polünoomi $d_n(x)$ leidmiseks tuleb nüüd vaid välja kirjutada $z^n/n!$ kordaja selles eksponentsiaalsete genereerivate funktsioonide korrutises. Definitsiooni (4.7) kohaselt

$$d_n(x) = \sum_{i=0}^{n} \binom{n}{i} (-x)^i c_{n-i}(x) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \sum_{k=i}^{n} c(n-i, k-i)x^k =$$
$$= \sum_{k=0}^{n} x^k \sum_{i=0}^{k} (-1)^i \binom{n}{i} c(n-i, k-i)$$

ning otsitava arvu $d(n,k)$ saame siit lihtsalt kui x^k kordaja. Seega ülal $c(n,k)$ jaoks leitud avaldist arvestades

$$d(n,k) = \sum_{i=0}^{k} (-1)^i \binom{n}{i} c(n-i, k-i) =$$
$$= (-1)^{n+k} \sum_{i=0}^{k} (-1)^i \binom{n}{i} s(n-i, k-i).$$

Nende arvude (matemaatilises kirjanduses on neid mõnikord nimetatud ka Stirlingi esimest liiki arvude *kaasarvudeks*) tabeli tegelikuks koostamiseks vajaliku rekurrentse seose võib tuletada ülalsaadud võrdusest

$$e^{d(x)z} = e^{-xz}(1-z)^{-x}. \tag{12.3}$$

Selle sümboolse võrduse diferentseerimine z järgi annab

$$d(x)e^{d(x)z} = -x\,e^{-xz}(1-z)^{-x} + x\,e^{-xz}(1-z)^{-x-1},$$

mis võrduse (12.3) veelkordse kasutamise teel omandab kuju:

$$(1-z)d(x)\,e^{d(x)z} = x\,z\,e^{d(x)z}.$$

Tulemus kujutab endast sümboolselt üles kirjutatud astmeridade vahelist võrdust. Kui selles võrrelda $z^n/n!$ kordajaid, siis saame

$$d_{n+1}(x) - n\,d_n(x) = n\,x\,d_{n-1}(x),$$

millest vahetult järeldub x^k kordajate võrdsus:

$$d(n+1,k) = n\,d(n,k) + n\,d(n-1,k-1).$$

Selle rekurrentse seose kasutamisel arvude $d(n,k)$ tabeli koostamiseks võime lähtuda näiteks loomulikest rajaväärtustest $d(n,0) = 0$, $d(n,1) = (n-1)!$.

Sümmeetrilise rühmaga seotud ülesannetes on tihti tarvis loendada selliseid substitutsioone, milles teatavad etteantud elemendid või etteantud arv elemente osutuvad invariantseteks. *Invariantsete elementide* loendamisel saab täiesti vahetult ära kasutada elimineerimismeetodiga seoses saadud tulemusi.

Olgu põhihulgaks $\mathcal{R}$ nüüd mingi n-elemendilise hulga sümmeetriline rühm. Et meid järgnevas käsitluses huvitavad vaid teatud omadustega substitutsioonide arvud, siis võib kasutada triviaalseid kaalusid: iga $g \in \mathcal{R}$ korral $w(g) = 1$.

Seisnegu substitutsiooni $g = (j_1\ j_2\ \dots\ j_n)$ omadus a_i (kus $i = 1, 2, \dots, n$) selles, et $j_i = i$, s. t. element i osutub vastava substitutsiooni suhtes invariantseks. Nüüd võib kergesti veenduda, et iga $k = 0, 1, \dots, n$ ja defineeritud omaduste a_i mistahes k-kombinatsiooni $c(k) = \{i_1, i_2, \dots, i_k\}$ korral

$$\ell(a_{i_1} a_{i_2} \dots a_{i_k}) = (n-k)!,$$

kus vasak pool tähendab sellesse kombinatsiooni c kuuluvate omadustega substitutsioonide arvu. Tõepoolest, mingi k elemendi asukoha fikseerimine jätab ju vabaks $n-k$ elementi ja niisuguste substitutsioonide arv võrdub nende vabade elementide $(n-k)$-permutatsioonide arvuga. Järelikult definitsioonis (10.6) saame iga k korral

$$L_k = \sum_{c(k)} (n-k)! = \binom{n}{k}(n-k)! = \frac{n!}{k!}.$$

Loend $D(n,m)$ annab nüüd kõigi niisuguste substitutsioonide arvu, milles invariantseid elemente ehk 1-tsükleid leidub täpselt m tükki. Erijuhul $m = 0$ kasutatakse siin lühemat tähistust $D_n \equiv D(n,0)$, kus D_n on seega 1-tsükliteta substitutsioonide (öeldakse ka *inversioonide*) arv.

Äsjaleitud arvudega $d(n,k)$ seob arvu D_n muidugi valem

$$D_n = \sum_{k=1}^{n} d(n,k),$$

kuid tegelikeks arvutusteks see $d(n,k)$ avaldise keerulise kuju tõttu ei sobi. Arvutuslikult mugavamad seosed tulenevad valemeist (10.7) ja (10.8):

$$D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \tag{12.4}$$

$$D(n,m) = \sum_{k=m}^{n} (-1)^{k-m} \binom{k}{m} \frac{n!}{k!} = \frac{n!}{m!} \sum_{k=0}^{n-m} \frac{(-1)^k}{k!} = \binom{n}{m} D_{n-m}. \tag{12.5}$$

Rekurrentse seose arvude D_n leidmiseks võib nüüd täiesti vahetult tuletada võrdusest (12.4):

$$D_n = n! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} + (-1)^n = n\,D_{n-1} + (-1)^n.$$

Kui selles võrduses

$$D_n = n\,D_{n-1} + (-1)^n$$

kirjutada n asemele $n-1$, siis saame

$$D_{n-1} = (n-1)D_{n-2} + (-1)^{n-1},$$

mis eelmise võrdusega liitmisel annab põhiseose

$$D_n = (n-1)(D_{n-1} + D_{n-2}). \tag{12.6}$$

Rekurrentne võrrand (12.6) annab aluse nimetada vaadeldavaid arvusid D_n *subfaktoriaalideks*, sest ka tavalised *faktoriaalid* rahuldavad sama võrrandit (arvud D_n osutuvad selle lahendeiks rajatingimustel $D_0 = 1$, $D_1 = 0$, faktoriaalid $n!$ aga rajatingimustel $D_0 = D_1 = 1$).

Jada $\{D(n,m)\}_m$ polünomiaalsele genereerivale funktsioonile $D_n(x)$ võib võrdust (12.5) arvestades anda kuju

$$D_n(x) = \sum_{m=0}^{n} D(n,m)x^m = \sum_{m=0}^{n} \binom{n}{m} D_{n-m}x^m = (D+x)^n,$$

kus (nagu sümbolarvutuse sellistes võrdustes ikka) loeme, et $D^k \equiv D_k$.

Kõikide arvude $D(n,m)$ summa annab muidugi substitutsioonide koguarvu $n!$ ja seega iga n korral kehtib võrdus

$$n! = \sum_{m=0}^{n} D(n,m) = D_n(1) = (D+1)^n.$$

Sellest võrdusest järeldub vastavate jadade $\{n!\}_n$ ja $\{(D+1)^n\}_n$ eksponentsiaalsete genereerivate funktsioonide võrdsus:

$$(1-x)^{-1} = \sum_{n=0}^{\infty} n!\,\frac{x^n}{n!} = \sum_{n=0}^{\infty} (D+1)^n\,\frac{x^n}{n!} = e^{x(D+1)},$$

mis omakorda annab jada $\{D_n\}$ eksponentsiaalse genereeriva funktsiooni

$$e^{Dx} = e^{-x}(1-x)^{-1}.$$

Eksponentsiaalsete genereerivate funktsioonide korrutise definitsiooni (4.7) arvestades saame $x^n/n!$ kordajate võrdlemise teel siit

$$D_n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i (n-i)!\,.$$

Sellele tulemusele veidi kompaktsema kuju andmiseks arvestame, et *nihutamisoperaatori* E rakendamine funktsioonile $f(k) = k!$ annab

$$E^2\,k! = (k+2)!,\ \ldots,\ E^{n-i}\,k! = (k+n-i)!\,,$$

seega võrdust (4.5) arvestades saamegi

$$D_n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i E^{n-i}\,0! = (E-1)^n\,0! = \Delta^n\,0!\,,$$

s. t. subfaktoriaale D_n võib soovi korral leida funktsiooni $f(k) = k!$ jaoks koostatud *diferentsskeemi* teisest veerust:

n \ k	0	1	2	3	4	5	6
0	1	1	2	6	24	120	720
1	0	1	4	18	96	600	
2	1	3	14	78	504		
3	2	11	64	426			
4	9	53	362				
5	44	309					
6	265						

Kui põhihulgas $S = \overline{1,n} = \{1, 2, \ldots, n\}$ fikseerida loomulik järjestus, siis osutub selle hulga sümmeetrilise rühmaga seotud ülesannetes mõnikord vajalikuks loendada substitutsioonide kasvamis- või kahanemiskohti. Substitutsiooni $g = (j_1 \ j_2 \ \ldots \ j_n)$ *kasvamiskohaks* nimetatakse indeksi $i = 1, 2, \ldots, n-1$ sellist väärtust, kus $j_i < j_{i+1}$ ja kahanemiskohaks sellist väärtust, kus $j_i > j_{i+1}$. Näiteks kuueelemendilise hulga $\overline{1,6}$ substitutsioonil $(6 \ 1 \ 5 \ 3 \ 4 \ 2)$ on kaks kasvamiskohta $i = 2$, $i = 4$ ning kolm kahanemiskohta $i = 1$, $i = 3$ ja $i = 5$.

Substitutsiooni *tõusuks* nimetatakse tema kasvamiskohtade arvu (kahanemiskohtade arv avaldub tõusu k kaudu kujul $n - 1 - k$). Sümboliga $E(n, k)$ tähistame n-elemendilise hulga selliste substitutsioonide arvu, mille tõus on k. Ilmselt $k \geqslant n$ korral $E(n, k) = 0$ ja iga n korral $E(n, 0) = 1$, sest vaid substitutsiooni $(n \ \ n-1 \ \ldots \ 2 \ 1)$ tõus on 0. Lihtne on samuti veenduda, et iga $n > 1$ korral osutub arvude $E(n, k)$ järjend $E(n, 0)$, $E(n, 1)$, $\ldots$, $E(n, n-1)$ sümmeetriliseks:

$$E(n, k) = E(n, n-1-k). \tag{12.7}$$

Tõepoolest, kui substitutsiooni $g_1 = (j_1 \ j_2 \ \ldots \ j_{n-1} \ j_n)$ tõus on k, siis substitutsiooni $g_2 = (j_n \ j_{n-1} \ \ldots \ j_2 \ j_1)$ tõus on muidugi $n - 1 - k$, sest substitutsiooni "pööramisel" muutuvad kasvamiskohad kahanemiskohtadeks ja vastupidi.

Arvude $E(n, k)$ leidmiseks paneme tähele, et n-elemendilise hulga $\{1, 2, \ldots, n\}$ substitutsiooni $(j_1 \ \ldots \ j_i \ n \ j_{i+1} \ \ldots \ j_{n-1})$ võib saada $(n-1)$-elemendilise hulga $\{1, 2, \ldots, n-1\}$ substitutsioonist $g = (j_1 \ \ldots \ j_i \ j_{i+1} \ \ldots \ j_{n-1})$ elemendi n lisamise teel. Selgitame, kui mitmel juhul tekib niisuguse konstruktsiooni tulemusel substitutsioon, mille tõus on k.

Tõus ei muutu elemendi n lisamise tulemusel neil juhtudel, mil n lisatakse kas g algusesse või kasvamiskohta, s. t. niisuguse j_i järele, kus $j_i < j_{i+1}$. Kui g tõus on k, siis tõusu mitte muutva lisamise võimalusi on $k + 1$ ja sellisel viisil saame $(k + 1)E(n - 1, k)$ n-elemendilise hulga substitutsiooni.

Tõus kasvab elemendi n lisamisel ühe võrra neil juhtudel, kui n lisatakse kas g lõppu või kahanemiskohta, s. t. niisuguse j_i järele, kus $j_i > j_{i+1}$. Kui g tõus on $k - 1$, siis tõusu ühe võrra suurendava lisamise võimalusi on $n - k$ ja sellisel viisil saame $(n - k)E(n - 1, k - 1)$ n-elemendilise hulga substitutsiooni.

Kokku oleme niiviisi saanud n-elemendilise hulga kõik substitutsioonid tõusuga k, järelikult kehtib iga $n > 1$ ja $k = 1, 2, \ldots, n - 1$ korral võrdus

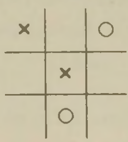
$$E(n, k) = (k + 1)E(n - 1, k) + (n - k)E(n - 1, k - 1).$$

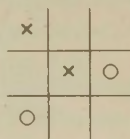
See tulemus langeb kokku võrrandiga (5.11). Et kokku langevad ka rajatingimused, siis on siindefineeritud arvud $E(n, k)$ lihtsalt *Euleri teist liiki arvud* ja me oleme järelikult selgitanud nende arvude kombinatoorse tähenduse. Paneme ühtlasi tähele, et juba nende arvude tabelis kajastus valemiga (12.7) väljendatud sümmeetria.

13. Rühmaga genereeritud ekvivalents

Diskreetses matemaatikas kerkib sageli selliseid loendamisülesandeid, mille lahendamisel genereerivad funktsioonid või teised seni vaadeldud lähenemisviisid osutuvad ebapiisavateks. Raskused tekivad peamiselt siis, kui loendada tuleb mitte vahetult lähtehulga elemente, vaid nende ekvivalentsiklasse, s. t. faktorhulga elemente.

Ekvivalentsiklasside loendamise ülesanded kerkivad reeglina siis, kui hulga erinevad elemendid osutuvad antud probleemis samaväärseteks ning neid peab lugema ühekordselt. Sellise olukorraga tuleb tegemist muuhulgas näiteks juhul, kui ülesandeks on trips-traps-trulli mängus esineda võivate oluliselt erinevate, s. t. üksteisest pöörete või peegelduste teel mitte saadavate seisude loendamine. Niisugusel juhul ei seisne küsimus lihtsalt etteantud 3×3 ruudustiku ristide ja sõõridega täitmise võimaluste loendamises. Tõepoolest, näiteks järgmised kaks seisu





on küll väliselt erinevad, kuid sisuliselt kirjeldavad nad mängu seisukohalt ühesuguseid olukordi ja tuleks seega nähtavasti ekvivalentseteks lugeda.

Lõplikul hulgal S defineeritud ekvivalents on tavaliselt tihedalt seotud selle hulga sümmeetrilise rühma mingi alamrühmaga $\mathcal{G}$. Öeldakse, et hulgal S on *genereeritud ekvivalents* selle hulga sümmeetrilise rühma vaadeldava alamrühma $\mathcal{G}$ abil, kui elemente $s_1, s_2 \in S$ loetakse ekvivalentseteks (ja tähistatakse $s_1 \sim s_2$) parajasti siis, kui leidub substitutsioon $g \in \mathcal{G}$ nii, et $g(s_1) = s_2$. Pole raske veenduda, et niiviisi defineeritud relatsioon $s_1 \sim s_2$ osutub ikka tõepoolest ekvivalentsiks, s. t. on refleksiivne, sümmeetriline ja transitiivne.

Järgnevat käsitlust saab kohaldada ka veidi üldisema juhu tarvis, mil $\mathcal{G}$ võib olla suvaliste elementidega rühm, kusjuures ei õnnestu korraldada selle üksühest vastavust põhihulga S substitutsioonide mingi rühmaga. Sellisel juhul peab aga siiski leiduma vähemalt rühma $\mathcal{G}$ *homomorfism* hulga S sümmeetrilisse rühma, s. t. igale elemendile $g \in \mathcal{G}$ peab olema seatud ühesesse vastavusse teatav substitutsioon u_g nii, et see kujutus rahuldab mistahes $g_1, g_2 \in \mathcal{G}$ korral tingimust

$$u_{g_1 g_2} = u_{g_1} u_{g_2}. \tag{13.1}$$

Elemente $s_1, s_2 \in \mathcal{S}$ loetakse sel juhul ekvivalentseteks (ning tähistatakse ikka $s_1 \sim s_2$) parajasti siis, kui leidub niisugune $g \in \mathcal{G}$, et $u_g(s_1) = s_2$.

Viimase definitsiooni näiliselt suurem üldisus avaldub tegelikult selles, et vaadeldava rühma $\mathcal{G}$ elemente saab küll teatud viisil tõlgendada substitutsioonidena, kuid erinevatele elementidele võib sealjuures vastata ühesugune substitutsioon. Et aga rühma $\mathcal{G}$ homomorfismi abil saadav hulk $\{u_g\colon g \in \mathcal{G}\}$ osutub alati sümmeetrilise rühma alamrühmaks, siis sisulist üldistust ei teki, sest niiviisi saadud alamrühm genereerib ju sellesama ekvivalentsi.

Rühma $\mathcal{G}$ abil genereeritud ekvivalentsi kasutamisel tuleb kõigepealt enamasti selgitada tekkivate *ekvivalentsiklasside arv*, mida tähistame sümboliga $E_{\mathcal{G}}(\mathcal{S})$. Osutub, et selle arvu saab kergesti leida.

Teoreem (*Burnside'i lemma*). Rühma $\mathcal{G}$ abil hulgal $\mathcal{S}$ genereeritavate ekvivalentsiklasside arv võrdub selle rühma elementidele homomorfismis vastavate substitutsioonide korral invariantsete elementide arvude aritmeetilise keskmisega:

$$E_{\mathcal{G}}(\mathcal{S}) = |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} k_1(u_g), \tag{13.2}$$

kus $|\mathcal{G}|$ on rühma $\mathcal{G}$ järk ja $k_1(u_g)$ tähendab hulga $\mathcal{S}$ niisuguste elementide s arvu, mis on substitutsiooni u_g suhtes invariantsed, s. t. $u_g(s) = s$ (tähis k_1 vihjab sellele, et tegemist on 1-tsüklite arvuga vastava substitutsiooni u_g tüübis).

Tõestuseks vaatleme kõigi niisuguste paaride (g, s) hulka, kus $g \in \mathcal{G}$, $s \in \mathcal{S}$ ja $u_g(s) = s$ ning leiame nende paaride koguarvu p kahel erineval viisil.

Kui iga fikseeritud $g \in \mathcal{G}$ korral leida vastava substitutsiooni u_g suhtes invariantsete elementide arv k_1, siis saame kohe

$$p = \sum_{g \in \mathcal{G}} k_1(u_g). \tag{13.3}$$

Teiselt poolt võime aga iga fikseeritud $s \in \mathcal{S}$ tarvis otsida välja kõik sellised elemendid $g \in \mathcal{G}$, mille korral $u_g(s) = s$. Rühma $\mathcal{G}$ kõigi niisuguse omadusega elementide hulga tähistame sümboliga $\mathcal{G}_s$ (pole muide raske veenduda, et hulk $\mathcal{G}_s$, mida nimetatakse ka elemendi s stabilisaatoriks, osutub koguni rühma $\mathcal{G}$ alamrühmaks). Seega avaldub paaride koguarv kujul

$$p = \sum_{s \in \mathcal{S}} |\mathcal{G}_s| \tag{13.4}$$

ja meil jääb veel vaid arvud $|\mathcal{G}_s|$ seostada ekvivalentsiklasside arvuga. Niisuguse seoseni võib jõuda näiteks rühma $\mathcal{G}$ jaotamisel klassidesse selle järgi, milliseks osutub vaadeldava elemendi s kujutis vastava substitutsiooniga (s. t. ühte klassi loetakse need $g \in \mathcal{G}$, mille korral $u_g(s)$ on ühesugune).

Kui $s \sim s'$, siis ekvivalentsi definitsiooni kohaselt leidub vähemalt üks element $h \in \mathcal{G}$ nii, et $u_h(s') = s$. Lugedes sellise h fikseerituks näeme, et igale niisugusele elemendile $g \in \mathcal{G}$, mille korral $u_g(s) = s'$, vastab kindel element $hg \in \mathcal{G}_s$, sest $u_{hg}(s) = s$. See vastavus hulkade $\{g: u_g(s) = s'\}$ ja $\mathcal{G}_s$ vahel osutub üksüheseks: iga $f \in \mathcal{G}_s$ korral $h^{-1}f \in \{g: u_g(s) = s'\}$. Seega leidub täpselt $|\mathcal{G}_s|$ niisugust elementi $g \in \mathcal{G}$, mille korral $u_g(s) = s'$, kus s' on fikseeritud element ekvivalentsiklassis $\bar{s}$.

Elementi s sisaldava ekvivalentsiklassi $\bar{s}$ abil saab rühma $\mathcal{G}$ järelikult tükeldada nii, et igale elemendile $s' \in \bar{s}$ vastab täpselt $|\mathcal{G}_s|$ erinevat elementi g rühmast $\mathcal{G}$: need, mille korral $u_g(s) = s'$. Summeerides need võrdsed arvud üle kõigi elementide $s' \in \bar{s}$ saame $\sum |\mathcal{G}_s| = |\mathcal{G}|$. Et tulemus $|\mathcal{G}|$ ei sõltu valitud ekvivalentsiklassist, siis üle kõigi ekvivalentsiklasside summeerimine annab

$$\sum_{s \in \mathcal{S}} |\mathcal{G}_s| = |\mathcal{G}| \cdot E_{\mathcal{G}}(\mathcal{S}),$$

mille võrdlemine võrdustega (13.3) ja (13.4) tõestabki teoreemis väidetud valemi (13.2). $\square$

Illustreerime seda teoreemi ja tema tõestamisel kasutatud mõttekäiku paari lihtsa näitega, kusjuures piirdume juhuga, mil ekvivalents on genereeritud vahetult substitutsioonide rühmaga $\mathcal{G}$.

Olgu põhihulga $\mathcal{S}$ elementideks 3×3 ruudustiku lahtrid, mis on nummerdatud üheteistkümnendas jaotises näidatud viisil. Ekvivalentsi sellel hulgal genereerime ruudu pöörete ja peegelduste rühmaga $\mathcal{G}$. Sisuliselt see tähendab, et me loeme ekvivalentseteks need lahtrid, millest üks mingi pöörde või peegeldusega teise kohale satub. Vajadus niisuguse ekvivalentsi järele tekib näiteks siis, kui pole otstarbekohane fikseerida, millisest suunast seda ruudustikku peab vaatama.

Täiendame selle rühma $\mathcal{G}$ teisenduste jaoks koostatud tabelit, varustades iga teisenduse tähisega $(g_0, g_1, \ldots, g_7)$ ja märkides ära põhihulga invariantsed elemendid:

Tähis	Substitutsioon	Invariandid	$k_1(g)$
g_0	(1 2 3 4 5 6 7 8 9)	1,2,...,9	9
g_1	(7 8 1 2 3 4 5 6 9)	9	1
g_2	(5 6 7 8 1 2 3 4 9)	9	1
g_3	(3 4 5 6 7 8 1 2 9)	9	1
g_4	(7 6 5 4 3 2 1 8 9)	4, 8, 9	3
g_5	(3 2 1 8 7 6 5 4 9)	2, 6, 9	3
g_6	(1 8 7 6 5 4 3 2 9)	1, 5, 9	3
g_7	(5 4 3 2 1 8 7 6 9)	3, 7, 9	3

Selle tabeli viimase veeru ja valemi (13.2) kohaselt saame nüüd

$$E_{\mathcal{G}}(\mathcal{S}) = \frac{1}{8} \cdot (9 + 1 + 1 + 1 + 3 + 3 + 3 + 3) = 3.$$

Antud juhul pole muidugi raske neid kolme ekvivalentsiklassi ka vahetult leida, sest ilmselt on nendeks nurkmiste lahtrite hulk $\{1, 3, 5, 7\}$, külgmiste lahtrite hulk $\{2, 4, 6, 8\}$ ja keskmine lahter $\{9\}$ (kerge on veenduda, et näiteks $1 \sim 3$, sest $g_3(1) = 3$, $1 \sim 5$, sest $g_2(1) = 5$, $4 \sim 8$, sest $g_5(4) = 8$ jne.).

Kirjutame veel iga $s \in \mathcal{S}$ jaoks välja vastava alamrühma $\mathcal{G}_s$:

s	1	2	3	4	5	6	7	8	9
$\mathcal{G}_s$	$\{g_0, g_6\}$	$\{g_0, g_5\}$	$\{g_0, g_7\}$	$\{g_0, g_4\}$	$\{g_0, g_6\}$	$\{g_0, g_5\}$	$\{g_0, g_7\}$	$\{g_0, g_4\}$	$\mathcal{G}$

Sellest tabelist näeme, et kuigi ühe ekvivalentsiklassi erinevatel elementidel s on üldiselt erinev $\mathcal{G}_s$, osutub nende alamrühmade järk $|\mathcal{G}_s|$ ühe ekvivalentsiklassi piires ikka tõepoolest ühesuguseks (antud juhul on see järk võrdne kahega koguni mõlemas esimesena nimetatud ekvivalentsiklassis).

Paneme ühtlasi tähele, et kui $\mathcal{G}$ on põhihulga substitutsioonide rühm, siis valemis (13.2) vajaliku summa saab vahetult välja kirjutada rühma $\mathcal{G}$ tsüklilisuse indikaatori kaudu: selleks summaks tuleb polünoomi $P_{\mathcal{G}}$ kordajate ning muutuja x_1 vastavate astendajate korrutiste summa. Nii näiteks äsjavaadeldud juhul saame tsüklilisuse indikaatori (11.5) abil:

$$\sum_{g \in \mathcal{G}} k_1(g) = 1 \cdot 9 + 4 \cdot 3 + 1 \cdot 1 + 2 \cdot 1 = 24.$$

Kui $\mathcal{S}$ on kuubi tahkude hulk ja $\mathcal{G}$ heksaeedri rühm, siis valemi (13.2) ning vastava tsüklilisuse indikaatori (11.6) järgi leiame

$$E_{\mathcal{G}}(\mathcal{S}) = \frac{1}{24} \cdot (1 \cdot 6 + 3 \cdot 2 + 6 \cdot 2 + 6 \cdot 0 + 8 \cdot 0) = 1.$$

Seega ekvivalentsi niisuguse definitsiooni korral on kuubi mistahes kaks tahku ekvivalentsed, s. t. alati leidub pööre, mis teisendab ühe tahu teiseks.

Võtame nüüd vaatlusele mingil lõplikul hulgal $\mathcal{S}$ määratud *funktsioonid* f, mille väärtused kuuluvad mingisse teise lõplikku hulka $\mathcal{R}$, s. t. $f\colon \mathcal{S} \to \mathcal{R}$. Kõigi niisuguste *funktsioonide hulka* tähistatakse diskreetses matemaatikas teatavasti sümboliga $\mathcal{R}^{\mathcal{S}}$ ja see hulk sisaldab ilmselt $|\mathcal{R}^{\mathcal{S}}| = |\mathcal{R}|^{|\mathcal{S}|}$ elementi.

Märgime, et funktsioon $f \in \mathcal{R}^{\mathcal{S}}$ on definitsiooni kohaselt eeskiri, mis määrab hulga $\mathcal{S}$ kujutuse hulka $\mathcal{R}$. Vajaduse korral võib aga funktsiooni interpreteerida ka kui kordumistega $|\mathcal{S}|$-permutatsiooni $|\mathcal{R}|$ erinevast elemendist, mida kõiki on olemas kuitahes palju eksemplare.

Ekvivalentsi funktsioonide hulgal $\mathcal{R}^{\mathcal{S}}$ saaks muidugi defineerida selle hulga substitutsioonide mingi rühma abil. Praktikas aga ei leidu enamasti loomulikku teed niisuguse rühma fikseerimiseks, kuigi reeglina võib fikseerida loomulikku ekvivalentsi defineeriva rühma näiteks määramispiirkonna $\mathcal{S}$ (või väärtuste hulga $\mathcal{R}$) jaoks.

Meid huvitabki järgnevalt küsimus sellest, kuidas kanda hulgal $\mathcal{S}$ defineeritud ekvivalents üle funktsioonide hulka $\mathcal{R}^{\mathcal{S}}$. Tarbetute komplikatsioonide vältimiseks piirdume siinjuures juhuga, mil ekvivalents hulgal $\mathcal{S}$ on defineeritud vahetult selle hulga substitutsioonide mingi fikseeritud rühmaga $\mathcal{G}$.

Põhihulgas $\mathcal{S}$ substitutsioonide teatava rühmaga $\mathcal{G}$ genereeritud ekvivalentsi kõige loomulikumaks ülekandmisviisiks hulgale $\mathcal{R}^{\mathcal{S}}$ näib olevat järgmine. Funktsioone $f_1, f_2 \in \mathcal{R}^{\mathcal{S}}$ nimetame *ekvivalentseteks* (ja tähistame $f_1 \sim f_2$) parajasti siis, kui leidub $g \in \mathcal{G}$ nii, et iga $s \in \mathcal{S}$ korral

$$f_1(g(s)) = f_2(s). \tag{13.5}$$

Võrdust (13.5) võib lühemalt kirjutada ka kujul $f_1 g = f_2$, kui kujutuste järjestrakendamist tähistada korrutisena ja funktsioonide võrdumist tõlgendada ikka nende väärtuste võrdumisena määramispiirkonna igas punktis.

Ekvivalentsi niisuguse definitsiooni loomulikkust aitab selgitada järgmine näide. *Trips-traps-trulli* seisu saame teatavasti sel teel, kui 3×3 ruudustiku mõningatesse lahtritesse kanname ristid või söörid. Seega võib niisugust seisu tõlgendada kui teatavat konkreetset funktsiooni lahtrite hulgast $\mathcal{S}$ hulka $\mathcal{R} = \{\sqcup, \times, \bigcirc\}$, kus $\sqcup$ tähendab tühikut ehk sümboli puudumist lahtris.

Kui meil ei ole mingit erilist põhjust fikseerida, millisest suunast tuleb just mängulauda vaadata, siis ongi seise loomulik lugeda ekvivalentseteks (s. t. mängu seisukohalt samaväärseteks) just juhul, mil ühe neist võib saada teisest ruudustiku mingi pöörde või peegelduse teel. Nii näiteks käesoleva jaotise alguses osutatud seisud $f_1 \equiv (\times, \sqcup, \bigcirc, \sqcup, \sqcup, \bigcirc, \sqcup, \sqcup, \times)$ ja $f_2 \equiv (\times, \sqcup, \sqcup, \bigcirc, \sqcup, \sqcup, \bigcirc, \sqcup, \times)$ on ekvivalentsed sellepärast, et $f_1 g_6 = f_2$, kus g_6 tähendab ülaltoodud tabeli kohaselt peegeldust peadiagonaali suhtes.

Vaatleme veel üht näidet, mil $\mathcal{S}$ on kuubi tahkude hulk, $\mathcal{G}$ heksaeedri rühm ja $\mathcal{R} = \{\text{sinine}, \text{punane}\}$ (rõhutame, et ei määramispiirkonna $\mathcal{S}$ elementidega ega ka funktsiooni väärtustega pole meil kavas sooritada algebralisi operatsioone!). Sellisel juhul on funktsioon $f \in \mathcal{R}^{\mathcal{S}}$ tõlgendatav kuubi tahkude *värvimisviisina*, kusjuures iga tahk värvitakse üleni ühe värviga.

Kahe funktsiooni ekvivalentsus tähendab nüüd, et vastaval viisil värvitud kuubid pole pöörete lubatavuse korral eristatavad ja neid värvimisviise võib seega samaväärseteks lugeda. Siit näeme ühtlasi, et pakub huvi leida meetod hulga $\mathcal{R}^{\mathcal{S}}$ ekvivalentsiklasside arvu (antud juhul eristatavate värvimisviiside arvu) määramiseks ja ka nende klasside struktuuri lähemaks kirjeldamiseks.

Vaadeldaval lihtsal erijuhul (lihtne on see erijuht sellepärast, et väärtuste hulk $\mathcal{R}$ sisaldab ainult kaks elementi) pole küll raske ekvivalentsiklasse ka ilma eriliste meetoditeta üle lugeda. Nimelt saame järgmised kümme klassi ehk värvimisviisi, kus sulgudes on iga klassi juures näidatud sellesse klassi kuuluvate funktsioonide koguarv:

1) kõik tahud värvitakse siniseks (niisuguseid funktsioone on ainult 1);

2) viis tahku värvitakse siniseks, üks tahk punaseks (kuubi ühe tahu saab valida kuuel viisil, seega niisuguseid funktsioone on 6);

3) kaks vastastahku värvitakse punaseks, ülejäänud neli tahku siniseks (vastastahkude paare ja seega ka niisuguseid funktsioone on 3);

4) kaks naabertahku värvitakse punaseks, ülejäänud neli tahku siniseks (kuubi servi ehk naabertahkude paare ja seega ka niisuguseid funktsioone on 12);

5) kolm ühise tipuga tahku värvitakse punaseks, ülejäänud kolm tahku siniseks (kuubi tippe ja seega ka niisuguseid funktsioone on 8);

6) kaks vastastahku ja veel üks tahk värvitakse punaseks, ülejäänud kolm tahku siniseks (vastastahkude paare leidub kolm ja kolmandat punast tahku saab igale paarile lisada neljal viisil, seega niisuguseid funktsioone on kokku 12);

7) kaks naabertahku värvitakse siniseks, ülejäänud neli tahku punaseks (naabertahkude paare ja seega ka niisuguseid funktsioone on 12);

8) kaks vastastahku värvitakse siniseks, ülejäänud neli tahku punaseks (vastastahkude paare ja seega ka niisuguseid funktsioone on 3);

9) viis tahku värvitakse punaseks, üks tahk siniseks (kuubi tahkusid ja seega ka niisuguseid funktsioone on 6);

10) kõik tahud värvitakse punaseks (niisuguseid funktsioone on ainult 1).

Kõigi nende klasside juures näidatud funktsioonide koguarvusid liites veendume, et kõik $|\mathcal{R}|^{|S|} = 2^6$ funktsiooni on ikka arvesse võetud:

$$1 + 6 + 3 + 12 + 8 + 12 + 12 + 3 + 6 + 1 = 64.$$

Ekvivalentsiklasside niisuguse vahetu ülelugemise teel saab lahendada ka näiteks analoogilised ülesanded tetraeedri või oktaeedri tahkude värvimise kohta kahe erineva värviga. Seevastu aga üleminek kolmele värvile (näiteks kui valida funktsioonide väärtuste hulgaks $\mathcal{R} = \{\mathsf{sinine},\ \mathsf{punane},\ \mathsf{kollane}\}$) muudab eristatavate kuupide või tetraeedrite või oktaeedrite vahetu ülelugemise

üsna raskeks, üleminek neljale värvile aga juba lootusetult raskeks ülesandeks.

Üsna efektiivse tee ekvivalentsiklasside loendamisel kerkivate raskuste ületamiseks näitas G. Polya, kes aastail 1935 – 40 lõi nn. *loendamisteooria*, mille lihtsaimate mõistetega tutvume järgmises kahes jaotises.

14. Loendamisteooria põhimõisteid

Kui funktsioonide hulgal $\mathcal{R}^{\mathcal{S}}$ on põhihulga $\mathcal{S}$ substitutsioonide rühmaga $\mathcal{G}$ genereeritud ekvivalents, siis saadavate ekvivalentsiklasside loendamisega seotud ülesannete lahendamisel osutub jälle sobivaks kasutada loendi mõistet.

Olgu vaadeldavate funktsioonide väärtuste hulga $\mathcal{R}$ elementidele omistatud kaalud, s. t. iga $r \in \mathcal{R}$ jaoks on üheselt määratud tema kaal $w(r)$ – mingi fikseeritud integriteetkonna $\mathcal{W}$ element. *Funktsiooni* $f \in \mathcal{R}^{\mathcal{S}}$ ***kaaluks*** on sellisel juhul otstarbekohane lugeda tema kõikide väärtuste kaalude korrutist

$$w(f) = \prod_{s \in \mathcal{S}} w(f(s)) \tag{14.1}$$

(niiviisi defineerimisel me arvestame integriteetkonna $\mathcal{W}$ kommutatiivsust, sest muidu peaks korrutises (14.1) täpsustama tegurite järjekorra). Paneme siinjuures tähele, et funktsiooni kaal ei tarvitse osutuda ühegi elemendi $r \in \mathcal{R}$ kaaluks.

Niisuguse definitsiooni korral osutub, et ekvivalentsetel funktsioonidel on ühesugused kaalud. Tõepoolest, kui näiteks $f_1 \sim f_2$ (s. t. õnnestub fikseerida vähemalt üks $g \in \mathcal{G}$ nii, et $f_1 g = f_2$), siis hulga $\mathcal{S}$ elementide s läbivaatamise asendamine nende kujutiste $g(s)$ läbivaatamisega annab

$$w(f_1) = \prod_{s \in \mathcal{S}} w(f_1(s)) = \prod_{s \in \mathcal{S}} w(f_1(g(s))) = \prod_{s \in \mathcal{S}} w(f_2(s)) = w(f_2).$$

Seega võime rääkida ka funktsioonide f ***ekvivalentsiklassi*** $\overline{f}$ ***kaalust*** $w(\overline{f})$, mõistes selle all vastava klassi funktsioonide ühist kaalu. Tuleb muidugi arvestada, et erinevatel ekvivalentsiklassidel ei tarvitse olla erinevad kaalud.

Kui näiteks kuubi tahkude kahe värviga värvimise ülesandes omistada hulga $\mathcal{R} = \{\textbf{sinine}, \textbf{punane}\}$ elementidele kaalud $w(\textbf{sinine}) = x$ ja $w(\textbf{punane}) = y$ (hulgaks $\mathcal{W}$ on niisuguse valiku korral loomulik lugeda kahe muutuja täisarvuliste kordajatega polünoomide ring $\mathbb{Z}[x, y]$), siis ekvivalentsiklasside kaaludeks saame eelmisel leheküljel toodud loetelu järjekorras:

$$x^6,\ x^5y,\ x^4y^2,\ x^4y^2,\ x^3y^3,\ x^3y^3,\ x^2y^4,\ x^2y^4,\ xy^5,\ y^6.$$

Muuhulgas näeme siit, et vaadeldaval kümnel ekvivalentsiklassil on ühtekokku ainult seitse erinevat kaalu.

Kaaludega varustatud hulga elementide inventuuri teostamiseks ehk loendamiseks kasutusele võetud kaalude täpsusega tuleb moodustada selle hulga *loend* – tema kõikide elementide kaalude summa. Seega vaadeldavate funktsioonide väärtuste hulga $\mathcal{R}$ loendiks on

$$\ell(\mathcal{R}) = \sum_{r \in \mathcal{R}} w(r),$$

funktsioonide eneste hulga $\mathcal{R}^S$ loendiks aga

$$\ell(\mathcal{R}^S) = \sum_{f \in \mathcal{R}^S} w(f) = \sum_{f \in \mathcal{R}^S} \prod_{s \in S} w(f(s)). \tag{14.2}$$

Näiteks kui tegemist on kuubi tahkude värvimisviiside loendamisega ja ülalnimetatud kaaludega, siis eelmises jaotises osutatud arvude abil saame funktsioonide (ehk värvimisviiside) hulga loendi kirjutada kujul

$$\ell(\mathcal{R}^S) = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6.$$

Siit leiame iga $i = 0, 1, \ldots, 6$ jaoks kohe niisuguste värvimisviiside arvu, mille korral i tahku on sinised ja ülejäänud $6 - i$ tahku punased: näiteks leidub 20 värvimisviisi, kus nii siniste kui ka punaste tahkude arv võrdub kolmega.

Viimast polünoomi lähemalt vaadeldes pole raske märgata, et selle võib binoomvalemi kohaselt kirjutada kujul $\ell(\mathcal{R}^S) = (x+y)^6$. See tähelepanek pole muidugi juhuslik, sest kehtib järgmine üldine seos.

Teoreem 1. Funktsioonide hulga $\mathcal{R}^S$ loend avaldub nende funktsioonide väärtuste hulga $\mathcal{R}$ loendi kaudu kujul

$$\ell(\mathcal{R}^S) = (\ell(\mathcal{R}))^{|S|} = \Big(\sum_{r \in \mathcal{R}} w(r)\Big)^{|S|}. \tag{14.3}$$

Tõestuseks paneme tähele, et võrduse (14.3) viimast astet tuleb tõlgendada $|S|$ ühesuguse teguri korrutisena (nii defineeritakse ju aste kommutatiivses ringis $\mathcal{W}$). Korraldame mingi üksühese vastavuse nende tegurite ja hulga S elementide vahel.

Sulgude avamisel korrutises (14.3) tuleb meil nüüd mingi ühe liikme saamiseks valida igast tegurist välja üks liidetav $w(r)$, s. t. fikseerida üks element $r \in \mathcal{R}$. Selline valik on aga korraldatud üksühese vastavuse tõttu samaväärne igale elemendile $s \in S$ mingi konkreetse $r \in \mathcal{R}$ vastavusse seadmisega ehk niisuguse funktsiooni $f \in \mathcal{R}^S$ fikseerimisega, mis selles punktis s omandab väärtuse $f(s) = r$.

Seega sulgude avamisel saadavaid liikmeid tuleb sama palju, kui leidub erinevaid funktsioone f hulgas $\mathcal{R}^S$, iga liige aga omandab kuju

$$\prod_{s \in S} w(f(s)) = w(f).$$

Võrduse (14.2) kohaselt selliste liikmete niisugune summa aga ongi hulga $\mathcal{R}^S$ loend ning valemi (14.3) võib tõestatuks lugeda.

Enamasti pole funktsioonide loendamisega seotud ülesannetes vaatlusel kogu hulk $\mathcal{R}^{\mathcal{S}}$, vaid üksnes selle teatav alamhulk, s. t. mingeid täiendavaid tingimusi rahuldavate funktsioonide hulk. Demonstreerime selliste alamhulkade loendi leidmise metoodikat ühe üsna lihtsa, kuid järgnevas vajaliku erijuhu korral.

Olgu antud määramispiirkonna $\mathcal{S}$ *tükeldus*, s. t. $\mathcal{S}$ olgu jaotatud ühisosata alamhulkadeks (tükkideks) $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ nii, et $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \ldots \cup \mathcal{S}_k$. Võtame vaatlusele hulga $\mathcal{R}^{\mathcal{S}}$ sellise alamhulga, millesse kuuluvad funktsioonid on igal alamhulgal $\mathcal{S}_i$ konstantsed, s. t. iga fikseeritud $i = 1, 2, \ldots, k$ ja mistahes elementide $s_1, s_2 \in \mathcal{S}_i$ korral $f(s_1) = f(s_2)$. Rõhutame, et niisuguse *tükiti konstantse funktsiooni* väärtused erinevatel alamhulkadel muidugi võivad (kuid ei tarvitse) erineda.

Neid funktsioone võib tõlgendada kui liitfunktsioonisid $f = ht$, kus t seab elemendile $s \in \mathcal{S}$ vastavusse seda elementi sisaldava alamhulga $\mathcal{S}_i$ indeksi i (seega alati $s \in \mathcal{S}_{t(s)}$) ja h on funktsioon hulgast $\mathcal{K} = \{1, 2, \ldots, k\}$ hulka $\mathcal{R}$, s. t. $h \in \mathcal{R}^{\mathcal{K}}$. Paneme tähele, et $t \in \mathcal{K}^{\mathcal{S}}$ on hulga $\mathcal{S}$ etteantud tükeldusega $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ üheselt määratud funktsioon. Seega võib vaadeldavate funktsioonide f hulga üksühese vastavuse mõttes samastada funktsioonide h hulgaga $\mathcal{R}^{\mathcal{K}}$.

Teoreem 2. Funktsioonide hulga $\mathcal{R}^{\mathcal{K}}$ loend avaldub kujul

$$\ell(\mathcal{R}^{\mathcal{K}}) = \prod_{i=1}^{k} \sum_{r \in \mathcal{R}} (w(r))^{|\mathcal{S}_i|}. \tag{14.4}$$

Tõestus on jälle täiesti vahetu: sulgude avamisel korrutises (14.4) tuleb mingi ühe liikme saamiseks igast summast

$$\sum_{r \in \mathcal{R}} (w(r))^{|\mathcal{S}_i|}$$

(s. t. iga i puhul) valida üks liidetav. Selline valik on aga samastatav ühe konkreetse funktsiooniga $h \in \mathcal{R}^{\mathcal{K}}$, sest me ju fikseerime iga $i = 1, 2, \ldots, k$ jaoks mingi $r \in \mathcal{R}$. Funktsiooni h fikseerimine annab meile arendise liikme

$$(w(h(1)))^{|\mathcal{S}_1|}(w(h(2)))^{|\mathcal{S}_2|} \ldots (w(h(k)))^{|\mathcal{S}_k|} = \prod_{i=1}^{k} (w(h(i)))^{|\mathcal{S}_i|}.$$

Kui nüüd tähistada $f = ht$, kus t on etteantud tükeldusega $\mathcal{S}_1$, $\mathcal{S}_2, \ldots, \mathcal{S}_k$ määratud funktsioon, siis

$$(w(h(i)))^{|\mathcal{S}_i|} = \prod_{s \in \mathcal{S}_i} w(ht(s)) = \prod_{s \in \mathcal{S}_i} w(f(s))$$

ja seega

$$\prod_{i=1}^{k} (w(h(i)))^{|\mathcal{S}_i|} = \prod_{i=1}^{k} \prod_{s \in \mathcal{S}_i} w(f(s)) = \prod_{s \in \mathcal{S}} w(f(s)) = w(f).$$

Et võrduse (14.4) paremal pool olev korrutis avaldub niisuguse kujuga liikmete summana üle kõikide funktsioonide $h \in \mathcal{R}^{\mathcal{K}}$ (ehk nimetatud üksühese vastavuse mõttes üle kõikide $f \in \mathcal{R}^{\mathcal{K}}$), siis olemegi võrduse (14.4) tõestanud:

$$\prod_{i=1}^{k} \sum_{r \in \mathcal{R}} (w(r))^{|S_i|} = \sum_{f \in \mathcal{R}^{\mathcal{K}}} w(f) = \ell(\mathcal{R}^{\mathcal{K}}).$$

Paneme tähele, et teoreem 1 kujutab endast lihtsat järeldust teoreemist 2. Tõepoolest, hulga $\mathcal{R}^{\mathcal{S}}$ suvalist funktsiooni saab alati tõlgendada niisuguse tükiti konstantse funktsioonina, mis vastab määramispiirkonna $\mathcal{S}$ lahutusele üheelemendilisteks alamhulkadeks $\mathcal{S}_1$, $\mathcal{S}_2, \ldots, \mathcal{S}_k$. Sellisel juhul aga $k = |\mathcal{S}|$, iga i korral $|\mathcal{S}_i| = 1$ ja valemist (14.4) järeldub vahetult valem (14.3):

$$\ell(\mathcal{R}^{\mathcal{S}}) = \prod_{i=1}^{|\mathcal{S}|} \sum_{r \in \mathcal{R}} (w(r))^1 = \Big(\sum_{r \in \mathcal{R}} w(r)\Big)^{|\mathcal{S}|} = \big(\ell(\mathcal{R})\big)^{|\mathcal{S}|}.$$

Võtame nüüd siiski vaatlusele kogu funktsioonide hulga $\mathcal{R}^{\mathcal{S}}$ ning eeldame, et selles on hulga $\mathcal{S}$ substitutsioonide teatava rühma $\mathcal{G}$ abil eelmises jaotises kirjeldatud viisil genereeritud ekvivalents: $f \sim f'$ parajasti siis, kui leidub $g \in \mathcal{G}$ nii, et $f = f'g$. See ekvivalents määrab hulga $\mathcal{R}^{\mathcal{S}}$ funktsioonide jaotumise ekvivalentsiklassideks $\overline{f}$ ja järgnevas meid huvitabki just kõikide nende ekvivalentsiklasside hulk ehk hulga $\mathcal{R}^{\mathcal{S}}$ *faktorhulk* $\mathcal{F} = \{\overline{f}\}$.

Faktorhulga $\mathcal{F}$ loendi leidmise eeskirja annab järgmine teoreem, mis on kogu loendamisteoorias keskse tähtsusega.

Teoreem 3 (*Polya teoreem*). Hulgal $\mathcal{R}^{\mathcal{S}}$ hulga $\mathcal{S}$ substitutsioonide rühma $\mathcal{G}$ abil genereeritud ekvivalentsiga määratud faktorhulga loend avaldub kujul

$$\ell(\mathcal{F}) = |\mathcal{G}|^{-1} P_{\mathcal{G}}\Big(\sum_{r \in \mathcal{R}} w(r), \sum_{r \in \mathcal{R}} (w(r))^2, \sum_{r \in \mathcal{R}} (w(r))^3, \ldots\Big),$$

kus $P_{\mathcal{G}}(x_1, x_2, x_3, \ldots)$ on rühma $\mathcal{G}$ tsüklilisuse indikaator.

Tõestus jaguneb loomulikul viisil kahte ossa, kusjuures esimese osa sisuks on mingi fikseeritud kaaluga ekvivalentsiklasside arvu leidmine. Olgugi v funktsioonide kaalu üks võimalik väärtus ning

$$\mathcal{V} = \{f : f \in \mathcal{R}^{\mathcal{S}},\ w(f) = v\}$$

kõikide selle kaaluga funktsioonide hulk. Selleks, et leida ekvivalentsiklasside arvu hulgas $\mathcal{V}$ (s. t. niisuguste ekvivalentsiklasside $\overline{f}$ arvu, mille korral $w(\overline{f}) = v$) ei saa vahetult kasutada valemit (13.2) – kõigepealt peame vaadeldava ekvivalentsi seostama hulga $\mathcal{V}$ substitutsioonidega.

Kui mingi $g \in \mathcal{G}$ korral $f = f'g$, siis funktsioonide ekvivalentsi definitsiooni kohaselt $f \sim f'$ ning nende funktsioonide kaalud on võrdsed. Järelikult $f \in \mathcal{V}$ korral alati ka $f' = fg^{-1} \in \mathcal{V}$, mis teisiti öeldes tähendab, et suvalisele substitutsioonile $g \in \mathcal{G}$ vastab hulga $\mathcal{V}$ kujutus iseendasse:

$$u_g(f) = fg^{-1}. \tag{14.5}$$

See kujutus u_g osutub üksüheseks, s. t. hulga $\mathcal{V}$ substitutsiooniks, sest iga g korral eksisteerib ju pöördkujutus $u_{g^{-1}}$: kui $u_g(f) = fg^{-1} = f'$, siis

$$u_{g^{-1}}(f') = f'g = fg^{-1}g = f.$$

Eeskiri (14.5), mis seab rühma $\mathcal{G}$ elemendile g (hulga $\mathcal{S}$ substitutsioonile) vastavusse hulga $\mathcal{V}$ substitutsiooni u_g osutub homomorfismiks (vt. (13.1)), sest

$$u_{g_1g_2}(f) = f(g_1g_2)^{-1} = fg_2^{-1}g_1^{-1} = u_{g_2}(f)g_1^{-1} = u_{g_1}(u_{g_2}(f)) = (u_{g_1}u_{g_2})(f).$$

Funktsioonide ekvivalents vahetult rühma $\mathcal{G}$ mõttes langeb muidugi kokku selle ekvivalentsiga, mille saab defineerida substitutsioonide u_g kaudu. Tõepoolest, niisuguse $g \in \mathcal{G}$ leidumine, mille korral $u_g(f) = f'$ tähendab ju sama, mis niisuguse $g \in \mathcal{G}$ leidumine, et $f = f'g$. Järelikult saame ekvivalentsiklasside arvu $E_\mathcal{G}(\mathcal{V})$ leidmiseks hulgas $\mathcal{V}$ nüüd juba kasutada valemit (13.2), mis annab

$$E_\mathcal{G}(\mathcal{V}) = |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} k_1^v(g), \tag{14.6}$$

kus sümboliga $k_1^v(g)$ on tähistatud niisuguste elementide $f \in \mathcal{V}$ arv, mis fikseeritud g korral rahuldavad seost $fg^{-1} = f$ ehk $fg = f$.

Faktorhulga $\mathcal{F}$ otsitava loendi saamiseks tarvitseb nüüd ainult korrutada ekvivalentsiklasside leitud arv (14.6) hulga $\mathcal{V}$ funktsioonide ühise kaaluga v ja summeerida need korrutised üle v kõikide võimalikkude väärtuste (tegelikult üle kõikide $v \in \mathcal{W}$, sest kui mingi v ei esine ühegi funktsiooni kaaluna, siis vastav $\mathcal{V}$ on tühi ja ekvivalentsiklasside arv muidugi null):

$$\ell(\mathcal{F}) = \sum_{\bar{f}} w(\bar{f}) = |\mathcal{G}|^{-1} \sum_v \sum_{g \in \mathcal{G}} k_1^v(g)\, v.$$

Paneme siin tähele, et fikseeritud $g \in \mathcal{G}$ korral

$$\sum_v k_1^v(g)\, v = \sum_{f = fg} w(f),$$

kus viimane summa võetakse üle kõigi niisuguste funktsioonide $f \in \mathcal{R}^S$, mis selle g puhul rahuldavad tingimust $f = fg$. Seega summeerimise järjekorra vahetamine loendi $\ell(\mathcal{F})$ viimases avaldises annab

$$\ell(\mathcal{F}) = |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} \sum_{f = fg} w(f). \tag{14.7}$$

Sisemise summa leidmiseks arvestame nüüd, et g on hulga $\mathcal{S}$ substitutsioon ja $\mathcal{S}$ jaguneb selle fikseeritud g suhtes teatavasti ühesel viisil tsükliteks. Tingimus $f = fg$ tähendab, et mistahes $s \in \mathcal{S}$ korral alati

$$f(s) = f(g(s)) = f(g^2(s)) = \ldots,$$

s. t. f on substitutsiooni g igal tsüklil konstantne, sest $s, g(s), g^2(s), \ldots$ kuuluvad ju (11.1) kohaselt alati samasse tsüklisse. Samuti kehtib aga ka vastassuunaline seos: suvaline funktsioon f, mis vaadeldava g igal tsüklil konstantseks osutub, rahuldab tingimust $f = fg$, sest s ja $g(s)$ kuuluvad iga s korral samasse tsüklisse. Seega loendi (14.7) sisemine summa

$$\sum_{f=fg} w(f) \tag{14.8}$$

pole midagi muud, kui kõikide vaadeldava substitutsiooni g tsüklitel konstantsete funktsioonide hulga loend $\ell(\{f = fg\})$.

Olgu vaadeldava substitutsiooni g tsüklid $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ ning kasutame loendi (14.8) leidmiseks valemit (14.4). Kui substitutsiooni g tsüklitüüp on $(k_1, k_2, \ldots)$, siis see tähendab, et arvude $|\mathcal{S}_1|, |\mathcal{S}_2|, \ldots, |\mathcal{S}_k|$ hulgas esineb arv üks k_1 korda, arv kaks k_2 korda jne. Seega valemi (14.4) võib tegurite (ehk alamhulkade $\mathcal{S}_i$) järjekorra sobiva muutmise teel esitada kujul

$$\ell(\{f = fg\}) = \sum_{f=fg} w(f) = \Big(\sum_{r\in\mathcal{R}} w(r)\Big)^{k_1} \Big(\sum_{r\in\mathcal{R}} (w(r))^2\Big)^{k_2} \ldots,$$

mis võrdusesse (14.7) asendamisel annab

$$\ell(\mathcal{F}) = |\mathcal{G}|^{-1} \sum_{g\in\mathcal{G}} \Big(\sum_{r\in\mathcal{R}} w(r)\Big)^{k_1} \Big(\sum_{r\in\mathcal{R}} (w(r))^2\Big)^{k_2} \ldots$$

Kui siin iga $i = 1, 2, \ldots$ korral tähistada

$$x_i = \sum_{r\in\mathcal{R}} (w(r))^i,$$

siis definitsiooniga (11.3) võrreldes näeme, et $\ell(\{f = fg\})$ näol on tegemist just rühma $\mathcal{G}$ tsüklilisuse indikaatori $P_\mathcal{G}$ selle liikmega, mis vastab konkreetsele substitutsioonile g. See tõestabki teoreemi 3.

Paneme veel tähele, et triviaalsete kaalude juhul, kui iga $r \in \mathcal{R}$ korral $w(r) = 1$, annab viimane teoreem lihtsalt *ekvivalentsiklasside arvu*:

$$E_\mathcal{G}(\mathcal{R}^\mathcal{S}) = |\mathcal{G}|^{-1} P_\mathcal{G}(|\mathcal{R}|, |\mathcal{R}|, |\mathcal{R}|, \ldots). \tag{14.9}$$

Kui rühm $\mathcal{G}$ on ainult ühiksubstitutsioonist g_0 koosnev nn. ühikrühm, siis muidugi $P_\mathcal{G} = x_1^{|\mathcal{S}|}$ ja teoreem 3 taandub teoreemiks 1.

Teoreemi 3 saab mitmel viisil üldistada. Nimetame siin ühe näitena võimaliku üldistuse, mis tekib funktsioonide ekvivalentsi teistsuguse, mõnevõrra üldisema definitsiooni juhul.

Olgu peale hulga $\mathcal{S}$ substitutsioonide teatava rühma $\mathcal{G}$ fikseeritud veel hulga $\mathcal{R}$ substitutsioonide teatav rühm $\mathcal{H}$. Funktsioone $f_1, f_2 \in \mathcal{R}^{\mathcal{S}}$ loeme nüüd *ekvivalentseteks* (ning kirjutame $f_1 \sim f_2$) parajasti siis, kui leiduvad $g \in \mathcal{G}$ ja $h \in \mathcal{H}$ nii, et $f_1 g = h f_2$, s. t. iga $s \in \mathcal{S}$ korral

$$f_1(g(s)) = h(f_2(s)) \tag{14.10}$$

(paneme tähele, et funktsioonide ülalvaadeldud ekvivalentsi saame siit sellel juhul, kui rühm $\mathcal{H}$ koosneb üksnes ühiksubstitutsioonist).

Olgu nüüd hulga $\mathcal{R}^{\mathcal{S}}$ elementidele f omistatud kaalud $w(f)$ (ikka mingi integriteetkonna $\mathcal{W}$ elemendid) nii, et ekvivalentsete *funktsioonide kaalud* osutuvad võrdseteks. Siin on samuti tegemist üldistusega, sest me ei piirdu enam reegliga (14.1), mis seostas funktsiooni kaalu hulga $\mathcal{R}$ elementide kaaludega. Veelgi enam, hulgas $\mathcal{R}$ ei tarvitse mingisuguseid kaalusid isegi üldse defineeritud olla.

Ilma vastavat põhjendust siinkohal esitamata (see langeb muide suurel määral kokku teoreemi 3 tõestusega) nimetame, et ekvivalentsi (14.10) abil genereeritava faktorhulga $\mathcal{F}$ loend avaldub kujul

$$\ell(\mathcal{F}) = |\mathcal{G}|^{-1}|\mathcal{H}|^{-1} \sum_{g \in \mathcal{G}} \sum_{h \in \mathcal{H}} \sum_{fg=hf} w(f), \tag{14.11}$$

kus sisemine summa võetakse üle kõikide niisuguste funktsioonide $f \in \mathcal{R}^{\mathcal{S}}$, mis vaadeldavate g ja h korral rahuldavad tingimust $fg = hf$, s. t. igas punktis $s \in \mathcal{S}$

$$f(g(s)) = h(f(s)).$$

Ekvivalentsiklasside arvu saamiseks valemist (14.11) tuleb funktsioonidele muidugi omistada triviaalsed kaalud: iga $f \in \mathcal{R}^{\mathcal{S}}$ korral $w(f) = 1$. Vastavate teisenduste tulemusel selgub, et *ekvivalentsiklasside arv* avaldub nüüd kujul

$$E_{\mathcal{G}\mathcal{H}}(\mathcal{R}^{\mathcal{S}}) = |\mathcal{G}|^{-1}|\mathcal{H}|^{-1} \sum_{h \in \mathcal{H}} P_{\mathcal{G}}(x_1, x_2, \ldots), \tag{14.12}$$

kus iga konkreetse $h \in \mathcal{H}$ korral tuleb rühma $\mathcal{G}$ tsüklilisuse indikaatori $P_{\mathcal{G}}(x_1, x_2, \ldots)$ argumentide x_i väärtused valida substitutsiooni h tsüklitüübi $(k_1, k_2, \ldots)$ järgi järgmise reegli kohaselt (summeerimine toimub üle i kõikide jagajate j):

$$x_i = \sum_{j \mid i} j k_j.$$

Juhul kui $\mathcal{H}$ koosneb ainult ühiksubstitutsioonist, on selle tsüklitüüp muidugi $(1^{|\mathcal{R}|})$, s. t. $k_1 = |\mathcal{R}|$, $k_2 = k_3 = \ldots = 0$. Seega iga i korral saame $x_i = |\mathcal{R}|$ ja valem (14.12) muutub valemiks (14.9).

15. Konkreetseid loendamisülesandeid

Eelmise jaotise teoreemi 2 kasutamisvõimaluste illustreerimiseks vaatleme järgmist lihtsat ülesannet: selgitada, kui mitmel erineval viisil saab m ühesugust objekti jaotada viie erineva pesa vahel nii, et esimeses kahes pesas oleks mõlemas ühepalju objekte ja kolmandas ning neljandas pesas samuti mõlemas ühepalju objekte.

Võtame põhihulgaks $\mathcal{S} = \{1,2,3,4,5\}$ pesade järjekorranumbrite hulga. Meid huvitavad sellel hulgal määratud funktsioonid f väärtuste hulgaga $\mathcal{R} = \{0,1,\ldots,m\}$, mis rahuldavad tingimusi

$$f(1) + f(2) + f(3) + f(4) + f(5) = m, \tag{15.1}$$

$$f(1) = f(2), \qquad f(3) = f(4). \tag{15.2}$$

Kuigi meil funktsioonide suuremaid väärtusi kui m tarvis ei lähe, osutub arvutuslikult mugavamaks võtta ülalnimetatud lõpliku $\mathcal{R}$ asemel vaatlusele kõikide naturaalarvude lõpmatu hulk $\mathcal{R} = \mathrm{N} = \{0,1,2,\ldots\}$ (pealegi peaks muidu iga erineva m korral kasutama erinevat hulka $\mathcal{R}$). Seame selle hulga $\mathcal{R}$ elementidele vastavusse kaalud 1, x, $x^2, \ldots$, s. t. valime $w(r) = x^r$. Siis võrdus (15.1) tähendab, et meid huvitavad vaid funktsioonid kaaluga m.

Võrdusi (15.2) võib tõlgendada kui selliste funktsioonide vaatlemisega piirdumist, mis on hulkadel $\mathcal{S}_1 = \{1,2\}$, $\mathcal{S}_2 = \{3,4\}$ ja $\mathcal{S}_3 = \{5\}$ konstantsed. Nende funktsioonide hulga loend ℓ omandab aga valemi (14.4) põhjal kuju

$$\ell = (1^2 + x^2 + x^4 + \cdots)^2(1 + x + x^2 + \cdots).$$

Püstitatud ülesande kohaselt huvitab meid siin kõigi niisuguste funktsioonide arv, mille kaal on x^m. See arv pole aga midagi muud, kui x^m kordaja saadud loendi ℓ reaksarenduses. Kui ℓ esitada algmurdude summana kujul

$$\ell = (1-x^2)^{-2}(1-x)^{-1} = \frac{3}{16}(1-x)^{-1} + \frac{1}{4}(1-x)^{-2} + \\ + \frac{1}{4}(1-x)^{-3} + \frac{3}{16}(1+x)^{-1} + \frac{1}{8}(1+x)^{-2},$$

siis võime x^m kordaja kohe välja kirjutada. Selleks tuleb

$$\frac{3}{16} + \frac{1}{4}\binom{m+1}{m} + \frac{1}{4}\binom{m+2}{m} + \frac{3}{16}\cdot(-1)^m + \frac{1}{8}\cdot(-1)^m\binom{m+1}{m} = \\ = \frac{1}{16}\cdot(3 + 2(m+1)(m+4) + (-1)^m\cdot(2m+5)).$$

Seega paarisarvulise m korral leidub $\frac{1}{8}(m+2)(m+4)$ võimalust ning paaritu m korral $\frac{1}{8}(m+1)(m+3)$ võimalust nende viie pesa täitmiseks nõutud viisil.

Eelmise jaotise teoreemi 3 kasutamise näitena vaatleme kõigepealt jälle kuubi tahkude värvimise ülesannet. Meenutame, et siin loomulikku ekvivalentsi genereeriva heksaeedri rühma $\mathcal{G}$ tsüklilisuse indikaator avaldub valemi (11.6) kohaselt kujul

$$P_{\mathcal{G}}(x_1, x_2, \ldots, x_6) = x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2.$$

Kui tegemist on kahe värviga, s. t. $\mathcal{R} = \{\textbf{sinine}, \textbf{punane}\}$, siis triviaalsete kaalude $w(\textbf{sinine}) = w(\textbf{punane}) = 1$ korral saame kõikide eristatavate *värvimisviiside* arvu kohe valemist (14.9):

$$E_{\mathcal{G}}(\mathcal{R}^S) = \frac{1}{24} \cdot (2^6 + 3 \cdot 2^4 + 6 \cdot 2^3 + 6 \cdot 2^3 + 8 \cdot 2^2) = 10,$$

mis muidugi on kooskõlas ülal vahetu loendamise teel saadud tulemusega.

Kui ülesandeks on nende värvimisviiside struktuuri lähem selgitamine, siis peame valima näiteks kaalud $w(\textbf{sinine}) = x$, $w(\textbf{punane}) = y$, millega saame eristatavate värvimisviiside hulga loendi kujul

$$\begin{aligned}\ell(\mathcal{F}) = \frac{1}{24} \cdot \Big((x+y)^6 + 3(x+y)^2(x^2+y^2)^2 + \\ + 6(x+y)^2(x^4+y^4) + 6(x^2+y^2)^3 + 8(x^3+y^3)^2\Big) = \\ = x^6 + x^5y + 2x^4y^2 + 2x^3y^3 + 2x^2y^4 + xy^5 + y^6.\end{aligned}$$

Siit näeme, et kuue, viie, ühe ja mitte ühegi sinise tahuga värvimisviise on igaühte vaid üks; nelja, kolme ja kahe sinise tahuga värvimisviise aga igaühte kaks (nagu me varem ka vahetu loendamise teel leidsime).

Kui tegemist on kolme värviga, s. t. $\mathcal{R} = \{\textbf{sinine}, \textbf{punane}, \textbf{kollane}\}$, siis eristatavate värvimisviiside arvuks saame valemi (14.9) kohaselt

$$E_{\mathcal{G}}(\mathcal{R}^S) = \frac{1}{24} \cdot (3^6 + 3 \cdot 3^4 + 6 \cdot 3^3 + 6 \cdot 3^3 + 8 \cdot 3^2) = 57.$$

Nende värvimisviiside struktuuri lähemaks selgitamiseks tuleb jälle sobival viisil valida hulga $\mathcal{R}$ elementide kaalud. Nii näiteks täieliku ülevaate saamiseks kõikidest ekvivalentsiklassidest võib valida $w(\textbf{sinine}) = x$, $w(\textbf{punane}) = y$, $w(\textbf{kollane}) = z$, mis annab eristatavate värvimisviiside hulga loendi kujul

$$\begin{aligned}\ell(\mathcal{F}) = \frac{1}{24} \cdot \Big((x+y+z)^6 + 3(x+y+z)^2(x^2+y^2+z^2)^2 + \\ + 6(x+y+z)^2(x^4+y^4+z^4) + 6(x^2+y^2+z^2)^3 + 8(x^3+y^3+z^3)^2\Big).\end{aligned}$$

Kui meid nüüd huvitab näiteks niisuguste eristatavate värvimisviiside arv, mille korral üks tahk on sinine, kaks tahku punased ja kolm tahku kollased, siis tarvitseb vaid leida liikme xy^2z^3 kordaja viimases polünoomis. Ilma sulgusid täielikult avamata leiame üsna väikese vaevaga, et see kordaja tuleb 3 (vaatlema peab vaid suluavaldise kaht esimest liidetavat, kus meid huvitavateks kordajateks on vastavalt 60 ja 12).

Kui meid aga huvitab üksnes näiteks niisuguste eristatavate värvimisviiside arv, mille korral täpselt kaks tahku on punased, siis osutub liialt töömahukaks leida viimases polünoomis liikmete x^4y^2, x^3y^2z, $x^2y^2z^2$, xy^2z^3 ja y^2z^4 kordajate summa. Hoopis kergem on valida hulga $\mathcal{R}$ elementidele kaalud $w(\textbf{sinine}) = w(\textbf{kollane}) = 1$, $w(\textbf{punane}) = x$ ja leida loendis

$$\ell(\mathcal{F}) = \frac{1}{24}\cdot\Big((x+2)^6 + 3(x+2)^2(x^2+2)^2 + \\ + 6(x+2)^2(x^4+2) + 6(x^2+2)^3 + 8(x^3+2)^2\Big)$$

lihtsalt liikme x^2 kordaja (selleks tuleb 16).

Teise näitena eelmise jaotise teoreemi 3 kasutamisvõimaluste kohta võtame vaatlusele *trips-traps-trulli* mängu ja püüame määrata selles mängus esineda võivate sisuliselt erinevate seisude arvu. Hulgaks $\mathcal{S}$ on nüüd loomulik võtta 3×3 ruudustiku lahtrite hulk, rühmaks $\mathcal{G}$ ruudu pöörete ja peegelduste rühm, mille tsüklilisuse indikaator valemi (11.5) kohaselt avaldub kujul

$$P_{\mathcal{G}}(x_1, x_2, \ldots, x_9) = x_1^9 + 4x_1^3x_2^3 + x_1x_2^4 + 2x_1x_4^2$$

ning hulgaks $\mathcal{R}$ näiteks hulk $\{\,\sqcup, \times, \bigcirc\,\}$.

Ekvivalentsiklasside koguarv meid antud juhul ei huvita (kuigi pole raske leida, et see arv tuleb 2862), sest nende hulgas on palju mängu seisukohalt ebahuvitavaid, näiteks ei saa mängulaud olla täidetud ainult ristidega. Huvi pakuvad vaid niisugused seisud (s. t. funktsioonid hulgast $\mathcal{R}^{\mathcal{S}}$), kus kas ristid ja sõõrid esinevad võrdsel arvul või riste on ühe võrra rohkem kui sõõre. Esimene juht vastab seisudele, kus käigul on ristimängija, teine seisudele, kus käigul on sõõrimängija. Tõsi küll, nimetatud seisude hulka tulevad ka mõned sellised, kus näiteks mõlemad mängijad on võitnud, kuid lihtsuse huvides ei hakka me neid siin välja eraldama.

Meid huvitavate seisude struktuuri tõttu on otstarbekohane valida hulga $\mathcal{R}$ elementide kaalud nii, et ristid ja sõõrid paarikaupa "taanduksid". Lihtsaim võimalus selleks on valida kaalud näiteks järgmiselt: $w(\sqcup) = 1$, $w(\times) = x$ ja $w(\bigcirc) = 1/x$ (kaalude integriteetkonna $\mathcal{W}$ moodustavad sel juhul funktsioonid

$$\sum_{i=-\infty}^{\infty} a_i x^i,$$

kus kordajad a_i on täisarvulised). Seisude ekvivalentsiklasside hulga loend omandab niisuguste kaalude korral kuju

$$\ell(\mathcal{F}) = \frac{1}{8}\cdot\Bigg(\Big(1+x+\frac{1}{x}\Big)^9 + 4\Big(1+x+\frac{1}{x}\Big)^3\Big(1+x^2+\frac{1}{x^2}\Big)^3 + \\ + \Big(1+x+\frac{1}{x}\Big)\Big(1+x^2+\frac{1}{x^2}\Big)^4 + 2\Big(1+x+\frac{1}{x}\Big)\Big(1+x^4+\frac{1}{x^4}\Big)^2\Bigg).$$

Püstitatud ülesande kohaselt pole meil vaja neid sulgusid täielikult avada. Jätkub vaid vabaliikme ning esimese astme liikme kordaja leidmisest. Suhteliselt lihtsate arvutuste tulemusel saame nendeks vastavalt 438 ja 412. Näiteks vabaliikme leidmine võib toimuda järgmiselt:

$$\frac{1}{8}\cdot\Bigg(\Big(\frac{9!}{9!\,0!\,0!}+\frac{9!}{7!\,1!\,1!}+\frac{9!}{5!\,2!\,2!}+\frac{9!}{3!\,3!\,3!}+\frac{9!}{1!\,4!\,4!}\Big)+$$
$$+4\cdot\Big(\Big(\frac{3!}{3!\,0!\,0!}+\frac{3!}{1!\,1!\,1!}\Big)^2+\Big(\frac{3!}{1!\,2!\,0!}\cdot\frac{3!\cdot 2}{2!\,1!\,0!}\Big)\cdot 2\Big)+$$
$$+\Big(\frac{4!}{4!\,0!\,0!}+\frac{4!}{2!\,1!\,1!}+\frac{4!}{0!\,2!\,2!}\Big)+2\cdot\Big(\frac{2!}{2!\,0!\,0!}+\frac{2!}{0!\,1!\,1!}\Big)\Bigg)=438.$$

Seega leidub 438 niisugust sisuliselt erinevat seisu, kus käigul on ristimängija ning 412 niisugust sisuliselt erinevat seisu, kus käigul on sõõrimängija või kus kogu ruudustik osutub täidetuks.

Veel ühe näitena eelmise jaotise teoreemi 3 kasutamise kohta vaatleme nn. *tsükliliste permutatsioonide* moodustamist. Täpsemalt, põhihulga n-elemendilisi järjestatud alamhulki nimetatakse tsüklilisteks n-permutatsioonideks siis, kui samastatakse üksteisest tsüklilise nihkega saadavad permutatsioonid ehk sõned

$$a_1a_2\ldots a_n\,,\quad a_2a_3\ldots a_na_1\,,\quad \ldots\,,\quad a_na_1a_2\ldots a_{n-1}$$

(järjestatud hulkade sellise tsüklilise samastamisega oli meil tegemist ka juba näiteks substitutsioonitsüklite vaatlemisel).

Koosnegu põhihulk m erinevast elemendist, neist igaüks suvalises arvus eksemplarides (ehk teisiti öeldes: põhihulgaks on multihulk m-elemendilise baasiga ja näiteks spetsifikatsiooniga $(n, n, \ldots, n)$). Tsükliliste n-permutatsioonide moodustamisega niisuguse põhihulga korral puutume kokku näiteks juhtudel, kui ülesandeks on selgitada, kui palju leidub võimalusi kas n tooli paigutamiseks ümber ümmarguse laua, kusjuures kasutada saab m erinevat liiki toole, või siis n-helmelise kaelakee moodustamiseks m erinevat liiki helmestest.

Vaadeldava põhihulga tavaliste n-permutatsioonide hulka võib teatavasti tõlgendada kui funktsioonide hulka $\mathcal{R}^{\mathcal{S}}$, kus $\mathcal{S} = \{1, 2, \ldots, n\}$ ja $\mathcal{R} = \{r_1, r_2, \ldots, r_m\}$. Tsükliliste n-permutatsioonide hulga saame aga siis, kui selles hulgas $\mathcal{R}^{\mathcal{S}}$ genereerime ekvivalentsi hulga $\mathcal{S}$ nihkerühmaga $\mathcal{G}$.

Kui hulga $\mathcal{R}$ elementidele omistada kaalud $y_1, y_2, \ldots, y_m$ (s. t. valida iga j korral $w(r_j) = y_j$), siis tsüklilisuse indikaatorist (11.4) saame tsükliliste n-permutatsioonide hulga $\mathcal{F}$ loendi teoreemi 3 kohaselt kujul

$$\ell(\mathcal{F}) \doteq \frac{1}{n}\sum_{i\,|\,n}\varphi(i)\Big(y_1^i + y_2^i + \cdots + y_m^i\Big)^{\frac{n}{i}}. \tag{15.3}$$

Kui meid huvitab vaid tsükliliste n-permutatsioonide arv $T(m,n)$, siis selle leiame valemist (15.3) valides iga i puhul $y_i = 1$:

$$T(m,n) = \frac{1}{n}\sum_{i\mid n}\varphi(i)m^{\frac{n}{i}}. \tag{15.4}$$

Nii näiteks kuue tooli paigutamiseks ümber laua leidub kahe tooliliigi (ütleme siniste ja punaste) olemasolu korral valemi (15.4) kohaselt

$$T(2,6) = \frac{1}{6}\cdot\left(\varphi(1)\cdot 2^6 + \varphi(2)\cdot 2^3 + \varphi(3)\cdot 2^2 + \varphi(6)\cdot 2^1\right) = 14$$

eristatavat võimalust. Nende võimaluste täpsemaks iseloomustamiseks võime valida hulga $\mathcal{R} = \{\mathsf{s}, \mathsf{p}\}$ elementide kaaludeks vastavalt $w(\mathsf{s}) = x$ ja $w(\mathsf{p}) = y$, millega saame paigutamisvõimaluste hulga loendi kujul

$$\begin{aligned}\ell(\mathcal{F}) &= \frac{1}{6}\cdot\left((x+y)^6 + (x^2+y^2)^3 + 2(x^3+y^3)^2 + 2(x^6+y^6)\right) = \\ &= x^6 + x^5y + 3x^4y^2 + 4x^3y^3 + 3x^2y^4 + xy^5 + y^6.\end{aligned}$$

Siit näeme, et leidub näiteks kokku neli paigutamisvõimalust, mille korral nii siniseid kui ka punaseid toole kasutatakse mõlemaid kolm tükki. Need neli võimalust saab esitada järgmiste sõnede kujul:

sssppp, sspspp, ssppsp, spspsp.

Kui laua ümber mahub täpselt 11 tooli, siis nendesama kahe tooliliigi korral leiame valemist (15.4) paigutamisvõimaluste arvu

$$T(2,11) = \frac{1}{11}\cdot\left(\varphi(1)\cdot 2^{11} + \varphi(11)\cdot 2^1\right) = 188$$

ja valemist (15.3) vastava faktorhulga loendi kujul

$$\begin{aligned}\ell(\mathcal{F}) = \frac{1}{11}\cdot\left((x+y)^{11} + 10\cdot(x^{11}+y^{11})\right) &= x^{11} + x^{10} + 5x^9y^2 + 15x^8y^3 + \\ &+ 30x^7y^4 + 42x^6y^5 + 42x^5y^6 + 30x^4y^7 + 15x^3y^8 + 5x^2y^9 + xy^{10} + y^{11}.\end{aligned}$$

Sellest homogeensest polünoomist (mille kordajate summa on muidugi 188) näeme, et näiteks kolme sinise ja kaheksa punase tooli paigutamiseks on olemas viisteist võimalust, mida saab esitada järgmiste sõnedena:

ssspppppppp, sspsppppppp, ssppspppppp, sspppsppppp, ssppppspppp,
sspppppsppp, ssppppppspp, sspppppppsp, spspspppppp, spsppsppppp,
spspppspppp, spsppppsppp, spspppppspp, sppsppspppp, sppspppsppp.

16. Järjestatud hulgad ja nende tükeldused

Binaarne seos ehk *relatsioon* $\rho \equiv \rho(\mathcal{X},\mathcal{Y})$ antud hulkade $\mathcal{X}$ ja $\mathcal{Y}$ elementide vahel tähendab teatavasti nende hulkade otsekorrutise alamhulka: $\rho \subseteq \mathcal{X} \times \mathcal{Y}$ (erijuhul $\mathcal{X} = \mathcal{Y}$ räägitakse relatsioonist hulgal $\mathcal{X}$). Kuuluvust $(x,y) \in \rho$ tähistatakse sageli ka kujul $x \rho y$. Näiteks relatsioon $\rho = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 \leqslant 25\}$ määrab juhul $\mathcal{X} = \mathcal{Y} = \mathbb{R}$ ringi raadiusega 5 ja keskpunktiga nullpunktis. Ka võib funktsiooni $f : \mathcal{X} \to \mathcal{Y}$ tõlgendada relatsioonina $\rho_f = \{(x,y) \in \mathcal{X} \times \mathcal{Y} : f(x) = y\}$.

Kaht liiki relatsioonid leiavad matemaatikas eriti tihti kasutamist. Nendeks on *ekvivalents* (refleksiivne, sümmeetriline ja transitiivne relatsioon) ning *järjestus* (refleksiivne, antisümmeetriline ja transitiivne relatsioon). Järgnevas käsitluses ongi üheks põhiliseks mõisteks hulk koos sellel fikseeritud järjestusrelatsiooniga.

Definitsioon. Öeldakse, et hulk $\mathcal{X}$ on *järjestatud hulk* (ehk lühidalt *o-hulk*), kui temal on fikseeritud mingi relatsioon ρ, mis rahuldab nõudeid

O1. iga $x \in \mathcal{X}$ korral $x\rho x$, (refleksiivsus)

O2. kui $x\rho y$ ja $y\rho x$, siis $x = y$, (antisümmeetria)

O3. kui $x\rho y$ ja $y\rho z$, siis $x\rho z$. (transitiivsus)

Märgime lahkuminekut üsna levinud terminoloogiast, kus relatsiooni ρ omadustega O1 – O3 nimetatakse osaliseks järjestuseks. Käesolevas käsitluses on loobutud täiendsõnast "osaline" ja lisatakse täiendsõnu teistel vajalikel juhtudel (näiteks lineaarne järjestus jms.). Kui meid ühel ja samal hulgal $\mathcal{X}$ korraga huvitavad kaks järjestust ρ ja σ, siis tähistame vastavaid o-hulki $(\mathcal{X};\rho)$ ja $(\mathcal{X};\sigma)$. Kui hulgal $\mathcal{X}$ vaadeldakse vaid üht järjestust, siis tähistatakse seda tavaliselt sümboliga $\leqslant$ ja kirjutist $x \leqslant y$ loetakse "x on väiksem-võrdne kui y" ehk "x eelneb y-le". Sedasama tähendab ka $y \geqslant x$, mida loetakse "y on suurem-võrdne kui x" ehk "y järgneb x-le". Kui $x \leqslant y$ ja $x \neq y$, siis kirjutatakse $x < y$ ning loetakse "x eelneb rangelt y-le".

Öeldakse, et element y *katab* elementi x, kui element x rangelt eelneb elemendile y (s.t. $x < y$) ja ei leidu elementi $z \in \mathcal{X}$ nii, et $x < z < y$. See mõiste võimaldab lõpliku o-hulgaga $\mathcal{X}$ siduda tema *diagrammi*: orienteeritud graafi $G(\mathcal{X})$, mille tippudeks on hulga $\mathcal{X}$ elemendid ja servadeks kõik need järjestatud paarid (x,y), kus y katab elementi x. Joonisel tähistatakse $G(\mathcal{X})$ tippe väikeste ringikestega ning $x < y$ korral asetatakse elementi y esindav ringikene elementi x esindavast ringikesest kõrgemale. Järgnevalt on toodud mõned o-hulkade tüüpilised näited.

(1) Täisarvude hulk $\mathbb{Z}$ oma tavalise järjestusega: $x \geqslant y$ tähendab $x - y \in \mathbb{N}$.

(2) Naturaalarvude hulk $\mathbb{N}$ ning selle lõplik alamhulk $\overline{1,n} = \{1,2,\ldots,n\}$ nende tavalise järjestusega on samuti o-hulkade näideteks.

(3) Naturaalarvude hulk $\mathbb{N}\backslash\{0\}$ osutub o-hulgaks ka jaguvuse kaudu antud järjestuse korral: $m \leqslant n$ tähendab, et arv m on arvu n jagaja (tähistus $m \mid n$).

(4) Olgu $\mathcal{D}_n$ naturaalarvu n kõikide jagajate hulk. Kui järjestus hulgal $\mathcal{D}_n$ defineerida nagu eelmises näites, siis saame lõpliku o-hulga.

(5) Hulga $\mathcal{H}$ kõikide alamhulkade hulk $\mathfrak{B}(\mathcal{H})$ osutub o-hulgaks, kui temas defineerida $\mathcal{M} \leqslant \mathcal{N}$ tähenduses $\mathcal{M} \subseteq \mathcal{N}$. Sümboliga $\mathfrak{B}_l(\mathcal{H})$ tähistame selle o-hulga niisugust alamhulka, mille moodustavad hulga $\mathcal{H}$ kõik lõplikud alamhulgad.

(6) Rühma $\mathcal{G}$ kõigi alamrühmade hulk, milles järjestus on antud alamrühmade kui hulga $\mathcal{G}$ alamhulkade sisalduvusseose $\subset$ kaudu on samuti o-hulk.

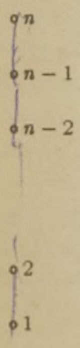
(7) Vektorruumi $\mathcal{V}(\mathbb{R})$ kõikide alamruumide hulk osutub o-hulgaks, kui järjestus anda seose $\subset$ kaudu. Kui ruum on lõplikumõõtmeline ja põhikorpuseks lõplik korpus $\mathbb{F}(p^m)$, siis vastav vektorruum $\mathcal{V}_n(\mathbb{F}(p^m))$ annab lõpliku o-hulga $\mathfrak{V}_n = \mathfrak{V}_n(p^m)$.

(8) Hulga $\mathcal{S}$ kõikvõimalikkude ekvivalentside hulka $\mathfrak{E}(\mathcal{S})$ saab vaadelda o-hulgana, sest $\mathfrak{E}(\mathcal{S}) \subset \mathfrak{B}(\mathcal{S} \times \mathcal{S})$ tõttu indutseerib näites (5) kasutatud järjestus hulgal $\mathfrak{B}(\mathcal{S} \times \mathcal{S})$ järjestuse ka hulgal $\mathfrak{E}(\mathcal{S})$: $\pi \leqslant \sigma$ tähendab, et $\pi \subseteq \sigma$, s. t. kui $a\pi b$, siis $a\sigma b$. Juhul $|\mathcal{S}| = n$ saame siin lõpliku o-hulga $\mathfrak{E}_n$.

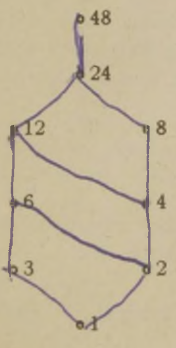
(9) Olgu $\pi : n = p_1 + \cdots + p_k$ ja $\sigma : n = s_1 + \cdots + s_l$ naturaalarvu n suvalised lahutused naturaalarvuliste liidetavate p_i ja s_j summaks. Loeme $\pi \leqslant \sigma$ siis, kui lahutuse σ saab lahutusest π selle liidetavate ühendamise (ja võimaliku ümberjärjestamise) tulemusel; nõuded O1 – O3 on täidetud ning tekib lõplik o-hulk $\mathcal{P}_n$.

(10) Suvalise hulga $\mathcal{X}$ ja o-hulga $\mathcal{Y}$ vaheliste funktsioonide $f : \mathcal{X} \to \mathcal{Y}$ hulga $\mathcal{Y}^{\mathcal{X}}$ saab muuta o-hulgaks, lugedes $f \leqslant g$ siis, kui hulgas $\mathcal{Y}$ iga $x \in \mathcal{X}$ korral $f(x) \leqslant g(x)$.

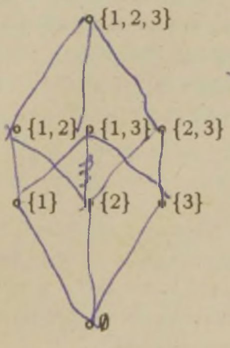
Toome ära mõnede äsjavaadeldud o-hulkade diagrammid (ringikestest paremale on kirjutatud hulga $\mathcal{X}$ elemendid, mida need ringikesed esindavad):



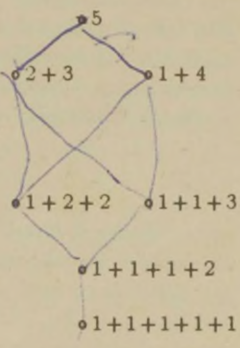
$\overline{1,n}$



$\mathcal{D}_{48}$



$\mathfrak{B}(\overline{1,3})$



$\mathcal{P}_5$

Järjestatud hulgas $\mathfrak{B}(\overline{1,3})$ on elemendid $\emptyset$ ja $\{1,2,3\}$ vastavalt vähim ja suurim: iga $\mathcal{M} \in \mathfrak{B}(\overline{1,3})$ korral $\emptyset \leqslant \mathcal{M} \leqslant \{1,2,3\}$. Üldiselt nimetataksegi o-hulga $\mathcal{X}$ elementi $\mathbf{0}$ *vähimaks elemendiks* siis, kui iga $x \in \mathcal{X}$ korral $\mathbf{0} \leqslant x$. Vähimat elementi katvaid elemente nimetatakse *aatomeiks*. Elementi $\mathbf{1} \in \mathcal{X}$ nimetatakse o-hulga $\mathcal{X}$ *suurimaks elemendiks* siis, kui iga $x \in \mathcal{X}$ korral $x \leqslant \mathbf{1}$. Üle ühe vähima elemendi ning üle ühe suurima elemendi o-hulgas leiduda ei saa. Selliseid tõkkeid ei tarvitse aga o-hulgal alati olla – näites (1) vaadeldud o-hulgas pole olemas ei suurimat ega ka vähimat elementi. Isegi lõplikel o-hulkadel ei pruugi tõkkeid olla: o-hulgas $\mathfrak{B}(\overline{1,3})\backslash\emptyset$ puudub vähim element ning o-hulgas $\mathfrak{B}(\overline{1,3})\backslash\{1,2,3\}$ suurim element.

Öeldakse, et element m on *minimaalne* hulgas $\mathcal{X}$, kui see hulk ei sisalda elemendile m rangelt eelnevaid elemente. Element M on *maksimaalne* hulgas $\mathcal{X}$, kui selles hulgas pole elemendile M rangelt järgnevaid elemente. Ilmselt iga lõplik o-hulk sisaldab nii minimaalse kui ka maksimaalse elemendi, kuid juba lõplikkudel o-hulkadel võib olla mitu minimaalset elementi (näiteks elemendid $\{1\}$, $\{2\}$ ja $\{3\}$ o-hulgas $\mathfrak{B}(\overline{1,3})\backslash\emptyset$) ja analoogiliselt ka mitu maksimaalset elementi.

Paneme tähele, et o-hulga $\mathcal{X}$ iga alamhulk $\mathcal{H}$ on sama järjestuse suhtes samuti o-hulk. Kui elemendid $a, b \in \mathcal{X}$ on fikseeritud, kusjuures $a \leqslant b$, siis alamhulka $[a,b] = \{x \in \mathcal{X} : a \leqslant x \leqslant b\}$ nimetatakse *lõiguks* o-hulgas $\mathcal{X}$. Järjestatud hulki, mille kõik lõigud on lõplikud, nimetatakse *lokaalselt lõplikeks o-hulkadeks*. Sellised on muidugi kõik lõplikud o-hulgad, aga ka näiteis (1) – (3) vaadeldud o-hulgad ja samuti o-hulgad $\mathfrak{B}_l(\mathcal{H})$.

Alamhulka $\mathcal{I}$ nimetatakse o-hulga $\mathcal{X}$ *ideaaliks*, kui iga $y \in \mathcal{X}$ korral sellest, et $x \in \mathcal{I}$ ja $y \leqslant x$ järeldub $y \in \mathcal{I}$. Ideaali $\mathcal{I}$ nimetatakse *peaideaaliks*, kui leidub selline $a \in \mathcal{X}$, et $\mathcal{I} = \{x \in \mathcal{X} : x \leqslant a\}$.

Kui alamhulgas $\mathcal{A} \subseteq \mathcal{X}$ iga kaks elementi $x, y \in \mathcal{M}$ osutuvad *võrreldavaiks* (s. t. alati kas $x \leqslant y$ või $y \leqslant x$), siis sellist alamhulka $\mathcal{A}$ nimetatakse *ahelaks* o-hulgas $\mathcal{X}$, erijuhul $\mathcal{A} = \mathcal{X}$ kõneldakse aga *lineaarselt järjestatud* hulgast $\mathcal{X}$. Ahela iga alamhulk on samuti ahel. Lõpliku ahela $\mathcal{A} \subseteq \mathcal{X}$ *pikkuseks* $l(\mathcal{A})$ loetakse arvu $n-1$, kus $n = |\mathcal{A}|$ ja o-hulga $\mathcal{X}$ *pikkuseks* $l(\mathcal{X})$ on ülemraja

$$\sup_{\mathcal{A} \in \mathfrak{A}} l(\mathcal{A}),$$

kus sümboliga $\mathfrak{A}$ oleme tähistanud o-hulga $\mathcal{X}$ kõikide ahelate hulga. Kui $l(\mathcal{X})$ on naturaalarv, siis räägitakse *lõpliku pikkusega hulgast* $\mathcal{X}$. Kui o-hulgas $\mathcal{X}$ leidub fikseeritud elemendipaari $a < b$ korral ahel $a = x_0 < x_1 < \cdots < x_m = b$, siis räägitakse ahelast a ja b vahel. Kui seejuures iga element x_i katab elementi x_{i-1}, siis vastavat ahelat nimetatakse *tihedaks ahelaks*.

Järjestatud hulga $(\mathcal{X};\rho)$ elemente x ja y nimetatakse *võrreldamatuteks* (ning tähistatakse $x \asymp_\rho y$ või $x \asymp y$) siis, kui $(x,y) \notin \rho$ ja $(y,x) \notin \rho$. Kui mingis alamhulgas $\mathcal{A} \subseteq \mathcal{X}$ iga kaks elementi on võrreldamatud, siis $\mathcal{A}$ on o-hulga $(\mathcal{X};\rho)$ *antiahel*.

Olgu σ-hulga $\mathcal{X}$ vähim element $\mathbf{0}$. Elemendi $x \in \mathcal{X}$ ***kõrguseks*** $h(x)$ nimetatakse $\mathbf{0}$ ja x vahel leiduvate ahelate pikkuste ülemraja. On selge, et $h(x) = 1$ leiab aset parajasti siis, kui x on aatom. Kui σ-hulgal $\mathcal{X}$ on suurim element $\mathbf{1}$, siis $h(\mathbf{1}) = l(\mathcal{X})$.

Funktsioon $q : \mathcal{X} \to \mathbb{Z}$ *gradueerib* σ-hulga $\mathcal{X}$, kui ta rahuldab tingimusi:

Q1. kui $x > y$, siis $g(x) > g(y)$,

Q2. kui x katab elementi y, siis $g(x) = g(y) + 1$.

Öeldakse, et σ-hulk rahuldab *Jordan-Dedekindi tingimust* ehk on *JD-hulk* siis, kui kõik tihedad ahelad iga antud elemendipaari vahel on alati ühe ja sama lõpliku pikkusega. Märkame, et σ-hulk $\mathcal{X}$, mille kõik ahelad on lõplikud ja milles leidub vähim element $\mathbf{0}$ osutub JD-hulgaks parajasti siis, kui kõrgusfunktsioon $h : \mathcal{X} \to \mathbb{Z}$ teda gradueerib. Tõepoolest, kui kõrgus h gradueerib hulga $\mathcal{X}$, siis on iga paari $x < y$ korral kõik tihedad ahelad x ja y vahel pikkusega $h(y) - h(x)$. Kui aga $\mathcal{X}$ on JD-hulk, siis iga tiheda ahela pikkus $\mathbf{0}$ ja x vahel tuleb $h(x)$, s. t. funktsiooni $h : \mathcal{X} \to \mathbb{Z}$ korral on täidetud omadus Q2. Omaduse Q1 täidetus tuleneb definitsioonist.

Edasises on vajalikud veel järgmised kolm konstruktsiooni.

Iga σ-hulka $(\mathcal{X}; \rho)$ saadab nn. *duaalne σ-hulk* $(\mathcal{X}^*; \sigma)$, kus $\mathcal{X}^*$ ühtib hulgaga $\mathcal{X}$, kuid järjestus $x\sigma y$ defineeritakse tähenduses $y\rho x$.

Antud σ-hulkade $(\mathcal{X}; \rho)$ ja $(\mathcal{Y}; \sigma)$ *korrutiseks* $\mathcal{X} \times \mathcal{Y}$ nimetatakse kõikvõimalike järjestatud paaride (x, y) σ-hulka, kus $x \in \mathcal{X}$, $y \in \mathcal{Y}$, aga järjestus $(x, y)\pi(x', y')$ tähendab, et $x\rho x'$ ja $y\sigma y'$. Analoogiliselt saab mistahes lõpliku hulga $\mathcal{I}$ korral defineerida ka σ-hulkade $\mathcal{X}_i$ korrutise, kus $i \in \mathcal{I}$.

Antud σ-hulkade $(\mathcal{X}; \rho)$ ja $(\mathcal{Y}; \sigma)$ *summaks* $\mathcal{X} + \mathcal{Y}$ nimetatakse disjunktset ühendit $\mathcal{X} \cup \mathcal{Y}$ (kui $\mathcal{X} \cap \mathcal{Y} \neq \emptyset$, siis võetakse σ-hulkade $\mathcal{X}$ ja $\mathcal{Y}$ disjunktsed koopiad), milles järjestus π defineeritakse reegliga: $x\pi y$ tähendab, et kas $\{x, y\} \subset \mathcal{X}$ ja $x\rho y$ kehtib σ-hulgas $\mathcal{X}$ või $\{x, y\} \subset \mathcal{Y}$ ja $x\sigma y$ kehtib σ-hulgas $\mathcal{Y}$. Kui üks elementidest x, y kuulub hulka $\mathcal{X}$ ja teine hulka $\mathcal{Y}$, siis loetakse need kaks elementi võrreldamatuteks.

Vaatleme nüüd σ-hulga $(\mathcal{X}; \rho)$ järjestust säilitavaid ehk *isotoonseid kujutusi* σ-hulka $(\mathcal{Y}, \sigma)$, s. t. kujutusi $f : \mathcal{X} \to \mathcal{Y}$, milles $x\rho x'$ korral ka $f(x)\sigma f(x')$. Kõigi niisuguste nn. *σ-homomorfismide* hulk $\mathcal{H}^\circ(\mathcal{X}, \mathcal{Y})$ on samuti vaadeldav σ-hulgana (vt. näide (10)). Öeldakse, et σ-hulgad $\mathcal{X}$ ja $\mathcal{Y}$ on *isomorfsed*, kui leidub järjestust säilitav bijektiivne kujutus $\mathcal{X} \to \mathcal{Y}$, mille pöördkujutus on ka järjestust säilitav. Kui $\mathcal{X}$ ja $\mathcal{Y}^*$ on isomorfsed, siis öeldakse, et $\mathcal{X}$ ja $\mathcal{Y}$ on *antiisomorfsed*. Kui σ-hulk $\mathcal{X}$ on isomorfne σ-hulgaga $\mathcal{X}^*$, siis nimetatakse σ-hulka $\mathcal{X}$ *eneseduaalseks*. Edasises kasutame elemendi x kujutise tähistusega $f(x)$ võrdväärselt ka tähistust x^f.

Sulundioperaatoriks (või ka sulundioperatsiooniks) σ-hulgal $\mathcal{X}$ nimetatakse kujutust $\Delta : \mathcal{X} \to \mathcal{X}$, millel on järgmised kolm omadust:

G1. iga $x \in \mathcal{X}$ korral $(x^\Delta)^\Delta = x^\Delta$,

G2. iga $x \in \mathcal{X}$ korral $x \leqslant x^\Delta$,

G3. kui $x \leqslant y$, siis $x^\Delta \leqslant y^\Delta$.

Elemente $x \in \mathcal{X}$ omadusega $x = x^\Delta$ nimetatakse *Δ-kinnisteks*. Alamhulga $\mathcal{H} \subset \mathcal{X}$ *Δ-sulund* $\mathcal{H}^\Delta$ defineeritakse kui tema kujutis: $\mathcal{H}^\Delta = \{x^\Delta \colon x \in \mathcal{H}\}$. Kui kogu arutluses on juttu ühest ja samast sulundioperaatorist Δ o-hulgal $\mathcal{X}$, siis võib Δ-sulundit nimetada lihtsalt *sulundiks* ja tähistada $\mathcal{H}^\Delta$ asemel sümboliga $\overline{\mathcal{H}}$. Muuhulgas on sobiv üheelemendilist hulka $\{x\}$ tähistada lihtsalt x ja tema sulundit $\overline{x}$.

Hulga *tükelduseks* nimetatakse tema esitust paarikaupa ühisosata alamhulkade (*tükkide* ehk *komponentide*) ühendina. Käesolevas jaotises huvitavad meid üksnes o-hulga ahelaikstükeldused. Triviaalne võimalus selliseks tükelduseks on alati olemas, kui võtta kõik tükid üheelemendilisteks. Milline on aga ahelate minimaalne võimalik arv sellisel tükeldusel? Kerge on mõista, et see arv ei saa olla väiksem elementide arvust vaadeldava o-hulga ükskõik millises antiahelas. Elementide maksimaalarvu o-hulga $\mathcal{X}$ antiahelas nimetatakse o-hulga *laiuseks* ja tähistatakse $w(\mathcal{X})$.

2 **Teoreem 1** (*Dilworthi teoreem*). Tükkide minimaalne võimalik arv lõpliku o-hulga ahelaikstükeldusel võrdub selle o-hulga laiusega.

Tõestus toimub induktsiooniga o-hulga $\mathcal{X}$ elementide arvu järgi. Juht $|\mathcal{X}| = 1$ on triviaalne. Olgu $\mathcal{X}$ suvaline o-hulk laiusega n. Oletame teoreemi kehtivust kõigis o-hulkades $\mathcal{Y}$, kus $|\mathcal{Y}| < |\mathcal{X}|$. Et hulga $\mathcal{X}$ ahelaikstükeldused alla n tükiga pole võimalikud, siis tuleb näidata n-tükilise ahelaikstükelduse võimalikkus. Konstrueerime selle eraldi (kõiki võimalusi ammendavatel) juhtudel α) ja β):

α) leidub n-elemendiline antiahel $\mathcal{A} \subset \mathcal{X}$, mis ei sisalda ei hulga $\mathcal{X}$ kõiki minimaalseid ega ka kõiki tema maksimaalseid elemente,

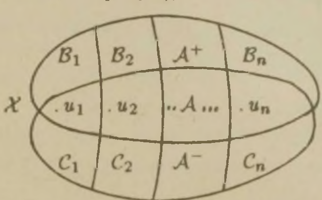
β) iga n-elemendiline antiahel kas sisaldab o-hulga $\mathcal{X}$ kõik maksimaalsed elemendid (ehk hulga $\mathcal{X}_{\max}$) või kõik minimaalsed elemendid (ehk hulga $\mathcal{X}_{\min}$).

Juhul α) defineerime hulgad

$$\mathcal{A}^+ = \{x \in \mathcal{X} : \exists u \in \mathcal{A}, x \geqslant u\} \qquad \text{ja} \qquad \mathcal{A}^- = \{y \in \mathcal{X} : \exists v \in \mathcal{A}, y \leqslant v\}.$$

Osutub, et $\mathcal{A}^+ \cap \mathcal{A}^- = \mathcal{A}$ ja $\mathcal{A}^+ \cup \mathcal{A}^- = \mathcal{X}$. Tõepoolest, definitsioonidest nähtuvad $\mathcal{A} \subset \mathcal{A}^+ \cap \mathcal{A}^-$ ja $\mathcal{A}^+ \cup \mathcal{A}^- \subset \mathcal{X}$. Kui seejuures eksisteeriks element $x \in \mathcal{A}^+ \cap \mathcal{A}^-$ nii, et $x \notin \mathcal{A}$, siis leiduksid $u \in \mathcal{A}$ ja $v \in \mathcal{A}$ nii, et $u < x < v$ ehk $u < v$, kuigi $\mathcal{A}$ iga kaks elementi peaksid olema võrreldamatud. Tingimust $x \notin \mathcal{A}^+ \cup \mathcal{A}^-$ rahuldava elemendi $x \in \mathcal{X}$ olemasolu korral oleks see element võrreldamatu $\mathcal{A}$ kõigi elementidega. Seega $\{x\} \cup \mathcal{A}$ oleks antiahel, mis räägib vastu $\mathcal{A}$ maksimaalsusele.

Et $\mathcal{A}^+ \neq \mathcal{X} \neq \mathcal{A}^-$ (järeldub tingimusest α)) ja $w(\mathcal{A}^+) = n = w(\mathcal{A}^-)$ (konstruktsiooni põhjal), siis tuleneb indukstiooni oletusest, et leiduvad tükeldused



$$\mathcal{A}^+ = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_n \quad \text{ja} \quad \mathcal{A}^- = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_n,$$

kusjuures kõigis ahelais $\mathcal{B}_i$ ja $\mathcal{C}_j$ võib sisalduda (ja ka peab sisalduma) täpselt üks element antiahelast $\mathcal{A}$. Seetõttu võime lugeda, et antiahela $\mathcal{A} = \{u_1, u_2, \ldots, u_n\}$ elemendid on nummerdatud kooskõlas nende kuuluvusega ahelaisse $\mathcal{B}_i$ ja ahelad C_j nummerdame vajaduse korral ümber kooskõlas elementide u_j kuuluvusega neisse. Nii saavutame, et tükid B_i ja C_i sisaldavad üht ja sedasama elementi $u_i \in \mathcal{A}$.

Vaatleme nüüd hulkasid $B_1 \cup C_1, \ldots, B_n \cup C_n$ ja näitame, et kõik need hulgad on ahelad, s. t. iga kaks elementi x ja y hulgast $B_i \cup C_i$ on võrreldavad. Tõepoolest, et B_i ja C_i on ahelad, siis võime vaadelda vaid juhtu $x \in B_i$ ja $y \in C_i$, mis aga $B_i \subset \mathcal{A}^+$, $C_i \subset \mathcal{A}^-$ ning $(B_i \cup C_i) \cap \mathcal{A} = \{u_i\}$ tõttu annab $x \geqslant u_i \geqslant y$, s. t. $x \geqslant y$. Hulgad $B_i \cup C_i$ katavad kogu $\mathcal{X}$, sest $\mathcal{X} = \mathcal{A}^+ \cup \mathcal{A}^- = (\bigcup_i B_i) \cup (\bigcup_i C_i) = \bigcup_i (B_i \cup C_i)$. Need hulgad $B_i \cup C_i$ on veel paarikaupa ühisosata, milles veendumiseks tuleb võrduse

$$(B_i \cup C_i) \cap (B_j \cup C_j) = (B_i \cap B_j) \cup (C_i \cap C_j) \cup (B_i \cap C_j) \cup (B_j \cap C_i)$$

tõttu vaid näidata, et $i \neq j$ korral $B_i \cap C_j = \emptyset$. See aga on tõepoolest nii, sest võrduse $B_i \cap C_j \subset \mathcal{A}^+ \cap \mathcal{A}^- = \mathcal{A}$ tõttu $B_i \cap C_j \subset B_i \cap \mathcal{A} = \{u_i\}$ ja samuti $B_i \cap C_j \subset \mathcal{A} \cap C_j = \{u_j\}$.

Kokkuvõttes on $\mathcal{X} = (B_1 \cup C_1) \cup \ldots \cup (B_n \cup C_n)$ seega soovitud tükeldus.

Juhul β) vaatleme suvalist n-elemendilist antiahelat $\mathcal{A}$, mille korral näiteks $\mathcal{X}_{\max} \subset \mathcal{A}$ (juhul $\mathcal{X}_{\min} \subset \mathcal{A}$ on arutlused analoogilised). Fikseerides mingi elemendi $b \in \mathcal{X}_{\max}$ vaatleme o-hulka $\mathcal{X}_b = \{x \in \mathcal{X} : x \leqslant b\}$ ja selles suvalist minimaalset elementi a. Siis $a \leqslant b$ ning ilmselt $a \in \mathcal{X}_{\min}$. Tähistame $\mathcal{D}_1 = \{a, b\}$ ning $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}_1$, kusjuures $\mathcal{Y} \subset \mathcal{X}$ tõttu muidugi $w(\mathcal{Y}) \leqslant w(\mathcal{X})$. Et oletus $w(\mathcal{Y}) = n$ viiks $\mathcal{X}$ jaoks siin võimatu juhu α) juurde, siis peab kehtima $w(\mathcal{Y}) \leqslant n-1$. Seejuures sisaldab antiahel $\mathcal{A} \cap \mathcal{Y}$ täpselt $n-1$ elementi, mistõttu $\mathcal{Y}$ laiuseks on $n-1$. Induktsiooni oletuse kohaselt leidub o-hulga $\mathcal{Y}$ ahelaikstükeldus $\mathcal{Y} = \mathcal{D}_2 \cup \ldots \cup \mathcal{D}_n$. Siis aga $\mathcal{X} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \ldots \cup \mathcal{D}_n$ on o-hulga $\mathcal{X}$ soovitud tükeldus.

Hoopis lihtsam on veenduda, et kehtib Dilworthi teoreemiga duaalne väide.

Teoreem 2 (*Mirsky teoreem*). Kui lõplikus o-hulgas puuduvad $(n+1)$-elemendilised ahelad, siis see o-hulk on tükeldatav n antiahelaks.

Tõestuse saame induktsiooniga n järgi. Tähistame teoreemi väidet $P(n)$. Väite $P(1)$ kehtivus on ilmne. Oletame väidete $P(2), \ldots, P(n-1)$ kehtivust ning olgu $\mathcal{X}$ selline o-hulk, milles puuduvad $(n+1)$-elemendilised ahelad. Kõigi maksimaalsete elementide alamhulk $\mathcal{X}_{\max}$ on ilmselt antiahel. Vaatleme o-hulka $\mathcal{Y} = \mathcal{X} \setminus \mathcal{X}_{\max}$ ning oletame, et ta sisaldab ahela $x_1 < x_2 < \cdots < x_n$. Vastavalt teoreemi tingimusele on see ahel maksimaalne o-hulgas $\mathcal{X}$. Sellest järelduv $x_n \in \mathcal{X}_{\max}$ on aga vastuolus tingimusega $\mathcal{Y} \cap \mathcal{X}_{\max} = \emptyset$. Seega pole hulgas $\mathcal{Y}$ n-elemendilisi ahelaid ja induktsiooni oletusest tuleneb, et $\mathcal{Y}$ tükeldub $n-1$ antiahelaks. See tükeldus koos antiahelaga $\mathcal{X}_{\max}$ annab hulga $\mathcal{X}$ soovitud tükelduse ning väide $P(n)$ on tõestatud.

Iga relatsiooni $\rho \subset \mathcal{X} \times \mathcal{Y}$ korral määrab mistahes element $x \in \mathcal{X}$ hulga $\mathcal{Y}$ alamhulga $\rho(x) = \{y \in \mathcal{Y} : (x, y) \in \rho\}$, mida nimetatakse elemendi x *ρ-naabruseks*. Hulga $\rho(x)$ elemente nimetatakse sealjuures elemendi x *ρ-naabriteks*. Üldisemalt võib rääkida ka alamhulga $\mathcal{H} \subset \mathcal{X}$ ρ-naabrusest

$$\rho(\mathcal{H}) = \bigcup_{x \in \mathcal{H}} \rho(x).$$

13

Öeldakse, et relatsioon ρ on *separaabel*, kui leidub alamrelatsioon $\mu \subset \rho$ nii, et hulga $\mathcal{X}$ igal elemendil on täpselt üks μ-naaber ja $\mathcal{X}$ erinevail elementidel pole ühiseid μ-naabreid (iga sellist relatsiooni μ nimetatakse ***kooskõlaks*** ρ suhtes).

Teoreem 3 (*P. Halli teoreem*). Lõplike ühisosata hulkade $\mathcal{X}$ ja $\mathcal{Y}$ korral on relatsioon $\rho \subset \mathcal{X} \times \mathcal{Y}$ separaabel parajasti siis, kui hulga $\mathcal{X}$ iga alamhulga $\mathcal{H}$ korral on täidetud tingimus $|\rho(\mathcal{H})| \geqslant |\mathcal{H}|$.

Tõestus. Teoreemis toodud tingimuse tarvilikkus on ilmne, sest kui ρ on separaabel, siis leidub relatsioon μ nii, et iga alamhulga $\mathcal{H} \subset \mathcal{X}$ korral

$$|\rho(\mathcal{H})| \geqslant |\mu(\mathcal{H})| = \Big| \bigcup_{x \in \mathcal{H}} \mu(x) \Big| = \sum_{x \in \mathcal{H}} |\mu(x)| = |\mathcal{H}|.$$

Piisavuse tõestamiseks märkame, et hulka $\mathcal{Z} = \mathcal{X} \cup \mathcal{Y}$ võib vaadelda o-hulgana, lugedes temas iga $z \in \mathcal{Z}$ korral $z \leqslant z$ ning $y \leqslant x$ siis, kui element $y \in \mathcal{Y}$ osutub elemendi $x \in \mathcal{X}$ ρ-naabriks. Seejuures on antiahela $\mathcal{Y}$ elementide arv o-hulga $\mathcal{Z}$ laiuseks. Tõepoolest, kui leidub antiahel $\mathcal{A} \subset \mathcal{Z}$ nii, et $|\mathcal{A}| > |\mathcal{Y}|$, siis $\rho(\mathcal{A} \cap \mathcal{X}) \subset \subset \mathcal{Y} \backslash (\mathcal{A} \cap \mathcal{Y})$, sest vastasel korral sisaldaks antiahel $\mathcal{A}$ (seose $\leqslant$ suhtes) võrreldavaid elemente. Sellest tuleneb $|\rho(\mathcal{A} \cap \mathcal{X})| \leqslant |\mathcal{Y} \backslash (\mathcal{A} \cap \mathcal{Y})|$. Samal ajal aga võrdusest $\mathcal{A} = (\mathcal{A} \cap \mathcal{X}) \cup (\mathcal{A} \cap \mathcal{Y})$ järeldub vahetult ka võrratus $|\mathcal{A}| \leqslant |\mathcal{A} \cap \mathcal{X}| + |\mathcal{A} \cap \mathcal{Y}|$ ning $|\mathcal{A}| > |\mathcal{Y}|$ tõttu $|\mathcal{Y} \backslash (\mathcal{A} \cap \mathcal{Y})| = |\mathcal{Y}| - |\mathcal{A} \cap \mathcal{Y}| \leqslant |\mathcal{Y}| - |\mathcal{A}| + |\mathcal{A} \cap \mathcal{X}| < |\mathcal{A} \cap \mathcal{X}|$. Kokkuvõttes näeme, et $|\rho(\mathcal{A} \cap \mathcal{X})| < |\mathcal{A} \cap \mathcal{X}|$, mis on vastuolus teoreemi tingimusega.

Teoreemi 1 põhjal saab o-hulga $\mathcal{Z}$ tükeldada kõige vähem $|\mathcal{Y}|$ ahelaks. Igaühes neist peab sisalduma täpselt üks element antiahelast $\mathcal{Y}$. Samal ajal ka hulga $\mathcal{X}$ iga element asub ühes neist $|\mathcal{Y}|$ ahelast, kusjuures vastavad ahelad peavad siis olema kaheelemendilised – tulenevalt seose $\leqslant$ definitsioonist ja faktist, et $\mathcal{Y}$ on antiahel. Need kahelelemendilised ahelad kõigi $x \in \mathcal{X}$ jaoks koos määravadki relatsiooni $\mu \subset \rho$.

Olgu antud hulga $\mathcal{H}$ alamhulkade mingi multihulk $\mathfrak{H} = \{\mathcal{H}_j : j \in \mathcal{J}\}$. Alamhulka $\mathcal{T} \subset \mathcal{H}$ nimetatakse multihulga $\mathfrak{H}$ *transversaaliks*, kui eksisteerib bijektsioon $\mu : \mathcal{T} \to \mathcal{J}$ nii, et iga $t \in \mathcal{T}$ korral $t \in \mathcal{H}_{\mu(t)}$.

Transversaali mõiste võimaldab anda teoreemile 3 järgmise sõnastuse.

Teoreem 3'. Lõpliku hulga $\mathcal{H}$ alamhulkade multihulgal $\mathfrak{H} = \{\mathcal{H}_j : j \in \mathcal{J}\}$ leidub transversaal parajasti siis, kui suvalise alamhulga $\mathcal{K} \subset \mathcal{J}$ korral kehtib tingimus

$$\Big| \bigcup_{j \in \mathcal{K}} \mathcal{H}_j \Big| \geqslant |\mathcal{K}|.$$

Tõepoolest, $\mathfrak{H} = \{\mathcal{H}_j : j \in \mathcal{J}\}$ määrab relatsiooni $\rho \subset \mathcal{J} \times \mathcal{H}$, kus $(j, x) \in \rho$ tähendab $x \in \mathcal{H}_j$. Seejuures $\rho(j) = \mathcal{H}_j$ ja iga $\mathcal{K} \subset \mathcal{J}$ korral $\rho(\mathcal{K}) = \bigcup_{j \in \mathcal{K}} \mathcal{H}_j$. Relatsioon ρ on separaabel, sest multihulga $\mathfrak{H}$ transversaali $\mathcal{T}$ määrava bijektsiooni μ graafik hulgas $\mathcal{J} \times \mathcal{H}$ osutub kooskõlaks ρ suhtes. Ka vastupidi, iga relatsioon $\rho \subset \mathcal{J} \times \mathcal{H}$ määrab hulga $\mathcal{H}$ alamhulkade multihulga $\mathfrak{H}$, kus $\mathcal{H}_j = \rho(j)$, $j \in \mathcal{J}$. Seejuures kooskõla määrava relatsiooni μ projektsioon hulgale $\mathcal{H}$ annab multihulga $\mathfrak{H}$ transversaali.

17. Võred

Võre mõiste toodi matemaatikasse küll juba R. Dedekindi poolt möödunud sajandi lõpul, kuid pikka aega tõlgendati seda üksnes näitena aksiomaatilisest lähenemisest. Mõiste rakenduslik väärtus hakkas täie selgusega ilmnema alles käesoleva sajandi 30. aastail (K. Menger, G. Birkhoff). Kombinatoorika paljude teooriate aluseks kujunesid võred paaril viimasel aastakümnel (G.-C. Rota ja tema koolkond).

Käesolevas jaotises defineeritakse võre kõigepealt kui teatava täiendava omadusega o-hulk, kuid seejärel näidatakse ka võimalus võre vaatlemiseks kahe operatsiooniga algebralise struktuurina. Kombinatoorikas leiavad nimelt olulist kasutamist mõlemad lähenemisviisid, kuigi näiteks mitmesuguste arvude süstematiseerimisel osutub piisavaks ainult esimene neist.

Alustame järgmisest tähelepanekust. Naturaalarvude m ja n suurim ühistegur $s = \mathrm{SÜT}(m, n)$ defineeritakse teatavasti kui naturaalarv s omadustega: $s \mid m$, $s \mid n$ ning kui leidub $k \in \mathbb{N}$ nii, et $k \mid m$ ja $k \mid n$, siis ka $k \mid s$.

Analoogiliselt defineeritakse arvude m ja n vähim ühiskordne $v = \mathrm{VÜK}(m, n)$ kui naturaalarv v omadustega: $m \mid v$, $n \mid v$ ning kui leidub $k \in \mathbb{N}$ nii, et $m \mid k$ ja $n \mid k$, siis ka $v \mid k$. Aritmeetikas tõestatakse, et naturaalarvude iga paari m, n korral leidub nii nende suurim ühistegur kui ka vähim ühiskordne.

Hulka $\mathbb{N} \setminus \{0\}$ võib teatavasti (vt. näide (3) eelmises jaotises) vaadelda o-hulgana ka siis, kui järjestus defineerida jaguvuse kaudu. Niiviisi saadud o-hulgas on suurima ühisteguri s definitsioon seega sõnastatav kujul: $s \leqslant m$, $s \leqslant n$ ning kui mingi k korral $k \leqslant m$ ja $k \leqslant n$, siis $k \leqslant s$. Teisiti öeldes: s on arvudele m ja n (vaadeldavas järjestuses!) eelnevate arvude hulgas selline, mis järgneb kõigile ülejäänutele. Analoogiliselt võib sõnastada ka vähima ühiskordse definitsiooni: v on arvudele m ja n järgnevate arvude hulgas selline, mis eelneb kõigile ülejäänutele.

Need kaheelemendilise alamhulga $\{m, n\} \subset \mathbb{N} \setminus \{0\}$ korral määratud mõisted saab kergesti üldistada igasuguse o-hulga $\mathcal{X}$ suvalise alamhulga $\mathcal{H}$ juhule.

Elementi $a \in \mathcal{X}$ nimetatakse alamhulga $\mathcal{H} \subset \mathcal{X}$ *alamtõkkeks* (ja tähistatakse $a \in \perp\mathcal{H}$), kui iga $x \in \mathcal{H}$ korral $a \leqslant x$. Ilmselt võib mõnel alamhulgal $\mathcal{H} \subset \mathcal{X}$ olla korraga mitu erinevat alamtõket, mõnel teisel alamhulgal aga ei ühtki.

Elementi $a \in \mathcal{X}$ nimetatakse alamhulga $\mathcal{H} \subset \mathcal{X}$ *alamrajaks*, kui $a \in \perp\mathcal{H}$ ning mistahes teise alamtõkke $a' \in \perp\mathcal{H}$ korral $a \geqslant a'$. Hulga $\mathcal{H}$ alamraja tähistatakse kas kujul $a = \wedge\mathcal{H}$ või kujul $a = \inf \mathcal{H}$.

Elementi $b \in \mathcal{X}$ nimetatakse alamhulga $\mathcal{H} \subset \mathcal{X}$ *ülemtõkkeks* (ja tähistatakse $b \in \top\mathcal{H}$), kui iga $x \in \mathcal{H}$ korral $b \geqslant x$. Alamhulga $\mathcal{H} \subset \mathcal{X}$ *ülemrajaks* nimetatakse hulga $\mathcal{H}$ sellist ülemtõket b, mis iga teise ülemtõkke $b' \in \top\mathcal{H}$ korral rahuldab tingimust $b \leqslant b'$. Asjaolu, et element $b \in \mathcal{X}$ osutub alamhulga $\mathcal{H} \subset \mathcal{X}$ ülemrajaks, tähistatakse kujul $b = \vee\mathcal{H}$ või $b = \sup\mathcal{H}$. Kaheelemendilise alamhulga $\mathcal{H} = \{x, y\}$ alamraja tähistatakse enamasti kujul $x \wedge y$ ning ülemraja kujul $x \vee y$, kuid samaväärsetena kasutatakse ka tähistusi $\inf\{x, y\}$ ning $\sup\{x, y\}$.

Ilmselt saab mistahes o-hulga mistahes alamhulgal olla ülimalt üks alamraja ja ülimalt üks ülemraja.

Definitsioon. *Võreks* nimetatakse järjestatud hulka, milles igal kaheelemendilisel alamhulgal on olemas nii alamraja kui ka ülemraja.

Eelmise jaotise näidetes (3), (4) ja (5) vaadeldud o-hulgad $(\mathbb{N}\setminus\{0\}; \mid)$, $(\mathcal{D}_n; \mid)$ ning $(\mathfrak{B}(\mathcal{H}); \subset)$ on võred: kahes esimeses neist tuleb lugeda $m \wedge n = \mathrm{SÜT}(m, n)$ ja $m \vee n = \mathrm{VÜK}(m, n)$, viimases aga $\mathcal{M} \wedge \mathcal{N} = \mathcal{M} \cap \mathcal{N}$ ja $\mathcal{M} \vee \mathcal{N} = \mathcal{M} \cup \mathcal{N}$.

Olulise klassi näiteid võredest annavad o-hulkadel määratud sulundioperaatorid. Nimelt kui sulundioperaatoriga Δ varustatud o-hulk $\mathcal{X}$ on tõlgendatav o-hulgana $(\mathfrak{B}(\mathcal{H}); \subset)$ või selle alamhulgana, kusjuures ta koos mingite elementidega (kui hulga $\mathcal{H}$ alamhulkadega) sisaldab ka nende ühisosa ja ühendi, siis hulga $\mathcal{X}$ Δ-kinnised elemendid moodustavad võre. Tõepoolest, kui suvalise kaheelemendilise alamhulga $\{\mathcal{M}, \mathcal{N}\} \subset \mathcal{X}$ korral võime elemente $\mathcal{M}$ ja $\mathcal{N}$ lugeda hulga $\mathcal{H}$ alamhulkadeks, siis sulundioperaatori Δ omadusi kasutades nähtub alamraja ja ülemraja definitsioonidest vahetult, et $\mathcal{M} \wedge \mathcal{N} = \mathcal{M} \cap \mathcal{N}$ ja $\mathcal{M} \vee \mathcal{N} = (\mathcal{M} \cup \mathcal{N})^{\Delta}$.

Nii näiteks võib vektorruumi $\mathfrak{V}_n(\mathbb{R})$ igale (lõplikule) alamhulgale $\mathcal{H}$ selle lineaarse katte $\lambda(\mathcal{H})$, afiinse katte $\alpha(\mathcal{H})$ või kumera katte $\gamma(\mathcal{H})$ vastavusse seadmise teel defineerida kolm (ruumi $\mathfrak{V}_n(\mathbb{R})$ lõplikel alamhulkadel määratud) sulundioperaatorit ning vastavalt ülaltoodule tekib sellega kolm võret.

Teoreem 1. Igas võres $\mathcal{V}$ rahuldavad alamraja $\wedge$ ja ülemraja $\vee$ samasusi (mis langevad kokku algebraliste operatsioonide siinnimetatud omadustega):

V1.	$x \wedge x = x$,	$x \vee x = x$,	(idempotentsus)
V2.	$x \wedge y = y \wedge x$,	$x \vee y = y \vee x$,	(kommutatiivsus)
V3.	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$,	$(x \vee y) \vee z = x \vee (y \vee z)$,	(assotsiatiivsus)
V4.	$x \wedge (x \vee y) = x$,	$x \vee (x \wedge y) = x$.	(neelduvus)

Tõestuses võime piirduda üksnes vasakpoolsete võrduste kontrollimisega, sest parempoolseid saab kontrollida nn. *duaalsete arutlustega* (mis saadakse, kui esitatavas arutluses märgid $\wedge$ ja $\vee$ ning $\leqslant$ ja $\geqslant$ vastavalt teineteisega vastastikku asendada kõikjal, kus nad esinevad).

Idempotentsus järeldub järjestuse refleksiivsusest, mille kohaselt $x \leqslant x$. Kui nüüd mõne $y \in \mathcal{V}$ korral kehtib $y \leqslant x$, siis $x \geqslant y$ ja seega $x \wedge x = x$.

Kommutatiivsus järeldub alamraja definitsioonist, sest elemendid x ja y esinevad hulgas $\mathcal{H} = \{x, y\}$ sümmeetriliselt.

Assotsiatiivsus järeldub alamraja definitsioonist tulenevatest seostest

$$(x \wedge y) \wedge z \leqslant x \wedge y \leqslant x, \quad (x \wedge y) \wedge z \leqslant x \wedge y \leqslant y \quad \text{ja} \quad (x \wedge y) \wedge z \leqslant z.$$

Tõepoolest, viimased kaks nendest võrratustest annavad $(x \wedge y) \wedge z \leqslant y \wedge z$, millest esimese võrratuse tõttu järeldub $(x \wedge y) \wedge z \leqslant x \wedge (y \wedge z)$. Täiesti analoogiliselt $x \wedge (y \wedge z) \leqslant x \wedge y$ ning $x \wedge (y \wedge z) \leqslant y \wedge z \leqslant z$ annavad vastassuunalise võrratuse $x \wedge (y \wedge z) \leqslant (x \wedge y) \wedge z$. Järjestuse antisümmeetria tõttu on nende kahe võrratuse järelduseks võrdus $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

Neelduvuse näitamisel lähtume asjaolust, et alamraja definitsiooni kohaselt peab muuhulgas olema $x \wedge (x \vee y) \leqslant x$. Teiselt poolt aga $x \leqslant x$ ja $x \leqslant x \vee y$ tõttu $x \leqslant x \wedge (x \vee y)$, sest parem pool on siin ju hulga $\{x, x \vee y\}$ alamraja. Nende kahe võrratuse kokkuvõttena oleme seega saanud $x \leqslant x \wedge (x \vee y) \leqslant x$, millest tuleneb vajalik võrdus $x \wedge (x \vee y) = x$.

Teoreemist 1 järeldub muuhulgas, et iga võret võib vaadelda algebralise struktuurina, s. t. niisuguse hulgana, millel on määratud kaks binaarset algebralist operatsiooni (tähistame nende operatsioonide tehtemärke samade sümbolitega $\wedge$ ja $\vee$) selliselt, et osutuvad rahuldatuteks samasused V1 – V4.

Nii näiteks saab võret $(\mathfrak{B}(\mathcal{H}); \subset)$ vaadelda algebralise struktuurina tehetega $\cap$ ja $\cup$ vastavalt $\wedge$ ja $\vee$ osas (samasuste V1 – V4 kehtimine selles struktuuris on teada hulgateooriast). Märkame ka, et hulga $\mathcal{H}$ suvaliste alamhulkade $\mathcal{M}$ ja $\mathcal{N}$ korral on nii tingimus $\mathcal{M} \cap \mathcal{N} = \mathcal{M}$ kui ka tingimus $\mathcal{M} \cup \mathcal{N} = \mathcal{N}$ ekvivalentsed tingimusega $\mathcal{M} \subset \mathcal{N}$. Järelikult saab võres $(\mathfrak{B}(\mathcal{H}); \subset)$ tehteid $\cap$ ja $\cup$ anda üheainsa binaarse relatsiooni kaudu ja selleks relatsiooniks on järjestus $\subset$. Osutub, et analoogiline võimalus on olemas kõikides võredes.

Teoreem 2. Samasusi V1 – V4 rahuldavate binaarsete algebraliste operatsioonidega $\wedge$ ja $\vee$ varustatud hulga $\mathcal{X}$ saab muuta o-hulgaks, kui temas relatsioon $\leqslant$ defineerida kujul: $x \leqslant y$ parajasti siis, kui $x \wedge y = x$ (võrduse $x \wedge y = x$ võib asendada samaväärse võrdusega $x \vee y = y$). Nii saadud o-hulk osutub võreks, kusjuures selles võres kehtivad samasused

$$\inf\{x, y\} = x \wedge y \qquad \text{ja} \qquad \sup\{x, y\} = x \vee y.$$

Tõestuseks märkame, et võrdused $x \wedge y = x$ ja $x \vee y = y$ kehtivad samaaegselt. Tõepoolest, $x \wedge y = x$ korral $x \vee y = (x \wedge y) \vee y = y \vee (x \wedge y) = y$. Duaalse arutlusega järeldub võrdusest $x \vee y = y$ võrdus $x \wedge y = x$.

Defineerime nüüd hulgas $\mathcal{X}$ relatsiooni $\leqslant$ tähenduses: $x \leqslant y$ parajasti siis, kui kehtib võrdus $x \wedge y = x$ (või kui kehtib samaväärne võrdus $x \vee y = y$). Näitame kõigepealt, et see relatsioon on ikka järjestus.

Järjestatud hulga definitsiooni esimene tingimus O1 on antud relatsiooni korral rahuldatud, sest $x \wedge x = x$ kehtib samasuse V1 tõttu.

Tingimuse O2 rahuldatuse kontrollimiseks paneme tähele, et relatsiooni $\leqslant$ definitsiooni kohaselt $x \leqslant y$ korral $x \wedge y = x$ ja $y \leqslant x$ korral $y \wedge x = y$. Samasuse V2 tõttu aga $x \wedge y = y \wedge x$ ja seega ka $x = y$.

Tingimuse O3 kontrollimine kulgeb analoogiliselt: $x \leqslant y$ korral $x \wedge y = x$ ja $y \leqslant z$ korral $y \wedge z = y$, seega $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$ ehk a $x \leqslant z$.

Tõestame nüüd samasuse $\sup\{x, y\} = x \vee y$ (samasus $\inf\{x, y\} = x \wedge y$ saadakse duaalse arutlusega). Selleks märkame, et samasusest $x \wedge (x \vee y) = x$ tuleneb $x \leqslant x \vee y$ ning samasusest $y \wedge (y \vee x) = y$ tuleneb $y \leqslant x \vee y$, mistõttu ka $x \vee y \in \top\{x, y\}$ ehk $x \vee y \geqslant \sup\{x, y\}$. Teiselt poolt aga $z = \sup\{x, y\}$ definitsioonist tuleneb $z \geqslant x$ ning $z \geqslant y$, mistõttu $z \vee x = z$ ja $z \vee y = z$. Järelikult $z = z \vee x = (z \vee y) \vee x = z \vee (y \vee x)$ ning seega $z \geqslant y \vee x$. Et $y \vee x = x \vee y$, siis oleme saanud $z \geqslant x \vee y$ ning kokkuvõttes $x \vee y \geqslant z \geqslant x \vee y$ ehk $z = x \vee y$.

Teoreemid 1 ja 2 näitavadki, et võredest võib rääkida nii järjestuse kui ka algebraliste operatsioonide keeles. Järgnevates teoreemides on näidatud võrede mõningad olulisemad üldised omadused.

Teoreem 3. Võreoperatsioonid $\wedge$ ja $\vee$ säilitavad teoreemis 2 defineeritud järjestust selles mõttes, et kui $y \leqslant z$, siis võre $\mathcal{V}$ iga elemendi $x \in \mathcal{V}$ korral

$$x \wedge y \leqslant x \wedge z \qquad \text{ja} \qquad x \vee y \leqslant x \vee z.$$

Tõestuseks piisab ainult järelduse $x \wedge y \leqslant x \wedge z$ õigsuses veendumisest, sest teine väidetud järeldus tuletatakse duaalse arutlusega. Et $y \leqslant z$ tähendab sama, mis $y = y \wedge z$, siis teoreemi 1 põhjal saame

$$x \wedge y = (x \wedge x) \wedge (y \wedge z) = (x \wedge y) \wedge (x \wedge z),$$

millest järeldubki $x \wedge y \leqslant x \wedge z$.

Teoreem 4. Suvalises võres $\mathcal{V}$ kehtivad nn. distributiivsuse võrratused, s.t kõikide $x, y, z \in \mathcal{V}$ korral kehtib nii võrratus

$$x \wedge (y \vee z) \geqslant (x \wedge y) \vee (x \wedge z)$$

kui ka sellega duaalne võrratus

$$x \vee (y \wedge z) \leqslant (x \vee y) \wedge (x \vee z).$$

Tõestuses toetume teoreemile 3, mille kohaselt seosest $y \geqslant x \wedge y$ iga $z \in \mathcal{V}$ korral järelduvad seosed $y \vee z \geqslant (x \wedge y) \vee z \geqslant (x \wedge y) \vee (x \wedge z)$. Teiselt poolt seoste $x \geqslant x \wedge y$ ja $x \geqslant x \wedge z$ tõttu $x \geqslant (x \wedge y) \vee (x \wedge z)$. Järelikult $(x \wedge y) \vee (x \wedge z) \in \perp\{x, y \vee z\}$ ja seega $x \wedge (y \vee z) \geqslant (x \wedge y) \vee (x \wedge z)$. Duaalse võrratuse kehtivuse tõestab tooduga duaalne arutlus.

Teoreem 5. Suvalises võres $\mathcal{V}$ kehtib nn. modulaarsuse võrratus: kui $x \leqslant z$, siis iga $y \in \mathcal{V}$ korral

$$x \vee (y \wedge z) \leqslant (x \vee y) \wedge z.$$

Tõestus. Et $x \leqslant x \vee y$ ja $x \leqslant z$, siis $x \in \bot\{x \vee y, z\}$ ehk $x \leqslant (x \vee y) \wedge z$. Samuti märkame, et $y \wedge z \leqslant y \leqslant x \vee y$ ja $y \wedge z \leqslant z$ tõttu $y \wedge z \in \bot\{x \vee y, z\}$, millest $y \wedge z \leqslant (x \vee y) \wedge z$. Kokkuvõttes seega $(x \vee y) \wedge z \in \top(x, y \wedge z)$, nii et ülemraja definitsiooni kohaselt $x \vee (y \wedge z) \leqslant (x \vee y) \wedge z$.

Võre $\mathcal{V}$ *alamvõreks* nimetatakse alamhulka $\mathcal{H} \subset \mathcal{V}$, mis koos iga kahe oma elemendiga x ja y sisaldab ka elemente $\inf(x, y)$ ja $\sup(x, y)$. Näiteks, kui $\mathcal{N} \subset \mathcal{M}$, siis võre $(\mathfrak{B}(\mathcal{N}); \subset)$ osutub võre $(\mathfrak{B}(\mathcal{M}); \subset)$ alamvõreks.

Võrede $\mathcal{V}$ ja $\mathcal{W}$ ***korrutiseks*** $\mathcal{V} \times \mathcal{W}$ nimetatakse $\mathcal{V}$ ja $\mathcal{W}$ kui o-hulkade korrutist. Vahetu kontroll näitab, et võrede selline korrutis on võre, milles

$$\inf\{(x_1, y_1), (x_2, y_2)\} = (\inf\{x_1, x_2\}, \inf\{y_1, y_2\})$$

ning

$$\sup\{(x_1, y_1), (x_2, y_2)\} = (\sup\{x_1, x_2\}, \sup\{y_1, y_2\}),$$

s.t. kaheelemendilise hulga alamraja leitakse kui paaride vastavate komponentide alamrajadest moodustatud paar ning ülemraja kui vastavate komponentide ülemrajadest moodustatud paar (sealjuures mõlema paari esimene raja leitakse muidugi võre $\mathcal{V}$ ja teine võre $\mathcal{W}$ järjestuse mõttes).

Kui $\mathcal{V}$ ja $\mathcal{W}$ on võred, siis o-homomorfismi $\theta : \mathcal{V} \to \mathcal{W}$ nimetatakse *võrede homomorfismiks* juhul, kui kehtivad samasused

$$\theta(\inf\{x_1, x_2\}) = \inf\{\theta(x_1), \theta(x_2)\}$$

ja

$$\theta(\sup\{x_1, x_2\}) = \sup\{\theta(x_1), \theta(x_2)\}.$$

Märgime, et nende võrduste vasakutes pooltes inf ja sup tähistavad vastavalt alamraja ja ülemraja võres $\mathcal{V}$, paremal aga alamraja ja ülemraja võres $\mathcal{W}$.

Mittetühja alamhulka $\mathcal{I} \subset \mathcal{V}$ nimetatakse võre $\mathcal{V}$ *ideaaliks*, kui $x, y \in \mathcal{I}$ korral ka $\sup\{x, y\} \in \mathcal{I}$ ja $x \in \mathcal{I}$ ning $y \leqslant x$ korral $y \in \mathcal{I}$.

Võre $\mathcal{V}$ *duaalse ideaali* $\mathcal{I}$ mõiste defineeritakse duaalsel viisil, s.t. $x, y \in \mathcal{I}$ korral ka $\inf\{x, y\} \in \mathcal{I}$ ja $x \in \mathcal{I}$ ning $x \leqslant y$ korral $y \in \mathcal{I}$. Võres $(\mathfrak{B}(\mathcal{H}); \subset)$ kannab duaalne ideaal *filtri* nime.

Kõik toodud mõisted saab kergesti ümber sõnastada ka võres kui algebralises struktuuris antud operatsioonide $\vee$ ja $\wedge$ keeles. Nii näiteks võib võre $\mathcal{V}$ ideaali $\mathcal{I}$ defineerida kui alamhulga $\mathcal{I} \subseteq \mathcal{V}$, mis on kinnine operatsiooni $\vee$ suhtes ning mille korral kuuluvusest $x \vee y \in \mathcal{I}$ tuleneb ka $\{x, y\} \subseteq \mathcal{I}$.

Võre on *lõpliku pikkusega*, kui ta osutub lõpliku pikkusega o-hulgaks. *Poolmodulaarseks* (või ka *ülalt poolmodulaarseks*) nimetatakse lõpliku pikkusega võret $\mathcal{V}$, mis rahuldab tingimust:

PM. kui võre $\mathcal{V}$ erinevad elemendid x ja y mõlemad katavad mingit elementi $z \in \mathcal{V}$, siis element $x \vee y$ katab nii elementi x kui ka elementi y.

Teoreem 6. Iga poolmodulaarne võre rahuldab *Jordan-Dedekindi tingimust.*

Tõestus. Tähistagu $P(n)$ väidet "kui võre elementide $x < y$ jaoks leidub tihe ahel $\mathcal{X} : x = x_0 < x_1 < \cdots < x_n = y$ pikkusega n, siis iga teine tihe ahel elementide x ja y vahel on samuti pikkusega n". Märkame kõigepealt, et $P(1)$ kehtib, sest $n = 1$ korral element y katab elementi x ja teisi ahelaid elementide x ja y vahel polegi.

Näitame nüüd, et väite $P(n-1)$ kehtivusest järeldub väite $P(n)$ kehtivus. Oletame, et peale nimetatud ahela $\mathcal{X}$ pikkusega n leidub veel mingi teine tihe ahel $\mathcal{Y} : x = y_0 < y_1 < \cdots < y_m = y$, kus $m \neq n$. Siis peab olema $x_1 \neq y_1$, sest vastasel korral seoks elemente $x_1 = y_1$ ja y kaks erineva pikkusega ($n-1 \neq m-1$) tihedat ahelat, mis on vastuolus $P(n-1)$ oletatud kehtivusega. Et võre $\mathcal{V}$ rahuldab tingimust PM, siis element $z_2 = x_1 \vee y_1$ katab elemente x_1 ja y_1. Lisaks kehtib $z_2 \leqslant y$, sest $z_2 \vee y = (x_1 \vee y_1) \vee y = x_1 \vee (y_1 \vee y) = x_1 \vee y = y$. Et võre on lõpliku pikkusega, siis leidub lõplik tihe ahel $\mathcal{Z}$ elementide z_2 ja y vahel, kusjuures $l(\mathcal{Z}) = n-2$. Tõepoolest, et ahela $x_1 < \cdots < x_n = y$ pikkus on $n-1$, siis on ka ahela $(x_1, \mathcal{Z})$ ning ahela $(y_1, \mathcal{Z})$ pikkus $n-1$, millest $P(n-1)$ tõttu järeldub, et ahela $y_1 < \cdots < y_m = y$ pikkuseks tuleb samuti $n-1$, s. t. $m-1 = n-1$. Teoreem on tõestatud.

Alt poolmodulaarne on lõpliku pikkusega võre $\mathcal{V}$, mis rahuldab tingimust:

PM$'$. kui võre $\mathcal{V}$ erinevaid elemente x ja y mõlemaid katab mingi element $z \in \mathcal{V}$, siis nii element x kui ka element y katavad elementi $x \wedge y$.

Teoreemi 6 tõestuseks toodud arutlustega duaalsete arutluste abil võib veenduda, et Jordan-Dedekindi tingimus on täidetud ka igas alt poolmodulaarses võres.

Toome siinkohal ühe olulise näite. Hulgal $\mathcal{S}$ antud ekvivalentside π ja π^* korral loeme $\pi \leqslant \pi^*$ siis, kui hulga $\mathcal{S}$ kõigi elementide x ja y korral seosest $x\pi y$ järeldub alati seos $x\pi^* y$. Nii tekib hulga $\mathcal{S}$ kõigi ekvivalentside o-hulk $\mathfrak{E}(\mathcal{S})$, mis osutub võreks. Tõepoolest, relatsioon $\pi \wedge \pi^*$ (s. t. $x(\pi \wedge \pi^*)y$ parajasti siis, kui $x\pi y$ ja $x\pi^* y$) on ekvivalents ning vahetult definitsioonidest tuleneb, et $\pi \wedge \pi^* = \inf\{\pi, \pi^*\}$. Loeme $x(\pi \vee \pi^*)y$ parajasti siis, kui saab valida elementide $z_i \in \mathcal{S}$ järjendi selliselt, et $x = z_0$, $z_0 \hat{\pi} z_1, \ldots, z_{p-1} \hat{\pi} z_p$, $z_p = y$, kus $\hat{\pi}$ osas esineb kas ekvivalents π või ekvivalents π^*. Veendume nüüd, et see relatsioon $\pi \vee \pi^*$ on ikka ekvivalents.

Esiteks, et π kui ekvivalents on refleksiivne, siis kõigi $x \in \mathcal{S}$ korral kehtib $x\pi x$, mistõttu ka $x(\pi \vee \pi^*)x$ kehtib (siin loeme $z_0 = z_1 = x$ ja $\hat{\pi} = \pi$).

Teiseks, olgu $x(\pi \vee \pi^*)y$. Et relatsiooni $\pi \vee \pi^*$ defineeriva järjendi igas lülis esineb kas ekvivalents π või ekvivalents π^*, mis on sümmeetrilised, siis kehtivad ka $y = z_p$, $z_p \hat{\pi} z_{p-1}, \ldots, z_1 \hat{\pi} z_0$, $z_0 = x$, millest nähtub $y(\pi \vee \pi^*)x$ kehtivus.

Kolmandaks, relatsiooni $\pi \vee \pi^*$ transitiivsust aitab mõista järgmine skeem:

$$\underbrace{x = x_0 \;\hat{\pi}\; x_1 \;\hat{\pi}\; x_2 \;\cdots\; x_{p-1} \;\hat{\pi}\; x_p = y}_{x(\pi\vee\pi^*)y} \qquad\qquad \underbrace{y = y_0 \;\hat{\pi}\; y_1 \;\hat{\pi}\; y_2 \;\cdots\; y_{q-1} \;\hat{\pi}\; y_q = z}_{y(\pi\vee\pi^*)z}$$

$$\Downarrow \qquad\qquad\qquad\qquad\qquad\qquad \Downarrow$$

$$\underbrace{x = z_0 \;\hat{\pi}\; z_1 \;\hat{\pi}\; z_2 \;\cdots\; z_{p-1} \;\hat{\pi}\; z_p \;\hat{\pi}\; z_{p+1} \;\hat{\pi}\; z_{p+2} \;\cdots\; z_{p+q-1} \;\hat{\pi}\; z_{p+q} = z}_{x(\pi\vee\pi^*)z}$$

(skeemil on iga $i \in \overline{0,p}$ korral tähistatud $z_i = x_i$ ja iga $i \in \overline{1,q}$ korral $z_{p+i} = y_i$).

Lõpuks veendume, et $\pi \vee \pi^* = \sup\{\pi, \pi^*\}$. Seos $\pi \vee \pi^* \in \mathrm{T}\{\pi, \pi^*\}$ on ilmne. Olgu σ suvaline ekvivalents hulgal S, nii et $\pi \leqslant \sigma$ ja $\pi^* \leqslant \sigma$. Olgu ka $x(\pi \vee \pi^*)y$; siis leidub elementide $x_i \in S$ järjend nii, et $x = x_0$, $x_0\hat{\pi}x_1, \ldots, x_{p-1}\hat{\pi}x_p$, $x_p = y$. Seejuures, et igas lülis on $\hat{\pi}$ osas kas π või π^* ja need mõlemad eelnevad ekvivalentsile σ, siis kehtivad ka $x = x_0$, $x_0\sigma x_1, \ldots, x_{p-1}\sigma x_p$ ja $x_p = y$. Kuid ekvivalents σ on transitiivne, mistõttu kehtib $x\sigma y$. Järelikult ka $\pi \vee \pi^* \leqslant \sigma$. Kokkuvõttes on o-hulk $\mathfrak{E}(S)$ seega võre. Seda võret nimetame hulga S ***ekvivalentside võreks***.

Võrest $\mathfrak{E}(S)$ võib rääkida ka hulga S tükelduste keeles, sest hulgal S antud ekvivalents π määrab teatavasti hulga S tükelduse

$$\pi = \Big\{S_i : i \in \mathcal{I}_\pi;\ S_i \subset S;\ i \neq j \ \text{ korral } S_i \cap S_j = \emptyset;\ S = \bigcup_{i \in \mathcal{I}_\pi} S_i\Big\},$$

mille tükkideks S_i on parajasti π-klassid ja vastupidi. Tükelduste keeles tähendab $\pi \leqslant \pi^*$ seda, et iga π-tükk sisaldub mingis π^*-tükis. Ekvivalentsile $\pi \wedge \pi^*$ vastab tükeldus, mille annavad π-tükkide kõikvõimalikud lõiked π^*-tükkidega. Ekvivalentsile $\pi \vee \pi^*$ vastab peenim selline tükeldus τ hulgal S, et iga alamhulk, mis saadakse omavahel lõikuvate π-tüki ja π^*-tüki ühendina, sisaldub mingis τ-tükis. Võret $\mathfrak{E}(S)$ võib seetõttu nimetada ka hulga S ***tükelduste võreks***.

Vaatleme nüüd võret $\mathfrak{E}(S)$ juhul, kui hulk S on lõplik. Olgu $|S| = n$ ning tähistagu $n(\pi)$ kõigi π-tükkide arvu hulgal S. Kui ekvivalents σ katab ekvivalentsi π, siis tükelduste keeles see tähendab, et tükeldus σ on tükeldusest π saadud viimase kõigi tükkide säilitamisega peale mingi kahe π-tüki, mis ühendatakse hulga S üheks uueks σ-tükiks. Seega $n(\pi) = n(\sigma) + 1$, millest induktsiooniga saame iga $\pi \in \mathfrak{E}(S)$ kõrguse jaoks $h(\pi) = n - n(\pi)$. Võre $\mathfrak{E}(S)$ aatomeiks osutuvad tükeldused, milles kõik tükid peale ühe kaheelemendilise tüki on üheelemendilised.

Veendume, et juhul $|S| = n$ on võre $\mathfrak{E}_n = \mathfrak{E}(S)$ poolmodulaarne. Tingimuse PM kontrollimiseks olgu π, σ ja τ võre $\mathfrak{E}_n$ suvalised niisugused elemendid, et tükeldused π ja σ katavad mõlemad tükeldust τ. Olgu näiteks $\tau = \{S_1, S_2, \ldots, S_t\}$, kus $S_i \subset S$. Nüüd, et π ja σ katavad tükeldust τ, peab olema $\pi = \{S_1 \cup S_2, S_3, \ldots, S_t\}$ ja kas $\sigma = \{S_1, S_2, S_3 \cup S_4, \ldots, S_t\}$ või $\sigma = \{S_1 \cup S_3, S_2, S_4, \ldots, S_t\}$ (siin oleme konkreetsuse huvides, ilma üldisust kitsendamata lugenud, et esimesed kaks τ-tükki on ühendatud üheks π-tükiks ja järgmised kaks või siis esimene ja kolmas üheks σ-tükiks). Kui τ jaoks realiseerub esimene võimalus, siis $\pi \vee \sigma = \{\mathcal{S}_1 \cup \mathcal{S}_2, \mathcal{S}_3 \cup \mathcal{S}_4, \ldots, \mathcal{S}_t\}$, teisel juhul aga $\pi \vee \sigma = \{\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3, \ldots, \mathcal{S}_t\}$. Mõlemal juhul on vahetult näha, et tükeldus $\pi \vee \sigma$ katab tükeldusi π ja σ. Järelikult kehtib tingimus PM.

Definitsioon. Võret $\mathcal{V}$, milles on rahuldatud tingimus

M. kui $x \leqslant y$, siis $x \vee (y \wedge z) = (x \vee y) \wedge z$

nimetatakse *modulaarseks* (tingimust M nimetatakse ka modulaarsuse tingimuseks).

Modulaarsete võrede klass on (päris)alamklassiks poolmodulaarsete võrede klassis ning neid võresid saab iseloomustada kõrgusfunktsiooni termineis.

Teoreem 7 (*Dedekindi teoreem*). Modulaarses võres on kujutused

$$\Phi_a : [b, a \vee b] \to [a \wedge b, a], \quad \text{kus} \quad \Phi_a(x) = x \wedge a$$

ning

$$\Psi_b : [a \wedge b, a] \to [b, a \vee b], \quad \text{kus} \quad \Psi_b(y) = y \vee b$$

isotoonsed ja teineteise pöördkujutused, s. t. o-isomorfismid näidatud lõikude vahel.

Tõestus. Olgu elemendid x ja x' valitud lõigult $[b, a \vee b]$ nii, et $x \leqslant x'$. Teoreemi 3 põhjal siis

$$\Phi_a(x) = x \wedge a \leqslant x' \wedge a = \Phi_a(x'), \quad \text{s.t.} \quad \Phi_a(x) \leqslant \Phi_a(x').$$

Analoogiliselt, kui $y, y' \in [a \wedge b, a]$ on valitud nii, et $y \leqslant y'$, siis

$$\Psi_b(y) = y \vee b \leqslant y' \vee b = \Psi_b(y') \quad \text{s.t.} \quad \Psi_b(y) \leqslant \Psi_b(y').$$

Seega kujutused Φ_a ja Ψ_b on järjestust säilitavad. Suvalise $x \in [b, a \vee b]$ korral

$$\Psi_b(\Phi_a(x)) = (x \wedge a) \vee b = b \vee (a \wedge x) = (b \vee a) \wedge x = (a \vee b) \wedge x = x,$$

s. t. $(\Psi_b \Phi_a)(x) = x$, ehk $\Psi_b \Phi_a = 1$. Duaalselt, suvalise $y \in [a \wedge b, a]$ korral

$$\Phi_a(\Psi_b(y)) = (y \vee b) \wedge a = y \vee (b \wedge a) = y \vee (a \wedge b) = y,$$

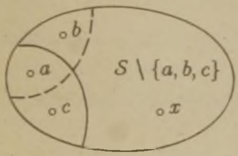
seega $(\Phi_a \Psi_b)(y) = y$ ehk $\Phi_a \Psi_b = 1$ ehk Φ_a ja Ψ_b on teineteise pöördkujutused.

Järeldus. Modulaarses võres on täidetud tingimused PM ja PM$'$.

Tõepoolest, olgu võres $\mathcal{V}$ antud elemendid $x \neq y$, mis katavad elementi $z \in \mathcal{V}$. Sel korral $z = x \wedge y$, mistõttu lõik $[x \wedge y, y]$ on o-isomorfne o-hulgaga $\{1, 2\}$. Kuid teoreemi 7 alusel on lõik $[x \wedge y, y]$ võres $\mathcal{V}$ o-isomorfne lõiguga $[x, x \vee y]$. Tulemuseks on o-isomorfism $[x, x \vee y] \cong \{1, 2\}$, mis näitab, et $x \vee y$ katab elementi x. Analoogiliselt saab veenduda, et $x \vee y$ katab ka elementi y ja seega võres $\mathcal{V}$ on täidetud tingimus PM. Duaalsete arutlustega saame näidata tingimuse PM$'$ kehtivuse võres $\mathcal{V}$.

Leiduvad poolmodulaarsed võred, mis pole modulaarsed, näiteks tükelduste võre $\mathfrak{E}(\mathcal{S})$ juhul $|\mathcal{S}| \geqslant 4$. Valides erinevad elemendid $a, b, c \in \mathcal{S}$ vaatleme tükeldusi

$$\pi = \{\{a, b\}, \mathcal{S} \setminus \{a, b\}\} \qquad \text{ja} \qquad \sigma = \{\{a, c\}, \mathcal{S} \setminus \{a, c\}\}.$$



Et iga elemendi $x \in \mathcal{S} \setminus \{a, b, c\}$ korral $x\sigma b$, $b\pi a$ ja $a\sigma c$, siis järeldame, et $\pi \vee \sigma = \mathbf{1}$. Samal ajal nähtub π ja σ definitsioonidest vahetult (vt. joonis), et

$$\pi \wedge \sigma = \{\{a\}, \{b\}, \{c\}, \mathcal{S} \setminus \{a, b, c\}\}.$$

Näeme, et tükeldus $\pi \vee \sigma$ katab tükeldusi π ja σ, kuid tükeldused π ja σ ei kata tükeldust $\pi \wedge \sigma$. Seega tingimus PM′ ei ole $n \geqslant 4$ korral võredes $\mathfrak{E}_n$ täidetud. Teoreemi 7 järeldusest tuleneb, et ekvivalentside võred $\mathfrak{E}_n$ pole $n \geqslant 4$ korral modulaarsed.

Teoreem 8. Lõpliku pikkusega võres $\mathcal{V}$, milles leidub vähim element, on ekvivalentsed järgmised tingimused:

(1) võre $\mathcal{V}$ on modulaarne;

(2) võres $\mathcal{V}$ on täidetud Jordan-Dedekindi tingimus ja kõrgusfunktsioon h selles võres rahuldab samasust

$$h(x) + h(y) = h(x \vee y) + h(x \wedge y).$$

Tõestuseks põhjendame kõigepealt implikatsiooni $(1) \Longrightarrow (2)$. Teoreemi 7 järeldusest näeme, et võre $\mathcal{V}$ on ülalt ja alt poolmodulaarne ning teoreemi 6 kohaselt rahuldab Jordan-Dedekindi tingimust. Tõestame nüüd, et tingimuse PM tõttu kehtib kõigi $x, y \in \mathcal{V}$ korral võrratus $h(x) + h(y) \geqslant h(x \vee y) + h(x \wedge y)$.

Seosest $x \wedge y \leqslant x$ ja $\mathcal{V}$ poolmodulaarsusest nähtub, et peab leiduma tihe ahel $x \wedge y = x_0 < x_1 < \cdots < x_m = x$. Analoogilisel põhjusel peab leiduma ka tihe ahel $x \wedge y = y_0 < y_1 < \cdots < y_n = y$. Ilmsetest võrdustest $x_0 \vee y_1 = y_0 \vee y_1 = y_1$, $x_1 \vee y_0 = x_1 \vee x_0 = x_1$ ja $x_0 \vee y_0 = (x \wedge y) \vee (x \wedge y) = x_0 = y_0$ näeme, et elemendid $x_0 \vee y_1$ ja $x_1 \vee y_0$ katavad elementi $x_0 \vee y_0$. Tingimusest PM tuleneb siis, et $x_1 \vee y_1 = (x_0 \vee y_1) \vee (x_1 \vee y_0)$ katab elemente $x_0 \vee y_1$ ja $x_1 \vee y_0$.

Näitame nüüd induktsiooniga $i + j$ järgi, et $x_i \vee y_j$ "ülimalt katab" elemente $x_{i-1} \vee y_j$ ja $x_i \vee y_{j-1}$ (s. t. $x_i \vee y_j$ kas katab neid elemente või võrdub nendega). Kui oletada, et elemendid $x_{i-1} \vee y_j$ ja $x_i \vee y_{j-1}$ ülimalt katavad elementi $x_{i-1} \vee y_{j-1}$, siis võrdustest $x_i \vee y_j = (x_{i-1} \vee x_i) \vee (y_j \vee y_{j-1}) = (x_{i-1} \vee y_j) \vee (x_i \vee y_{j-1})$ järeldub, et $x_i \vee y_j$ ülimalt katab elemente $x_{i-1} \vee y_j$ ja $x_i \vee y_{j-1}$. Tõepoolest, kui $x_{i-1} \vee y_j$ või $x_i \vee y_{j-1}$ ühtib elemendiga $x_{i-1} \vee y_{j-1}$, siis on see järeldus ilmne, kui aga $x_{i-1} \vee y_j$ ja $x_i \vee y_{j-1}$ katavad elementi $x_{i-1} \vee y_{j-1}$, siis tuleneb see järeldus tingimusest PM.

Võttes $i = m$ veendume, et iga $j \in \overline{1, n}$ korral element $x \vee y_j$ ülimalt katab elementi $x \vee y_{j-1}$. Seega iga niisuguse j korral $h(x \vee y_j) - h(x \vee y_{j-1}) \leqslant 1$ ja neid summeerides $h(x \vee y_n) - h(x \vee y_0) \leqslant n$ ehk $h(x \vee y) - h(x) \leqslant h(y) - h(x \wedge y)$ ehk $h(x) + h(y) \geqslant h(x \vee y) + h(x \wedge y)$.

Duaalsete arutluste tulemusel veendume, et tingimusest PM$'$ tuleneb võrratus $h(x)+h(y) \leqslant h(x\vee y)+h(x\wedge y)$, mis koos eelmisega annab, et võres $\mathcal{V}$ kehtib samasus

$$h(x) + h(y) = h(x \vee y) + h(x \wedge y).$$

Implikatsiooni (2) $\Longrightarrow$ (1) järgnev põhjendus tugineb printsiibil, et $x \leqslant y$ koos võrdusega $h(x) = h(y)$ annab vähimat elementi omavas lõpliku pikkusega võres $x = y$.

Olgu elemendid $x, y, z \in \mathcal{V}$ võetud nii, et $x \leqslant z$. Teoreemist 5 järeldame, et $x \vee (y \wedge z) \leqslant (x \vee y) \wedge z$.

Veendume, et $h(x \vee (y \wedge z)) = h((x \vee y) \wedge z)$. Tõepoolest,

$$\begin{aligned} h(x \vee (y \wedge z)) &= h(x) + h(y \wedge z) - h(x \wedge (y \wedge z)) = h(x) + h(y \wedge z) - h(x \wedge y) = \\ &= (h(x) - h(x \wedge y)) + h(y \wedge z) = h(x \vee y) - h(y) + h(y \wedge z) = \\ &= h(x \vee y) + h(z) - h(y \vee z) = h(z) + h(x \vee y) - h((x \vee y) \vee z) = \\ &= h((x \vee y) \wedge z). \end{aligned}$$

Vastavalt nimetatud printsiibile kehtib võrdus $x \vee (y \wedge z) = (x \vee y) \wedge z$. Sellega oleme tõestanud, et võres $\mathcal{V}$ on modulaarsuse tingimus täidetud.

Järgnevalt mõned näited modulaarsetest võredest.

(1) Suvalise rühma $\mathcal{G}$ normaaljagajad moodustavad modulaarse võre. Tõepoolest, vaatleme kujutust $\Delta : \mathfrak{B}(\mathcal{G}) \to \mathfrak{B}(\mathcal{G})$, mis igale alamhulgale $\mathcal{H} \subset \mathcal{G}$ seab vastavusse vähima alamhulka $\mathcal{H}$ sisaldava normaaljagaja $\mathcal{H}^{\Delta}$ rühmas $\mathcal{G}$. Kujutus Δ on sulundioperaator ning Δ-kinnised elemendid pole midagi muud kui rühma $\mathcal{G}$ normaaljagajad. Δ-kinnised elemendid (s. t. $\mathcal{G}$ normaaljagajad, nende hulka tähistame $\mathfrak{N}(\mathcal{G})$) moodustavad võre operatsioonide $\mathcal{A} \wedge \mathcal{B} = \mathcal{A} \cap \mathcal{B}$ ja $\mathcal{A} \vee \mathcal{B} = (\mathcal{A} \cup \mathcal{B})^{\Delta}$ suhtes.

Suvaliste $\mathcal{A}, \mathcal{B} \in \mathfrak{N}(\mathcal{G})$ korral $(\mathcal{A} \cup \mathcal{B})^{\Delta} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\} = \mathcal{AB}$, millest muuhulgas tuleneb $\mathcal{AB} = (\mathcal{A} \cup \mathcal{B})^{\Delta} = (\mathcal{B} \cup \mathcal{A})^{\Delta} = \mathcal{BA}$. Selle põhjendamiseks arvestame, et hulk $\mathcal{AB}$ on rühma $\mathcal{G}$ alamrühm, sest kõigi $a, a_1 \in \mathcal{A}$ ja $b, b_1 \in \mathcal{B}$ korral

$$(ab)(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} = \underbrace{aa_1^{-1}}_{\in\mathcal{A}} \cdot \underbrace{a_1 \cdot bb_1^{-1} \cdot a_1^{-1}}_{\in\mathcal{B}} \in \mathcal{AB}.$$

Kuid alamrühm $\mathcal{AB}$ on ka rühma $\mathcal{G}$ normaaljagaja, sest suvaliste $g \in \mathcal{G}$, $a \in \mathcal{A}$, $b \in \mathcal{B}$ korral $g^{-1} \cdot ab \cdot g = g^{-1}ag \cdot g^{-1}bg \in \mathcal{AB}$. Siit tuleneb $\mathcal{AB} = (\mathcal{AB})^{\Delta} \supset (\mathcal{A} \cup \mathcal{B})^{\Delta}$, kuna seos $\mathcal{AB} \supset \mathcal{A} \cup \mathcal{B}$ kehtib $a = a \cdot 1 \in \mathcal{AB}$ ja $b = 1 \cdot b \in \mathcal{AB}$ tõttu. Et normaaljagaja $(\mathcal{A} \cup \mathcal{B})^{\Delta}$ sisaldab muuhulgas ka oma elementide korrutisi, siis näeme, et $\mathcal{AB} \subset (\mathcal{A} \cup \mathcal{B})^{\Delta}$. Võrdus $(\mathcal{A} \cup \mathcal{B})^{\Delta} = \mathcal{AB}$ on põhjendatud.

Veendume nüüd võre $\mathfrak{N}(\mathcal{G})$ modulaarsuses. Olgu $\mathcal{A}, \mathcal{B}, \mathcal{C}$ rühma $\mathcal{G}$ normaaljagajad, nii et $\mathcal{A} \subset \mathcal{C}$. Teoreemist 5 tuleneb $\mathcal{A} \vee (\mathcal{B} \wedge \mathcal{C}) \subset (\mathcal{A} \vee \mathcal{B}) \wedge \mathcal{C}$. Võtame suvalise elemendi $x \in ((\mathcal{A} \cup \mathcal{B}) \cap \mathcal{C})^{\Delta}$. Et $x \in (\mathcal{A} \cup \mathcal{B})^{\Delta}$, siis leiduvad elemendid $a \in \mathcal{A}$, $b \in \mathcal{B}$, nii et $x = ab$; sealjuures $x \in \mathcal{C}$. Siit tuleneb $b = a^{-1}x \in \mathcal{AC} \subset \mathcal{C}$, s. t. $b \in \mathcal{C}$. Et ka $b \in \mathcal{B}$, siis näeme nüüd, et $b \in \mathcal{B} \cap \mathcal{C}$. Neist tähelepanekuist järeldub $x = ab \in \mathcal{A}(\mathcal{B} \cap \mathcal{C}) = (\mathcal{A} \cup (\mathcal{B} \cap \mathcal{C}))^{\Delta}$.

(2) Definitsioonidest järeldub, et modulaarse võre alamvõre on ka modulaarne. See tähelepanek võimaldab näite (1) baasil saada seeria uusi näiteid. Suvalise vektorruumi $\mathcal{V}(F)$ alamruumid moodustavad modulaarse alamvõre (aditiivse Abeli rühma) alamrühmade võres $\mathfrak{N}(\mathcal{V}(+))$. Kombinatoorika seisukohalt pakub erilist huvi järgmine erijuht. Fikseerime algarvu p ning naturaalarvud m ja n. Olgu F Galois' korpus $\mathbb{F}(p^m)$, $\mathcal{V}_n$ aga n-mõõtmeline vektorruum üle korpuse F. Ruumi $\mathcal{V}_n$ kõigi alamruumide hulk $\mathfrak{V}_n = \mathfrak{V}_n(p^m)$ on o-hulk relatsiooni $\subset$ suhtes ja ka võre, sest eksisteerivad $\mathcal{A} \wedge \mathcal{B} = \mathcal{A} \cap \mathcal{B}$ ja $\mathcal{A} \vee \mathcal{B} = (\mathcal{A} \cup \mathcal{B})^{\Delta}$. Ülalöeldust nähtub, et saadav võre $\mathfrak{V}_n$ on modulaarne.

Võret $(\mathcal{V}; \wedge, \vee)$ nimetatakse *distributiivseks*, kui lisaks samasustele V1 – V4 on võretehete $\wedge$ ja $\vee$ jaoks täidetud veel samasus

D. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

(mida nimetatakse ka distributiivsuse samasuseks). Distributiivsete võrede klass sisaldub modulaarsete võrede klassis ning sisaldab Boole'i võred alamklassina.

Distributiivse võre näiteks on hulga $\mathcal{H}$ alamhulkade võre $(\mathfrak{B}(\mathcal{H}); \cap, \cup)$, sest siin on distributiivsuse samasus täidetud samasusena $\mathcal{X} \cap (\mathcal{Y} \cup \mathcal{Z}) = (\mathcal{X} \cap \mathcal{Y}) \cup (\mathcal{X} \cap \mathcal{Z})$.

Olulise klassi näiteid distributiivsetest võredest annavad suvalise o-hulga ahelad. Selle fakti põhjendamiseks märkame kõigepealt, et ahel on võre, kuna ahelas igal kaheelemendilisel alamhulgal on olemas nii alamraja kui ülemraja. Täidetud on ka distributiivsuse samasus. Tõepoolest, olgu $\mathcal{A}$ ahel o-hulgas $\mathcal{X}$ ja elemendid $x, y, z \in \mathcal{A}$ suvalised. Kui osutub, et $x \in \top\{y, z\}$, siis $x \geqslant y \vee z$, millest $x \wedge (y \vee z) = y \vee z$. Et kehtivad veel võrdused $x \wedge y = y$ ja $x \wedge z = z$, siis saame soovitud võrduse $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Kui aga $x \notin \top\{y, z\}$, siis läbi vaadanud siin võimalikud neli juhtu ($x \leqslant y$ ja $y \leqslant z$, $x \leqslant y$ ja $y \geqslant z$, $x \leqslant z$ ja $y \leqslant z$ ning $x \leqslant z$ ja $y \leqslant z$) ning kasutanud aksioomi V4 märkame, et soovitud seos D kehtib võrdusena $x = x$.

Distributiivse võre alamvõred on distributiivsed, distributiivse võrega duaalne võre on samuti distributiivne, distributiivne on ka distributiivsete võrede korrutis.

Teoreem 9. Igas võres on distributiivsuse samasus D ekvivalentne sellega duaalse samasusega

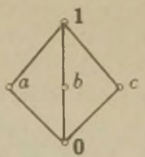
D$'$. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Tõestus. Näitame, et D $\Longrightarrow$ D$'$ (implikatsiooni D$'$ $\Longrightarrow$ D annavad toodavatega duaalsed võrdused). Tõepoolest,

$$\begin{aligned}(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) = (x \wedge (x \vee y)) \vee (z \wedge (x \vee y)) = \\ &= x \vee (z \wedge (x \vee y)) = x \vee ((z \wedge x) \vee (z \wedge y)) = \\ &= (x \vee (z \wedge x)) \vee (z \vee y) = x \vee (z \wedge y) = x \vee (y \wedge z).\end{aligned}$$

Järeldus. Iga distributiivne võre on ka modulaarne.

Tõestus. Tulenevalt teoreemist 9 piisab näidata, et D$'$ $\Longrightarrow$ M. Olgu distributiivses võres võetud suvalised elemendid x, y ja z nii, et $x \leqslant z$. Siis $z = x \vee z$, millest järeldub $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z$.



Samal ajal leiduvad modulaarsed mittedistributiivsed võred. Üks neist on oma diagrammina toodud kõrvaloleval joonisel. Vahetu kontroll näitab, et see võre on modulaarne. Tema distributiivsuse korral peaks kehtima võrdus

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

s. t. $a = \mathbf{0}$, mis on võimatu.

Teoreem 10. Distributiivses võres osutub iga a korral tõeseks implikatsioon

$$(a \wedge x = a \wedge y) \& (a \vee x = a \vee y) \Longrightarrow x = y.$$

Tõestus. Kasutades selle implikatsiooni antetsedenti moodustavaid võrdusi ning samasusi V1 – V4 ja D saame

$$x = x \vee (x \wedge a) = x \vee (y \wedge a) = (x \vee y) \wedge (x \vee a) = (x \vee y) \wedge (y \vee a) =$$
$$= (y \vee x) \wedge (y \vee a) = y \vee (x \wedge a) = y \vee (y \wedge a) = y.$$

Vaatleme võret $\mathcal{V}$, mis sisaldab suurimat ja vähimat elementi. Öeldakse, et sellise võre elemendil a leidub täiendeid, kui eksisteerib elemente $x \in \mathcal{V}$ nii, et

$$a \wedge x = \mathbf{0} \qquad \text{ja} \qquad a \vee x = \mathbf{1};$$

iga sellist elementi nimetatakse elemendi a *täiendiks*.

Teoreem 11. Suurimat ja vähimat elementi sisaldavas distributiivses võres $\mathcal{V}$ on igal elemendil ülimalt üks täiend (elemendi a ainsat täiendit on olemasolu korral loomulik tähistada a') ning täienditega elemendid moodustavad alamvõre.

Tõestus. Olgu x ja y elemendi a täiendeiks võres $\mathcal{V}$. Siis kehtivad võrdused $a \wedge x = \mathbf{0} = a \wedge y$ ja $a \vee x = \mathbf{1} = a \vee y$, millest teoreemi 10 põhjal tuleneb $x = y$.

Teise väite põhjendamiseks piisab näidata, et täiendiga elementide alamhulk võres $\mathcal{V}$ on võretehete suhtes kinnine. Olgu elementidel a ja b täiendid, s. t. leiduvad a' ja b' nii, et $a \wedge a' = \mathbf{0} = b \wedge b'$ ja $a \vee a' = \mathbf{1} = b \vee b'$. Siis märkame, et

$$(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = ((a \wedge a') \wedge b) \vee (a \wedge (b \wedge b')) = \mathbf{0}$$

ja

$$(a \wedge b) \vee (a' \vee b') = (a' \vee b') \vee (a \wedge b) = (a' \vee b' \vee a) \wedge (a' \vee b' \vee b) =$$
$$= ((a' \vee a) \vee b') \wedge (a' \vee (b' \vee b)) = \mathbf{1}$$

ning duaalselt

$$(a \vee b) \vee (a' \wedge b') = \mathbf{1} \qquad \text{ja} \qquad (a \vee b) \wedge (a' \wedge b') = \mathbf{0}.$$

Sellest nähtub, et elementidel $a \wedge b$ ja $a \vee b$ leiduvad samuti täiendid ning nendeks on vastavalt $a' \vee b'$ ja $a' \wedge b'$.

Boole'i võreks nimetatakse distributiivset võret, mis sisaldab suurimat ja vähimat elementi ning mille igal elemendil on olemas täiend. Selle klassi tuntuimaks näiteks on võre $(\mathfrak{B}(\mathcal{H}); \cap, \cup)$.

Boole'i võred on tihedalt seotud Boole'i algebratega. *Boole'i algebraks* nimetatakse hulka koos sellel antud kahe binaarse algebralise tehtega (korrutamine ($\cdot$) ja liitmine ($+$)) ning ühe unaarse algebralise tehtega (täiendi võtmine ($'$)), mis rahuldavad järgmisi samasusi ehk arvutusseadusi:

B1. $x \cdot x = x$, $\quad x + x = x$;
B2. $x \cdot y = y \cdot x$, $\quad x + y = y + x$;
B3. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\quad (x+y)+z = x+(y+z)$;
B4. $x \cdot (y + z) = x \cdot y + x \cdot z$, $\quad x+y \cdot z = (x+y) \cdot (x+z)$;
B5. $(x')' = x$,
B6. $(x \cdot y)' = x' + y'$, $\quad (x + y)' = x' \cdot y'$;
B7. $x \cdot x' + y = y$, $\quad (x + x') \cdot y = y$.

Boole'i algebra tuntuimaks näiteks on antud hulga $\mathcal{H}$ kõikide alamhulkade hulk $\mathfrak{B}(\mathcal{H})$, millel tehete $\cdot$, $+$ ja $'$ osas on vastavalt tehted $\cap$, $\cup$ ja alamhulga täiendi võtmine (hulga $\mathcal{H}$ suhtes).

Teoreem 12. Boole'i võret $(\mathcal{V}; \wedge, \vee)$ võib tõlgendada Boole'i algebrana, kui võretehteid $\wedge$ ja $\vee$ vaadelda vastavalt tehete $\cdot$ ja $+$ osas hulgal $\mathcal{V}$ ning tehteks $'$ hulgal $\mathcal{V}$ lugeda unaarset tehet, mis võre $\mathcal{V}$ igale elemendile seab vastavusse tema täiendi. Vastupidi, Boole'i algebrat $(\mathcal{V}; \cdot, +, ')$ saab tõlgendada Boole'i võrena, kui tehted $\cdot$ ja $+$ algebras $\mathcal{V}$ lugeda võreteheteks $\wedge$ ja $\vee$ hulgal $\mathcal{V}$.

Tõestus. Kui antud Boole'i võre $(\mathcal{V}; \wedge, \vee)$ korral toimida teoreemi esimeses pooles näidatud viisil, siis saame hulga $\mathcal{V}$ koos tehetega $\cdot$, $+$ ja $'$. Sealjuures tulenevalt teoreemist 1 on täidetud samasuste paarid B1 – B3. Esimene samasus B4 on uueks interpretatsiooniks (Boole'i võres kehtivale) samasusele D, teine samasus B4 aga uueks tõlgenduseks samasusele D$'$, mis kehtib võres $\mathcal{V}$ teoreemist 9 tulenevalt. Samasuste paar B5 kehtib kui uus tõlgendus võres $\mathcal{V}$ kehtivale samasusele $(x')' = x$, paar B6 on aga uueks tõlgenduseks samasustele $(x \vee y)' = x' \wedge y'$ ja $(x \wedge y)' = x' \vee y'$, mille kehtivuses me veendusime eelmist teoreemi tõestades. Samasused B7 on uueks tõlgenduseks Boole'i võres kehtivatele samasustele $(x \vee x') \wedge y = y$ ja $(x \wedge x') \vee y = y$.

Vastupidi, kui antud Boole'i algebra $(\mathcal{V}; \cdot, +, ')$ korral toimida teoreemi sõnastuse teises pooles näidatud viisil, siis saame hulga $\mathcal{V}$ koos sellel antud kahe binaarse tehtega $\wedge$ ja $\vee$, mis samasustest B1 – B3 tulenevalt rahuldavad samasusi V1 – V3. Et Boole'i algebras $\mathcal{V}$ kehtivad võrdused

$$x \cdot (x + y) = x \cdot x + x \cdot y = x + x \cdot y = x \cdot y + x = x \cdot y + x \cdot (y + y') =$$
$$= x \cdot y + (x \cdot y + x \cdot y') = (x \cdot y + x \cdot y) + x \cdot y' = x \cdot y + x \cdot y' = x \cdot (y + y') = x,$$

siis rahuldab hulk $\mathcal{V}$ koos temal antud tehetega $\wedge$ ja $\vee$ ka samasust V4 ning on teoreemist 1 tulenevalt võre. Esimese samasuse B4 uus tõlgendus näitab, et saadud võre $(\mathcal{V}; \wedge, \vee)$ on distributiivne. Samasustest B7 nähtub, et võrdused $x + x' = y + y'$ ja $x \cdot x' = y \cdot y'$ kehtivad kõigi $x, y \in \mathcal{V}$ korral. Seetõttu iga $z \in \mathcal{V}$ korral

$$(x + x') + z = (z + z') + z = (z' + z) + z = z' + (z + z) = z' + z = z + z' = x + x',$$

mis uues tõlgenduses tähendab (vt. teoreem 2), et $x + x' \geqslant z$. Analoogiliselt saame, et $x \cdot x' \leqslant z$. Siit näeme, et elemendid $\mathbf{0} = x \cdot x'$ ja $\mathbf{1} = x + x'$ on vastavalt vähimaks ja suurimaks elemendiks võres $\mathcal{V}$. Ühtlasi järeldame siit, et vaadeldavas võres on igal elemendil täiend. Kokkuvõttes näeme, et võre $(\mathcal{V}; \wedge, \vee)$ on Boole'i võre.

Toodud tõestuse esimeses osas saadud Boole'i algebrale vastav Boole'i võre langeb kokku esialgselt antud võrega ning tõestuse teises osas saadud Boole'i võrele vastav Boole'i algebra ühtib antud algebraga.

Teoreem 13 (*Stone'i teoreem*). Iga (lõplik) Boole'i algebra on isomorfne sobivalt valitud hulga kõikide alamhulkade Boole'i algebraga.

Tõestus. Tähistame antud lõpliku Boole'i algebra $\mathcal{A}$ aatomite hulga $\mathcal{H}$ ning olgu $\mathfrak{B} = \mathfrak{B}(\mathcal{H})$. Näitame, et soovitud isomorfismiks sobib kujutus $\sigma : \mathfrak{B} \to \mathcal{A}$, mis iga $\mathcal{X} \in \mathfrak{B}$ korral määratakse valemiga

$$\sigma(\mathcal{X}) = \sum_{z \in \mathcal{X}} z.$$

Suvalise $\mathbf{0} \neq x \in \mathcal{A}$ korral olgu $\mathcal{H}(x) = \{z \in \mathcal{H} : z \leqslant x\}$. Tähistame veel

$$y = \sum_{z \in \mathcal{H}(x)} z$$

ja näitame, et $x = y$. Kui $\mathcal{H}(x) = \{a_1, a_2, \ldots, a_n\}$, siis $a_1 \leqslant x$ tõttu $x = x + a_1$, millest $a_2 \leqslant x$ tõttu $x = x + a_2 = (x + a_1) + a_2 = x + a_1 + a_2$ jne. kuni lõpuks $x = x + a_1 + \cdots + a_n$ ja seega $y \leqslant x$. Kui nüüd väitevastaselt oletada, et $y < x$, siis $x = x(y + y') = xy + xy' = y + xy'$. Siinjuures $xy' \neq y$, sest muidu oleks $x = y$. Et $\mathcal{A}$ on lõplik, siis leidub aatom a nii, et $a \leqslant xy'$, kusjuures $xy' \leqslant x$ ja seega $a \in \mathcal{H}(x)$. Paneme tähele, et

$$a + \Big(a + \sum_{z \in \mathcal{H} \setminus \{a\}} z\Big) = a + \sum_{z \in \mathcal{H} \setminus \{a\}} z,$$

s. t. $a + y = y$, millest nähtub $a \leqslant y$ ja seega $ay = a \neq \mathbf{0}$. Teiselt poolt aga $a \leqslant xy'$ tõttu $a + xy' = xy'$ ehk $(a + xy')y = (xy')y$. Et $y'y = \mathbf{0}$, siis $(a + xy')y = \mathbf{0}$, s. t. oleme jõudnud vastuolulise tulemuseni $ay + (xy')y = ay = \mathbf{0}$, millest järelduvad võrdused $x = y = \sigma(\mathcal{H}(x))$ ja kujutuse σ sürjektiivsus.

Näitame nüüd, et $\sigma(\mathcal{X}) = x$ korral $\mathcal{X} = \mathcal{H}(x)$, millest $x = y$ tõttu järeldub kujutuse σ injektiivsus. Märkame esmalt, et $x = \sigma(\mathcal{X})$ tõttu on iga $z \in \mathcal{X}$ korral $z \leqslant x$ ning seega $\mathcal{X} \subseteq \mathcal{H}(x)$. Näiteks kui $\mathcal{X} = \{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\}$, siis iga aatomi $a_k \in \mathcal{H}(x)$ korral $\mathbf{0} \neq a_k = a_k x = a_k a_{i_1} + a_k a_{i_2} + \cdots + a_k a_{i_m}$, mistõttu leidub selline $j \in \overline{1, m}$, et $a_k a_{i_j} \neq \mathbf{0}$. Et aga a_k ja a_{i_j} on mõlemad aatomid, siis viimasest seosest järeldub $a_k = aa_{i_j} = a_{i_j}$, s. t. $\mathcal{H}(x) \subseteq \mathcal{X}$. Kokkuvõttes seega $\mathcal{X} = \mathcal{H}(x)$.

Teoreemi 13 tõestuse lõpetamiseks võib nüüd täiesti vahetult kontrollida, et kõigi alamhulkade $\mathcal{X}, \mathcal{X}_1, \mathcal{X}_2 \in \mathfrak{B}$ korral kehtivad seosed $\sigma(\mathcal{X}_1 \cup \mathcal{X}_2) = \sigma(\mathcal{X}_1) + \sigma(\mathcal{X}_2)$, $\sigma(\mathcal{X}_1 \cap \mathcal{X}_2) = \sigma(\mathcal{X}_1)\sigma(\mathcal{X}_2)$ ja $\sigma(\mathcal{X}') = \sigma(\mathcal{X})'$.

18. Tükelduste võrega seotud arvud

Fikseerime n-elemendilise hulga S ning vaatleme kõikvõimalikke funktsioone $f : S \to \mathcal{X}$ väärtustega lõplikus hulgas $\mathcal{X}$, kus $|\mathcal{X}| = x$. Selles funktsioonide hulgas $\mathcal{X}^S$ on x^n elementi. Iga funktsioon $f \in \mathcal{X}^S$ määrab hulgal S teatava ekvivalentsi π_f: $s \, \pi_f \, s'$ parajasti siis, kui $f(s) = f(s')$. Seda ekvivalentsi nimetatakse *funktsiooni f tuumaks* ja tähistatakse $\operatorname{Ker} f$.

Loomulik on küsida, kui paljudel erinevatel funktsioonidel $f \in \mathcal{X}^S$ on üks ja seesama tuum. Kõigepealt märkame, et tuuma π omava funktsiooni väärtuspiirkonnas on $n(\pi)$ erinevat elementi, kus eelmises jaotises defineeritud funktsioon $n(\pi)$ näitab ekvivalentsile π vastava tükelduse tükkide arvu. Tõepoolest, omandab ju selline funktsioon tervel π-tükil ühe ja sellesama väärtuse (hulgast $\mathcal{X}$). Järelikult taandub meie küsimus selliseks: kui palju leidub injektsioone $n(\pi)$-elemendilisest hulgast hulka $\mathcal{X}$? See uus küsimus lubab end sõnastada nii: kui mitmel erineval viisil saab hulgast $\mathcal{X}$ valida $n(\pi)$-elemendilist järjestatud alamhulka (mille elemendid oleks injektsiooni väärtusteks vastavalt esimesel, teisel, ..., $n(\pi)$-ndal tükil)? Vastus on meil varasemast teada – selliste valikute arvu annab kahanev faktoriaal $(x)_{n(\pi)}$.

Et iga ekvivalents π hulgal S on teatava funktsiooni $f : S \to \mathcal{X}$ tuumaks, siis saame võrduse

$$\sum_{\pi \in \mathfrak{E}_n} (x)_{n(\pi)} = x^n. \tag{18.1}$$

Teiselt poolt, et võrdus (18.1) kehtib lõpmata paljude naturaalarvude x korral, siis saab teda vaadelda kahe polünoomi võrdusena.

Belli arv (on kasutatud ka *eksponentsiaalarvu* nimetust) $B(n)$ defineeritakse kui n-elemendilise hulga erinevate ekvivalentside arv, s. t.

$$B(n) = |\mathfrak{E}_n|$$

(tähist $B(n)$ kasutame Belli arvude eristamiseks Bernoulli arvudest B_n). Leiame nende arvude mõned omadused, võttes käsitluse aluseks seose (18.1).

Kahanevate faktoriaalidena defineeritud polünoomid $p_i(x) = (x)_i$ (kus $i = 0, 1, 2, \ldots$) moodustavad ratsionaalarvuliste kordajatega polünoomide vektorruumi $\mathbb{Q}[x]$ baasi. Sellest tulenevalt defineerib iga $i = 0, 1, 2, \ldots$ korral kehtiv valem

$$F((x)_i) = 1 \tag{18.2}$$

üheselt teatava lineaarse funktsionaali $F : \mathbb{Q}[x] \to \mathbb{Q}$. Rakendanud funktsionaali F seose (18.1) mõlemale poolele ning arvestanud seejuures definitsiooni (18.2) ja $B(n)$ tähendust saame

$$B(n) = \sum_{\pi \in \mathfrak{E}_n} 1 = \sum_{\pi \in \mathfrak{E}_n} F((x)_{n(\pi)}) = F(x^n).$$

Tuginedes saadud seosele $B(n) = F(x^n)$ tuletame nüüd kõigepealt rekurrentse valemi Belli arvude jada $\{B(n)\}$ jaoks. Selleks lähtume tähelepanekust, et suvalise polünoomi $p(x) \in \mathbb{Q}[x]$ korral kehtib seos

$$F(p(x)) = F(x \cdot p(x-1)). \tag{18.3}$$

Tõepoolest, olgu

$$p(x) = \sum_{i=0}^{m} p_i\,(x)_i,$$

kus $p_i \in \mathbb{Q}$. Ühelt poolt siis

$$F(p(x)) = F\Big(\sum_{i=0}^{m} p_i\,(x)_i\Big) = \sum_{i=0}^{m} p_i\,F((x)_i) = \sum_{i=0}^{m} p_i,$$

teiselt poolt aga

$$F(x \cdot p(x-1)) = F\Big(\sum_{i=0}^{m} p_i\,x\,(x-1)_i\Big) = F\Big(\sum_{i=0}^{m} p_i\,(x)_{i+1}\Big) = \sum_{i=0}^{m} p_i.$$

Saadud tulemused on võrdsed, millest järeldubki seose (18.3) kehtivus.

Valime seoses (18.3) konkreetselt $p(x) = (x+1)^n$. Siis

$$F((x+1)^n) = F(x\,((x-1)+1)^n). \tag{18.4}$$

Võrduse (18.4) parema poole võib esitada kujul

$$F(x\,((x-1)+1)^n) = F(x^{n+1}) = B(n+1),$$

vasaku poole aga kujul

$$F((x+1)^n) = F\left(\sum_{k=0}^{n} \binom{n}{k} x^k\right) = \sum_{k=0}^{n} \binom{n}{k} F(x^k) = \sum_{k=0}^{n} \binom{n}{k} B(k),$$

millega olemegi saanud rekurrentse valemi

$$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k).$$

Leiame Belli arvude jaoks eksponentsiaalse genereeriva funktsiooni:

$$e^{Bz} = \sum_{n\geqslant 0} B(n)\frac{z^n}{n!} = \sum_{n\geqslant 0} \frac{F(x^n)}{n!}z^n = F\left(\sum_{n\geqslant 0}\frac{(zx)^n}{n!}\right) = F(e^{zx}).$$

Tähistades nüüd $e^z = 1 + y$ leiame binoomvalemit kasutades

$$F(e^{zx}) = F((1+y)^x) = F\left(\sum_{n\geqslant 0}\frac{(x)_n}{n!}y^n\right) = \sum_{n\geqslant 0}\frac{F((x)_n)}{n!}y^n = \sum_{n\geqslant 0}\frac{y^n}{n!} = e^y = e^{(e^z-1)},$$

millega saimegi soovitud tulemuse

$$e^{Bz} = \sum_{n\geqslant 0} B(n)\frac{z^n}{n!} = e^{(e^z-1)}.$$

Funktsionaali F võib toodud arutlusest elimineerida ning tema kasutamist siin tuleb vaadelda kiire vahendina kordajatevaheliste seoste saamiseks kahe (formaalse) rea võrdlemisel.

Lähedaste võtetega saab Belli arvude jaoks tuletada nn. *Dobinsky valemi*

$$B(n+1) = \frac{1}{e}\left(1^n + \frac{2^n}{1!} + \frac{3^n}{2!} + \cdots\right).$$

Selleks lähtume võrdustest

$$e = \sum_{k\geqslant 0}\frac{1}{k!} = \sum_{k\geqslant i}\frac{1}{(k-i)!} = \sum_{k\geqslant i}\frac{(k)_i}{k!},$$

millest näeme, et funktsionaal F rahuldab iga $i = 0, 1, 2, \ldots$ korral seost

$$F((x)_i) = 1 = \frac{1}{e}\sum_{k\geqslant i}\frac{(k)_i}{k!}.$$

Seetõttu suvalise polünoomi $p(x) = \sum_{i=0}^{m} p_i \cdot (x)_i$ korral

$$F(p(x)) = \sum_{i=0}^{m} p_i\left(\frac{1}{e}\sum_{k\geqslant i}\frac{(k)_i}{k!}\right) = \frac{1}{e}\left(\sum_{k\geqslant 0}\frac{1}{k!}\left(\sum_{i=0}^{m} p_i (k)_i\right)\right) = \frac{1}{e}\left(\sum_{k\geqslant 0}\frac{p(k)}{k!}\right).$$

Valides saadud võrduses konkreetselt $p(x) = (x+1)^n$ ning arvestades seost (18.4) jõuame soovitud valemini:

$$B(n+1) = F(x^{n+1}) = F((x+1)^n) = \frac{1}{e}\sum_{k\geqslant 0}\frac{(k+1)^n}{k!}.$$

Tähistagu δ_{ij} *Kroneckeri sümbolit*

$$\delta_{ij} = \begin{cases} 1, \text{ kui } i = j, \\ 0, \text{ kui } i \neq j. \end{cases}$$

Siis suvalise $i = 0, 1, 2, \ldots$ korral kehtiv valem

$$F_k(p_i(x)) = \delta_{ik}$$

defineerib iga $k = 0, 1, \ldots$ jaoks üheselt lineaarse funktsionaali $F_k : \mathbb{Q}[x] \to \mathbb{Q}$. Nende funktsionaalide definitsiooni arvestades võime n-elemendilist hulka k tükiks jaotavate ekvivalentside arvu

$$S(n,k) = |\{\pi \in \mathfrak{E}_n : n(\pi) = k\}|$$

definitsiooni üles kirjutada võrdusena

$$S(n,k) = \sum_{\substack{\pi \in \mathfrak{E}_n \\ n(\pi)=k}} 1 = F_k(x^n). \tag{18.5}$$

Märgime ühtlasi, et Belli arvude definitsioonist järeldub ilmne seos

$$B(n) = |\mathfrak{E}_n| = \sum_{k=1}^{n} S(n,k).$$

Võrdus (18.5) võimaldab selgitada arvude $S(n,k)$ omadusi. Kõigepealt veendume, et seos

$$F_k(x\,p(x)) = F_{k-1}(p(x)) + k\,F_k(p(x)) \tag{18.6}$$

on õige suvalise $p(x) \in \mathbb{Q}[x]$ korral. Funktsionaalide lineaarsuse tõttu piisab seose (18.6) kontrollimisest ruumi $\mathbb{Q}[x]$ baaspolünoomidel $p_i(x)$, s. t. tuleb näidata, et

$$F_k(x\,p_i(x)) = F_{k-1}(p_i(x)) + kF_k(p_i(x)) \tag{18.7}$$

kehtib iga $i = 0, 1, 2, \ldots$ korral. Ühelt poolt

$$\begin{aligned} F_k(x\,p_i(x)) &= F_k((x-i)\,p_i(x)) + i\,p_i(x)) = \\ &= F_k(p_{i+1}(x)) + i\,F_k(p_i(x)) = \delta_{k,i+1} + i\,\delta_{ki}, \end{aligned}$$

teiselt poolt aga võrduse (18.7) paremal poolel seisab arv $\delta_{k-1,i} + k{\cdot}\delta_{ki}$. Vaadanud läbi kolm võimalikku juhtu ($i = k$, $i = k-1$ ning $i > k$ või $i < k-1$) veendume, et võrdus $\delta_{k,i+1} + i{\cdot}\delta_{ki} = \delta_{k-1,i} + k{\cdot}\delta_{ki}$ kehtib. Valides äsjatõestatud seoses (18.6) konkreetselt $p(x) = x^n$ ja arvestades seost (18.5) saame

$$S(n+1,k) = S(n,k-1) + k\,S(n,k),$$

mis langeb kokku võrrandiga (5.10), s. t arvude $S(n,k)$ näol on nähtavasti tegemist *Stirlingi teist liiki arvudega* (ka (18.5) on samaväärne definitsiooniga (5.4)).

Tõestame veel rekurrentse seose

$$S(n+1,k)=\sum_{i=0}^{n}\binom{n}{i}S(i,k-1). \tag{18.8}$$

Märkame, et definitsioon (18.5) lubab sellele seosele anda kuju

$$F_k(x^{n+1})=\sum_{i=0}^{n}\binom{n}{i}F_{k-1}(x^i)$$

ehk

$$F_k(x\cdot((x-1)+1)^n)=F_{k-1}((x+1)^n). \tag{18.9}$$

Osutub, et suvalise $q(x)\in\mathbb{Q}[x]$ korral kehtib

$$F_k(x\cdot q(x-1))=F_{k-1}(q(x)). \tag{18.10}$$

Tõepoolest, avaldanud $q(x)$ baaspolünoomide $p_i(x)=(x)_i$ kaudu

$$q(x)=\sum_{i=0}^{m}q_i\,p_i(x),$$

kus $q_i\in\mathbb{Q}$ leiame, et nii $F_{k-1}(q(x))=q_{k-1}$ kui ka

$$F_k(x\cdot q(x-1))=F_k\Big(\sum_{i=0}^{m}q_i(x\,p_i(x-1))\Big)=F_k\Big(\sum_{i=0}^{m}q_ip_{i+1}(x)\Big)=q_{k-1},$$

millest järeldubki (18.10). Kui seoses (18.10) konkreetselt valida $q(x)=(x+1)^n$, siis veendume, et kehtib (18.9) ja seega ka (18.8).

13 Leiame nüüd jada $\{S(n,k)\}_n$ eksponentsiaalse genereeriva funktsiooni

$$S_k(z)=\sum_{n\geqslant 0}S(n,k)\frac{z^n}{n!},$$

kus k on fikseeritud. Selleks märkame, et

$$\sum_{n\geqslant 0}S(n,k)\frac{z^n}{n!}=\sum_{n\geqslant 0}F_k(x^n)\frac{z^n}{n!}=\sum_{n\geqslant 0}F_k\left(\frac{(xz)^n}{n!}\right)=F_k\left(\sum_{n\geqslant 0}\frac{(xz)^n}{n!}\right)=F_k(e^{xz}).$$

Kui tähistada $1+y=e^z$, siis $e^{xz}=(1+y)^x=\sum_{n\geqslant 0}\binom{x}{n}y^n$, mistõttu

$$F_k(e^{xz})=F_k\left(\sum_{n\geqslant 0}\binom{x}{n}y^n\right)=F_k\left(\sum_{n\geqslant 0}\frac{(x)_n}{n!}y^n\right)=$$

$$=\sum_{n\geqslant 0}\frac{F_k((x)_n)}{n!}y^n=\sum_{n\geqslant 0}\frac{\delta_{kn}}{n!}y^n=\frac{y^k}{k!}=\frac{1}{k!}(e^z-1)^k.$$

Kokkuvõttes seega näeme, et

$$S_k(z)=\frac{(e^z-1)^k}{k!},$$

mis muidugi langeb kokku varem nimetatud valemiga (6.7).

15

Stirlingi teist liiki arvude määratlus tükelduste võre kaudu võimaldab anda vahetu kombinatoorse tõestuse mitmetele tuntud valemitele, nende seas näiteks valemile

$$\sum_{k=0}^{n} \binom{n}{k} S(k,i) \cdot S(n-k,j) = \binom{i+j}{i} \cdot S(n,i+j). \tag{18.11}$$

Tõepoolest, olgu S lõplik n-elemendiline hulk. Fikseerime arvu $k \in \overline{1,n}$ ning tükeldame hulga S tükkideks S_1, S_2 nii, et $|S_1| = k, |S_2| = n-k$. Alamhulgad S_1 ja S_2 tükeldame edasi vastavalt i ja j tükiks. Et hulka S_1 saab $S(k,i)$ erineval viisil tükeldada i tükiks, hulka S_2 aga $S(n-k,j)$ erineval viisil j tükiks, siis k-elemendilise alamhulga $S_1 \subset S$ antud valiku korral (hulk $S_2 = S \setminus S_1$ on S valikuga juba üheselt määratud!) on $S(k,i) \cdot S(n-k,j)$ erinevat, vaadeldavat tüüpi tükeldust hulgal S. Kuid hulga S k-elemendilist alamhulka S_1 saab valida $\binom{n}{k}$ eri viisil, mistõttu fikseeritud k korral on hulgal S võimalik teostada $\binom{n}{k} S(k,i) \cdot S(n-k,j)$ vaadeldud tüüpi (ehk kahekordset) tükeldust. Üldse kokku on hulgal S võimalik teostada

$$\sum_{k=0}^{n} \binom{n}{k} S(k,i) \cdot S(n-k,j)$$

kahekordset tükeldust. Sellega on antud kombinatoorne interpretatsioon võrduse (18.11) vasakule poolele.

Teiselt poolt, n-elemendilise hulga S saab $S(n,i+j)$ erineval viisil tükeldada $i+j$ komponendiks ning iga sellise tükelduse korral võib saadava komponentide hulga $\binom{i+j}{i}$ eri viisil tükeldada kaheks klassiks – ühes i, teises j komponenti. Seetõttu on hulgal S võimalik teostada $\binom{i+j}{i} \cdot S(n,i+j)$ kahekordset tükeldust. On saadud kombinatoorne interpretatsioon võrduse (18.11) paremale poolele.

Et mõlemal juhul loendati ühe ja sama hulga elemente (kahekordseid tükeldusi n-elemendilisel hulgal S), siis on võrdsed ka saadud arvud, millega valem (18.11) on tõestatud.

Hulga S fikseeritud substitutsioon π lahutab selle hulga $n(\pi)$ tsükliks. Nendel tsüklitel konstantsete funktsioonide $f : S \to \mathcal{X}$ arv on seega $x^{n(\pi)}$. Iga niisugune funktsioon on aga tõlgendatav kompositsioonina $S \xrightarrow[\pi]{} S \xrightarrow[f']{} \mathcal{X}$, kus f' on kujutus hulgast S hulka $\mathcal{X}$. Et iga substitutsioon $\pi : S \to S$ määrab üheselt hulga S tükelduse tsükliteks, siis

$$\sum_{\pi} x^{n(\pi)} = \sum_{\mathfrak{C}^*_n} x^{n(\pi)},$$

kus esimene summa võetakse üle terve sümmeetrilise rühma, teises aga $\mathfrak{C}^*_n$ tähistab n-elemendilise hulga S kõikvõimalike erinevate tsükleikstükelduste hulka. Esimeses summas loendatakse iga funktsiooni $k_1! k_2! \dots k_x!$ korda, kus k_i on elemendi $i \in \mathcal{X}$ esinemiste arv selle funktsiooni väärtuste hulgas. Järjend $(k_1, k_2, \dots, k_x)$ ilmub seejuures $\binom{n}{k_1,k_2,\dots,k_x}$ korda, järelikult

$$\sum_{\pi} x^{n(\pi)} = n! \sum_{\Sigma k_i = n} 1 = x^{(n)},$$

s. t. jõuame võrduseni

$$x^{(n)} = \sum_{\pi \in \mathfrak{C}_n^*} x^{n(\pi)}. \tag{18.12}$$

Siinjuures, et hulka $\mathcal{X}$ saab valida lõpmata paljudel eri viisidel, siis (18.12) on x-polünoomide võrdus.

Võrdus (18.12) võimaldab uut viisi tõestada kaheteistkümnendas jaotises vaadeldud arvude

$$c(n,k) = |\{\pi \in \mathfrak{C}_n^* : n(\pi) = k\}|$$

omadusi (definitsioonist nähtub, et arvu $c(n,k)$ võib käsitleda kui täpselt k tsükliga n-substitutsioonide arvu). Võtame kasutusele lineaarsed funktsionaalid $G_k : \mathbb{Q}[x] \to \mathbb{Q}$, kus G_k on iga $k = 1, 2, \dots$ ja $i = 0, 1, 2, \dots$ korral defineeritud võrdusega

$$G_k(x^i) = \delta_{ki}.$$

Rakendanud funktsionaali G_k võrduse (18.12) pooltele, saame

$$G_k(x^{(n)}) = \sum_{\substack{\pi \in \mathfrak{C}_n^* \\ n(\pi) = k}} 1 = c(n,k). \tag{18.13}$$

Saadud võrdust $c(n,x) = G_k(x^{(n)})$ käsitleme kui arvude $c(n,k)$ uut definitsiooni ja tõestame rekurrentse valemi

$$c(n+1,k) = c(n,k-1) + nc(n,k). \tag{18.14}$$

Tõepoolest, vaadanud läbi kõik võimalikud juhud ($i = k$, $i = k-1$ ning $i > k$ või $i < k-1$) veendume, et vektorruumi $\mathbb{Q}[x]$ baasi $\{x^i : i = 0, 1, 2, \dots\}$ korral kehtib võrdus

$$G_k((x+n)x^i) = G_{k-1}(x^i) + n\,G_k(x^i)$$

s. t.

$$\delta_{k,i+1} + n\delta_{ki} = \delta_{k-1,i} + n\delta_{ki}.$$

Sellest järeldub, et iga polünoomi $p(x) \in \mathbb{Q}[x]$ korral kehtib seos

$$G_k((x+n)p(x)) = G_{k-1}(p(x)) + nG_k(p(x)).$$

Võtnud viimases valemis konkreetselt $p(x) = x^{(n)}$ saame

$$G_k((x+n)x^{(n)}) = G_{k-1}(x^{(n)}) + nG_k(x^{(n)})$$

ehk

$$G_k(x^{(n+1)}) = G_{k-1}(x^{(n)}) + nG_k(x^{(n)}),$$

s. t. valemi (18.14).

Seose (18.14) võib saada ka vahetu aruteluga, kui jaotada $(n+1)$-elemendilise hulga k-tsüklilised substitutsioonid kahte klassi. Leidub $c(n, k-1)$ sellist k-tsüklilist substitutsiooni, kus element $n+1$ osutub invariantseks. Kui aga see element invariantne ei ole, siis on n võimalust tema lisamiseks ülejäänud n elemendist moodustatud k-tsüklilisse substitutsiooni, kuid neid leidub $c(n, k)$ tükki.

Tükelduste võrega $\mathfrak{C}_n$ seonduvates loendamisülesannetes saab neis ettetulevate arvude genereerivaid funktsioone lihtsalt leida sobivat formaalset rida $c(x)$ ritta $e^x - 1$ superponeerides. Enne konkreetsete näidete esitamist tõestame ühe üldise tulemuse.

Olgu antud n-elemendilise hulga S k-tükeldus $\pi = \{S_1, S_2, \ldots, S_k\}$. Selle tükelduse *tüübiks* nimetatakse järjendit $(k_1, k_2, \ldots, k_n)$, mille komponentideks on mittenegatiivsed täisarvud $k_i = |\{j : |S_j| = i\}|$. Tähistame tükelduse π tüüpi edaspidi kujul $t(\pi)$, s. t. $t(\pi) \equiv (k_1, k_2, \ldots, k_n)$.

Suvalisest jadast $c = (0, c_1, c_2, \ldots)$ lähtuvalt defineerime iga $n \geqslant 1$ korral

$$b_n = \sum_{\substack{\pi \in \mathfrak{C}_n \\ t(\pi)=(k_1,\ldots,k_n)}} c_1^{k_1} c_2^{k_2} \ldots c_n^{k_n}, \tag{18.15}$$

ning võtame kasutusele eksponentsiaalsed formaalsed read

$$e^{cx} = \sum_{n\geqslant 1} c_n \frac{x^n}{n!} \quad \text{ja} \quad e^{bx} = \sum_{n \geqslant 1} b_n \frac{x^n}{n!}.$$

Teoreem. Võrdus (18.15) avaldub formaalse eksponendi E kaudu kujul

$$1 + e^{bx} = E(e^{cx}). \tag{18.16}$$

Tõestuseks märkame, et valemile (18.16) saab anda kuju $e^{bx} = (E(x) - 1) \circ e^{cx}$. Selle võrduse parem pool avaldub aga kujul

$$(E(x)-1) \circ e^{cx} = \sum_{k\geqslant 1} \frac{1}{k!} \Big[\sum_{i \geqslant 1} c_i \frac{x^i}{i!}\Big]^k = \sum_{k \geqslant 1} \frac{1}{k!} \sum_{(i_1,\ldots,i_k)} \frac{c_{i_1}}{i_1!} \cdot \frac{c_{i_2}}{i_2!} \cdot \ldots \cdot \frac{c_{i_k}}{i_k!} x^{i_1+i_2+\cdots+i_k},$$

kus sisemine summa võetakse üle kõigi järjendite $(i_1, \ldots, i_k) \in (\mathbb{N} \setminus 0)^k$. Tähistame sümboliga k_i nende kordade arvu, mil sulgude $[\ldots]^k$ avamisel valitakse $i_j = i$, siis $k = \sum_{i=1}^{n} k_i$ ning e^{bx} avaldise saab kirjutada kujul:

$$e^{bx} = \sum_{n \geqslant 1} \frac{x^n}{n!} \sum_{\Sigma i k_i = n} \frac{n! c_1^{k_1} c_2^{k_2} \ldots c_n^{k_n}}{(1!)^{k_1} (2!)^{k_2} \ldots (n!)^{k_n} \cdot k!} M(k_1, k_2, \ldots, k_n),$$

kus sisemine summeerimine toimub nüüd üle kõigi selliste mittenegatiivsete täisarvuliste komponentidega järjendite $(k_1, k_2, \dots, k_n)$, et $k_1 + 2k_2 + \dots + nk_n = n$. Ka oleme selle võrrandi iga lahendi korral summeerinud ühesugused liidetavad ning sümboliga $M(k_1, k_2, \dots, k_n)$ tähistanud niisuguste järjendite $(i_1, i_2, \dots, i_k)$ arvu, milles arvuga i võrdseid komponente on täpselt k_i tükki. Et arvud $M(k_1, k_2, \dots, k_n) = \frac{k!}{k_1!k_2!\dots k_n!}$ on multinoomkordajad, siis saame e^{bx} avaldise anda kujul

$$e^{bx} = \sum_{n\geqslant 1} \frac{x^n}{n!} \sum_{\Sigma i k_i = n} \frac{n!}{(1!)^{k_1}(2!)^{k_2}\dots(n!)^{k_n} k_1!k_2!\dots k_n!} c_1^{k_1} c_2^{k_2} \dots c_n^{k_n}.$$

Sisemises summas “monoomi” $c_1^{k_1} c_2^{k_2} \dots c_n^{k_n}$ ees olev kordaja on võrdne hulga $\overline{1,n}$ tüüpi $(k_1, k_2, \dots, k_n)$ tükelduste arvuga. Sellest nähtubki valem (18.16), kui me ka seost (18.15) silmas peame.

Kerge on kontrollida, et valemit (18.16) tõestavad arutlused jäävad kehtima ka järgmisel, kirjeldatust üldisemal juhul.

Olgu $y \in \mathbb{C}$ suvaline parameeter. Suvalisest jadast $c = (0, c_1, c_2, \dots)$ lähtuvalt võtame nüüd jada b asemele jada $b' = \{b'_n\}$, kus

$$b'_n = \sum_{\substack{\pi \in \mathfrak{E}_n \\ t(\pi) = (k_1, \dots, k_n)}} c_1^{k_1} c_2^{k_2} \dots c_n^{k_n} y^{n(\pi)}. \tag{18.17}$$

Sel korral kehtib seos

$$1 + e^{b'x} = E(ye^{cx}), \tag{18.18}$$

mille võib esitada ka kujul

$$e^{b'x} = (E(yx) - 1) \circ e^{cx}.$$

Märkame ka, et lugenud seoses (18.15) kõik $c_i \equiv 1$, saame

$$b_n = \sum_{k=1}^{n} S(n,k) y^k.$$

Sel erijuhul võtab valem (18.16) kuju

$$1 + \sum_{n\geqslant 1} \Big(\sum_{k=1}^{n} S(n,k) y^k \Big) \frac{x^n}{n!} = E(y \cdot (e^x - 1))$$

Kui edasi spetsialiseerida ka $y = 1$, siis saame

$$1 + \sum_{n\geqslant 1} B(n) \frac{x^n}{n!} = E(e^x - 1),$$

s. t. (eksponentsiaalse) genereeriva funktsiooni Belli arvudele $B(n)$.

Tähistagu b_n nende n-substitutsioonide arvu, mis astmel m annavad ühiksubstitutsiooni. Alumist rida sellise substitutsiooni standardses esituses kaherealise maatriksina võib vaadelda saaduna järgmise protseduuri teel. Kõigepealt võtame hulgal $\overline{1,n}$ mingi sellise tükelduse, kus iga tüki võimsus d on arvu m jagajaks. Valinud seejärel igal tükil ka selle elementide mingi tsüklilise paigutuse saamegi substitutsiooni, mis astmel m on ühiksubstitutsioon. Ilmselt saab d-elemendilises tükis juhul kui d on arvu m jagajaks, elementide tsüklilist paigutust valida $(d-1)!$ viisil. Valemist (18.16) saame nüüd

$$1+\sum_{n\geqslant 1} b_n \frac{x^n}{n!} = E\Big(\sum_{d\mid m}(d-1)!\frac{x^d}{d!}\Big) = E\Big(\sum_{d\mid m}\frac{x^d}{d}\Big).$$

Äsjavaadelduga mõneti sarnane on järgmine ülesanne. Hulk $\overline{1,n}$ tükeldatakse, igas tükis fikseeritakse üks elementidest (nn. juhtelement), tüki ülejäänud elementidel valitakse aga mingi tsükliline paigutus. Kui tükk on k-elemendiline, siis temal saab kirjeldatud struktuuri moodustada $k(k-2)!$ erineval viisil. Kogu hulgal $\overline{1,n}$ kirjeldatud struktuuri valikuvõimaluste üldarvu tähistame b_n. Valemist (18.16) ja formaalse logaritmi definitsioonist (9.4) tuleneb nüüd seos

$$\begin{aligned}1+\sum_{n\geqslant 1} b_n \frac{x^n}{n!} &= E\Big(\sum_{k\geqslant 2} k(k-2)!\frac{x^k}{k!}\Big) = E\Big(x\cdot\sum_{n\geqslant 1}\frac{x^n}{n}\Big) = \\ &= E\Big((-x)\cdot\sum_{n\geqslant 1}\frac{-x^n}{n}\Big) = E((-x)L(1-x)) = (1-x)^{-x}.\end{aligned}$$

Eespool kirjeldatud mõttekäike saab kasutada ka mitmesugustes graafidega seotud ülesannetes. Näiteks võime sel viisil leida n-tipuliste sidusate lihtgraafide (s. t. ilma silmuste ja kordsete servadeta graafide) arvu c_n. Tähistagu $b(n,k)$ nende n-tipuliste lihtgraafide arvu, millel on k sidususkomponenti. Sellise graafi saame, kui n-elemendiline hulk, s. t. tipuhulk $\mathcal{V}$ tükeldada k tükiks, seejärel aga igas tükis ära näidata sidusa graafi struktuur. Kui vaadeldavas tükis on sealjuures i tippu, siis vastavalt tehtud kokkuleppele on sellel tükil sidusa graafi struktuuri valikuks c_i erinevat võimalust. Öeldu lubab järeldada, et kehtib seos

$$\sum_{k\geqslant 1} b(n,k)y^k = \sum_{\substack{\pi\in\mathfrak{E}(\mathcal{V})\\ t(\pi)=(k_1,\ldots,k_n)}} c_1^{k_1}c_2^{k_2}\ldots c_n^{k_n}y^{k_1+k_2+\cdots+k_n}.$$

Valemitest (18.17) ja (18.18) nähtub nüüd, et

$$1+\sum_{n\geqslant 1}\Big(\sum_{k\geqslant 1} b(n,k)y^k\Big)\frac{x^n}{n!} = E(y\,e^{cx}).$$

Võttes viimases võrduses $y = 1$ ning arvestades $2^{\binom{n}{2}}$ erineva lihtgraafi struktuuri võimalikkust tipuhulgal $\mathcal{V}$ (selle väite õigsuses võib kergesti veenduda arutledes, kas antud tipupaar (s. t. serv) vaadeldavasse lihtgraafi kuulub või mitte), saame valemi

$$\sum_{n\geqslant 0} 2^{\binom{n}{2}} \frac{x^n}{n!} = E(e^{cx}).$$

Rõhutame, et siin on tegemist vastavate formaalsete ridade võrdsusega; rea koonduvusraadius on antud juhul isegi null!

Selle jaotuse lõpetuseks käsitleme graafide loendamise üht klassikalist ülesannet.

Olgu c_n erinevate juurega puude arv, mida saab moodustada n-elemendilisel tipuhulgal $\mathcal{V}$. Meenutame, et juurega puu on sidus, tsükliteta ning ühe väljaeraldatud tipuga (nn. juurega) lihtgraaf. Juurtega mets on aga tipuhulgal $\mathcal{V}$ antud lihtgraaf, mille sidususkomponentideks on juurega puud. Tähistagu b_n juurtega metsade üldarvu tipuhulgal $\mathcal{V}$. Valemist (18.16) järeldub antud juhul, et

$$1 + \sum_{n\geqslant 1} b_n \frac{x^n}{n!} = E\Big(\sum_{n\geqslant 1} c_n \frac{x^n}{n!}\Big). \tag{18.19}$$

Lisaks, õige on ka seos

$$b_n = \frac{c_{n+1}}{n+1}.$$

Tõepoolest, puu tipuhulgal $\mathcal{V} \cup \{w\}$ indutseerib metsa tipuhulgal $\mathcal{V}$, kui vaadeldavast puust eemaldame tipu w koos kõigi tipuga w intsidentsete servadega. Sealjuures loeme saadavas metsas kõik need tema tipud juurteks, mis algselt olid intsidentsed tipuga w. Et $(n + 1)$-tipulises puus on $n + 1$ võimalust juure valikuks, siis saamegi seose $c_{n+1} = (n + 1)b_n$. Seda seost arvestades näeme, et

$$\begin{aligned} 1 + \sum_{n\geqslant 1} b_n \frac{x^n}{n!} &= 1 + \sum_{n\geqslant 1} \frac{c_{n+1}}{n+1} \cdot \frac{x^n}{n!} = 1 + x^{-1} \sum_{n\geqslant 1} c_{n+1} \frac{x^{n+1}}{(n+1)!} = \\ &= 1 + x^{-1} \sum_{n\geqslant 2} c_n \frac{x^n}{n!} = x^{-1} \cdot \sum_{n\geqslant 1} c_n \frac{x_n}{n!}. \end{aligned}$$

Seost (18.19) kasutades saame võrduse

$$E(e^{cx}) = x^{-1} e^{cx}$$

ehk

$$e^{cx} = x\, E(e^{cx}).$$

Selle nn. *Cayley-Polya funktsionaalvõrrandi* lahendiks osutub

$$c_n = n^{n-1}.$$

16*

16

19. Alamruumide võrega seotud arvud

Fikseerime *lõpliku* ehk *Galois' korpuse* $F = \mathbb{F}(q)$ (kus $q = p^m$ ja p on algarv) ning vaatleme n-mõõtmelise vektorruumi $\mathcal{V}_n = \mathcal{V}_n(F)$ kõigi alamruumide lõplikku võret $\mathfrak{V}_n = \mathfrak{V}_n(p^m)$. Selle võre elementide koguarvu tähistame G_n, kõrgusega k elementide arvu aga sümboliga $\left[{n \atop k}\right]$. Seega

$$\left[{n \atop k}\right] = |\{\, \mathcal{W} \in \mathfrak{V}_n : \dim \mathcal{W} = k \,\}| \qquad \text{ja} \qquad G_n = |\mathfrak{V}_n| = \sum_{k=0}^{n} \left[{n \atop k}\right].$$

Arvud $\left[{n \atop k}\right]$, mida vahel tähistatakse ka $\binom{n}{k}_q$ olid arvuteoorias nn. *Gaussi polünoomidena* (või ka q-polünoomidena) tuntud ammu. Siin vaatleme neid nn. *Gaussi arvusid* $\left[{n \atop k}\right]$ ja *Galois' arvusid* G_n lineaaralgebra meetodil.

Olgu antud suvaline lõplikumõõtmeline vektorruum $\mathcal{X}$ üle korpuse F, kusjuures $x = |\mathcal{X}|$. Vaatleme kõikvõimalikke lineaarkujutusi ruumist $\mathcal{V}_n$ ruumi $\mathcal{X}$ ja leiame nende hulga $\mathcal{H}(\mathcal{X})$ võimsuse kahel erineval viisil.

Kõigepealt fikseerime ruumis $\mathcal{V}_n$ suvalise baasi $\{\bar{e}_1, \bar{e}_2 \ldots, \bar{e}_n\}$. Iga kujutus $P \in \mathcal{H}(\mathcal{X})$ on üheselt määratud oma väärtustega baasivektoreil, seega erinevaid võimalikke väärtuste komplekte kujutuse P jaoks on x^n tükki: $|\mathcal{H}(\mathcal{X})| = x^n$.

Teiselt poolt kasutame lineaarkujutuse nullruumi mõistet ja võimalust alamruumi baasi täiendamiseks kogu ruumi $\mathcal{V}_n$ baasini. Tõepoolest, olgu fikseeritud alamruum $\mathcal{W} \subseteq \mathfrak{V}_n$, kus $\dim \mathcal{W} = k$. Valime ruumis $\mathcal{V}_n$ baasi $\{\bar{e}_1, \ldots, \bar{e}_k, \bar{e}_{k+1}, \ldots, \bar{e}_n\}$ nii, et esimesed k vektorit moodustavad alamruumi $\mathcal{W}$ baasi. Valitud baasi seisukohalt tähendab lineaarkujutuse P nullruumi ühtimine alamruumiga $\mathcal{W}$ seda, et on rahuldatud järgmised kaks tingimust: (1) iga $i = 1, 2, \ldots, k$ korral $P(\bar{e}_i) = \bar{0}$ ja (2) operaator P ei kujuta ülejäänud baasivektorite $\bar{e}_{k+1}, \ldots, \bar{e}_n$ ühtki mittetriviaalset lineaarkombinatsiooni nullvektoriks. Seda arvestades saab kergesti loendada neid lineaarkujutusi $P \in \mathcal{H}(\mathcal{X})$, mille nullruumiks on alamruum $\mathcal{W}$. Selleks märkame, et P võib kujutada baasivektori $\bar{e}_{k+1}$ igaks nullist erinevaks vektoriks ruumis $\mathcal{X}$ — selliseid võimalusi on $x - 1$. Edasi võib P kujutada baasivektori $\bar{e}_{k+2}$ ruumi $\mathcal{X}$ igaks vektoriks, mis pole $P(\bar{e}_{k+1})$ kordne — niisuguseid võimalusi on $x - q$. Vektori $\bar{e}_{k+3}$ võib P kujutada ruumi $\mathcal{X}$ igaks vektoriks, mis ei asu $P(\bar{e}_{k+1})$ ja $P(\bar{e}_{k+2})$ poolt määratud F-tasandil — selliseid võimalusi on $x - q^2$. Niiviisi jätkates näeme, et võimalikke väärtuskomplekte $P(\bar{e}_{k+1}), P(\bar{e}_{k+2}), \ldots, P(\bar{e}_n)$ on

17

$$(x-1)\cdot(x-q)\cdots(x-q^{n-k-1})$$

tükki. Et ruumis $\mathcal{V}_n$ leidub $\left[{n \atop k}\right]$ k-mõõtmelist alamruumi ja iga $k = 0, 1, \ldots, n$ korral on igaüks neist teatava lineaarkujutuse $P \in \mathcal{H}(\mathcal{X})$ nullruumiks, siis

$$|\mathcal{H}(\mathcal{X})| = \sum_{k=0}^{n-1} \begin{bmatrix} n \\ k \end{bmatrix} (x-1)(x-q)\cdots(x-q^{n-k-1}) + 1.$$

Arvestades eespool saadud tulemust näeme seega, et

$$x^n = \sum_{k=0}^{n-1} \begin{bmatrix} n \\ k \end{bmatrix} (x-1)(x-q)\cdots(x-q^{n-k-1}) + 1. \tag{19.1}$$

Et seos (19.1) kehtib lõpmata paljude $x \in \mathbb{N}$ väärtuste korral (vektorruumi $\mathcal{X}$ valikut saab varieerida), siis võib seda tõlgendada kahe polünoomi võrdusena.

Tähistame $p_0(x) = 1$ ja iga $i = 1, 2, \ldots$ korral

$$p_i(x) = (x-1)(x-q)\cdots(x-q^{i-1}).$$

Et $p_i(x)$ on i-astme polünoom, siis polünoomide jada $\{p_i(x)\}$ osutub ratsionaalarvuliste kordajatega polünoomide vektorruumi $\mathbb{Q}[x]$ baasiks. Seetõttu saab iga lineaarset funktsionaali $\mathbb{Q}[x] \to \mathbb{Q}$ üheselt määrata tema väärtustega polünoomidel $p_i(x)$. Vaatleme järgnevas lineaarseid funktsionaale $L : \mathbb{Q}[x] \to \mathbb{Q}$ ja $L_k : \mathbb{Q}[x] \to \mathbb{Q}$ (kus $k = 0, 1, \ldots$), mis iga $i = 0, 1, \ldots$ korral määratakse valemitega

$$L(p_i(x)) = 1 \qquad \text{ja} \qquad L_k(p_i(x)) = \delta_{ki}.$$

Rakendades võrduse (19.1) mõlemale poolele funktsionaali L saame

$$L(x^n) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = G_n.$$

Summeerimisindeksi ja -järjekorra muutmisega võib võrdusele (19.1) anda kuju

$$x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ n-k \end{bmatrix} \cdot p_k(x),$$

mille mõlemale poolele funktsionaali L_k rakendades saame

$$L_k(x^n) = \begin{bmatrix} n \\ n-k \end{bmatrix}.$$

Galois' arvusid seob järgmine rekurrentne valem:

$$G_{n+1} = 2G_n + (q^n - 1) \cdot G_{n-1}, \tag{19.2}$$

millele seost $G_n = L(x^n)$ rakendades võib anda ka kuju

$$L(x^{n+1}) = 2L(x^n) + (q^n - 1) \cdot L(x^{n-1}). \tag{19.3}$$

Võtame nüüd kasutusele polünoomi $p(x)$ nn. *Euleri tuletise* – lineaarse operaatori $D_q : \mathbb{Q}[x] \to \mathbb{Q}[x]$, mis määratakse valemiga

$$D_q p(x) = \frac{1}{x}\Big(p(qx) - p(x)\Big).$$

Lihtne on veenduda, et iga i korral

$$D_q x^i = \frac{(qx)^i - x^i}{x} = (q^i - 1)\cdot x^{i-1} \tag{19.4}$$

ja

$$\begin{aligned} D_q p_i(x) &= \frac{1}{x}\Big((qx-1)(qx-q)\cdots(qx-q^{i-1}) - (x-1)\cdots(x-q^{i-1})\Big) = \\ &= \frac{1}{x}\Big(q^{i-1}(qx-1)\cdot p_{i-1}(x) - (x-q^{i-1})\cdot p_{i-1}(x)\Big) = (q^i-1)\cdot p_{i-1}(x). \end{aligned} \tag{19.5}$$

Kasutades võrdust (19.4), saab tõestatavale valemile (19.3) anda kuju

$$L(x\cdot x^n) = 2L(x^n) + L(D_q x^n). \tag{19.6}$$

Et $\{x^n : n \in \mathbb{N}\}$ on vektorruumi $\mathbb{Q}[x]$ baas, siis (operaatori D_q ja funktsionaali L lineaarsust kasutades) tuleneb siit, et iga $p(x) \in \mathbb{Q}[x]$ korral

$$L(x\cdot p(x)) = 2L(p(x)) + L(D_q p(x)). \tag{19.7}$$

Näitame, et see seos tõepoolest kehtib. Lähtume ühelt poolt võrdusest

$$p_{n+1}(x) + q^n\cdot p_n(x) = x\cdot p_n(x),$$

mis funktsionaali L rakendamise tulemusel annab

$$1 + q^n = L(x\cdot p_n(x)).$$

Teiselt poolt, kui võrduses (19.5) võtta $i = n$, liita mõlemale poolele $2p_{n-1}(x)$ ning rakendada funktsionaali L, siis saame

$$L(D_q p_n(x)) + 2L(p_n(x)) = q^n + 1,$$

mis koos eelmise võrdusega näitab, et

$$L(x\cdot p_n(x)) = 2L(p_n(x)) + L(D_q p_n(x)).$$

Et see võrdus kehtib ruumi $\mathbb{Q}[x]$ baasil $\{p_n(x)\}$, siis on lineaarsuse kaalutlustel õige ka (19.7), millest järeldub (19.6) ja seega osutub (19.2) tõestatuks.

19 Leiame nüüd Galois' arvude jada $\{G_n\}$ nn. *Euleri genereeriva funktsiooni*

$$G(t) = \sum_{n\geqslant 0} \frac{G_n t^n}{(1-q)(1-q^2)\cdots(1-q^n)}$$

ning näitame, et see formaalne rida on esitatav valemiga

$$G(t) = \prod_{k\geqslant 0} \frac{1}{(1-q^k t)^2}. \tag{19.8}$$

Lähtume seosest (19.7), kus $p(x)$ asendamine polünoomiga $D_q p(x)$ annab

$$L(x \cdot D_q p(x)) = 2L(D_q p(x)) + L(D_q^2 p(x)).$$

Valides nüüd konkreetselt $p(x) = x^n$ ja arvestades seoseid (19.4) leiame

$$L(x \cdot (q^n - 1)x^{n-1}) = 2L((q^n - 1)x^{n-1}) + L((q^n - 1)(q^{n-1} - 1)x^{n-2}),$$

millest funktsionaali L lineaarsuse tõttu tuleneb

$$q^n L(x^n) - L(x^n) = 2(q^n - 1)L(x^{n-1}) + (q^n - 1)(q^{n-1} - 1)L(x^{n-2})$$

ehk

$$q^n \cdot G_n = G_n - 2(1 - q^n)G_{n-1} + (1 - q^n)(1 - q^{n-1})G_{n-2}.$$

Kui nüüd viimase võrduse mõlemat poolt korrutada avaldisega

$$\frac{t^n}{(1-q)(1-q^2)\dots(1-q^n)}$$

ja summeerida üle kõigi mittenegatiivsete täisarvude n, siis saame

$$G(qt) = G(t) - 2t \cdot G(t) + t^2 \cdot G(t).$$

Sellest valemist näeme, et

$$G(t) = \frac{1}{(1-t)^2} \cdot G(qt), \quad G(qt) = \frac{1}{(1-qt)^2} \cdot G(q^2 t), \quad G(q^2 t) = \frac{1}{(1-q^2 t)^2} \cdot G(q^3 t), \ \dots,$$

kus järk-järgulised asendused viivadki valemini (19.8).

Tuletame nüüd arvude $\begin{bmatrix} n \\ k \end{bmatrix}$ mõned omadused, alustades valemist 18

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \frac{q^n - 1}{q^k - 1} \cdot \begin{bmatrix} n-1 \\ n-k \end{bmatrix}. \tag{19.9}$$

Tõestuseks veendume, et suvalise polünoomi $p(x) \in \mathbb{Q}[x]$ korral

$$(q^k - 1)L_k(p(x)) = L_{k-1}(D_q p(x)). \tag{19.10}$$

Tänu funktsionaali L_k ja operaatori D_q lineaarsusele piisab, kui seda seost kontrollida baaspolünoomide $p_i(x)$ korral, s. t. kui veenduda, et

$$(q^k - 1)L_k(p_i(x)) = L_{k-1}(D_q p_i(x)).$$

Seost (19.5) arvestades võib viimase võrduse kirjutada kujul

$$(q^k - 1) \cdot \delta_{ki} = (q^i - 1) \cdot \delta_{k-1,i-1}.$$

Vaadanud läbi võimalikud juhud $i = k$ ja $i \neq k$ veendume, et see seos tõesti kehtib, millega on põhjendatud ka (19.10), kus konkreetne valik $p(x) = x^n$ annab

$$(q^k - 1)L_k(x^n) = L_{k-1}(D_q x^n),$$

millest tulenebki (19.9). Valemit (19.9) korduvalt rakendades leiame

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \frac{q^n-1}{q^k-1}\cdot\begin{bmatrix} n-1 \\ n-k \end{bmatrix} = \frac{q^n-1}{q^k-1}\cdot\begin{bmatrix} n-1 \\ (n-1)-(k-1) \end{bmatrix} = \cdots$$

$$\cdots = \frac{q^n-1}{q^k-1}\cdot\frac{q^{n-1}-1}{q^{k-1}-1}\cdots\frac{q^{n-(k-1)}-1}{q-1}\cdot\begin{bmatrix} n-k \\ n-k \end{bmatrix}.$$

Et aga $\begin{bmatrix} n-k \\ n-k \end{bmatrix} = 1$, siis oleme saanud

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)},$$

millest muuhulgas nähtub

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$$

(kuigi see fakt tuleneb ka võre $\mathfrak{B}_n$ eneseduaalsusest). Tõepoolest, ühelt poolt

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}\cdot\frac{(q^{n-k}-1)\cdots(q-1)}{(q^{n-k}-1)\cdots(q-1)},$$

teiselt poolt aga

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-(n-k) \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{k+1}-1)}{(q^{n-k}-1)(q^{n-k-1}-1)\cdots(q-1)}\cdot\frac{(q^k-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)}.$$

Viimane tähelepanek näitab, et arvud $\begin{bmatrix} n \\ k \end{bmatrix}$ võib defineerida ka võrduste

$$\begin{bmatrix} n \\ k \end{bmatrix} = L_k(x^n) \tag{19.11}$$

abil. Seda asjaolu kasutame hiljem nende arvude mõningate täiendavate omaduste leidmisel. Lisaks on meil nüüd valem

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}. \tag{19.12}$$

Kehtib veel nn. *Pascali q-valem*

20

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + q^k\cdot\begin{bmatrix} n-1 \\ k \end{bmatrix}, \tag{19.13}$$

mille võrdus (19.11) lubab esitada kujul

$$L_k(x\cdot x^{n-1}) = L_{k-1}(x^{n-1}) + q^k L_k(x^{n-1}).$$

Osutub, et iga polünoomi $p(x) \in \mathbb{Q}[x]$ korral kehtib seos

$$L_k(x \cdot p(x)) = L_{k-1}(p(x)) + q^k L_k(p(x)),$$

milles konkreetne valik $p(x) = x^{n-1}$ annab soovitud võrduse. Tõepoolest, lineaarsuse tõttu võib seda seost kontrollida vaid baaspolünoomide $p_i(x)$ korral:

$$L_k(x \cdot p_i(x)) = L_{k-1}(p_i(x)) + q^k \cdot L_k(p_i(x))$$

ehk seost $x \cdot p_i(x) = p_{i+1}(x) + q^i \cdot p_i(x)$ arvestades

$$L_k(p_{i+1}(x)) + q^i \cdot L_k(p_i(x)) = q^k L_k(p_i(x)) + L_{k-1}(p_i(x)).$$

Funktsionaalide L_k definitsioonist nähtub, et viimane seos kujutab endast võrdust

$$\delta_{k,i+1} + q^i \cdot \delta_{ki} = q^k \cdot \delta_{ki} + \delta_{k-1,i}.$$

Vaadanud siin läbi kõik kolm võimalikku juhtu ($i = k-1$, $i = k$ ja $i > k$ või $i < k-1$) veendume, et see seos kehtib, millega on ühtlasi põhjendatud ka valem (19.13).

Tähistagu $N(k,1)$ kõigi nende k-mõõtmeliste alamruumide arvu n-mõõtmelises vektorruumis $\mathcal{V}_n(F)$ üle q-elemendilise korpuse F, mis sisaldavad ruumi $\mathcal{V}_n$ fikseeritud ühemõõtmelist alamruumi. Kehtib valem

$$N(k,1) = \begin{bmatrix} n-1 \\ n-k \end{bmatrix} = \frac{\begin{bmatrix} n \\ k \end{bmatrix} \cdot \begin{bmatrix} k \\ 1 \end{bmatrix}}{\begin{bmatrix} n \\ 1 \end{bmatrix}}. \tag{19.14}$$

Tõepoolest, olgu $\mathcal{I}$ kõnesolev ühemõõtmeline alamruum ruumis $\mathcal{V}_n$. Alamruumide võre $\mathfrak{V}_n$ eneseduaalsust kasutades märkame, et

$$N(k,1) = |\{\mathcal{W} : \mathcal{W} \subsetneq \mathfrak{V}_n, \dim \mathcal{W} = k, \mathcal{I} \subsetneq \mathcal{W}\}| =$$
$$= |\{\mathcal{W}^* : \mathcal{W}^* \subsetneq \mathfrak{V}_n, \dim \mathcal{W}^* = n-k, \mathcal{W}^* \subsetneq \mathcal{I}^*\}| = \begin{bmatrix} n-1 \\ n-k \end{bmatrix}.$$

Valemi (19.14) teise võrduse tõestamiseks võtame kasutusele (bikromaatilise) graafi $\mathcal{G}$ tipuhulgaga $\mathcal{V}(\mathcal{G}) = \mathcal{V}^{(1)} \cup \mathcal{V}^{(k)}$, kus $\mathcal{V}^{(1)}$ on ruumi $\mathcal{V}_n$ 1-mõõtmeliste alamruumide hulk ja $\mathcal{V}^{(k)}$ k-mõõtmeliste alamruumide hulk (muidugi $\mathcal{V}^{(1)} \cap \mathcal{V}^{(k)} = \emptyset$). Loeme, et paar $(\mathcal{A}, \mathcal{B}) \in \mathcal{V}^{(1)} \times \mathcal{V}^{(k)}$ on graafi $\mathcal{G}$ servaks siis, kui $\mathcal{A} \subsetneq \mathcal{B}$. Graafi $\mathcal{G}$ bikromaatilisust kasutades saab servade hulga $\mathcal{E}(\mathcal{G})$ loendada kahel erineval viisil. Tõepoolest, et iga tipu $\mathcal{B} \in \mathcal{V}^{(k)}$ valents $\rho(\mathcal{B})$ on $\left[{k \atop 1}\right]$ (s. t. ühemõõtmeliste alamruumide arv fikseeritud k-mõõtmelises alamruumis $\mathcal{B}$) ning $|\mathcal{V}^{(k)}| = \left[{n \atop k}\right]$, siis

$$|\mathcal{E}(\mathcal{G})| = \sum_{\mathcal{B} \in \mathcal{V}^{(k)}} \rho(\mathcal{B}) = \begin{bmatrix} n \\ k \end{bmatrix} \cdot \begin{bmatrix} k \\ 1 \end{bmatrix}.$$

Teiselt poolt aga iga tipu $\mathcal{A} \in \mathcal{V}^{(1)}$ valents on $N(k,1)$ ja selliseid tippe leidub $|\mathcal{V}^{(1)}| = \left[{n \atop 1}\right]$ tükki, millest

$$|\mathcal{E}(\mathcal{G})| = \sum_{\mathcal{A} \in \mathcal{V}^{(1)}} \rho(\mathcal{A}) = \begin{bmatrix} n \\ 1 \end{bmatrix} \cdot N(k,1).$$

Saadud tulemuste ühendamine annab soovitud võrduse.

22

Arvude $\left[{n \atop k}\right]$ määratlus alamruumide võre $\mathfrak{V}_n$ kaudu võimaldab kergesti tõestada ka nn. *Vandermonde'i q-valemi*, mille kohaselt suvaliste mittenegatiivsete täisarvude r, s ja k korral kehtib võrdus

$$\left[{r+s \atop k}\right] = \sum_{i=0}^{k} \left[{s \atop i}\right] \cdot \left[{r \atop k-i}\right] \cdot q^{i(r-k+i)}. \tag{19.15}$$

Tõepoolest, olgu $\mathcal{V}_{r+s}$ $(r+s)$-mõõtmeline vektorruum üle Galois' korpuse $\mathbb{F}(q)$ ning $\mathcal{V}_r$ selle ruumi mingi r-mõõtmeline alamruum, mille fikseerime kogu järgnevaks arutluseks. Asjaolu, et võrduse (19.15) vasak pool näitab ruumi $\mathcal{V}_{r+s}$ kõigi k-mõõtmeliste alamruumide arvu, viib mõttele interpreteerida samas vaimus ka võrduse (19.15) paremat poolt. Selleks vaatleme iga $i = 0, 1, \ldots, k$ korral ruumi $\mathcal{V}_{r+s}$ kõigi selliste k-mõõtmeliste alamruumide $\mathcal{W}$ hulka $\mathfrak{W}_i$, mille korral $\dim(\mathcal{V}_r \cap \mathcal{W}) = i$. Tähistame $n_i = |\mathfrak{W}_i|$ ning olgu $\mathfrak{W} = \bigcup_{i=0}^{k} \mathfrak{W}_i$. On selge, et

$$\left[{r+s \atop k}\right] = |\mathfrak{W}| = \left|\bigcup_{i=0}^{k} \mathfrak{W}_i\right| = \sum_{i=0}^{k} n_i.$$

Samuti aga osutub õigeks võrdus

$$n_i = \left[{r \atop i}\right] \cdot \left[{s \atop k-i}\right] \cdot q^{(r-i)(k-i)}, \tag{19.16}$$

millest saamegi valemi (19.15). Jääb ainult põhjendada võrdus (19.16). Märkame, et lineaarselt sõltumatud vektorid $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_i$ saab alamruumis $\mathcal{V}_r$ valida

$$(q^r - 1)(q^r - q) \cdots (q^r - q^{i-1})$$

erineval viisil. Iga sellise valiku korral saab ülejäänud $k - i$ lineaarselt sõltumatut vektorit $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_{k-i}$ valida

$$(q^{r+s} - q^r)(q^{r+s} - q^{r+1}) \cdots (q^{r+s} - q^{r+k-i-1})$$

erineval viisil nii, et vektorite komplekt $\{\bar{e}_1, \ldots, \bar{e}_i; \bar{b}_1, \ldots, \bar{b}_{k-i}\}$ oleks mingi alamruumi $\mathcal{W} \in \mathfrak{W}$ baasiks. Seejuures saab

$$(q^i - 1)(q^i - q) \cdots (q^i - q^{i-1})$$

viisil valida vektorite komplekti $\{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_i\}$ nii, et need määraksid ühe ning sama lõike $\mathcal{V}_r \cap \mathcal{W}$ ja iga niisuguse valiku korral veel

$$(q^k - q^i)(q^k - q^{i+1}) \cdots (q^k - q^{i+(k-i)-1})$$

erineval viisil valida ülejäänud $k - i$ vektorit $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_{k-i}$ nii, et saadavad komplektid $\{\bar{e}_1, \ldots, \bar{e}_i; \bar{b}_1, \ldots, \bar{b}_{k-i}\}$ määraksid ühe ja sellesama k-mõõtmelise alamruumi $\mathcal{W} \in \mathfrak{W}$. Kokkuvõttes näeme, et

$$n_i = \frac{(q^r-1)(q^r-q)\cdots(q^r-q^{i-1})(q^{r+s}-q^r)(q^{r+s}-q^{r+1})\cdots(q^{r+s}-q^{r+k-i-1})}{(q^i-1)(q^i-q)\cdots(q^i-q^{i-1})(q^k-q^i)(q^k-q^{i+1})\cdots(q^k-q^{i+(k-i)-1})} =$$

$$= \frac{q^{r(k-i)}\cdot(q^s-1)(q^s-q)\cdots(q^s-q^{k-i-1})}{q^{i(k-i)}\cdot(q^{k-i}-1)(q^{k-i}-q)\cdots(q^{k-i}-q^{k-i-1})}\cdot\begin{bmatrix} r \\ i \end{bmatrix} = \begin{bmatrix} r \\ i \end{bmatrix}\begin{bmatrix} s \\ k-i \end{bmatrix}\cdot q^{(r-i)(k-i)}.$$

Võrdus (19.16) on tõestatud ja koos sellega ka valem (19.15).

Tõestame veel nn. *Gaussi q-samasused*

23

$$\sum_{k=0}^{2m}(-1)^k\begin{bmatrix} 2m \\ k \end{bmatrix} = (1-q)(1-q^3)\cdots(1-q^{2m-1}),$$
$$\sum_{k=0}^{2m+1}(-1)^k\begin{bmatrix} 2m+1 \\ k \end{bmatrix} = 0. \tag{19.17}$$

Asjaolu, et $k > s$ korral $\begin{bmatrix} s \\ k \end{bmatrix} = 0$, lubab nendele seostele anda kompaktsema kuju, kui lisaks kasutada veel võrdusega $T = \sum_{k\geq 0}(-1)^k L_k$ defineeritud funktsionaali $T : \mathbb{Q}[x] \to \mathbb{Q}$. Nimelt saame seosed

$$T(x^{2m}) = (1-q)(1-q^3)\cdots(1-q^{2m-1}) \quad \text{ja} \quad T(x^{2m+1}) = 0, \tag{19.18}$$

milles veendumiseks piisab näidata, et iga $i \in \mathbb{N}$ korral

$$T(x^{i+2}) = (1-q^{i+1})\cdot T(x^i). \tag{19.19}$$

Tõepoolest, baaspolünoomide $p_i(x)$ korral $T(p_i(x)) = (-1)^i$, mistõttu

$$(-1)^1 = T(p_1(x)) = T(x-1) = T(x) - 1,$$
$$(-1)^2 = T(p_2(x)) = T((x-1)(x-q)) = T(x^2) + q.$$

Need võrdused $T(x) = 0$ ja $T(x^2) = 1 - q$ lubavad valemile (19.19) tuginedes saada seosed (19.18). Tõestame nüüd valemi (19.19), kirjutades ta kõigepealt ümber kujul

$$T(x^2\cdot x^i) = T(x^i) - q\cdot T((qx)^i).$$

Et $\{x^i\}$ on ruumi $\mathbb{Q}[x]$ baas, siis selle võrduse kohaselt iga $p(x) \in \mathbb{Q}[x]$ korral

$$T(x^2\cdot p(x)) = T(p(x)) - qT(p(qx)).$$

Lineaarsuse kaalutlused näitavad, et viimast seost võib kontrollida üksnes baaspolünoomidel $p_i(x) = (x-1)(x-q)\cdots(x-q^{i-1})$. Märkame, et

$$T(xp_i(x)) = T(\,p_{i+1}(x) + q^i\cdot p_i(x)\,) = \cdots = (-1)^i(q^i-1),$$
$$T(x^2p_i(x)) = T(\,p_{i+2}(x) + (q^i+q^{i+1})p_{i+1}(x) + q^{2i}\cdot p_i(x)\,) = \cdots$$
$$\cdots = (-1)^i(q^{2i} - q^{i+1} - q^i + 1),$$
$$T(p_i(qx)) = T(\,q^i\cdot p_i(x) + (q^{2i-1} - q^{i-1})\cdot p_{i-1}(x)\,) = \cdots = (-1)^i\cdot q^{i-1}\cdot(q^i - q - 1).$$

Seega tõestatav seos redutseerub baaspolünoomidel ilmseks võrduseks

$$(-1)^i\cdot(q^{2i} - q^{i+1} - q^i + 1) = (-1)^i - q\cdot(\,(-1)^{i-1}\cdot q^{i-1}\cdot(q^i - q - 1)\,),$$

millega valem (19.19) on tõestatud.

Pascali q-valemit korduvalt rakendades leiame

$$\begin{aligned}\begin{bmatrix} n \\ k \end{bmatrix} &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + q^k \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} = \\ &= \left(\begin{bmatrix} n-2 \\ k-2 \end{bmatrix} + q^{k-1} \cdot \begin{bmatrix} n-2 \\ k-1 \end{bmatrix}\right) + q^k \cdot \left(\begin{bmatrix} n-2 \\ k-1 \end{bmatrix} + q^k \cdot \begin{bmatrix} n-2 \\ k \end{bmatrix}\right) = \\ &= q^{2k} \cdot \begin{bmatrix} n-2 \\ k \end{bmatrix} + (q^k + q^{k-1}) \cdot \begin{bmatrix} n-2 \\ k-1 \end{bmatrix} + \begin{bmatrix} n-2 \\ k-2 \end{bmatrix} = \cdots\end{aligned}$$

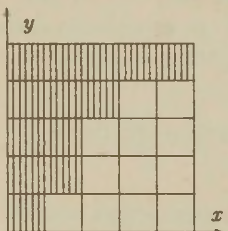
Piltlikult väljendades võimaldab see tulemus meil Gaussi arvude q-kolmnurgas tõusta samm-sammult ülemistele nivoodele, kuni näeme, et arvud $\begin{bmatrix} n \\ k \end{bmatrix}$, mis klassikalise definitsiooniga on antud kui ratsionaalavaldised suurusest q, osutuvad q-polünoomideks

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{\alpha=0}^{k \cdot (n-k)} P(n-k, k, \alpha) q^{\alpha} \tag{19.20}$$

(selle polünoomi aste $k \cdot (n-k)$ nähtub klassikalisest valemist (19.12), kus ta avaldub lugeja ja nimetaja kõrgeimate astendajate vahena).

Vaadeldes järgnevas Gaussi arvu $\begin{bmatrix} n \\ k \end{bmatrix}$ kui q-polünoomi anname tema kordajate P kombinatoorse interpretatsiooni naturaalarvude aditiivsete lahutuste keeles. Naturaalarvu α *aditiivseks lahutuseks* nimetatakse naturaalarvude sellist mittekasvavat järjendit $\alpha_1, \alpha_2, \ldots, \alpha_k$, mille korral $\alpha_1 + \alpha_2 + \cdots + \alpha_k = \alpha$. Arve α_i nimetatakse sealjuures lahutuse $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ ***komponentideks***, arvu k lahutuse ***sügavuseks***.

Vaatleme nüüd *$\mathbb{Z}$-võrku* tasandil, s. t. tasandi neid punkte, mille ristkoordinaatideks on täisarvude paar (x, y) (siinkohal huvitab see võrk meid ainult põhikvadrandis $x \geqslant 0$, $y \geqslant 0$). Punkt (x, y) liikugu igal "taktil" vaid kas paremale või üles mööda $\mathbb{Z}$-võrgu "tänavaid", sellise liikumise jälge nimetame ***siksakiks***.



Iga lahutusega $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_k)$ saab siduda nn. *Ferrersi tabeli* F_α, mille moodustavad $\mathbb{Z}$-võrgu kõik need ühikruudud, mille vasaku alumise tipu $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ koordinaadid rahuldavad nõudeid

$$0 \leqslant y \leqslant k-1 \quad \text{ja} \quad 0 \leqslant x \leqslant \alpha_{k-y} - 1.$$

Joonis illustreerib lahutusele $13 = (5, 3, 2, 2, 1)$ vastavat Ferrersi tabelit.

Teoreem 1. Arv $P(n-k, k, \alpha)$ võrdub naturaalarvu $\alpha \geqslant 1$ selliste aditiivsete lahutuste arvuga, mille sügavus on ülimalt k ja mille ükski komponent ei ületa arvu $n-k$. Kokkuleppeliselt loetakse $P(n-k, k, 0) = 1$.

Tõestus. Kasutades võimalust siduda iga lahutusega Ferrersi tabel saab teoreemi väitele anda järgmise, ekvivalentse kuju: arv $P(n-k, k, \alpha)$ võrdub nende siksakkide arvuga, mis kulgevad punktist $(0, 0)$ punkti $(n-k, k)$ ja mille kohal on pindala α. Siinjuures viimane fraas tähendab, et naturaalarvu α tõlgendatakse kui ühikruudukeste arvu Ferrersi tabelis F_α, s. t. kujundis, mida piiravad vasakult y-telg, ülalt sirge $y = k$ ning alt ja paremalt nimetatud siksak.

Viimase väite tõestame induktsiooniga n järgi. Induktsiooni baasina vaatleme (esimest sisukat) juhtu $n = 2$, $k = 1$, $n - k = 1$, mil pindala võimalikeks väärtusteks on $\alpha = 0$ ja $\alpha = 1$. Ilmselt leidub vaid üks siksak punktist (0,0) punkti (1,1) pindalaga 0 ning üks siksak pindalaga 1. Järelikult valemi (19.20) kohaselt

$$\begin{bmatrix}2\\1\end{bmatrix} = \sum_{\alpha=0}^{1\cdot 1} P(1,1,\alpha)q^{\alpha} = P(1,1,0)q^0 + P(1,1,1)q^1 = 1\cdot q^0 + 1\cdot q^1 = 1 + q,$$

mis langeb kokku Gaussi arvu $\left[{2 \atop 1}\right]$ valemist (19.12) saadava väärtusega.

Seega on induktsiooni baasväide tõestatud ja tuleb veel põhjendada üleminek $(n-1)$-lt n-le. Kasutame tähistust $s = n - k$ ja tugineme intuitiivselt selgele tähelepanekule, et $\mathbb{Z}$-võrgu iga punktis (0,0) algav ja punktis (s, k) lõppev siksak läbib kas punkti $(s, k-1)$ või punkti $(s-1, k)$. Sellest tähelepanekust tuleneb, et siksakke $(0,0) \to (s,k)$, mille peal on pindala α leidub sama palju kui on kokku siksakke $(0,0) \to (s-1,k)$ pindalaga α ja siksakke $(0,0) \to (s, k-1)$ pindalaga $\alpha - s$. Vastavalt induktsiooni oletusele on esimene nimetatud arv $P(s-1,k,\alpha)$ ja teine $P(s, k-1, \alpha - s)$. Seega piisab, kui tõestada võrdus

$$P(s,k,\alpha) = P(s-1,k,\alpha) + P(s,k-1,\alpha - s). \tag{19.21}$$

Valemi (19.20) kohaselt

$$\begin{aligned}
\begin{bmatrix}n\\k\end{bmatrix} &= \sum_{\alpha\geqslant 0} P(s,k,\alpha)q^{\alpha},\\
\begin{bmatrix}n-1\\k\end{bmatrix} &= \sum_{\alpha\geqslant 0} P(s-1,k,\alpha)q^{\alpha},\\
\begin{bmatrix}n-1\\k-1\end{bmatrix} &= \sum_{\alpha\geqslant s} P(s,k-1,\alpha - s)q^{\alpha - s}.
\end{aligned} \tag{19.22}$$

Et aga

$$(q^s-1)\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix} - (q^k-1)\cdot\begin{bmatrix}n-1\\k\end{bmatrix} = (q^s-1)\cdot\frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{s+1}-1)}{(q-1)(q^2-1)\cdots(q^{k-1}-1)} -$$

$$-(q^k-1)\cdot\frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{s}-1)}{(q-1)(q^2-1)\cdots(q^{k}-1)} = 0,$$

siis Pascali q-valemi kohaselt

$$\begin{bmatrix}n\\k\end{bmatrix} = \begin{bmatrix}n-1\\k\end{bmatrix} + q^s\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix},$$

mille seoseid (19.22) kasutades saab esitada kujul:

$$\sum_{\alpha\geqslant 0} P(s,k,\alpha)q^{\alpha} = \sum_{\alpha\geqslant 0} P(s-1,k,\alpha)q^{\alpha} + q^s\cdot\sum_{\alpha\geqslant s} P(s,k-1,\alpha-s)q^{\alpha-s}.$$

Võrreldes siin kordajaid q^{α} ees veendume võrduse (19.21) õigsuses.

Illustreerime veel teoreemi 1 väidet q-polünoomi $\begin{bmatrix}5\\2\end{bmatrix}$ korral:

$$\begin{bmatrix}5\\2\end{bmatrix} = \begin{bmatrix}4\\2\end{bmatrix} + q^3 \cdot \begin{bmatrix}4\\1\end{bmatrix} = \begin{bmatrix}3\\2\end{bmatrix} + q^2 \cdot \begin{bmatrix}3\\1\end{bmatrix} + q^3 \cdot \begin{bmatrix}4\\1\end{bmatrix} =$$
$$= \frac{q^3-1}{q-1} + q^2 \cdot \frac{q^3-1}{q-1} + q^3 \cdot \frac{q^4-1}{q-1} = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6.$$

Nüüd on lihtne koostada Ferrersi diagrammid vastavalt tabelile:

α	0	1	2	3	4	5	6
$P(3,2,\alpha)$	1	1	2	2	2	1	1

Teoreemiga 1 arvudele $P(n-k,k,\alpha)$ antud kombinatoorset interpretatsiooni nimetatakse *Sylvesteri q-teoreemiks*, kuid analoogilise interpretatsiooni saab võre $\mathfrak{V}_n(q)$ termineis anda ka võrduse (19.20) liidetavatele $P(n-k,k,\alpha)q^\alpha$.

Teoreem 2 (*Knuthi teoreem*). Leidub elementide kõrgusi säilitav o-epimorfism

$$\nabla : \mathfrak{V}_n(q) \to \mathfrak{B}(\overline{1,n}).$$

Tõestus. Fikseerime ruumis $\mathcal{V} = \mathcal{V}_n(q)$ mingi baasi $\{\overline{e}_1, \overline{e}_2, \ldots, \overline{e}_n\}$, misjärel ruumi $\mathcal{V}$ vektoreid $\overline{x}$ saab üheselt anda nende koordinaatide $(x_1, x_2, \ldots, x_n)$ kaudu selles baasis. Nüüd on iga k-mõõtmelise alamruumiga $\mathcal{A} \subseteq \mathcal{V}$ ühesel viisil seotud teatav alamhulk $\mathcal{A}^\nabla = \{\nu_1, \nu_2, \ldots, \nu_k\} \subset \overline{1,n}$, kus arvud ν_i määratakse rekursiivselt:

$$\nu_1 = \max\{\, j : \exists (x_1, x_2, \ldots, x_n) \in \mathcal{A}, x_j \neq 0\,\},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\nu_k = \max\{\, j : \exists (x_1, x_2, \ldots, x_n) \in \mathcal{A}, x_{\nu_1} = \cdots = x_{\nu_{k-1}} = 0, x_j \neq 0\,\}.$$

Ilmselt $n \geqslant \nu_1 > \nu_2 > \cdots > \nu_k \geqslant 1$, kusjuures nende arvude definitsioonist nähtub, et kujutus $\mathcal{A} \to \mathcal{A}^\nabla$ säilitab elementide kõrgusi: k-mõõtmelisele alamruumile $\mathcal{A}$ vastab k-elemendiline alamhulk $\mathcal{A}^\nabla \subset \overline{1,n}$. Samuti nähtub arvude ν_i definitsioonist, et kujutus ∇ on järjestusseost säilitav – ruumi $\mathcal{V}$ suvaliste alamruumide $\mathcal{A} \subset \mathcal{B}$ korral leiab hulgas $\overline{1,n}$ aset seos $\mathcal{A}^\nabla \subset \mathcal{B}^\nabla$.

Kujutuse ∇ sürjektiivsus järeldub sellest, et ruumi $\mathcal{V}$ igas k-mõõtmelises alamruumis $\mathcal{A}$ saab ühesel viisil fikseerida kanoonilise baasi $\{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_k\}$, kus vektorite

$$\overline{a}_i = \sum_{j=1}^{n} a_{ij}\overline{e}_j$$

koordinaadid a_{ij} rahuldavad iga $i = 1, 2, \ldots, k$ korral tingimusi:

$$a_{i\nu_i} = 1, \quad j > \nu_i \text{ korral } a_{ij} = 0 \quad \text{ja} \quad l < i \quad \text{korral} \quad a_{l\nu_i} = 0. \tag{19.23}$$

Kanoonilise baasi olemasolus on kerge veenduda, tarvitseb vaid lähtuda alamruumi $\mathcal{A}$ suvalisest baasist $\{\overline{a}'_1, \overline{a}'_2, \ldots, \overline{a}'_k\}$ ja rakendada $(k \times n)$-maatriksi (a'_{ij}) ridadele sobivaid elementaarteisendusi. Alamruumi $\mathcal{A}$ selline baas on üheselt määratud, sest iga $i = 1, 2, \ldots, k$ korral on $\bar{a}_i \in \mathcal{A}$ ainus selline vektor, et $a_{i\nu_j} = \delta_{ij}$, kus $j = 1, 2, \ldots, k$. Faktiliselt määravad arvud n, k ja $\nu_1, \nu_2, \ldots, \nu_k$ alamruumi kanoonilise baasi üheselt. Näiteks juhul $n = 6$, $k = 3$, $\nu_1 = 5$, $\nu_2 = 3$, $\nu_3 = 2$ näeme, et kanoonilise baasi skeem tuleb kujul:

$$\begin{aligned}\bar{a}_1 &= (a_{11},\ 0,\ 0, a_{14},\ 1,\ 0),\\ \bar{a}_2 &= (a_{21},\ 0,\ 1,\ \ 0,\ \ 0,\ 0),\\ \bar{a}_3 &= (a_{31},\ 1,\ 0,\ \ 0,\ \ 0,\ 0).\end{aligned}$$

Antud n ja k korral määrab iga alamhulk $\{\nu_1, \nu_2, \ldots, \nu_k\} \subset \overline{1, n}$ tingimused (19.23) ja seega ka skeemi, kus iga $i = 1, 2, \ldots, k$ korral jääb i-ndas vektoris $\bar{a}_i$ täpsustamata $(\nu_i - (k - i) - 1)$ koordinaati. Nende koordinaatide iga konkretiseerimine annab k vektorist koosneva hulga, mille lineaarne kate ruumis $\mathcal{V}$ on konstruktsiooni kohaselt selline alamruum, mis kujutub ∇ abil alamhulgaks $\{\nu_1, \nu_2, \ldots, \nu_k\}$.

See tähelepanek viib järgmise, ammu kasutusel oleva (empiirilise) printsiibi juurde: kui mingi (algebraline) seos kehtib Gaussi arvude korral, siis kehtib sama tüüpi seos ka binoomkordajate jaoks. Eespool tõestatu annab võimaluse saada hulgaliselt näiteid selle printsiibi rakendustest: valemist (19.9) tuleneb

$$\binom{n}{n-k} = \frac{n}{k} \cdot \binom{n-1}{n-k};$$

valemist (19.13) tuleneb *Pascali kolmnurga* moodustamise reegel

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k};$$

Vandermonde'i q-valemist (19.15) tuleneb nn. *liitmisvalem*

$$\binom{r+s}{k} = \sum_{i=0}^{k} \binom{s}{i} \binom{r}{k-i},$$

millest erijuhul $r = s = k = n$ saame

$$\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2;$$

Gaussi q-samasused (19.17) annavad võrduse (7.1).

Teoreemis 2 kirjeldatud vastavuse omadusi selgitab järgmine tulemus.

Teoreem 3. Ruumi $\mathcal{V}_n(q)$ igale k-mõõtmelisele alamruumile vastab üheselt teatav lahutus sügavusega ülimalt k, mille ükski komponent ei ületa arvu $n - k$. Vastupidi, arvu α igale lahutusele sügavusega ülimalt k, mille ükski komponent ei ületa arvu $n - k$, vastab q^α k-mõõtmelist alamruumi ruumis $\mathcal{V}_n(q)$.

Tõestus. Eespool nägime, et iga k-mõõtmeline alamruum $\mathcal{A} \subseteq \mathcal{V}_n$ määrab üheselt alamhulga $\{\nu_1, \nu_2, \ldots, \nu_k\} \subset \overline{1, n}$, mille elemendid loeme tähistatuks kahanevas järjekorras. Vaatleme arvusid $\alpha_i = \nu_i - (k - i) - 1$, kus $i = 1, 2, \ldots, k$.

Et iga $i = 1, 2, \ldots, k-1$ korral on $\nu_i > \nu_{i+1}$, siis ka $\nu_i - 1 \geqslant \nu_{i+1}$ ja seega $\alpha_i = (\nu_i - 1) + i - k \geqslant \nu_{i+1} + i - k = \alpha_{i+1}$, s.t. $\alpha_i \geqslant \alpha_{i+1}$. Et kehtib $\nu_k \geqslant 1$, siis $\alpha_k = \nu_k - (k-k) - 1 = \nu_k - 1$, s.t. $\alpha_k \geqslant 0$. Et kehtib $\nu_1 \leqslant n$, siis $\alpha_1 = \nu_1 - (k-1) - 1 = \nu_1 - k \leqslant n - k$, s.t. $\alpha_1 \leqslant n - k$. Seega arvud $n \geqslant \nu_1 > \nu_2 > \cdots > \nu_k \geqslant 1$, määravad üheselt arvu $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k$ lahutuse $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{k'})$ sügavusega $k' \leqslant k$ (s.t. $\alpha_{k'+1} = \ldots = \alpha_k = 0$), milles kõik komponendid $\alpha_i \leqslant n - k$.

Vastupidi, olgu antud lahutus $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{k'})$ sügavusega $k' \leqslant k$, kus $n - k \geqslant \alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_{k'} \geqslant 0$. Loeme, et $\alpha_{k'+1} = \cdots = \alpha_k = 0$ ning võtame kasutusele arvud $\nu_i = \alpha_i - i + k + 1$. Komponentide α_i omadustest tulenevalt

$$\nu_{i+1} = \alpha_{i+1} - (i+1) + k + 1 = \alpha_{i+1} - i + k \leqslant \alpha_i - i + k < \alpha_i - i + k + 1 = \nu_i,$$

s.t. $\nu_{i+1} < \nu_i$. Seejuures $\nu_1 = \alpha_1 - 1 + k + 1 = \alpha_1 + k \leqslant (n-k) + k = n$, s.t. $\nu_1 \leqslant n$ ning ka $\nu_k = \alpha_k - k + k + 1 = \alpha_k + 1 \geqslant 1$. Seega igale lahutusele sügavusega ülimalt k ja kõigi komponentidega $\alpha_i \leqslant n-k$ vastab kanoonilise baasi vektorite skeem baasivektoreis kokku α koordinaadi spetsialiseerimise võimalusega. See skeem lubab q^α erinevat spetsialisatsiooni korpuses $\mathbb{F}(q)$, millest igaüks määrab ruumi $\mathcal{V}_n$ teatava (ülejäänuist erineva) k-mõõtmelise alamruumi.

Et arvu α lahutusi sügavusega ülimalt k ja komponentidega $\alpha_i \leqslant n-1$ on $P(n-k, k, \alpha)$ tükki, siis arvu α kõigile vaadeldavat tüüpi lahutustele vastab kokku $P(n-k, k, \alpha)\, q^\alpha$ k-mõõtmelist alamruumi ruumis $\mathcal{V}_n(q)$.

Tõestatud teoreemiga 3 on seosele (19.20) antud uus sisu: tema parema poole liidetavaid ei vaadelda q-monoomidena – neil on nüüd ka kombinatoorne tähendus.

Teoreem 4. Kui $P_k(x, y) = (x-y)(x-qy)\cdots(x-q^{k-1}y)$ ning x, y ja z tähistavad muutujaid, siis kehtib nn. *q-binoomvalem*

$$P_n(x, z) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} \cdot P_{n-k}(x, y) \cdot P_k(y, z). \tag{19.24}$$

Tõestus. Märgime kõigepealt, et muutuja y esineb selles valemis vaid formaalselt: osutub, et ta koondub parema poole arendamisel välja.

Olgu $\mathcal{V} = \mathcal{V}_n(\mathbb{F}(q))$ ning $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ suvalised vektorruumid üle korpuse $\mathbb{F}(q)$ sellised, et $\mathcal{Z} \subset \mathcal{Y} \subset \mathcal{X}$ ja $\dim \mathcal{Z} > n$. Et ruumide $\mathcal{X}$, $\mathcal{Y}$ ja $\mathcal{Z}$ põhikorpus on lõplik, siis sisaldavad vaadeldavad ruumid igaüks lõpliku arvu vektoreid: olgu $|\mathcal{X}| = x$, $|\mathcal{Y}| = y$ ja $|\mathcal{Z}| = z$. Tõestuse idee on selles, et võrduse (19.24) pooled loendavad selliste regulaarsete lineaarteisenduste $f : \mathcal{V} \to \mathcal{X}$ arvu, mille puhul $f(\mathcal{V}) \cap \mathcal{Z} = \{\overline{0}\}$.

Ühelt poolt, olgu $\{\overline{e}_1, \overline{e}_2, \ldots, \overline{e}_n\}$ ruumi $\mathcal{V}$ baas. Loendame, kui mitmel eri viisil saab neid vektoreid $\overline{e}_i$ kujutada n lineaarselt sõltumatuks vektoriks ruumis $\mathcal{X}$ niimoodi, et kujutisvektorite lineaarse katte lõige ruumiga $\mathcal{Z}$ oleks $\{\overline{0}\}$. Seejuures esinevate võimaluste arvu saame loendada nii: vektori $\overline{e}_1$ kujutamiseks on $x - z$ võimalust ($\overline{e}_1$ kujutiseks võib olla ruumi $\mathcal{X}$ iga vektor, mis ei kuulu alamruumi $\mathcal{Z}$);

vektori $\bar{e}_2$ kujutamiseks on $x - qz$ võimalust ($\bar{e}_2$ kujutiseks võib olla ruumi $\mathcal{X}$ iga vektor, mis ei kuulu alamruumi $\lambda(\mathcal{Z}, f(\bar{e}_1)) \equiv \lambda_{\mathbb{F}(q)}(\mathcal{Z}, f(\bar{e}_1))$; viimane kujutab endast alamruumi $\mathcal{Z}$ vektorite ja vektori $f(\bar{e}_1)$ lineaarset katet üle korpuse $\mathbb{F}(q)$ ning selles on $z \cdot q$ vektorit); vektori $\bar{e}_3$ kujutamiseks on $x - zq^2$ võimalust — ruumi $\mathcal{X}$ iga vektor peale vektorite lineaarsest kattest $\lambda(\mathcal{Z}, f(\bar{e}_1), f(\bar{e}_2))$. Et lineaarkujutus $f : \mathcal{V} \to \mathcal{X}$ on üheselt määratud oma väärtustega baasivektoreil $\bar{e}_i$, siis oleme soovitud omadustega lineaarkujutuste üldarvuks saanud

$$(x - z)(x - qz)(x - q^2 z) \cdots (x - q^{n-1} z) = P_n(x, z).$$

Teiselt poolt loendame jälle neid regulaarseid lineaarteisendusi $f : \mathcal{V} \to \mathcal{X}$, kus $f(\mathcal{V}) \cap \mathcal{Z} = \{\bar{0}\}$, kuid arvestame nüüd ka alamruumi $f(\mathcal{V})$ "positsiooni" ruumi $\mathcal{Y}$ suhtes. Olgu $\dim(f(\mathcal{V}) \cap \mathcal{Y}) = k$. Siis on alamruum $f(\mathcal{V}) \cap \mathcal{Y}$ ruumi $\mathcal{V}$ mõne k-mõõtmelise alamruumi $\mathcal{U}$ kujutiseks tulenevalt kujutuse f regulaarsusest. Sellest arutlusest nähtub, et soovitud omadusega kujutusi $f : \mathcal{V} \to \mathcal{X}$ saab järgmisel viisil: valinud suvalise $\mathcal{U} \subset \mathcal{V}$ määrame algul kujutuse $\mathcal{U} \to (\mathcal{Y} \backslash \mathcal{Z}) \cup \{\bar{0}\}$ ning seejärel kujutuse $\mathcal{V} \backslash \mathcal{U} \to (\mathcal{X} \backslash \mathcal{Y}) \cup \{\bar{0}\}$ nii, et tulemuseks oleks regulaarne lineaarteisendus $f : \mathcal{V} \to \mathcal{X}$. Olgu ruumi $\mathcal{V}$ baas $\{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n\}$ valitud selliselt, et esimesed k vektorit selles moodustavad alamruumi $\mathcal{U}$ baasi. Samuti nagu käesoleva tõestuse esimeses osas leiame, et lineaarteisendusi $f : \mathcal{U} \to (\mathcal{Y} \backslash \mathcal{Z}) \cup \{\bar{0}\}$, mis kujutavad vektorid $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_k$ lineaarselt sõltumatuiks vektoreiks ruumis $\mathcal{Y}$, nii et $\lambda(f(\bar{e}_1), \ldots, f(\bar{e}_k)) \cap \mathcal{Z} = \{\bar{0}\}$, on $P_k(y, z) = (y - z)(y - qz) \cdots (y - q^{k-1} z)$ tükki. Lineaarteisenduse $f : \mathcal{V} \to \mathcal{X}$ regulaarsuseks on tarvilik, et ruumi $\mathcal{V}$ baasi ülejäänud $n - k$ vektorit $\bar{e}_{k+1}, \ldots, \bar{e}_n$ kujutuksid regulaarselt hulka $(\mathcal{X} \backslash \mathcal{Y}) \cup \{\bar{0}\}$; see saab toimuda $P_{n-k}(x, y)$ eri viisil. Et suvalisele lineaarselt sõltumatule alamhulgale $\mathcal{S} \subset \mathcal{V}$ mingi vektori $\bar{v} \in \mathcal{V}$, $\bar{v} \notin \lambda(\mathcal{S})$ lisamine viib jällegi lineaarselt sõltumatu alamhulgani $\mathcal{S} \cup \{\bar{v}\}$ näeme, et fikseeritud k-mõõtmelise alamruumi $\mathcal{U}$ korral leidub $P_k(y, z) \cdot P_{n-k}(x, y)$ regulaarset lineaarkujutust $f : \mathcal{U} \to \mathcal{X}$, mille puhul $f(\mathcal{U}) \cap ((\mathcal{X} \backslash \mathcal{Z}) \cup \{\bar{0}\}) = f(\mathcal{U})$. Võttes arvesse ka ruumi $\mathcal{U}$ valikuvõimalused näeme, et regulaarseid lineaarteisendusi $f : \mathcal{V} \to \mathcal{X}$, mille korral $f(\mathcal{V}) \cap \mathcal{Z} = \{\bar{0}\}$ on $\sum_{k=0}^{n} \left[{n \atop k} \right] \cdot P_{n-k}(x, y) \cdot P_k(y, z)$ tükki. Võrdsustades selle tulemuse ülalsaadud arvuga $P_n(x, z)$, jõuamegi q-binoomvalemini (19.24).

Huvi pakuvad selle valemi kaks erijuhtu. Esiteks, võttes $z = 0$ ja $y = 1$ saame

$$x^n = \sum_{k=0}^{n} \left[{n \atop k} \right] (x - 1)(x - q) \cdots (x - q^{n-k-1}) = \sum_{k=0}^{n} \left[{n \atop k} \right] (x - 1)(x - q) \cdots (x - q^{k-1}).$$

Teiseks, võttes $z = 1$ ja $y = 0$ saame

$$(x - 1)(x - q) \cdots (x - q^{n-1}) = \sum_{k=0}^{n} \left[{n \atop k} \right] x^{n-k} \cdot (-1)^k \cdot q^{\binom{k}{2}} =$$

$$= \sum_{k=0}^{n} \left[{n \atop n-k} \right] x^{n-(n-k)} \cdot (-1)^{n-k} \cdot q^{\binom{n-k}{2}} = \sum_{k=0}^{n} \left[{n \atop k} \right] (-1)^{n-k} \cdot q^{\binom{n-k}{2}} \cdot x^k.$$

20. Dirichlet' printsiip

Tähistame $\mathbb{N}_1 = \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}$ ning vaatleme sellel loomuliku järjestusega hulgal väidete jada $\{P(k) : k \in \mathbb{N}_1\}$, milles väide $P(1)$ olgu tõene, kusjuures iga $k \in \mathbb{N}_1$ korral olgu tõene ka implikatsioon $P(k) \Rightarrow P(k+1)$. Aksioomi, mille kohaselt nendel eeldustel on tõesed kõik väited $P(k)$, tuntakse *induktsiooniprintsiibina*. Sellest printsiibist järeldub omakorda nn. *languse printsiip*: igal mittetühjal alamhulgal $\mathcal{H} \subseteq \mathbb{N}_1$ on olemas vähim element.

Tõepoolest, tähendagu $P(k)$ väidet "kui mõni naturaalarvudest $x \leqslant k$ sisaldub alamhulgas $\mathcal{H} \subseteq \mathbb{N}_1$, siis leidub hulgas $\mathcal{H}$ vähim element". Nüüd osutub väide $P(1)$ tõeseks, sest $1 = x \in \mathcal{H}$ korral on arv 1 muidugi hulga $\mathcal{H}$ vähim element. Tõene on ka implikatsioon $P(k) \Rightarrow P(k+1)$, sest kui $\mathcal{H}$ sisaldab mõnd arvudest $x < k+1$, siis tuleneb vähima elemendi olemasolu hulgas $\mathcal{H}$ eeldusest, et $P(k)$ on tõene. Kui aga hulgas $\mathcal{H}$ sellist naturaalarvu $x < k+1$ ei leidu, siis on arv $k+1$ ise hulga $\mathcal{H}$ vähim element. Seega osutub tõeseks ka väide $P(k+1)$. Et induktsiooniprintsiibi kohaselt on nüüd tõesed kõik väited $P(k)$, kus $k \in \mathbb{N}_1$ ning $x \in \mathcal{H}$ korral sealhulgas ka väide $P(x)$, siis näeme, et $\mathcal{H}$ sisaldab vähima elemendi. Märgime, et tegelikult järeldub induktsiooniprintsiip kergesti ka languse printsiibist, kuid seda järeldumist me alljärgnevas ei vaja.

Teoreem 1. Kui naturaalarvude m ja n korral $m < n$, siis ei eksisteeri injektiivset kujutust $\overline{1,n} \to \overline{1,m}$.

Tõestus. Järgnevas arutluses tähistame injektiivsete kujutuste $\overline{1,n} \to \overline{1,m}$ hulka lühidalt sümboliga $\mathcal{I}_{n,m}$. Kui teoreemi väide ei kehti, siis on hulk

$$\mathcal{H} = \{k : \text{leidub } m < k \text{ nii, et eksisteerib } f \in \mathcal{I}_{k,m}\}$$

mittetühi ja sisaldab languse printsiibi kohaselt vähima elemendi, mille tähistame n. Fikseerime nüüd suvalise naturaalarvu $m < n$, mille korral eksisteerib $f^* \in \mathcal{I}_{n,m}$. Seejuures võime eeldada, et $m > 1$ ehk $m - 1 \in \mathbb{N}_1$, sest võrdusest $m = 1$ tuleneks ju $g \in \mathcal{I}_{n,1}$ olemasolu, mis $n > 1$ tõttu on võimatu.

Kui $f^*(n) = m$, siis funktsiooni f^* ahendi $f^{**} \in \mathcal{I}_{n-1,m-1}$ olemasolu annab vastuolu sellega, et n on hulga $\mathcal{H}$ vähim element. Kui aga $f^*(a) = m$ mingi $a \leqslant n-1$ korral, siis $f^*(n) = b \neq m$ ja sama vastuolu andva funktsiooni $f^{**} \in \mathcal{I}_{n-1,m-1}$ võime defineerida kujul

$$f^{**}(x) = \begin{cases} f^*(x), & \text{kui } x \neq a, \\ b\ , & \text{kui } x = a. \end{cases}$$

Teoreem on tõestatud.

Kui $\mathcal{X}$ ja $\mathcal{Y}$ on lõplikud hulgad, siis funktsiooni $f : \mathcal{X} \to \mathcal{Y}$ võib nimetada *paigutuseks*, tõlgendades võrdust $f(x) = y$ elemendi x paigutamisena "pesasse" y. Paneme tähele, et juhul $n = |\mathcal{X}| > |\mathcal{Y}| = m$ ei leidu injektiivset paigutust. Seda tähelepanekut nimetatakse *Dirichlet' printsiibiks*, kuigi kasutatakse ka nimetust *lahterdamisprintsiip* (pigeonhole principle): kui n objekti paigutuvad m pessa ning seejuures $n > m$, siis leidub pesa, kuhu satub vähemalt kaks objekti. Eeltoodud arutlusest nähtub, et Dirichlet' printsiipi pole tarvis vaadelda uue aksioomina, sest ta tuleneb induktsiooniprintsiibist. Kui aga kasutada funktsiooni tuuma mõistet, siis nähtub kergesti, et Dirichlet' printsiibi saab sõnastada ka järgmises vormis: iga naturaalarvu n jaoks leidub arv N nii, et suvalises vähemalt N-elemendilises hulgas $\mathcal{X}$ leidub iga funktsiooni $f : \mathcal{X} \to \mathcal{X}$ jaoks n-elemendiline alamhulk $\mathcal{X}' \subseteq \mathcal{X}$ nii, et f ahend hulgal $\mathcal{X}'$ on kas konstantne või üksühene.

Esimese näitena Dirichlet' printsiibi rakendamisest veendume, et igas vähemalt kaheliikmelises seltskonnas $\mathcal{S}$ leidub alati kaks inimest, kellel on selles seltskonnas ühe palju sõpru (kui x' ja x'' on sõbrad, siis tähistame seda $x' \sim x''$, kusjuures loeme ka $x'' \sim x'$ ja $x \not\sim x$). Selle väite põhjendamiseks tähistame $s(x)$ elemendi $x \in \mathcal{S}$ "sõprade" arvu hulgas $\mathcal{S}$ ning märkame, et juhul $|\mathcal{S}| = n$ on $s(x) \in \{0, 1, \ldots, n-1\}$. Kui leiduks element $x' \in \mathcal{S}$, mille korral $s(x') = n - 1$, siis hulga $\mathcal{S}$ ühelgi elemendil ei oleks null sõpra. Sellest tulenevalt $\{0, n-1\} \not\subseteq \{s(x) : x \in \mathcal{S}\}$, mistõttu näeme, et $|\mathcal{S}| > |\{s(x) : x \in \mathcal{S}\}|$. Võtnud nüüd $\mathcal{X} = \mathcal{S}$ ja $\mathcal{Y} = \{s(x) : x \in \mathcal{S}\}$ veendumegi, et arutluse alguses sõnastatud väide tuleneb printsiibist otseselt.

Teise näitena tõestame, et igal kumeral hulktahukal leidub alati kaks tahku, mida piirab ühesugune arv servi. Tõepoolest, olgu hulktahuka tahku piiravate servade maksimaalarvuks n. Lahterdame kõik tahud neid piiravate servade arvu järgi pesadesse märgenditega 3, 4, …, n. Et tahk, mida piirab n serva, külgneb n erineva tahuga, siis tahkude üldarv pole väiksem kui $n + 1$. Dirichlet' printsiibist tulenevalt peab ühte pesadest 3, 4, …, n nüüd sattuma vähemalt kaks erinevat tahku, millel seega ongi ühepalju piiravaid servi.

Kolmanda näitena tõestame, et ükskõik kuidas me ka ei valiks diskreetselt lõigult $\overline{1,100}$ kümme arvu, saab nende hulgas $\mathcal{S}$ alati teha kaks täiesti erinevat valikut (s. t. vältides neis valikutes ühesuguseid arve), mis annavad ühesuguse summa. Näiteks kui $\mathcal{S} = \{1, 7, 8, 17, 19, 21, 22, 27, 57, 99\}$, siis $1 + 7 = 8 \in \mathcal{S}$, aga ka $1 + 21 + 22 = 8 + 17 + 19$. Esitatud väite põhjendamiseks märkame kõigepealt, et hulka $\mathcal{S}$ kuuluvate arvude summa pole suurem kui $90 + 91 + \cdots + 99 = 945$. Seetõttu saame $\mathcal{S}$ alamhulgad lahterdada nendes sisalduvate arvude summa järgi pesadesse märgenditega 1, 2, …, 945. Lahterdamisele tulevate (mittetühjade) alamhulkade arv on aga $2^{10} - 1 = 1023$, seega ühes neist 945 pesast peab sisalduma vähemalt kaks erinevat alamhulka, tähistame neid $\mathcal{A}$ ja $\mathcal{B}$. Jättes neist hulkadest välja nende ühisosa, s. t. vaadeldes alamhulkasid $\mathcal{A} \setminus (\mathcal{A} \cap \mathcal{B})$ ja $\mathcal{B} \setminus (\mathcal{A} \cap \mathcal{B})$, saamegi hulga $\mathcal{S}$ kaks ühisosata alamhulka, milles sisalduvate arvude summad on võrdsed.

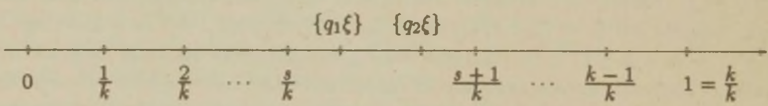
Neljanda näitena rakendame $m \times n$ maatriksile (a_{ij}) (kus $a_{ij} \in \mathbb{R}$) järgmist protseduuri. Järjestame kõigepealt mittekahanevalt maatriksi (a_{ij}) read ja saadud uues maatriksis (a'_{ij}) järjestame mittekasvavalt veerud. Osutub, et niisuguse protseduuri tulemusena saadavas maatriksis (a''_{ij}) on read jäänud mittekahanevalt järjestatuks. Selle väite põhjendamiseks oletame väitevastaselt, et i-ndas reas leiab mingite $k < j$ korral aset seos $a''_{ik} > a''_{ij}$. Samal ajal kehtivad aga veergudes loodud järjestuse tõttu seosed $a''_{ik} \leqslant a''_{i-1,k} \leqslant \cdots \leqslant a''_{1k}$ (tähistame k-nda veeru seda "lõiku" sümboliga K) ning samuti $a''_{ij} \geqslant a''_{i+1,j} \geqslant \cdots \geqslant a''_{mj}$ (seda j-nda veeru lõiku tähistame sümboliga J). Öeldust tulenevalt on lõigu K iga element suurem kui lõigu J suvaline element; tähistame seda asjaolu sümboolselt kujul $K > J$.

Kui nüüd vaadeldava protseduuri lõppseisust (a''_{ij}) tagasi pöörduda vahepealsesse seisu (a'_{ij}), siis tuleb muuhulgas lõigu K elemendid viia tagasi nende kohtadele maatriksi (a'_{ij}) k-ndas veerus ning lõigu J elemendid tagasi nende kohtadele maatriksi (a'_{ij}) j-ndas veerus. Tõlgendame elementide kirjeldatud tagasipaigutamist kui hulga $K \cup J$ elementide lahterdamist pesadesse $1, 2, \ldots, m$, kus pesade märgenditena tõlgendame ridade numbreid. Et $|K \cup J| = m + 1$, siis vähemalt kaks elementi (tähistame neid lühidalt a ja b) hulgast $K \cup J$ satuvad ühte pessa, märgendiga näiteks l. Vaadeldavad elemendid a ja b ei saa olla ühelt ja samalt lõigult K või J, sest nende lõikude elemendid satuvad tagasipaigutamisel erinevatesse ridadesse. Konkreetsuseks olgu näiteks $a \in K$ ja $b \in J$, siis $K > J$ tõttu kehtib $a > b$. Et aga element a jääb tagasipaigutamisel j-ndasse veergu ning b k-ndasse veergu, siis tekib vastuolu tõsiasjaga, et maatriksi (a'_{ij}) l-is rida on järjestatud mittekahanevalt. Saadud vastuolu tõestabki väite.

Viienda näitena tõestame, et iga positiivse irratsionaalarvu ξ korral leidub lõpmata palju ratsionaalarvusid $\frac{p}{q}$ (kus p ja q on ühistegurita) nii, et

$$\left|\xi - \frac{p}{q}\right| \leqslant \frac{1}{q^2}.$$

Vaatleme suvalise $k \in \mathbb{N}_1$ korral arvusid $0, \{\xi\}, \{2\xi\}, \ldots, \{k\xi\}$, kus $\{\beta\}$ tähistab arvu β murdosa. Jaotame lõigu $[0, 1]$ punktidega $\frac{1}{k}, \ldots, \frac{k-1}{k}$ kokku k intervalliks:



Nendesse k intervalli peavad paigutuma vaadeldavad $k+1$ arvu $0, \{\xi\}, \{2\xi\}, \ldots, \{k\xi\}$. Dirichlet' printsiibi kohaselt leidub intervall, milles asub korraga kaks vaadeldavaist murdosadest. Seega leiduvad naturaalarvud $q_1 < q_2$ ning s nii, et

$$\frac{s}{k} \leqslant \{q_1\xi\} < \frac{s+1}{k} \quad \text{ja} \quad \frac{s}{k} \leqslant \{q_2\xi\} < \frac{s+1}{k}.$$

Kui nüüd tähistada $q = q_2 - q_1$, siis $0 < q \leqslant k$, $q_2\xi - \{q_2\xi\} = [q_2\xi] \in \mathbb{Z}$ ning $q_1\xi - \{q_1\xi\} = [q_1\xi] \in \mathbb{Z}$. Viimaseid võrdusi pooliti lahutades saame

$$q\xi - (\{q_2\xi\} - \{q_1\xi\}) = [q_2\xi] - [q_1\xi] = p \in \mathbb{Z}.$$

Siit nähtub, et

$$q\xi - p = \{q_2\xi\} - \{q_1\xi\} < \frac{1}{k},$$

millest järeldub

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{kq} < \frac{1}{q^2}.$$

Oletame nüüd, et leidub vaid lõplik arv t taandumatuid murdusid

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_t}{q_t} \quad \text{nii, et iga} \quad i \in \overline{1,t} \quad \text{korral} \quad \left|\xi - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}.$$

Et ξ on irratsionaalarv, siis saame valida sellise arvu k_0, et iga $i \in \overline{1,t}$ korral

$$\left|\xi - \frac{p_i}{q_i}\right| > \frac{1}{k_0}.$$

Korrates nüüd eeltoodud mõttekäiku arvuga k_0 arvu k asemel leiame taandumatu murru $\frac{p}{q}$ selliselt, et $|\xi - \frac{p}{q}| < \frac{1}{k_0 q} < \frac{1}{q^2}$. Seosest $\frac{1}{k_0 q} < \frac{1}{k_0}$ nähtub $\frac{p}{q} \notin \{\frac{p_i}{q_i} : i \in \overline{1,t}\}$, mis on vastuolus t valikuga. Seega kõnesolnud murdusid $\frac{p_i}{q_i}$ ei saa olla lõplik arv.

Kuuenda näitena tõestame veel järgmise väite.

Teoreem 2. Igas järjendis $a = (a_1, a_2, \dots, a_{n^2+1})$, mille komponentideks on n^2+1 erinevat elementi lineaarselt järjestatud hulgast $\mathcal{H}$, saab leida sellise alamjärjendi $(a_{i_1}, a_{i_2}, \dots, a_{i_{n+1}})$ (kus $i_1 < i_2 < \dots < i_{n+1}$), milles kas

$$a_{i_1} < a_{i_2} < \dots < a_{i_{n+1}} \qquad \text{või} \qquad a_{i_1} > a_{i_2} > \dots > a_{i_{n+1}}.$$

Tõestus. Konkreetsuseks oletame, et antud järjendil a puuduvad kahanevad alamjärjendid pikkusega $n+1$ ja näitame, et siis leidub kasvav alamjärjend pikkusega $n+1$. Fikseerime antud järjendi a suvalise elemendi a_i ning vaatleme kõiki selle elemendiga algavaid kahanevaid alamjärjendeid. Nende alamjärjendite seas peab vähemalt üks olema maksimaalse pikkusega – selle pikkuse tähistame sümboliga l_i (tehtud oletuse kohaselt $1 \leqslant l_i \leqslant n$). Seega oleme antud järjendi iga elemendi a_i taglastanud naturaalarvuga l_i, selle elemendiga algavate kahanevate alamjärjendite maksimaalse pikkusega (kui elemendile a_i selles järjendis väiksemaid elemente ei järgne, siis loeme $l_i = 1$).

Tähistagu $N(l)$ naturaalarvuga l taglastuvate elementide arvu järjendis a. Et $N(1) + N(2) + \dots + N(n) = n^2 + 1$, siis leidub $l \in \overline{1,n}$, mille korral $N(l) \geqslant n+1$, sest vastasel juhul saaksime ilmse vastuolu:

$$N(1) + N(2) + \dots + N(n) \leqslant \underbrace{n + n + \dots + n}_{n \text{ korda}} = n^2.$$

Sümboli $N(l)$ tähendusest nähtub, et järjendis a leidub vähemalt $n+1$ elementi (tähistame neid $a_{i_1}, a_{i_2}, \ldots, a_{i_{n+1}}$ nende järjendis a esinemise järjekorras), millest igaühe korral temast algavate kahanevate alamjärjendite maksimaalpikkuseks on üks ja seesama arv l. Osutub, et niiviisi moodustatud alamjärjend $(a_{i_1}, a_{i_2}, \ldots, a_{i_{n+1}})$ on kasvav. Tõepoolest, iga $k = 1, 2, \ldots, n$ korral $a_{i_k} < a_{i_{k+1}}$, sest juhul $a_{i_k} > a_{i_{k+1}}$ oleks $a_{i_{k+1}}$ ju oma valiku tõttu alguselemendiks mingile l-elemendilisele kahanevale alamjärjendile ja a_{i_k} osutuks seega $(l+1)$-elemendilise kahaneva alamjärjendi alguselemendiks, mis on aga vastuolus elemendi a_{i_k} valikuga.

Saadud tulemus ei ole triviaalse iseloomuga. Tõesti, kui lugeda $\mathcal{H} \subseteq \mathbb{Z}$, siis tuleks meil juhul $n = 2$ vahetult läbi vaadata hulga $\overline{1,5}$ kõik $5! = 120$ permutatsiooni, et veenduda igas neist 3-liikmelise kasvava või kahaneva alamjärjendi olemasolus (juhul $n = 3$ tuleks läbi vaadata juba $10! = 3628000$ permutatsiooni).

1927. aastal tõestas B. L. van der Waerden nn. *Baudet' hüpoteesi*: kui naturaalarvude hulk tükeldada kaheks osaks, siis vähemalt ühes neist leidub kuitahes pikki aritmeetilisi progressioone. Eriti viljaka üldistuse van der Waerdeni tulemusele ja ka Dirichlet' printsiibile andis 1930. aastal inglise matemaatik F. P. Ramsey. Tema tulemustest on viimaste aastakümnetega välja kasvanud terve uus kombinatoorika haru, nn. *Ramsey teooria*, mis üsna üldiselt väljendudes püüab selgitada, millised struktureeritud hulga omadused tema iga tükelduse mõnes tükis säilivad. Üheks näiteks on van der Waerdeni juba mainitud tulemus, teiseks näiteks aga järgnev teoreem, milles üldistatakse Dirichlet' printsiibile tuginevaid kaalutlusi.

Teoreem 3. Kui naturaalarvud t, n_1, n_2, ..., n_t ja m on valitud selliselt, et $m \leqslant \min(n_1, n_2, \ldots, n_t)$, siis leidub *Ramsey arvuks* nimetatav (minimaalne) naturaalarv $N = N(n_1, n_2, \ldots, n_t; m)$ nii, et iga naturaalarvu $n \geqslant N$ korral suvalise n-elemendilise hulga S kõigi m-elemendiliste alamhulkade pere $\mathfrak{B}_m(S)$ mistahes tükelduse

$$\mathfrak{B}_m(S) = \mathfrak{S}_1 \cup \mathfrak{S}_2 \cup \ldots \cup \mathfrak{S}_t$$

jaoks leidub selline $i \in \overline{1,t}$ ja n_i-elemendiline alamhulk $S' \subset S$, et $\mathfrak{B}_m(S') \subset \mathfrak{S}_i$.

Tõestus. Esimese sammuna vaatleme juhtu $t = 1$. Sel korral on teoreemi väide triviaalne. Tõepoolest, siis $\mathfrak{B}_m(S) = \mathfrak{S}_1$. Seega kui võtta $N(n_1; m) = n_1$, siis $n \geqslant n_1$ korral leidub igas n-elemendilises hulgas S (seose $m \leqslant n_1$ kehtivuse tõttu) n_1-elemendilisi alamhulkasid $S' \subset S$, mille korral $\mathfrak{B}_m(S') \subset \mathfrak{S}_1$.

Tõestuse teise sammuna redutseerime juhu $t = 3$ juhule $t = 2$, s.t. näitame, et kui juhul $t = 2$ teoreemi väide kehtib, siis kehtib ta ka juhul $t = 3$, mil meil on tegemist tükeldusega $\mathfrak{B}_m(S) = \mathfrak{S}_1 \cup \mathfrak{S}_2 \cup \mathfrak{S}_3 = \mathfrak{S}_1 \cup (\mathfrak{S}_2 \cup \mathfrak{S}_3)$. Kui teoreem juhul $t = 2$ kehtib, siis leidub arv $n_2' = N(n_2, n_3; m)$ ja seega ka arv $N(n_1, n_2'; m)$. Olgu naturaalarv $n \geqslant N(n_1, n_2'; m)$ ja hulk S (kus $|S| = n$) suvalised. Siis on võimalikud kaks juhtu:

(1) leidub n_1-elemendiline alamhulk $S' \subset S$ nii, et $\mathfrak{B}_m(S') \subset \mathfrak{S}_1$ või

(2) leidub n_2'-elemendiline alamhulk $S' \subset S$ nii, et $\mathfrak{B}_m(S') \subset \mathfrak{S}_2 \cup \mathfrak{S}_3$.

Reduktsiooni põhjendamiseks piisab vaadelda juhtu (2). Sel korral võtame hulga $\mathcal{S}'$ hulga $\mathcal{S}$ osas baashulgana. Et kehtib $|\mathcal{S}'| \geqslant N(n_2, n_3; m)$, siis arvu $N(n_2, n_3; m)$ definitsioonist tulenevalt kas leidub n_2-elemendiline alamhulk $\mathcal{S}'' \subset \mathcal{S}'$, mille korral $\mathfrak{B}_m(\mathcal{S}'') \subset \mathfrak{S}_2 \cap \mathfrak{B}_m(\mathcal{S}') \doteq \mathfrak{S}'_2$ või siis leidub n_3-elemendiline alamhulk $\mathcal{S}'' \subset \mathcal{S}'$, mille korral $\mathfrak{B}_m(\mathcal{S}'') \subset \mathfrak{S}_3 \cap \mathfrak{B}_m(\mathcal{S}') \doteq \mathfrak{S}'_3$. Et $\mathcal{S}'' \subset \mathcal{S}' \subset \mathcal{S}$ ja $\mathfrak{S}'_2 \subset \mathfrak{S}_2$, $\mathfrak{S}'_3 \subset \mathfrak{S}_3$, siis näeme, et teoreemi väide kehtib ka juhul $t = 3$, tingimusel, et ta kehtib juhul $t = 2$.

Kolmanda sammuna vihjame tõestuse üldskeemi. Eelmise sammu reduktsiooni $t = 3 \rightsquigarrow t = 2$ võib nimelt vaadelda kui analoogiliste reduktsioonide näidist ja niimoodi saab üles ehitada reduktsioonide ahela $t = n \rightsquigarrow t = n - 1 \rightsquigarrow \cdots \rightsquigarrow t = 2$.

Neljanda sammuna näitame, et juhul $t = 2$ kehtivad seosed

$$N(n_1, n_2; 1) = n_1 + n_2 - 1, \tag{20.1}$$

$$N(n_1, m; m) = n_1, \tag{20.2}$$

$$N(m, n_2; m) = n_2. \tag{20.3}$$

Seose (20.1) tõestamiseks eeldame, et on antud suvalised naturaalarvud n_1 ja n_2, $(n_1 + n_2 - 1)$-elemendiline hulk $\mathcal{S}$ ning vastav tükeldus $\mathfrak{B}_1(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2$. Vaadeldaval juhul ($m = 1$) on üsna ilmne, et kas leidub n_1-elemendiline alamhulk $\mathcal{S}' \subset \mathcal{S}$, mille korral $\mathfrak{B}_1(\mathcal{S}') = \mathcal{S}' \subset \mathfrak{S}_1$ või siis leidub n_2-elemendiline alamhulk $\mathcal{S}'' \subset \mathcal{S}$, mille korral $\mathfrak{B}_1(\mathcal{S}'') = \mathcal{S}'' \subset \mathfrak{S}_2$. Toodud arutlusest nähtub, et $N(n_1, n_2; 1) \leqslant n_1 + n_2 - 1$. Vastupidine võrratus on ilmne, sest oletus $N(n_1, n_2; 1) = n_1 + n_2 - k$, kus $k \geqslant 2$ annab vastuolu: $(n_1 + n_2 - 2)$-elemendilise hulga $\mathcal{S}$ ja tükelduse $\mathfrak{B}_1(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2$ korral, kus $|\mathfrak{S}_1| = n_1 - 1$ ja $|\mathfrak{S}_2| = n_2 - 1$ ei leidu hulgas $\mathcal{S}$ n_1-elemendilist alamhulka, mis sisalduks hulgas $\mathfrak{S}_1$ ega n_2-elemendilist alamhulka, mis sisalduks hulgas $\mathfrak{S}_2$.

Seose (20.2) tõestuseks olgu m ja n_1 sellised naturaalarvud, et $m \leqslant n_1$. Olgu veel antud naturaalarv $n \geqslant n_1$, n-elemendiline hulk $\mathcal{S}$ ja suvaline tükeldus $\mathfrak{B}_m(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2$. Juhul $\mathfrak{S}_2 \neq \emptyset$ leidub m-elemendiline alamhulk $\mathcal{S}' \subset \mathcal{S}$ nii, et $\mathcal{S}' \in \mathfrak{S}_2$, s. t. soovitud väide kehtib. Juhul $\mathfrak{S}_2 = \emptyset$ leidub n_1-elemendiline alamhulk $\mathcal{S}' \subset \mathcal{S}$, mille korral $\mathfrak{B}_m(\mathcal{S}') \subset \mathfrak{B}_m(\mathcal{S}) = \mathfrak{S}_1$, s. t. $\mathfrak{B}_m(\mathcal{S}') \subset \mathfrak{S}_1$. Neist arutlustest nähtub $N(n_1, m; m) \leqslant n_1$. Oletame, et $N(n_1, m; m) < n_1$. Võtnud suvalise $N(n_1, m; m)$-elemendilise hulga $\mathcal{S}$ ja tükelduse $\mathfrak{S}_1 = \mathfrak{B}_m(\mathcal{S})$, $\mathfrak{S}_2 = \emptyset$ näeme, et ei saa valida ei n_1-elemendilist alamhulka $\mathcal{S}' \subset \mathcal{S}$ nii, et $\mathfrak{B}_m(\mathcal{S}') \subset \mathfrak{S}_1$, ega ka m-elemendilist alamhulka $\mathcal{S}' \subset \mathcal{S}$, mille korral $\mathfrak{B}_m(\mathcal{S}') \subset \mathfrak{S}_2$. Saadud vastuolu tõestabki võrduse (20.2). Seose (20.3) tõestus on analoogiline äsjatooduga.

Viienda sammuna täpsustame juhul $t = 2$ kõigepealt induktsiooni baasi. Seosed (20.1) – (20.3) lubavad eeldada, et kehtib võrratus $m < \min(n_1, n_2)$.

Eeldame arvude $N(n_1 - 1, n_2; m) = p_1$ ja $N(n_1, n_2 - 1; m) = p_2$ leidumist, samuti ka arvude $N(n'_1, n'_2; m - 1)$ leidumist juhtudel $1 < m - 1 \leqslant \min(n'_1, n'_2)$, millest tuleneb arvu $N(p_1, p_2; m - 1)$ eksisteerimine. Nendel eeldustel tahame näidata, et eksisteerib arv $N(n_1, n_2; m)$, kusjuures

$$N(n_1, n_2; m) \leqslant N(p_1, p_2; m - 1) + 1. \tag{20.4}$$

Kuuenda sammuna viime läbi induktsiooni. Olgu antud naturaalarv n, mis rahuldab tingimust $n \geqslant N(p_1,p_2;m-1)+1$, n-elemendiline hulk $\mathcal{S}$ ning tükeldus $\mathfrak{B}_m(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2$. Fikseerime mingi elemendi $x \in \mathcal{S}$ ja olgu $\mathcal{S} = \mathcal{T} \cup \{x\}$. Alamhulkade hulga $\mathfrak{B}_m(\mathcal{S})$ antud tükeldusega saame siduda uue tükelduse

$$\mathfrak{B}_{m-1}(\mathcal{T}) = \mathfrak{S}_1^- \cup \mathfrak{S}_2^- \tag{20.5}$$

järgmiselt: suvalise $(m-1)$-elemendilise alamhulga $\mathcal{R} \subset \mathcal{T}$ korral kui $\mathcal{R} \cup \{x\} \subset \mathfrak{S}_1$, siis loeme $\mathcal{R} \in \mathfrak{S}_1^-$, kui aga $\mathcal{R} \cup \{x\} \subset \mathfrak{S}_2$, siis loeme $\mathcal{R} \in \mathfrak{S}_2^-$. Konstruktsioonist on selge, et $|\mathcal{T}| \geqslant N(p_1,p_2;m-1)$. Seega kas

a) $\mathcal{T}$ sisaldab p_1-elemendilist alamhulka, mille kõik $(m-1)$-elemendilised alamhulgad pärinevad perest $\mathfrak{S}_1^-$ või

b) $\mathcal{T}$ sisaldab p_2-elemendilist alamhulka, mille kõik $(m-1)$-elemendilised alamhulgad pärinevad perest $\mathfrak{S}_2^-$.

Järgnevas analüüsime juhtu a), mil leidub p_1-elemendiline alamhulk $\mathcal{T}' \subset \mathcal{T}$ nii, et $\mathfrak{B}_{m-1}(\mathcal{T}') \subset \mathfrak{S}_1^-$. Et aga $p_1 = N(n_1-1,n_2;m)$, siis leidub selline alamhulk $\mathcal{T}'' \subset \mathcal{T}'$, et kas

$$|\mathcal{T}''| = n_1 - 1 \quad \text{ja} \quad \mathfrak{B}_m(\mathcal{T}'') \subset \mathfrak{S}_1 \cap \mathfrak{B}_m(\mathcal{T}') \tag{20.6}$$

või

$$|\mathcal{T}''| = n_2 \quad \text{ja} \quad \mathfrak{B}_m(\mathcal{T}'') \subset \mathfrak{S}_2 \cap \mathfrak{B}_m(\mathcal{T}'). \tag{20.7}$$

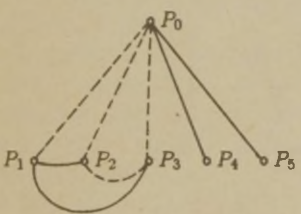
Oletame algul, et aset leiab juht (20.7). Siis $\mathcal{T}'' \subset \mathcal{T}' \subset \mathcal{S}$, $|\mathcal{T}''| = n_2$ ja $\mathfrak{B}_m(\mathcal{T}'') \subset \mathfrak{S}_2$ näitavad, et täidetud on kõik nõuded ning selles suunas osutub väide (20.4) tõestatuks.

Oletame nüüd, et aset leiab juht (20.6). Siis on meil $\mathcal{T}'' \subset \mathcal{T}'$, $|\mathcal{T}''| = n_1 - 1$ ja $\mathfrak{B}_m(\mathcal{T}'') \subset \mathfrak{S}_1$. Olgu $\mathcal{T}^* = \mathcal{T}'' \cup \{x\}$, siis $|\mathcal{T}^*| = n_1$ ning saab näidata, et $\mathfrak{B}_m(\mathcal{T}^*) \subset \mathfrak{S}_1$. Selleks vaatleme suvalist m-elemendilist alamhulka $\mathcal{M} \subset \mathcal{T}^*$. Kui osutub, et $x \notin \mathcal{M}$, siis $\mathcal{M} \subset \mathcal{T}''$ ja seoste (20.6) tõttu seega $\mathcal{M} \in \mathfrak{S}_1$. Kui aga $x \in \mathcal{M}$, siis $\mathcal{M} = \{x\} \cup \mathcal{M}'$, kus $\mathcal{M}' \subset \mathcal{T}''$, $|\mathcal{M}'| = m-1$. Et $\mathcal{T}'' \subset \mathcal{T}'$, siis $\mathfrak{B}_{m-1}(\mathcal{T}'') \subset \mathfrak{B}_{m-1}(\mathcal{T}') \subset \mathfrak{S}_1^-$ (viimane sisalduvus juhu a) vaatlemise tõttu). Seega kehtib $\mathfrak{B}_{m-1}(\mathcal{T}'') \subset \mathfrak{S}_1^-$, millest $\mathcal{M}' \in \mathfrak{S}_1^-$ ning siit tükelduse $\mathfrak{S}_1^- \cup \mathfrak{S}_2^-$ definitsiooni arvestades tuleneb omakorda, et $\mathcal{M} = \mathcal{M}' \cup \{x\} \in \mathfrak{S}_1$. Kokkuvõttes oleme tõestanud, et nii juhul (20.6) kui ka juhul (20.7) kehtib $\mathcal{M} \in \mathfrak{S}_1$, millega seos $\mathfrak{B}_m(\mathcal{T}^*) \subset \mathfrak{S}_1$ on ka põhjendatud. Järelikult, alamhulk $\mathcal{T}^* \subset \mathcal{S}$ on soovitud omadustega: $|\mathcal{T}^*| = n_1$ ja $\mathfrak{B}_m(\mathcal{T}^*) \subset \mathfrak{S}_1$. Väite (20.4) tõestus on juhul a) sellega ammendatud, tõestus juhul b) toimub aga täiesti analoogiliselt.

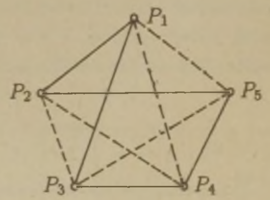
Toome ka ära teadaolevate Ramsey arvude $N(n_1,n_2;2)$ tabeli, mis on autori Stanisław P. Radziszowski loal võetud tema aruandest "Small Ramsey Numbers" (Technical Report RIT–TR–93–009, Rochester Institute of Technology, Rochester, NY, February, 1993). Arvude paariga $^{a}\ _{b}$ toodava tabeli ühes lahtris on tähistatud olukorda, mil vastava Ramsey arvu kohta teatakse esialgu vaid tõkkeid $a \leqslant N(n_1, n_2; 2) \leqslant b$, s. t. see arv kuulub lõiku $[a, b]$. Valemeid (20.2) ja (20.3) arvestades on tabelis ära jäetud juhud $n_1 = 2$ ja $n_2 = 2$:

n_1 \ n_2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	6	9	14	18	23	28	36	40 43	46 51	51 60	59 69	66 78	73 89
4	9	18	25	35 41	49 62	53 85	69 116	80 151	93 191	97 238	112 291	119 349	121 417
5	14	25 26	43 50	58 89	76 145	95 219	? 320						
6	18	35 41	58 89	102 166	? 304	? 499	? 786						
7	23	49 62	76 145	? 304	205 582	? 1048	? 1783						
8	28	53 85	95 219	? 499	? 1048	282 1998	? 3675						
9	36	69 116	? 320	? 786	? 1783	? 3675	565 7134						
10	40 43	80 151						798 ?					

Arvutame näitena arvu $N(3,3;2)$, vaadeldes vastavat ülesannet graafiteoreetilises interpretatsioonis. Olgu antud kuuetipuline täielik graaf, kus iga serv on värvitud kas punaseks või siniseks. Näitame, et sellises graafis sisaldub monokromaatiline kolmnurk. Toetudes vasakpoolsele joonisele fikseerime tipu P_0 ning vaatleme servade P_0P_1, P_0P_2, $\ldots$, P_0P_5 hulka. Et kasutatud on ainult kaht värvi, siis mingid kolm nendest viiest servast peavad olema üht värvi, olgu näiteks P_0P_1, P_0P_2 ja P_0P_3 punased. Kui nüüd vähemalt üks servadest P_1P_2, P_1P_3 või P_2P_3 osutub punaseks, siis oleks punane kolmnurk meil käes, näiteks kui P_2P_3 on punane, siis on seda ka kolmnurk $\Delta(P_0, P_2, P_3)$. Seega peame eeldama, et servad P_1P_2, P_1P_3 ja P_2P_3 on sinised, millega oleme aga leidnud sinise kolmnurga $\Delta(P_1, P_2, P_3)$. See arutlus näitab, et $N(3,3;2) \leqslant 6$.



Parempoolsel joonisel on toodud viietipuline täielik graaf ning antud tema servade niisugune värvimisviis kahe värviga, mille korral selles graafis ei teki monokromaatilist kolmnurka. Sellest konkreetsest näitest järeldub, et $N(3,3;2) > 5$. Kokkuvõttes oleme seega saanud võrduse $N(3,3;2) = 6$.



Teise näitena tõestame, et

$$N(\underbrace{3,\ldots,3}_{t};t) \leqslant [e{\cdot}t!] + 1, \tag{20.8}$$

kus $[x]$ tähendab arvu x täisosa ning $e = 2,71828182\ldots$ on naturaallogaritmide alus. Seose (20.8) põhjendame induktsiooniga t järgi, toetudes tähelepanekule, et juhtu $t = 2$ käsitlesime juba eelmises näites. Vaatleme $([e{\cdot}t!] + 1)$-elemendilise tipuhulgaga $\mathcal{V}$ täielikku graafi $G = G(\mathcal{V})$, mille servad olgu värvitud t erineva värviga. Märkame, et siis on mistahes tipuga $v \in \mathcal{V}$ intsidentseid servi $[e{\cdot}t!]$ tükki ning need servad võivad olla t erinevat värvi. Et aga

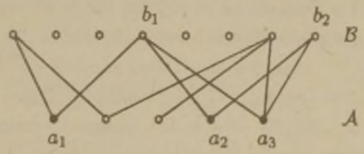
$$[e{\cdot}t!] = \Big[\sum_{k\geqslant 0}\frac{t!}{k!}\Big] = \sum_{k=0}^{t}\frac{t!}{k!} = 1 + t\sum_{k=0}^{t-1}\frac{(t-1)!}{k!} = 1 + t[e{\cdot}(t-1)!],$$

siis üks värvidest (näiteks sinine) esineb tipuga v intsidentsetel servadel vähemalt $1+[e{\cdot}(t-1)!]$ korda. Tähistame sümboliga $\mathcal{V}'$ nende tippude alamhulka, mis on tipuga v intsidentsed sinise serva kaudu. Kui $\mathcal{V}'$ mõnd tipupaari $\{v', v''\}$ ühendaks sinine serv, siis see paar koos tipuga v moodustaks monokromaatilise (sinise) kolmnurga. Kui aga alamhulga $\mathcal{V}'$ ükski tipupaar sinise servaga seotud ei ole, siis tipuhulgaga $\mathcal{V}'$ indutseeritud $([e{\cdot}(t-1)!] + 1)$-tipulise täieliku alamgraafi G' servade hulk oleks värvitud mitte rohkem kui $(t-1)$ värviga. Sellest ning induktsiooni oletusest tulenevalt sisaldaks graaf G' monokromaatilise kolmnurga ühega nendest $(t-1)$ värvist. See arutlus põhjendabki induktsiooni sammus vajaliku ülemineku $(t-1)$-lt t-le.

Vahetu järeldusena äsjatõestatud hinnangust (20.8) saame: kui antud n-elemendilise hulga mittetühjadel alamhulkadel on tehtud t-värvimine, siis küllalt suure n korral leiduvad alati kaks mittetühja disjunktset alamhulka $\mathcal{A}$ ja $\mathcal{B}$ nii, et $\mathcal{A}, \mathcal{B}$ ja $\mathcal{A} \cup \mathcal{B}$ on samavärvilised. Tõepoolest, olgu $n = [e{\cdot}t!]$ ning olgu (mingi) hulga $\mathcal{H}_{n+1} = \{h_1, h_2, \ldots, h_n, h_{n+1}\}$ alamhulga $\mathcal{H}_n = \{h_1, h_2, \ldots, h_n\}$ mittetühjad alamhulgad t-värvitud. Moodustades täieliku graafi $G(\mathcal{H}_{n+1})$ võtame selle servadel kasutusele uue värvimisviisi niisuguse reegliga: tipupaari $\{h_i, h_j\}$, kus $1 \leqslant i < j \leqslant n+1$ värvime sama värviga, millega on värvitud alamhulk $\{h_i, \ldots, h_{j-1}\} \subseteq \mathcal{H}_n$. Tänu äsjatõestatud seosele (20.8) leidub graafis $G(\mathcal{H}_{n+1})$ monokromaatiline kolmnurk. Seejuures, kui selle kolmnurga tippudeks on h_u, h_v ja h_w hulgast $\mathcal{H}_{n+1}$, siis osutuvad alamhulgad $\mathcal{A} = \{h_u, \ldots, h_{v-1}\}$, $\mathcal{B} = \{h_v, \ldots, h_{w-1}\}$ ja $\mathcal{A} \cup \mathcal{B} = \{h_u, \ldots, h_{w-1}\}$ kõik kolm ühe ja sama värvilisteks, s. t. täidavad soovitud nõudeid.

Graafiteoreetiline käsitlus võimaldab siin enamatki. Olgu antud bikromaatiline graaf $G = G(\mathcal{V}, \mathcal{E})$ servahulgaga $\mathcal{E}$ ning tipuhulga tükeldusega $\mathcal{V} = \mathcal{A} \cup \mathcal{B}$, kus $\mathcal{A}$ olgu omakorda t-tükeldatud ehk t-värvitud (s. t. kui tõlgendada hulga $\mathcal{A}$ tükeldamisel tekkinud tükke värvidena). Ütleme, et tipp $b \in \mathcal{B}$ on *monokromaatiliselt seotud*, kui kõik temaga intsidentsed tipud $a \in \mathcal{A}$ on üht ja sama värvi, s. t. kuuluvad antud t-värvimise ühte ja samasse tükki.

Kõrvaloleval joonisel on bikromaatilise graafi tipuhulgas $\mathcal{A}$ näidatud 2-värvimine, mille korral tipud $b_1, b_2 \in \mathcal{B}$ osutuvad monokromaatiliselt seotuks. Graafi G nimetame *t-separaatseks*, kui igasuguste $t' \leqslant t$ ja hulga $\mathcal{A}$ t'-värvimise korral leidub hulgas $\mathcal{B}$ monokromaatiliselt seotud tipp. Küsimus sellest, millised bikromaatilised graafid on t-separaatsed, osutub graafiteoorias üsna oluliseks. Järgnevalt veendumegi, et Ramsey teooria mitmeid põhitulemusi saab sõnastada kui vastust nimetatud küsimusele.



Esimese näitena defineerime bikromaatilise graafi $G_n = G_n(\mathcal{A} \cup \mathcal{B}, \mathcal{E})$ järgmiselt. Fikseerime naturaalarvud m ja t ning olgu $\mathcal{A} = \overline{1,n}$ ja $\mathcal{B}$ m-liikmeliste aritmeetiliste progressioonide hulk vaadeldaval lõigul $\overline{1,n}$. Tipud $a \in \mathcal{A}$ ja $b \in \mathcal{B}$ loeme graafis G_n servaga seotuiks siis, kui naturaalarv a sisaldub aritmeetilises progressioonis b. *Van der Waerdeni teoreemi* (aritmeetilistest progressioonidest) saab nüüd sõnastada kui väidet: leidub selline funktsioon $W(m,t)$, et iga $n \geqslant W(m,t)$ korral on graaf G_n t-separaatne. Tavaliselt sõnastatakse seda väidet kujul: kui antud m ja t korral t-värvida piisavalt pikk naturaalarvude lõik, siis sellel lõigul eksisteerib monokromaatiline m-liikmeline aritmeetiline progressioon.

Teise näitena defineerime bikromaatilise graafi $G_n = G_n(\mathcal{A} \cup \mathcal{B}, \mathcal{E})$ järgmiselt: $\mathcal{A} = \overline{1,n}$, $\mathcal{B} = \{\{x, y, x+y\} : \{x, y\} \subseteq \overline{1,n}\}$ ning tipud $a \in \mathcal{A}$ ja $\{x, y, x+y\} = b \in \mathcal{B}$ loeme ühendatuiks servaga siis, kui $a \in b$. Nõue graafi G_n t-separaatsusest on ilmsesti samaväärne väitega, et kehtib järgmine *I. Schuri teoreem*: leidub selline funktsioon $S(t)$ hulgal N_1, et iga $n \geqslant S(t)$ ning lõigu $\overline{1,n}$ suvalise t-värvimise korral leidub monokromaatiline kolmik $\{x, y, z\} \subseteq \overline{1,n}$ omadusega $x + y = z$. Selle tulemuse tõestame hiljem teoreemina 9, kuigi teda saaks üldistada ka näiteks $x, y, z \in \overline{1,n}$ korral kõikidest elementidest kujul x, y, z, $x+y$, $x+z$, $y+z$, $x+y+z$ koosnevale hulgale, mis viib nn. Folkmani teoreemi juurde.

Kolmanda näitena olgu $m \in \mathrm{N}_1$ fikseeritud ning vaatleme bikromaatilist graafi $G_\infty(\mathcal{A} \cup \mathcal{B}, \mathcal{E})$, kus $\mathcal{A}$ on mingi loenduva hulga S kõigi m-elemendiliste alamhulkade hulk ning $\mathcal{B}$ on sellesama hulga kõigi lõpmatute alamhulkade hulk, kusjuures tipud $a \in \mathcal{A}$ ja $b \in \mathcal{B}$ loeme seotuiks servaga siis, kui $a \subsetneq b$. Ramsey teoreemi lõpmatu versioon sõnastub neis termineis kujul: graaf G_∞ on t-separaatne $t \in \mathrm{N}_1$ iga valiku puhul. Tõestamegi nüüd selle väite järgmises sõnastuses.

Teoreem 4. Olgu antud suvaline naturaalarv t, loenduv hulk $\mathcal{S}$ ning selle kõigi m-elemendiliste alamhulkade hulga $\mathfrak{B}_m(\mathcal{S})$ t-tükeldus

$$\mathfrak{B}_m(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2 \cup \ldots \cup \mathfrak{S}_t.$$

Siis leiduvad lõpmatu alamhulk $\mathcal{S}' \subsetneq \mathcal{S}$ ja indeks $i \in \overline{1,t}$ nii, et $\mathfrak{B}_m(\mathcal{S}') \subsetneq \mathfrak{S}_i$.

Tõestus. Juht $m = 1$ on samaväärne Dirichlet' printsiibi lõpmatu versiooniga: kui lõpmata palju objekte paigutub lõplikku arvu pesadesse, siis leidub pesa, millesse paigutub lõpmata palju objekte.

Juhul $m = 2$ tõlgendame $\mathfrak{B}_2(\mathcal{S})$ kui servade hulka täielikus graafis tipuhulgaga $\mathcal{S} = \{h_1, h_2, \ldots\}$ ning tükeldust $\mathfrak{B}_2(\mathcal{S}) = \mathfrak{S}_1 \cup \mathfrak{S}_2 \cup \ldots \cup \mathfrak{S}_t$ kui selle hulga t-värvimist $\phi : \mathfrak{B}_2(\mathcal{S}) \to \overline{1,t}$. Et tipuga h_1 intsidentseid servi $\{h_1, h_j\}$ on lõpmata palju, siis peab nendel servadel üks värvidest (olgu see $v_1 \in \overline{1,t}$) esinema lõpmata hulk kordi. Tähistame vastavate servade tipust h_1 erinevatest otspunktidest moodustuvat hulka

$$\mathcal{S}_1 = \{h_{x_j} : h_{x_j} \in \mathcal{S} \text{ ja } \phi(\{h_1, h_{x_j}\}) = v_1\}$$

ning vaatleme seejärel servi kujul $\{h_{x_1}, h_{x_j}\}$, kus $j > 1$. Et ka neid servi on lõpmata palju, siis peab nende seas ühevärvilisi (näiteks värvi v_2) olema lõpmata palju. Olgu

$$\mathcal{S}_2 = \{h_{y_j} : h_{y_j} \in \mathcal{S}_1 \text{ ja } \phi(\{h_{x_1}, h_{y_j}\}) = v_2\}$$

ning vaatleme servi kujuga $\{h_{y_1}, h_{z_j}\}$. Analoogiliselt jätkates saame lõpuks hulga

$$\mathcal{S}_* = \{h_1, h_{x_1}, h_{y_1}, h_{z_1}, \ldots\},$$

millesse kuuluvate tippude h_{p_1} ja h_{q_1} paari kui serva värvi määrab täielikult ära arv $\min\{p_1, q_1\}$. Seetõttu ilmneb hulgal $\mathcal{S}_*$ uus värvimine ϕ_*, kus

$$\phi_*(h_{p_1}) = \phi(\{h_{p_1}, h_{q_1}\})$$

suvaliste $h_{q_1} \in \mathcal{S}_*$ ja $q_1 > p_1$ korral. Vastavalt Dirichlet' printsiibi lõpmatule versioonile leidub lõpmatu ja ϕ_*-monokromaatiline alamhulk $\mathcal{S}'_* \subsetneq \mathcal{S}_*$. Värvimisviisi ϕ_* definitsioonist nähtuvalt on servad kujuga $\{h_{p'_1}, h_{q_1}\}$ (kus $h_{p'_1} \in \mathcal{S}'_*$ ja $q_1 > p'_1$) kõik ühevärvilised värvimise ϕ suhtes. Olemegi saanud soovitud tulemuse erijuhul $m = 2$.

Teoreemi 4 saab tõestada induktsiooniga m järgi. Et aga induktiivse üleminekuga m-lt $(m+1)$-le seotu ilmneb oma põhilises osas selgesti juba üleminekul 2-lt 3-le, siis tekib võimalus hoiduda raskepärase üldjuhu käsitlusest ja siiski saavutada veendumus selle võimalikkuses. Üleminekut 2-lt 3-le vaadeldes defineerime antud värvimisviisi $\phi : \mathfrak{B}_3(\mathcal{S}) \to \overline{1,t}$ korral uue värvimisviisi $\phi_1 : \mathfrak{B}_2(\mathcal{S} \setminus \{h_1\}) \to \overline{1,t}$ reegliga

$$\phi_1(\{h_j, h_k\}) = \phi(\{h_1, h_j, h_k\}).$$

Kasutades juhul $m = 2$ saadud tulemust näeme, et leidub lõpmatu ja ϕ_*-monokromaatiline (näiteks värvi v_1) alamhulk $\mathcal{S}^{(1)}$ niisuguse omadusega, et kõigi elementide $h_{x_*} \in \mathcal{S}^{(1)}$ korral $\phi_1(\{h_{x_j}, h_{x_k}\}) = v_1$, kus $k > 1$. Hulgal $\mathfrak{B}_2(\mathcal{S}^{(1)} \setminus \{h_{x_1}\})$ defineerime uue värvimisviisi

$$\phi_2(\{h_{x_j}, h_{x_k}\}) = \phi(\{h_{x_1}, h_{x_j}, h_{x_k}\}).$$

Jällegi leidub monokromaatiline (näiteks värvi v_2) alamhulk

$$\mathcal{S}^{(2)} = \{h_{y_j} : j = 1, 2, \ldots\} \subseteq \mathcal{S}^{(1)} \setminus \{h_{x_1}\}$$

selline, et $\phi_2(\{h_{y_j}, h_{y_k}\}) = v_2$. Niiviisi jätkates moodustame lõpuks hulga

$$\mathcal{S}^{(*)} = \{h_1, h_{x_1}, h_{y_1}, \ldots\},$$

mille elementidest moodustatud kolmikutel $\{h_{p_1}, h_{q_1}, h_{r_1}\}$ määrab värvi täielikult indeks $\min\{p_1, q_1, r_1\}$. Analoogiliselt eespooltoodule saab hulgas $\mathcal{S}^{(*)}$ leida lõpmatu alamhulga $\mathcal{S}' \subseteq \mathcal{S}^{(*)}$, mille elementide kõik kolmikud on ühevärvilised. See aga ongi soovitud tulemuseks juhul $m = 3$.

Ramsey teoorias on lõpmatu ja lõplik versioon siiski tihedamas seoses kui mujal kombinatoorikas. Seda asjaolu kajastab ka nn. ***kompaktsuse printsiibi*** üks järgmistest erivormidest.

Teoreem 5. Olgu $\mathcal{H} = \{h_1, h_2, \ldots\}$ loenduv hulk ning P tema lõplike alamhulkade mingi omadus. Kui hulga $\mathcal{H}$ iga t-värvimise korral leidub monokromaatiline lõplik alamhulk omadusega P, siis leidub ka naturaalarv M selliselt, et (suvaliselt) t-värvides lõpliku alamhulga $\mathcal{H}_M = \{h_1, h_2, \ldots, h_M\}$ leidub temas monokromaatiline alamhulk omadusega P.

Tõestus on vastuväiteline: oletame, et iga $M \in \mathbb{N}_1$ korral leidub hulga $\mathcal{H}_M$ selline t-värvimine ϕ_M, mis ei anna monokromaatilist alamhulka omadusega P. Et me kasutame vaid $t < \infty$ värvi, siis mingi üks vaadeldavatest värvidest $\phi_M(h_1)$ ilmub lõpmatu hulk kordi, s. t. leidub naturaalarvude jada $(M_1^{(1)}, M_2^{(1)}, \ldots)$ nii, et

$$\phi_{M_1^{(1)}}(h_1) = \phi_{M_2^{(1)}}(h_1) = \cdots = \phi(h_1).$$

Edasi vaatleme värve $\phi_{M_i^{(1)}}(h_2)$, kus $i = 1, 2, \ldots$ Et nende värvide seas jällegi ei saa olla rohkem kui t erinevat, siis eksisteerib selline alamjada $(M_1^{(2)}, M_2^{(2)}, \ldots) \subseteq$ $\subseteq (M_1^{(1)}, M_2^{(1)}, \ldots)$, et

$$\phi_{M_1^{(2)}}(h_2) = \phi_{M_2^{(2)}}(h_2) = \cdots = \phi(h_2).$$

Sel viisil jätkates saamegi defineerida uued värvid $\phi(h_1), \phi(h_2), \ldots, \phi(h_n)$, kusjuures leidub lõpmata palju indekseid $M_i^{(n)}$, mille puhul kehtib $\phi_{M_i^{(n)}}(h_n) = \phi(h_n)$.

Jätkame ülalkirjeldatud viisil: et värvide $\{\phi_{M_i^{(n)}}(h_{n+1}) : i \in \mathrm{N}_1\}$ seas esineb üks värvidest (tähistame selle $\phi(h_{n+1})$) lõpmata palju kordi, siis eksisteerib alamjada $(M_1^{(n+1)}, M_2^{(n+1)}, \dots) \subseteq (M_1^{(n)}, M_2^{(n)}, \dots)$. Niiviisi jätkates saame hulgal $\mathcal{H}$ teatud t-värvimise ϕ. Osutub, et selle värvimisviisi korral $\mathcal{H}$ ükski ϕ-monokromaatiline lõplik alamhulk ei saa olla omadusega P. Tõepoolest, kui taoline alamhulk $\mathcal{H}'$ siiski leiduks, siis eksisteeriks ka arv $n \in \mathrm{N}_1$ selliselt, et juba $\mathcal{H}' \subseteq \mathcal{H}_n$, mistõttu oleks $\phi_{M_1^{(n)}}(h) = \phi(h)$ iga $h \in \mathcal{H}'$ korral. Sellest nähtub, et hulga $\mathcal{H}_{M_1^{(n)}} \subseteq \mathcal{H}$ $\phi_{M_1^{(n)}}$-värvimise korral oleks alamhulk $\mathcal{H}'$ monokromaatiline ning ka omadusega P. See aga räägiks vastu tõestuse alguses tehtud oletusele.

Teoreemi 5 eelduses toodud nõue, et hulga $\mathcal{H} = \{h_1, h_2, \dots\}$ iga t-värvimise korral leiduks monokromaatiline lõplik alamhulk omadusega P, ei ole täidetud automaatselt. Tõepoolest, olgu $\mathcal{H} = \mathrm{N}_1$ ning P tähendagu omadust olla arvukolmik $(x_1, x_2, x_3) \in \mathrm{N}_1^3$, mis rahuldab võrrandit $x_1 + x_2 - 3x_3 = 0$. Fikseerime suvalise naturaalarvu $p \geqslant 5$ ning teostame hulga N_1 $(p-1)$-värvimise järgmiselt: esitame iga naturaalarvu n kujul

$$n = p^{\nu(n)} \cdot (p \cdot n' + v_n), \quad \text{kus} \quad v_n \in \overline{1, p-1}$$

ja loeme v_n arvu $n \in \mathrm{N}_1$ värviks (näiteks $n = p = p^1 \cdot (p \cdot 0 + 1)$ saab värvi 1). Osutub, et sellise $(p-1)$-värvimise korral ei leidu hulgas N_1 monokromaatilist lõplikku alamhulka omadusega P. Tõepoolest, vastupidist oletades saame võrduse

$$p^{\nu(x_1)}(px_1' + v) + p^{\nu(x_2)}(px_2' + v) - 3p^{\nu(x_3)}(px_3' + v) = 0.$$

Tähistame $\nu = \min \nu(x_i)$, jagame viimase võrduse pooled arvuga p^ν ja tõlgendame saadud võrdust kongruentsina mooduli p järgi. Nii saame

$$\delta_1 v + \delta_2 v - 3\delta_3 v \equiv 0 \pmod{p},$$

kus oleme tähistanud

$$\delta_i = \begin{cases} 1, & \text{kui } \nu = \nu(x_i), \\ 0, & \text{kui } \nu < \nu(x_i). \end{cases}$$

Et arvud v ja p on ühistegurita, siis viimane kongruents omandab kuju

$$\delta_1 + \delta_2 - 3\delta_3 \equiv 0 \pmod{p},$$

mille ainsaks võimalikuks lahendiks osutub $\delta_1 = \delta_2 = \delta_3 = 0$. See annab aga vastuolu, sest ν peab ju võrduma ühega arvudest $\nu(x_i)$, s. t. vähemalt üks arvudest δ_i peab võrduma ühega. Märgime, et sama mõttekäik töötab ka lõplikus hulgas $\mathcal{H} = \overline{1, M}$.

Olgu antud lõplik hulk $\mathcal{H} = \{h_1, h_2, \dots, h_m\}$ ja naturaalarv n. Kui fikseerida pärisalamhulk $\mathcal{I} \subset \overline{1, n}$ ning funktsioon $f : \mathcal{I} \to \overline{1, m}$, siis sellega on määratud otseastme $\mathcal{H}^n = \{x : x = (x_1, \dots, x_n),\ x_i \in \mathcal{H}\}$ alamhulk

$$\mathcal{L}^{(\mathcal{I},f)} = \{(x_1,\dots,x_n) : i,j \notin \mathcal{I} \text{ korral } x_i = x_j \text{ ja } i \in \mathcal{I} \text{ korral } x_i = h_{f(i)} \in \mathcal{H}\},$$

mida nimetatakse *jooneks* hulgas $\mathcal{H}^n$. Joone punktides on seega kõik hulgast $\mathcal{I}$ pärinevate indeksitega komponendid konstantsed, ülejäänud aga muutuvad nii, et nad on alati omavahel võrdsed. Näiteks juhul $\mathcal{H} = \{h_1, h_2, h_3\}$ saame hulga $\mathcal{H}^2$ joonte moodustamiseks valida kas $\mathcal{I} = \{1\}$, või $\mathcal{I} = \{2\}$, või $\mathcal{I} = \emptyset$. Kolm võimalikku funktsiooni f annavad esimesel juhul kolm "vertikaaljoont" ning teisel juhul kolm "horisontaaljoont", kolmas juht annab aga "diagonaali" $\{(h_1,h_1), (h_2,h_2), (h_3,h_3)\}$.

Joone mõiste võimaldab näiteks käsitleda *trips-traps-trulli* teatavat üldistust "kuubistikku" $\underbrace{\mathsf{m} \times \mathsf{m} \times \cdots \times \mathsf{m}}_{n \text{ korda}}$: kaks mängijat paigutavad vaheldumisi kuubistikku üks riste ja teine sõõre ning võitjaks loetakse see, kes esimesena täidab mingi joone oma m sümboliga. Kui suvalise etteantud arvu m korral võtta n piisavalt suurena, siis võidab selle mängu alati avakäigu teinud mängija. See üllatav asjaolu järeldub järgmisest teoreemist.

Teoreem 6. Igasuguse m-elemendilise hulga $\mathcal{H}$ ja arvu $t \in \mathbb{N}_1$ jaoks leidub arv $\overline{n} = \overline{n}(m,t)$ selliselt, et kõigi $n \geqslant \overline{n}$ ning järjendite hulga $\mathcal{H}^n$ iga t-värvimise korral eksisteerib hulgas $\mathcal{H}^n$ selle värvimise suhtes monokromaatiline joon.

Tõestuse saame üheaegse induktsiooniga m ja t järgi. Juhul $m = 1$ on teoreemi väide ilmne. Oletame, et mõne $m \geqslant 2$ korral teoreemi väide kehtib kõigi nende hulkade $\mathcal{H}_*$ jaoks, kus $|\mathcal{H}_*| < m$. Valime siis nii suure arvu n_1, et $n - n_1 \ll n_1$, tõlgendame järjendite hulka $\mathcal{H}^n$ hulgana $\mathcal{H}^{n-n_1} \times \mathcal{H}^{n_1}$ ja indutseerime antud t-värvimisest $\phi : \mathcal{H}^n \to \overline{1,t}$ lähtuvalt uue värvimise $\phi_{(1)} : \mathcal{H}^{n_1} \to \overline{1,t}^{\mathcal{H}^{n-n_1}}$ reegliga: võrdus

$$\phi_{(1)}((a_1,\dots,a_{n_1})) = \phi_{(1)}((b_1,\dots,b_{n_1}))$$

kehtib parajasti siis, kui kõigi $(x_1,\dots,x_{n-n_1}) \in \mathcal{H}^{n-n_1}$ korral on õige võrdus

$$\phi((x_1,\dots,x_{n-n_1},a_1,\dots,a_{n_1})) = \phi((x_1,\dots,x_{n-n_1},b_1,\dots,b_{n_1})).$$

Märgime täiendavalt, et järjendit $a \in \mathcal{H}^{n_1}$ värvitakse siin sõltuvalt funktsioonist $\phi(x,a)$, kus $x \in \mathcal{H}^{n-n_1}$, mistõttu $\phi_{(1)}$ näol on tegemist $t^{m^{n-n_1}}$-värvimisega. Et aga $\phi_{(1)}$ on ühtlasi värvimiseks ka alamhulga $\mathcal{H}_1 = \{h_1,\dots,h_{m-1}\} \subset \mathcal{H}$ otseastmel $\mathcal{H}_1^{n_1}$, siis induktsiooni oletuse tõttu (kui n_1 on võetud piisavalt suurena) leidub $\phi_{(1)}$-monokromaatiline joon $\mathcal{L}_1 \subset \mathcal{H}_1^{n_1}$. Järjenditel hulgast $\mathcal{H}^{n-n_1} \times \mathcal{L}_1$ on viimased n_1 komponenti määratud joone $\mathcal{L}_1$ punktidena ning vastavaid spetsifikatsioone tähistame $L_1(i_1)$, kus $i_1 \in \overline{1,m-1}$: kui joont $\mathcal{L}_1$ määravaks indeksite hulgaks on $\mathcal{I}_1 \subset \overline{1,n_1}$ ja funktsiooniks f_1, siis

$$L_1(i_1) = (\dots, h_{i_1}, \dots, h_{f_1(i)}, \dots),$$

kusjuures koordinaadid $h_{f_1(i)}$ on joone $\mathcal{L}_1$ kõigis punktides spetsifitseeritud ühtviisi.

Kordame nüüd toodud mõttekäiku hulgaga $\mathcal{H}^{n-n_1}$ hulga $\mathcal{H}$ rollis. Valinud seejuures n_2 nii suurena, et $(n-n_1)-n_2 \ll n_2$ ning vaadeldes hulka $\mathcal{H}^{n-n_1}$ kui hulka $\mathcal{H}^{n-n_1-n_2} \times \mathcal{H}^{n_2}$, indutseerime reegliga: võrdus

$$\phi_{(2)}(a_1,\dots,a_{n_2}) = \phi_{(2)}(b_1,\dots,b_{n_2})$$

kehtib siis ja ainult siis, kui seos

$$\phi((x_1,\dots,x_{n-n_1-n_2},a_1,\dots,a_{n_2})\times L_1(1)) = \phi((x_1,\dots,x_{n-n_1-n_2},b_1,\dots,b_{n_2})\times L_1(1))$$

kehtib kõikide $(x_1,\dots,x_{n-n_1-n_2}) \in \mathcal{H}^{n-n_1-n_2}$ korral. Siin $\phi_{(2)}$-värvitakse järjendeid $a \in \mathcal{H}^{n_2}$ seega funktsioonide $\phi((x,a) \times L_1(1))$ abil, kus $x \in \mathcal{H}^{n-n_1-n_2}$. Lisaks märgime, et $\mathcal{L}_1$ monokromaatilisuse tõttu me võinuks siin kasutada $L_1(2)$ või ka $L_1(i)$ argumendi i iga teise väärtuse $i \in \overline{1,m-1}$ korral. Analoogiliselt ülaltoodule ahendame $\phi_{(2)}$ hulga $\mathcal{H}_1^{n_2}$ peale ning siis induktsiooni oletusele tuginedes märkame, et leidub $\phi_{(2)}$-monokromaatiline joon $\mathcal{L}_2 = \{L_2(i_2) : i_2 \in \overline{1,m-1}\} \subseteq \mathcal{H}_1^{n_2}$. Tulenevalt esitatud konstruktsioonist sõltub ϕ-värv suvalisel punktil nende $(m-1)^2$-elemendilisest alamhulgast

$$\{(x_1,\dots,x_{n-n_1-n_2}) \times L_2(i_2) \times L_1(i_1) : i_1, i_2 \in \overline{1,m-1}\}$$

hulgas $\mathcal{H}^{n-n_1-n_2} \times \mathcal{L}_2 \times \mathcal{L}_1$ vaid nende ühise, fikseeritud “päise” $(x_1,\dots,x_{n-n_1-n_2})$ valikust nendel punktidel ning ei sõltu üldse mitte argumentide i_1 ja i_2 väärtuste valikust. Kui tähistada veel sümboliga $L_2(h_m)$ punkti, mis saadakse kui joone $\mathcal{L}_2$ punktide $L_2(i_2)$ mittekonstantsetele komponentidele omistada “väärtus” h_m, siis värv $\phi((x_1,\dots,x_{n-n_1-n_2})\times L_2(h_m)\times L_1(i_1))$ ei sõltu argumendi i_1 väärtuse valikust lõigul $\overline{1,m-1}$.

Analoogilisel viisil toimides ning arutluste kirjeldatud tsüklit t korda korrates saame tulemusena m^t punkti hulgast $\mathcal{H}^n$, mis kirjutame üles kujul

$$L_t(j_t)\dots L_{k+1}(j_{k+1})L_k(j_k)\dots L(j_1),$$

kus $j_i \in \overline{1,m}$ ja värv

$$\phi(L_t(j_t)\dots L_{k+1}(j_{k+1})L_k(i_k)\dots L_1(i_1))$$

ei sõltu jälle ühegi argumendi i_* väärtuse konkreetsest valikust, kui $i_* \in \overline{1,m-1}$.

Vaatleme nüüd $t+1$ punkti

$$P_k = L_t(h_m)\dots L_{k+1}(h_m)L_k(h_1)\dots L_1(h_1), \quad \text{kus} \quad 0 \leqslant k \leqslant t.$$

Mingi punktide paar nende $t+1$ punkti seast peab olema üht ja sama värvi; moodustugu see punktipaar näiteks punktidest P_q $(k=q)$ ja P_p $(k=p)$, kus loeme $q>p$. Seejärel vaatleme punkte

$$P(i) = L_t(h_m)\dots L_{k+1}(h_m)L_q(h_i)\dots L_{p+1}(h_i)L_p(h_1)\dots L_1(h_1),$$

kus $i \in \overline{1,m}$. Seejuures $i < m$ korral on punktil $P(i)$ värv sama mis punktil P_q, aga $i = m$ korral punkti $P(m)$ värv ühtib punkti P_p värviga. Kuid see viimane värv on ju paari $\{p,q\}$ valiku tõttu sama mis on punktil P_q. Sellest järeldub, et punktihulk $\{P(i) : i \in \overline{1,m}\}$ sobib otsitavaks monokromaatiliseks jooneks järjendite hulgas $\mathcal{H}^n$, millega teoreemi tõestav arutlusskeem on leitud. Jääb vaid täiendavalt ära näidata, et saab soovitud viisil arvusid $n_1, n_2, \ldots$ valida. Soovitud valikute olemasolus veendumiseks loeme, et $\bar{n}(1,t) = 1$, aga juhtudel $m \geqslant 2$ defineerime arvud $\bar{n}(m,t)$ rekursiivselt: võtame $r_t = \bar{n}(m-1,t)$ ning juhtudel $1 \leqslant k \leqslant t-1$ loeme, et

$$r_k = \bar{n}(m-1, t^{m^{r_t + \cdots + r_{k+1}}}),$$

seejärel aga võtame $\bar{n}(m,t) = r_t + r_{t-1} + \cdots + r_1$. See annabki soovitud tulemuse.

Teoreem 7. Antud naturaalarvude m ja t korral leidub selline arv $W(m,t)$, et kui (suvaliselt) t-värvida naturaalarvude lõik $\overline{1, W(m,t)}$, siis sisaldub temas monokromaatiline m-liikmeline aritmeetiline progressioon.

Tõestus. Antud m ja t korral t-värvime (suvaliselt!) naturaalarvude lõigu $\overline{1, m^{\bar{n}(m,t)}}$ ning tõestame, et see lõik juba sisaldabki võetud värvimise ϕ suhtes monokromaatilist m-liikmelist aritmeetilist progressiooni. Väite põhjendamiseks kirjutame arvud $x \in \overline{1, m^{\bar{n}(m,t)}}$ üles alusel m (ehk m-ndsüsteemis):

$$x = \sum_{i=0}^{\bar{n}(m,t)-1} x_i m^i, \quad \text{kus} \quad x_i \in \{0,1,\ldots,m-1\},$$

mis seostab arvuga x järjendi $x = (x_0, x_1, \ldots, x_{\bar{n}(m,t)-1})$. Teoreemi 6 kohaselt leidub ϕ-monokromaatiline joon $\mathcal{L}^{(\mathcal{I})} = \{P(l) : l = 0,1,\ldots,m-1\}$, kus $P(l)$ on see punkt joonelt $\mathcal{L}^{(\mathcal{I})}$, millel kui järjendil $(x_0, \ldots, x_{\bar{n}(m,t)-1})$ omandavad kõik mittekonstantsed komponendid (s. t. komponendid $x_j, j \notin \mathcal{I}$) väärtust $l \in \{0,1,\ldots,m-1\}$. Need m naturaalarvu x, mida esindavad järjendid $P(l)$, moodustavadki soovitud aritmeetilise progressiooni. Tõestusest nähtub muuhulgas, et $W(m,t) \leqslant m^{\bar{n}(m,t)}$.

Märgime samuti, et teoreemile 6 tuginedes saab ka üsna lihtsasti tõestada, et antud naturaalarvude r ja t korral kui t-värvida kõik punktid üle Galois' korpuse $\mathbb{F}(q)$ võetud afiinses (projektiivses) ruumis $\mathfrak{R}_n(q)$, siis piisavalt suure (ning vaid arvudest r ja t sõltuva) n valiku korral eksisteerib ruumis $\mathfrak{R}_n(q)$ r-mõõtmeline alamruum, mis koosneb ühevärvilistest punktidest. Veel lisame, et ka teoreemis 7 toodud väide lubab järgmist üldistust: antud naturaalarvu m korral leidub niisugune arv n, et iga kujutuse $\overline{1,n} \to \overline{1,n}$ jaoks leidub lõigul $\overline{1,n}$ selline m-liikmeline aritmeetiline progressioon, mille liikmetest moodustunud alamhulgale ahendatult on antud kujutus kas üksühene või siis konstantne.

Ligi 60 aastat tagasi alustas R. Rado uuringuid lineaarsete diofantiliste võrrandite monokromaatilistest lahenditest ning jõudis teoreemideni, millest selles jaotises eespool mainitud teoreemid tulenevad erijuhtudena. Tutvume järgnevalt ühe sellise tulemusega (*Rado teoreemiga*).

Teoreem 8. Olgu antud naturaalarv t ning lineaarne diofantiline võrrand

$$\mathfrak{D} : a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0, \tag{20.9}$$

milles kõik kordajad $a_i \in \mathbb{Z}$ erinegu nullist. Naturaalarvude hulga $\mathbb{N}_1$ iga t-värvimise ϕ korral leidub võrrandil $\mathfrak{D}$ ϕ-monokromaatiline lahend parajasti siis, kui leidub tema kordajate selline alamhulk $\mathcal{A}' \subseteq \{a_1, a_2, \ldots, a_n\}$ et

$$\sum_{a_j \in \mathcal{A}'} a_j = 0 \tag{20.10}$$

(tingimust (20.10) rahuldavat diofantilist võrrandit (20.9) nimetame *regulaarseks*).

Tõestus. Tarvilikkus. Oletame väitevastaselt, et ei leidu niisugust alamhulka $\mathcal{A}' \subseteq \{a_1, a_2, \ldots, a_n\}$, mille korral oleks täidetud tingimus (20.10), kuigi võrrandil (20.9) leidub monokromaatiline lahend iga t-värvimise $\phi : \mathbb{N}_1 \to \overline{1,t}$ korral. Võttes nüüd suvalise algarvu p defineerime hulgal $\mathbb{N}_1$ järgmise $(p-1)$-värvimise ϕ_p: kui arv $x \in \mathbb{N}_1$ esitub kujul

$$x = p^{\nu_p(x)} \cdot (pu + v), \quad \text{kus} \quad 1 \leqslant v \leqslant p - 1,$$

siis tema värv määratakse võrdusega $\phi_p(x) = v$. Eelduse kohaselt on võrrandil $\mathfrak{D}$ ϕ_p-monokromaatiline lahend $\bar{x} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$; vastavat värvi tähistame samuti v. Esitanud lahendi kõik komponendid äsja näidatud kujul

$$\bar{x}_i = p^{\nu_p(\bar{x}_i)} \cdot (pu_i + v)$$

(kus $i = 1, 2, \ldots, n$) võime üldsust kitsendamata lugeda seejuures, et

$$\nu_p(\bar{x}_1) = \cdots = \nu_p(\bar{x}_k) < \nu_p(\bar{x}_{k+1}) \leqslant \nu_p(\bar{x}_{k+2}) \leqslant \cdots \leqslant \nu_p(\bar{x}_n),$$

kus $k \geqslant 1$. Seetõttu nähtub võrdusest

$$0 = \sum_{i=1}^{n} a_i\bar{x}_i = \sum_{i=1}^{n} a_i p^{\nu_p(\bar{x}_i)}(pu_i + v)$$

et

$$\sum_{i=1}^{k} a_i(pu_i + v) \equiv 0 (\operatorname{mod} p),$$

millest omakorda järeldub $\sum_{i=1}^{k} a_i \equiv 0 (\operatorname{mod} p)$. Kui algarv p valida piisavalt suurena (näiteks võttes $p > \sum_{i=1}^{n} |a_i|$) järeldame viimatinimetatud kongruentsist, et $\sum_{i=1}^{k} a_i = 0$. See on aga vastuolus oletusega võrrandi $\mathfrak{D}$ mitteregulaarsusest.

Piisavus. Olgu nüüd diofantiline võrrand (20.9) regulaarne. Tingimusest (20.10) tulenevalt saab siis hulga $\{a_1, a_2, \ldots, a_n\}$ esitada alamhulga $\mathcal{A}'$ ja sellega disjunktse alamhulga $\mathcal{A}''$ ühendina. Valime seejärel kordaja $a_{j'} \in \mathcal{A}'$ suvaliselt ning moodustame diofantilise võrrandi

$$\mathfrak{D}' : a_{j'}x - a_{j'}y + \Big(\sum_{a_j \in A''} a_j\Big)z = 0. \tag{20.11}$$

Võrrand $\mathfrak{D}'$ on konstruktsiooni kohaselt regulaarne, kusjuures selle iga monokromaatiline lahend $(\bar{x}, \bar{y}, \bar{z})$ indutseerib ka lähtevõrrandi $\mathfrak{D}$ monokromaatilise lahendi $(\bar{x}_j)$. Selles veendumiseks piisab võtta $\bar{x}_{j'} = \bar{x}$, juhtudel $a_j \in A'\backslash\{a_{j'}\}$ lugeda $\bar{x}_j = \bar{y}$ ning juhtudel $a_j \in A''$ määrata lahendi komponendid võrdusega $\bar{x}_j = \bar{z}$. Sellest näeme, et edasistes arutlustes piisab algse diofantilise võrrandina $\mathfrak{D}$ vaadelda võrrandit kujul

$$ux - uy + vz = 0. \tag{20.12}$$

Jätkame nüüd arutlusi induktsiooniga t järgi. Juhul $t = 1$ on võrrandi (20.12) monokromaatilise lahendi olemasolu ilmne. Seetõttu olgu $t > 1$ ning teoreemi väide $t-1$ värvi korral kehtiv. Teoreemi 5 kasutades nähtub sellest, et leidub niisugune arv M, et kui hulk $\overline{1, M}$ (suvaliselt) värvida $t-1$ värviga, siis võrrandil (20.12) on ühevärviliste komponentidega lahend kõigi komponentidega sellest hulgast.

Olgu nüüd kogu $\mathbb{N}_1$ (suvaliselt) t-värvitud. Teoreemi 7 kohaselt leidub ühevärviline (näiteks sinine hulgal $\mathbb{N}_1$ võetud värvimise suhtes) aritmeetiline progressioon

$$a, a+d, \ldots, a+vMd.$$

Et seejuures kehtib võrdus

$$ua - u(a + v\mu d) + v(\mu ud) = 0,$$

siis juhul kui μud oleks sinine mõne $\mu \in \overline{1, M}$ korral, siis oleks võrrandi (20.12) monokromaatiline lahend leitud. Jääb uurida juhtu, mil μud pole sinine iga $\mu \in \overline{1, M}$ korral. Et kasutatavaid värve on nüüd ühe võrra vähem, siis M valiku tõttu saame leida arvud x', y', z' nii, et arvud $x'ud$, $y'ud$ ja $z'ud$ oleksid üht ja sama värvi ning samal ajal kehtib ka $u(x'ud) - u(y'ud) + v(z'ud) = 0$. Jällegi oleme diofantilise võrrandi (20.12) soovitud monokromaatilise lahendi leidnud ja teoreem on tõestatud.

Et diofantiline võrrand $x + y - z = 0$ on ilmselt regulaarne, siis vahetu järeldusena äsjatõestatud teoreemist saame järgmise teoreemi (I. Schur).

Teoreem 9. Vastavalt suvalisele naturaalarvule t leidub selline naturaalarv $S(t)$, et iga $n \geqslant S(t)$ korral hulga $\overline{1, n}$ mistahes t-värvimise jaoks leiduvad sellel lõigul ühevärvilised arvud x, y ja z, mille puhul $x + y = z$.

Seda tulemust kasutades on kerge tõestada järgmist teoreemi.

Teoreem 10. Kõigi piisavalt suurte algarvude p korral on Fermat' kongruents $x^n + y^n \equiv z^n \pmod{p}$ alati lahenduv.

Tõestus. Olgu $d = \text{SÜT}(n, p-1)$ ning g algjuur mooduli p järgi. Elementi $\bar{g} = g \pmod{p}$ võib tõlgendada jäägiklassikorpuse $\mathbb{Z}_p$ multiplikatiivse rühma $\mathbb{Z}_p^*$ moodustajana. Fermat' teoreemi kohaselt kehtib korpuses $\mathbb{Z}_p$ seos $\bar{g}^{p-1} = 1$, mistõttu $\mathbb{Z}_p^*$

alamhulgad $\{\bar{g}^{ns} : s \in \mathbb{Z}\}$ ja $\{\bar{g}^{ds} : s \in \mathbb{Z}\}$ ühtivad. Selle tõttu ning tulenevalt ka seosest $d\,|\,(p-1)$ võib eeldada, et $n\,|\,(p-1)$. Iga elemendi $\bar{c} \in \mathbb{Z}_p^*$ saame nüüd esitada kujul $\bar{c} = \bar{g}^{v+nu}$, kus arv $v < n$ määratakse sealjuures üheselt. Seda asjaolu kasutades defineerime reegliga $\phi(\bar{g}^{v+nu}) = v$ hulga $\mathbb{Z}_p^*$ n-värvingu $\phi : \mathbb{Z}_p^* \to \overline{1,n}$. Eelmisest teoreemist ning teoreemist 5 lähtuvalt saame piisavalt suure algarvu p korral leida ühevärviliste jääkidega (mod p) arvud x, y ja z nii, et kehtib ka seos $x + y = z$. Et algarvu p saab valida piisavalt suurena, siis võib lugeda arvud x, y ja z algarvuga p mittejaguvaiks. Rühma $\mathbb{Z}_p^*$ elementide eespool näidatud esitamisvõimalust ning jäägiklasside $\bar{x}$, $\bar{y}$ ja $\bar{z}$ monokromaatilisust arvestades järeldame, et

$$\bar{x} = \bar{g}^{v+nu_x}, \quad \bar{y} = \bar{g}^{v+nu_y} \quad \text{ja} \quad \bar{z} = \bar{g}^{v+nu_z},$$

mistõttu võrdusest $\bar{x} + \bar{y} = \bar{z}$ saame nüüd, et

$$(\bar{g}^{u_x})^n + (\bar{g}^{u_y})^n = (\bar{g}^{u_z})^n$$

kehtib korpuses $\mathbb{Z}_p$. See aga tähendab, et kehtib vastav täisarvuline kongruents

$$(g^{u_x})^n + (g^{u_y})^n \equiv (g^{u_z})^n \pmod{p},$$

millest teoreemi väite õigsus nähtubki.

Vaatleme nüüd lõpliku pikkusega o-hulki, millel leidub vähim element ning mis rahuldavad Jordan-Dedekindi tingimust. Sellist tüüpi o-hulkade jada $\mathfrak{S} = (S_0, S_1, S_2, \dots)$ (kus o-hulga S_n pikkus on n) ning antud naturaalarvude m, l ja t (kus $m \leqslant l$) korral öeldakse, et $\mathfrak{S}$ on omadusega $R(m,l,t)$, kui eksisteerib (vähim) naturaalarv $N = N_{\mathfrak{S}}(m,l,t)$ nii, et iga $n \geqslant N$ ja suvalise kujutuse $\nu : S_n[m] \to \overline{1,t}$ jaoks leiduvad $i \in \overline{1,t}$ ja $a \in S_n[l]$, mille korral $\{x : x \in S_n[m]$ ja $x \leqslant a\} \subseteq \nu^{-1}(i)$ (siin kasutasime ajutist tähistust $S[m] = \{x : x \in S,\ h(x) = m\}$, sest jaotises 16 öeldust nähtub, et iga sellist o-hulka S gradueerib tema kõrgusfunktsioon h). Arvusid $N_{\mathfrak{S}}(m,l,t)$ nimetatakse jada $\mathfrak{S}$ *Ramsey arvudeks*. Jada nimetatakse *Ramsey jadaks*, kui tal on omadus $R(m,l,t)$ parameetrite m, l ja t kõigi naturaalarvuliste väärtuste korral, kus vaid $m \leqslant l$.

Teoreemis 4 kirjeldatud situatsioon juhib järgmise üldise mõiste juurde. Olgu antud naturaalarvud $t, n_1, \dots, n_t$ ja $m \leqslant \min(n_1, \dots, n_t)$. Öeldakse, et jada $\mathfrak{S}$ on omadusega $R(n_1, \dots, n_t; m)$, kui leidub (vähim) naturaalarv $N = N_{\mathfrak{S}}(n_1, \dots, n_t; m)$ nii, et iga $n \geqslant N$ ja suvalise kujutuse $\nu : S_n[m] \to \overline{1,t}$ jaoks eksisteerivad $i \in \overline{1,t}$ ning $a \in S_n[n_i]$, mille korral $\{x : x \in S_n[m]$ ja $x \leqslant a\} \subset \nu^{-1}(i)$. Nii saadud arvusid $N_{\mathfrak{S}}(n_1, \dots, n_t; m)$ nimetatakse samuti jada $\mathfrak{S}$ *Ramsey arvudeks*.

Neist definitsioonidest nähtub, et jada $\mathfrak{S}$, millel on omadus $R(n_1, \dots, n_t; m)$ parameetrite $t, n_1, \dots, n_t$ ja m kõigi (mõeldavate) naturaalarvuliste väärtuste korral, osutub Ramsey jadaks. Kehtib ka vastupidine väide, mis nähtub samuti definitsioonidest, kui võtta $l = \max(n_1, \dots, n_t)$ ja märgata, et seosest $l \leqslant l^*$ tuleneb implikatsiooni $R(m,l^*,t) \Rightarrow R(m,l,t)$ tõesus. Need märkused lubavad teoreemi 4 sõnastada väitena, et jada $\mathfrak{B} = \{\mathfrak{B}(n) : n = 0, 1, 2, \dots\}$ on Ramsey jada. Teoreemist 4 järeldub veel, et tükelduste võrede jada $\mathfrak{E} = \{\mathfrak{E}_n : n = 1, 2, \dots\}$ on Ramsey jada.

Indeks

Ülo Kaasik, Uno Kaljulaid
KOMBINATOORIKA ANALÜÜTILISI JA ALGEBRALISI MEETODEID
Tartu Ülikool
EE2400 Tartu, Ülikooli 18
9,88. 10,0. T. 118. 300
TÜ trükikoda. EE2400 Tartu, Tiigi 78