University of Tartu
Faculty of Science and Technology
Institute of Mathematics and Statistics

Karl Hannes Veskus

Combinatorial Nullstellensatz and its Applications

Major of Mathematics
Bachelor's Thesis (9 EAP)

Supervisor: PhD Ago-Erik Riet

Tartu 2019

Combinatorial Nullstellensatz and its Applications

Bachelor's Thesis
Karl Hannes Veskus

Abstract. In 1999, Noga Alon proved a theorem, which he called the Combinatorial Nullstellensatz, that gives an upper bound to the number of zeros of a multivariate polynomial. The theorem has since seen heavy use in combinatorics, and more specifically in graph theory. In this thesis we will give an overview of the theorem, and of how it has since been applied by various researchers. Finally, we will provide an attempt at a proof utilizing a generalized version of the Combinatorial Nullstellensatz of the GM-MDS Conjecture.

CERCS research specialisation: P110 Mathematical logic, set theory, combinatorics.
Keywords: Graph Theory, Combinatorics, Polynomials, Combinatorial Nullstellensatz.

Kombinatoorne Nullkohalemma ja selle rakendused

Bakalaureusetöö
Karl Hannes Veskus

Lühikokkuvõte. Noga Alon tõestas 1999. aastal teoreemi, mida ta ise nimetas kombinatoorseks nullkohalemmaks, mitmemuutuja polünoomi nullkohtade arvu ülemise piiri kohta. Teoreemi avaldamisest saadik on seda laialdaselt kasutatud kombinatoorsete ning eriti just graafiteoreetiliste tulemuste tõestamisel. Bakalaureusetöö annab ülevaate Noga Aloni kombinatoorsest nullkohtalemmast ning tänu sellele saavutatud tulemustest. Lõpuks pakutakse välja ka võimalik tõestus GM-MDS hüpoteesile, kasutades kombinatoorse nullkohalemma üldistatud versiooni.

CERCS teaduseriala: P110 Matemaatiline loogika, hulgateooria, kombinatoorika.
Märksõnad: Algebra, graafiteooria, kombinatoorika, polünoomid, kombinatoorne nullkohalemma.

Contents

Introduction

In 1999 Noga Alon [1] stated and proved two theorems, which he called the Combinatorial Nullstellensatz. The theorems are an extention on Hilbert's Nullstellensatz from 1893 [2], and give an upper bound to the number of zeros that a given multivariate polynomial can have. Being a fairly new result the Combinatorial Nullstellensatz is not yet widely known, however recent research in graph theory suggests that it is indeed a very powerful theorem.

The aim of the thesis is to give an overview of Alon's Combinatorial Nullstellensatz, along with examples of how it is commonly used, and where it has been used since it was stated in 1999 [1]. The secondary goal of the thesis is to give a proof of the GM-MDS Conjecture by using the Combinatorial Nullstellensatz.

The first section defines some necessary terms and properties of multivariate polynomials. The Combinatorial Nullstellensatz is stated in the second section and examples of how to use it in proofs is given in the third section. Additionally, an overview of some recent results in graph theory that utilize the Combinatorial Nullstellensatz will be given in the fourth section. Lastly, an attempt at a proof is made in section five for a conjecture about the well known MDS error-correcting codes, a subset of which are the widely used Reed-Solomon codes. While the secondary goal of the thesis has not been achieved, there is hope that the gaps in the given proof can be filled by future research.

All rings in the thesis will be commutative rings with unity. Additionally, we will be using the notation $[k] := \{1, 2, \ldots, k\}$, where $k \in \mathbb{N}$, and $\mathbb{F}_q$, where q is a power of a prime number and $\mathbb{F}_q$ is a field of q elements. While most of the terms are defined, the reader is expected to have some basic knowledge of multivariate polynomials, abstract algebra, and graph theory. The reader may refer to S. Juknas *Extremal Combinatorics With Applications in Computer Science* [3], J. Matoušek's and J. Nešetril's *Invitation to Discrete Mathematics* [4], or V. Laan's *Algebra II* [5] if needed.

1 Polynomials

Before stating and proving any results, we give a quick overview of the prerequisites. As we will be dealing a lot with multivariate polynomials and manipulations with them, then in this section we will state some important results and definitions which we will be using.

Def 1.1 *[3]*
*Let $x_1, \ldots, x_n$ be formal variables. A **monomial** in n variables of degree t is a formal product $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$, where $t_i \geq 0$ and $t_1 + t_2 + \ldots + t_n = t$.*

Two monomials $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ and $x_1^{t_1'} x_2^{t_2'} \ldots x_n^{t_n'}$ in variables $x_1, x_2, \ldots, x_n$ are considered equal iff $t_i = t_i' \quad \forall i \in [n]$. Additionally, we identify x_i^0 with 1.

Def 1.2 *[3]*
*A **polynomial in n variables** over a ring R is an linear combination of monomials in n variables, with coefficents from R.*

Def 1.3 *[3]*
*Let $R[x_1, \ldots, x_n]$ denote the **polynomial ring** in variables $x_1, \ldots, x_n$ over the ring R. Its elements are all polynomials in the variables $x_1, \ldots, x_n$ with respect to the usual polynomial addition and multiplication.*

Def 1.4 *[3]*
*The **degree** $\deg(f)$ of the polynomial $f \in R[x_1, \ldots, x_n]$ is the maximum of the degrees of its monomials with non-zero coefficients.*

Def 1.5
*A polynomial f is called **identically zero** iff each monomial in f has a zero coefficient.*

Def 1.6
*We say that the polynomial $f(x_1, \ldots, x_n)$ over the field $\mathbb{F}$ **vanishes** on a set of points $\{s_1, \ldots, s_n\} \subseteq \mathbb{F}^n$ iff $f(s_1, \ldots, s_n) = 0 \quad \forall s \in S$.*

Def 1.7
*We say that a polynomial $f(x_1, \ldots, x_n)$ over the ring R **evaluates to zero everywhere** iff $f(s_1, \ldots, s_n) = 0 \quad \forall (s_1, \ldots, s_n) \in R^n$.*

It is also interesting to note that if a polynomial is identically zero this implies that the polynomial evaluates to zero everywhere, but the converse is not true in general.

Def 1.8
*We say that a polynomial f is **linear** iff $\deg(f) = 1$.*

Def 1.9 *[5]*
*A field $\mathbb{F}$ is **algebraically closed** iff every non-constant polynomial of $\mathbb{F}[x]$ can be factored into a product of linear polynomials in $\mathbb{F}[x]$.*

2 Combinatorial Nullstellensatz

The original Nullstellensatz, which translates roughly to: "The zero placement lemma," was first stated and proved by Hilbert [2]. Hilbert's Nullstellensatz can be stated as follows.

Theorem 2.1 *[1] (Hilbert's Nullstellensatz)*
Let $\mathbb{F}$ be an algebraically closed field and let $f, g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that f vanishes at all common zeros of $g_1, \ldots, g_m$. Then there exists a positive integer $k \in \mathbb{N}$ and the polynomials $h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that

$$f^k = \sum_{i=1}^{n} h_i g_i$$

By specifing and relaxing the assumptions in Hilbert's Nullstellensatz suitably, Alon [1] derives a slightly stronger theorem, which he calls the Combinatorial Nullstellensatz.

Theorem 2.2 *[1]*

- *Let $\mathbb{F}$ be a field.*
- *Let f be a polynomial in n variables over the field $\mathbb{F}$, that is*

$$f = f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n].$$

- *Let be $S_1, \dots, S_n$ be nonempty subsets of $\mathbb{F}$, that is*

$$\emptyset \neq S_i \subseteq \mathbb{F} \quad \forall i \in [n].$$

- *Let $g_1, \dots, g_n$ be univariate polynomials over $\mathbb{F}$ defined as*

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

If f vanishes at all the common zeros of $g_1, \dots, g_n$, then there exist polynomials $h_1, \dots, h_n \in \mathbb{F}[x_1, \dots, x_n]$ for which $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that

$$f = \sum_{i=1}^{n} h_i g_i.$$

The assertion still holds if the polynomials $f, g_1, \dots, g_n$ lie in $R[x_1, \dots, x_n]$ for some subring $R \subseteq \mathbb{F}$. Then $h_i \in R[x_1, \dots, x_n] \quad \forall i \in [n]$.

Let us note the differences from Hilbert's Nullstellensatz. First we no longer require $\mathbb{F}$ to be algebraically closed, indeed it suffices for $\mathbb{F}$ to be any field. Secondly, we require that the polynomials $g_1, \dots, g_n$ be of a certain form $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. Defining each g_i in this way allows us to easily find the zeros of a given g_i, which are all the elements $s \in S_i$. Therefore a common zero of the polynomials $g_1, \dots, g_n$ is any element $s \in \mathbb{F}^n$ such that $\forall i \in [n] \quad s_i \in S_i$.

As a result of these modifications all h_i will be of a degree less or equal to the difference of the degrees of f and g_i, and the resulting sum of the products of h_i and g_i is equal to f instead of f^k for some k. Furthermore, the theorem also holds if all the polynomials are in some subring of $\mathbb{F}$.

Alon expands on this to reach an even more useful proposition.

Theorem 2.3 *[1] (The Combinatorial Nullstellensatz)*

- *Let $\mathbb{F}$ be a field.*
- *Let $f = f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$.*
- *Let the degree of f be the sum of n integers $t_i \geq 0$ ($\deg(f) = \sum_{i=1}^{n} t_i$).*

- *Let the coefficient of the monomial $\prod_{i=1}^{n} x_i^{t_i}$ in f be nonzero.*
- *Let $S_1, \dots, S_n$ be subsets of $\mathbb{F}$ such that $|S_i| > t_i$, $\forall i \in [n]$.*

Then there are $s_i \in S_i$ such that $f(s_1, \dots, s_n) \neq 0$.

By the definition of the degree of a polynomial, if $\deg(f) = \sum_{i=1}^{n} t_i$, then $\prod_{i=1}^{n} x_i^{t_i}$ is one of the largest degree monomials in f and $\deg(\prod_{i=1}^{n} x_i^{t_i}) = \deg(f)$. In essence this theorem states that however one chooses the subsets S_i, as long as they are of required sizes, it is always possible to pick a combination of elements from these sets such that f does not vanish on those elements.

Additionally, M. Lason [6] has found a generalization to the above theorem that requires weaker assumptions about the monomials. For that he uses the concept of the support of a polynomial.

Def 2.1 *[6] (Support)*
*Let $\mathbb{F}$ be a field and let f be a polynomial in $\mathbb{F}[x_1, \dots, x_n]$. The **support** of f is a set of lists of powers of monomials in f with non-zero coefficients, or*
Supp$(f) := \{(t_1, \dots, t_2) \in (\mathbb{N} \cup \{0\})^n \mid$ the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is non-zero.$\}$

We will also need a partial ordering on the support of a polynomial, allowing us to talk about maximal elements of the support. Since the support of any polynomial is finite, at least one maximal element exists whenever the support is non-empty. Note that the support of a polynomial is empty iff the polynomial is identically zero.

Def 2.2 *[6]*
Let $(t_1, \dots, t_n) \in (\mathbb{N} \cup \{0\})^n$ and let $(k_1, \dots, k_n) \in (\mathbb{N} \cup \{0\})^n$. We say that $(t_1, \dots, t_n) \leq (k_1, \dots, k_n)$ iff $t_i \leq k_i \quad \forall i \in [n]$.

Def 2.3
Let f be a polynomial in $\mathbb{F}[x_1, \dots, x_n]$. We say that $(t_1, \dots, t_n) \in$ Supp(f) is a maximal element in the support of f iff there does not exist an element that is larger than it, or symbolically

$$(t_1, \dots, t_n) \in \max(\mathit{Supp}(f)) \Leftrightarrow$$

$$\{(k_1, \dots, k_n) \mid (k_1, \dots, k_n) \in \mathit{Supp}(f), (k_1, \dots, k_n) \geq (t_1, \dots, t_n)\} = \{(t_1, \dots, t_n)\}$$

Theorem 2.4 *[6] (Generalized Combinatorial Nullstellensatz)*

- *Let $\mathbb{F}$ be a field.*
- *Let $f = f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$.*
- *Let $(t_1, \dots, t_n)$ be a maximal element in Supp(f).*
- *Let $S_1, \dots, S_n$ be subsets of $\mathbb{F}$ such that $|S_i| > t_i$, $\forall i \in [n]$.*

Then there are $s_i \in S_i$ such that $f(s_1, \dots, s_n) \neq 0$.

Note that we no longer need any information about the degree of the polynomial f to reach the same result as before.

3 Use of the Combinatorial Nullstellensatz

In this section we will look at a few older and already known results for which new elegant proofs have been found by using the Combinatorial Nullstellensatz. These proofs serve as good examples of how Alon's method can be used and how powerful it can be.

The first example is an extention of the well known Chevalley-Warning theorem [7].

Theorem 3.1 *[7] (Chevalley–Warning)*

- *Let p be a prime, and let $q := p^m$ for some $m \in \mathbb{N}$.*
- *Let $\mathbb{F}_q$ be a field with q elements.*
- *Let $f_1, \dots, f_m$ be polynomials in n variables in $\mathbb{F}_q[x_1, \dots, x_n]$.*

If $\sum_{i=1}^{m} \deg(f_i) < n$ then the number of common zeros of $f_1, \dots, f_m$ is divisible by p.

In Alon's paper from 1999 [1] he gives a proof of the slightly simplified version:

Theorem 3.2 *[1]*

- *Let p be a prime.*
- *Let $f_1, \dots, f_m$ be polynomials in n variables in $\mathbb{F}_p[x_1, \dots, x_n]$.*

If $\sum_{i=1}^{m} \deg(f_i) < n$ and if the polynomials have a common zero $(s_1, \dots, s_n)$, then there exists an another common zero.

Proof [1]: Suppose the theorem is false, then the polynomials $f_1, \dots, f_m$ have only one common zero $(s_1, \dots, s_n)$. Let

$$G = G(x_1, \dots, x_n) = \prod_{i=1}^{m} (1 - f_i(x_1, \dots, x_n)^{p-1}) - \sigma \prod_{k=1}^{n} \prod_{s \in \mathbb{F}_p, s \neq s_k} (x_k - s),$$

where σ is a constant chosen depending on the zero $(s_1, \dots, s_n)$ such that

$$G(s_1, \dots, s_n) = 0.$$

Note that $\prod_{k=1}^{n} \prod_{s \in \mathbb{F}_p, s \neq s_k} (x_k - s)$ is equal to 0 for all arguments, except $(x_1, \dots, x_n) = (s_1, \dots, s_n)$. Let us denote the value of the product at $(s_1, \dots, s_n)$ as $\pi_0 \in \mathbb{F}_p$. We now have

$$\prod_{k=1}^{n} \prod_{s \in \mathbb{F}_p, s \neq s_k} (x_k - s) = \begin{cases} \pi_0, \text{ if } (x_1, \dots, x_n) = (s_1, \dots, s_n) \\ 0, \text{ otherwise.} \end{cases}$$

Note that $\prod_{i=1}^{m} (1 - f_i(x_1, \dots, x_n)^{p-1})$ can only obtain the values 1 and 0. Clearly the value 0 is obtained for most arguments, since by Fermat's little theorem if $f_i(x_1, \dots, x_n)^{p-1} \neq 0$ for some $(x_1, \dots, x_n)$, then it must be equal to 1 in $\mathbb{F}_p$. Furthermore, the product is equal to 1 only if $f_i(x_1, \dots, x_n)^{p-1} = 0$ for all $i \in [m]$, and that will only happen if $(x_1, \dots, x_n)$ is the common zero of all functions $f_1, \dots, f_m$. As per our assumption, the only such zero is $(s_1, \dots, s_n)$. So we get that

$$\prod_{i=1}^{m}(1 - f_i(x_1, \dots, x_n)^{p-1}) = \begin{cases} 1, \text{ if } (x_1, \dots, x_n) = (s_1, \dots, s_n) \\ 0, \text{ otherwise.} \end{cases}$$

Since every non-zero element in $\mathbb{F}_p$ has an unique inverse, then the value of σ is also determined uniquely by $\sigma := (\pi_0)^{-1}$. Now is simple to see that G is identically 0, or

$$G(x_1, \dots, x_n) = \begin{cases} 1 - \sigma \cdot \pi_0 = 0, \text{ if } (x_1, \dots, x_n) = (s_1, \dots, s_n) \\ 0, \text{ otherwise.} \end{cases}$$

Note that the degree of $\prod_{i=1}^{m}(1 - f_i(x_1, \dots, x_n)^{p-1})$ is $(p-1)\sum_{i=1}^{m} \deg(f_i) < n(p-1)$. Let us now show that the coefficient of the degree $n(p-1)$ monomial $x_1^{p-1}x_2^{p-1} \dots x_n^{p-1}$ in G is $-\sigma$. As determined before, $-\sigma \neq 0$. It is indeed so, since $\deg(\prod_{s \in \mathbb{F}_p, s \neq s_k}(x_k - s)) = p - 1$ and $\deg(\prod_{k=1}^{n}\prod_{s \in \mathbb{F}_p, s \neq s_k}(x_k - s)) = n(p-1)$. From this we also get that

$$\deg(G) = \max\left\{(p-1)\sum_{i=1}^{m}\deg(f_i), n(p-1)\right\} = n(p-1).$$

For consistency in notation let us define $t_1 = t_2 = \dots = t_n = p - 1$, then the monomial becomes $x_1^{t_1}x_2^{t_2} \dots x_n^{t_n}$. Now we have a field $\mathbb{F}_p$, a function $G(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ of degree $\deg(G) = \sum_{i=1}^{n} t_i$, a monomial $x_1^{t_1}x_2^{t_2} \dots x_n^{t_n}$ in G with a non-zero coefficient. As the final step we can now directly use the Combinatorial Nullstellensatz with $S_1 = S_2 = \dots = S_n = \mathbb{F}_p$, and find that there must exist $s'_1, \dots, s'_n \in \mathbb{F}_p$ such that $G(s'_1, \dots, s'_n) \neq 0$. But that is a contradiction since we showed that G was identically zero. □

Another theorem, which was first proven centuries ago and has found numerous uses since, is the Cauchy-Davenport theorem [8]. Just as before, the Combinatorial Nullstellensatz can be used to give a short and direct proof.

The reader should keep in mind that here $A+B$ is a set resulting from pointwise addition of the elements from both sets, or $A+B := \{a+b \mid a \in A, b \in B\}$. We define the subtraction analogously $A - B := \{a - b \mid a \in A, b \in B\}$. We define similiarly the addition and subtraction of an element and a set: $x + A := \{x + a \mid a \in A\}$, and $x - A := \{x - a \mid a \in A\}$.

Theorem 3.3 *[3] (Cauchy–Davenport)*
Let p be a prime, and let A, B be non-empty subsets of $\mathbb{F}_p$. Then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof [1]:
Let us distinguish two cases: first if $|A| + |B| > p$, and second if $|A| + |B| \leq p$.

If $|A| + |B| > p$, then by the pidgeonhole principle $A \cap (x - B) \neq \emptyset$ for every $x \in \mathbb{F}_p$, which implies that $A + B = \mathbb{F}_p$. From the last equality we get $|A + B| = p$ and the statement holds.

In the case of $|A| + |B| \leq p$ let us assume that the statement is false, then $|A + B| < |A| + |B| - 1$. We can then find a subset C of $\mathbb{F}_p$ such that $|C| = |A|+|B|-2$ and $A+B \subseteq C$. As the most crucial step we now define a polynomial $f(x, y) := \prod_{c \in C}(x + y - c)$. Since C contains all elements from $A + B$, then for any pair $a + b$, where $a \in A, b \in B$, there is also $c \in C$ such that $a + b = c$. Therefore, for any pair $(a, b) \in A \times B \quad f(a, b) = 0$.

Notice that the polynomial f is of degree $|C| = |A|+|B|-2 = |A|-1+|B|-1$. Defining $t_1 := |A| - 1$ and $t_2 := |B| - 1$, then by the binomial theorem the coefficient of $x^{t_1}y^{t_2}$ in f is $\binom{t_1+t_2}{t_1} = \binom{|A|+|B|-2}{|A|-1}$. As we have that $|A| + |B| \leq p$, then $|A| + |B| - 2 < p$ and $\binom{|A|+|B|-2}{|A|-1} \neq 0$ in $\mathbb{F}_p$. Using the notation $S_1 := A$ and $S_2 := B$ we have all the necessary prerequisites to use the Combinatorial Nullstellensatz, which gives us that there must exist $a' \in A$ and $b' \in B$ such that $f(a', b') \neq 0$. This however contradicts $\forall(a, b) \in A \times B \quad f(a, b) = 0$, which means the original theorem must hold. □

The proofs above illustrate well the power of the Combinatorial Nullstellensatz. Note that both of the proofs follow quite a similar structure. After carefully constructing a polynomial, which under our assumptions is zero at all possible evaluations, we immidiately get a contradiction from the Combinatorial Nullstellensatz. However, constructing a suitable polynomial seems to be the most challenging part in creating these proofs.

For a slightly more recent example there is a theorem by Noga Alon from 1993 [9], for which he gives a simple proof using the Combinatorial Nullstellensatz.

Theorem 3.4 *[9] (Covering the cube by affine hyperplanes)*
Suppose that the hyperplanes $H_1, H_2, \ldots, H_m$ in $\mathbb{R}^n$ avoid the point 0, but otherwise cover all $2^n - 1$ vertices of the cube $\{0, 1\}^n$. Then $m \geq n$.

Proof [1]: Let $x := (x_1, \ldots, x_n) \in \mathbb{R}^n$, and for any two vectors $a, b \in \mathbb{R}^n$ let $\langle a, b\rangle$ be their inner product. Let the hyperplanes be defined as $H_i = \{x \in \mathbb{R}^n \mid \langle a_i, x\rangle = b_i\}$. Since the hyperplanes do not cover the origin, then $b_i \neq 0$ for all $i \in [m]$. As with previous proofs, assume that the theorem is false, which is equivalent to assuming $m < n$. Define the polynomial $f \colon \mathbb{R}^n \to \mathbb{R}$ as

$$f(x) := \left((-1)^{n+m} \prod_{j=1}^{m} b_j\right) \prod_{i=1}^{n}(x_i - 1) - \prod_{i=1}^{m}(\langle a_i, x\rangle - b_i).$$

As we assumed that $m < n$, then the degree of f is n. In addition to that, the coefficient of the monomial $x_1x_2 \ldots x_n$ is $(-1)^{n+m} \prod_{j=1}^{m} b_j$, which can not be zero since none of the b_i are zero. Taking $S_1 = \ldots = S_n = \{0, 1\}$ gives us all the prerequisites to use the Combinatorial Nullstellensatz, which says there has to be a vertex $x' \in \{0,1\}^n$ of the cube such that $f(x') \neq 0$. Note that such x' can not be the zero vector, since

$$f(\mathbf{0}) = \left((-1)^{n+m} \prod_{j=1}^{m} b_j \right) (-1)^n - \prod_{i=1}^{m} (-b_i) = (-1)^m \prod_{j=1}^{m} b_j - (-1)^m \prod_{i=1}^{m} b_i = 0.$$

Therefore, there is $x_i \in x'$ such that $x_i = 1$, which in turn implies that $\prod_{i=1}^{n}(x_i - 1) = 0$. Additionally, x' has to be a vertex that is covered by some H_i, but then $\langle a_i, x' \rangle - b_i = 0$ for some $i \in [n]$. However, since now $\prod_{i=1}^{n}(x_i - 1) = 0$ and $\langle a_i, x' \rangle - b_i = 0$, then also $f(x') = 0$, which is a contradiction. □

4 Graph colouring

In recent years many new results have been proved in graph theory, and more specifically in relation to graph colourings, by using the Combinatorial Nullstellensatz and the polynomial method. Before diving into said results, let us quickly go through the more important definitions and notions we will be using.

4.1 Terms and definitions

Firstly some general graph theoretic notions, which are useful for specifying various bounds later.

Def 4.1
Let $G = (V, E)$ be a graph. Let $d(v)$ be the degree of a vertex $v \in V$. The ***maximum degree*** *of G, denoted $\Delta(G)$, is the maximum degree of its vertices, or*

$$\Delta(G) := \max\{d(v) \mid v \in V\}.$$

Def 4.2 *[10]*
Let $G = (V, E)$ be a graph. The ***average degree*** *of G, denoted* $\mathrm{ad}(G)$ *is the average of all vertex degrees in G, or*

$$\mathrm{ad}(G) := \frac{2|E|}{|V|}.$$

Def 4.3 *[10]*
Let $G = (V, E)$ be a graph. The ***maximum average degree*** *of G, denoted* $\mathrm{mad}(G)$*, is the maximum of average degrees of all non-empty subgraphs of G, or*

$$\mathrm{mad}(G) := \max(\{\mathrm{ad}(G') \mid G' = (V', E') \subseteq (V, E), \quad |V'| \neq 0\}).$$

4.1.1 Basic colourings

Now we define terms for colouring just the vertices or just the edges of a graph.

Def 4.4 *[4] (The chromatic number)*
Let $G = (V, E)$ be a graph, and let $k \in \mathbb{N}$. A mapping $c \colon V \to [k]$ is called ***a proper vertex colouring*** *of the graph G iff for every edge $\{v, u\} \in E$ it holds that $c(v) \neq c(u)$.*
The chromatic number *of G, denoted by $\chi(G)$, is the minimum integer k such that there exists a proper vertex colouring $c \colon V \to [k]$.*

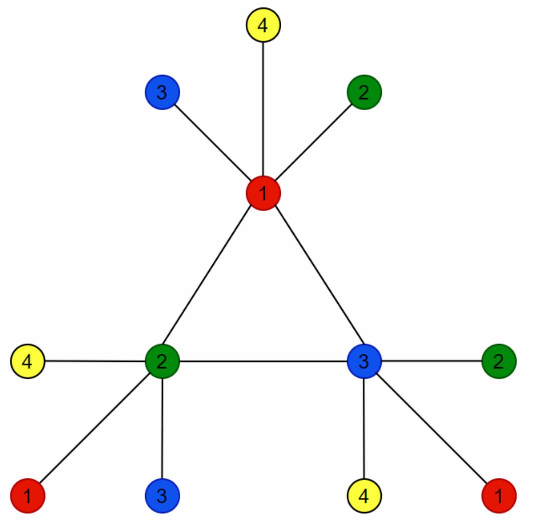

Figure 1: A proper vertex colouring.

In short, a proper vertex colouring of a graph is any colouring of the vertices, such that no two adjacent vertices have the same colour. The chromatic number is the smallest possible number of colours needed to colour the vertices of a given graph properly. An example of a proper vertex coloring can be seen in Figure 1.

Quite analogously we can define **a proper edge colouring** (assigning colours to the edges, so that no two adjacent edges are of the same colour) and the minimum number of colours needed for a proper edge colouring of a graph G.

Def 4.5 *(The chromatic index)*
Let $G = (V, E)$ be a graph, and let $k \in \mathbb{N}$. A mapping $c \colon E \to [k]$ is called ***a proper edge colouring*** *of the graph G iff for any two edges $e = \{v, w\} \in E$ and $a = \{v, u\} \in E$ that share a vertex $v \in V$ it holds that $c(e) \neq c(a)$.*
The chromatic index *of G, denoted by $\chi'(G)$, is the minimum integer k such that there exists a proper edge colouring $c \colon E \to [k]$.*

One may also think of the chromatic index of G as the chromatic number of the line graph of G. [1] An example of a proper edge coloring can be seen in Figure 2.

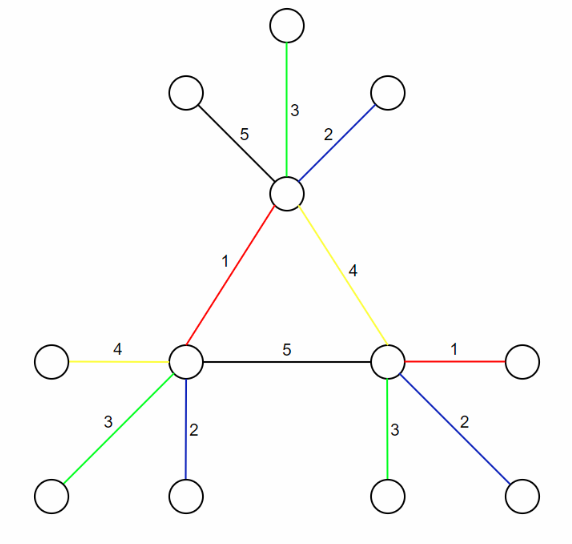

Figure 2: A proper edge colouring.

The famous four-colour theorem gives us an upper bound for the chromatic number of all planar graphs. By the theorem, if G is a planar graph, then it is always possible to colour it with no more than 4 colours. Or in notation,

$$G \text{ is a planar graph} \Rightarrow \chi(G) \leq 4.$$

Let us now assume that each vertex has a fixed list of colours and a vertex can only be coloured with a colour that belongs to its corresponding list. A colouring satisfying this property is called a **list-colouring**. As with normal colourings, we would like to know what the minimum number of colours is that we need to colour such a graph.

Def 4.6 *[1] (The choice number)*
Let $G = (V, E)$ be a finite graph. Let $f\colon V \to \mathbb{N}$ be a function assigning a positive integer (list size) to each vertex, and let $S\colon V \to \mathcal{P}(\mathbb{N})$, where $\mathcal{P}(\mathbb{N})$ is the powerset of $\mathbb{N}$, be a function assigning a set of positive integers (colours) to each vertex.
*The graph G is **f-choosable** iff for every possible assignement $S(V)$ of integer sets to vertices such that $\forall v \in V\colon |S(v)| = f(v)$, there exists a proper vertex colouring $c\colon V \to \mathbb{N}$ such that $\forall v \in V\colon c(v) \in S(v)$. Or symbolically:*

$$\begin{aligned} &G \text{ is } f\text{-choosable} \Leftrightarrow \\ &\qquad \forall S\colon V \to \mathcal{P}(\mathbb{N}) \text{ s.t. } (\forall v \in V : |S(v)| = f(v)), \\ &\qquad \exists c\colon V \to \mathbb{N} \text{ s.t. } (\forall v \in V : c(v) \in S(v)), \text{ and} \\ &\qquad c \text{ is a proper vertex colouring.} \end{aligned}$$

We say that G is ***k-choosable*** *iff for all $f\colon V \to \mathbb{N}$ such that $\forall v \in V : f(v) \geq k$ we have that G is f-choosable.*
The choice number *of G, denoted $\operatorname{ch}(G)$, is the minimum integer k such that G is k-choosable.*

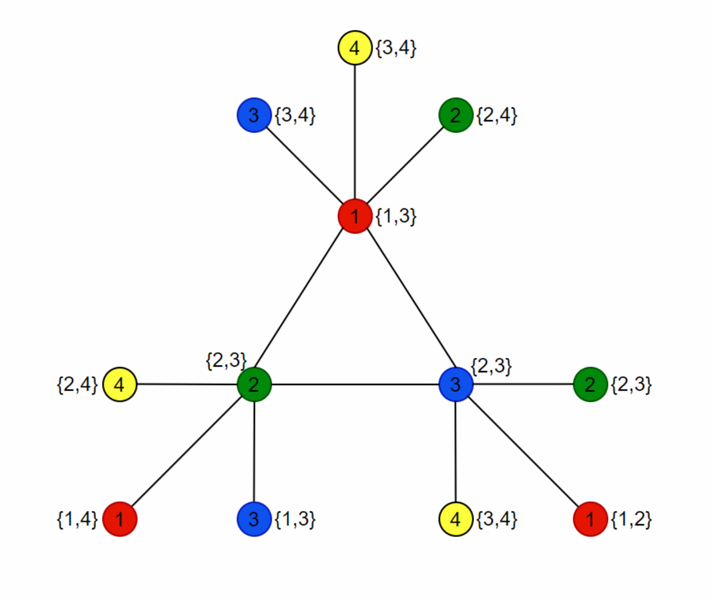

Figure 3: An illustration of k-choosability.

Again we can define an analogue for the edges of a graph.

Def 4.7 *[1] (The list chromatic index)*
Let $G = (V, E)$ be a finite graph. Let $f\colon E \to \mathbb{N}$ be a function assigning a positive integer (list size) to each edge, and let $S\colon E \to \mathcal{P}(\mathbb{N})$, where $\mathcal{P}(\mathbb{N})$ is the powerset of $\mathbb{N}$, be a function assigning a set of positive integers (colours) to each edge.
The graph G is ***f-list-choosable*** *iff for every possible assignement $S(E)$ of integer sets to edges such that $\forall e \in E\colon |S(e)| = f(e)$, there exists a proper edge colouring $c\colon E \to \mathbb{N}$ such that $\forall e \in E\colon c(e) \in S(e)$. Or symbolically:*

$$\begin{aligned} &G \textit{ is } f\textit{-list-choosable} \Leftrightarrow \\ &\qquad \forall S\colon E \to \mathcal{P}(\mathbb{N}) \textit{ s.t. } (\forall e \in E : |S(e)| = f(e)), \\ &\qquad \exists c\colon E \to \mathbb{N} \textit{ s.t. } (\forall e \in E : c(e) \in S(e)), \textit{ and} \\ &\qquad c \textit{ is a proper edge colouring.} \end{aligned}$$

We say that G is ***k-list-choosable*** *iff for all $f\colon E \to \mathbb{N}$ such that $\forall e \in E : f(e) \geq k$ we have that G is f-list-choosable.*

The list chromatic index *of G, denoted $ch'(G)$, is the minimum integer k such that G is k-list-choosable.*

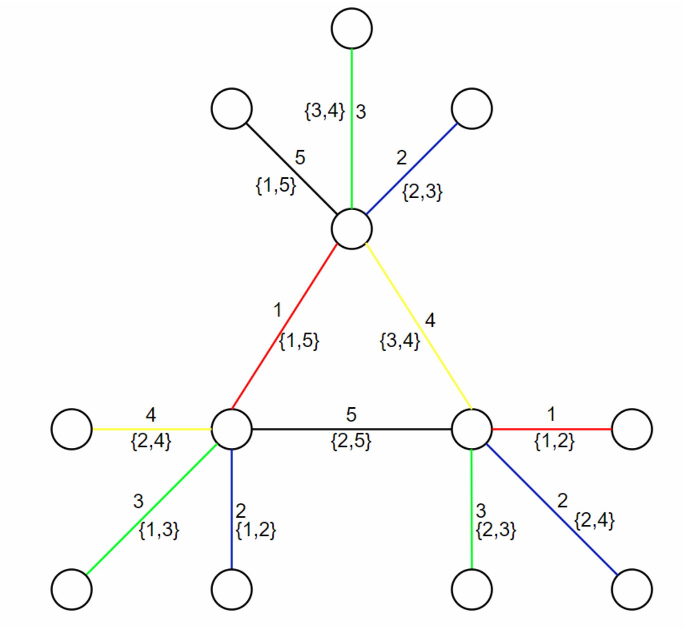

Figure 4: An illustration of k-list-choosability.

Just as with the chromatic index, the list chromatic index of G can be viewed as the choice number for the line graph of G. Examples for both k-choosability and k-list-choosability can be seen in Figures 3 and 4 respectively.

4.1.2 Neighbour-distinguishing colourings

Let us say we wish to make sure that in a proper edge-colouring not only the adjacent edges are of different colours, but also whole sets of edge-colours around adjacent vertices are distinguishable. We then reach a concept called neighbour-distinguishing colourings.

Def 4.8 *[10] (Neighbour set distinguishing colouring)*
Let $G = (V, E)$ be a graph, let k be a positive integer, let $c\colon E \to [k]$ be a proper edge-k-colouring ($\chi'(G) = k$), and let $S(v) = \{c(e) \mid e \in E, v \in e\} \subseteq [k]$ be the set of colours of edges incident to a vertex $v \in V$.
We call the edge-k-colouring c ***neighbour set distinguishing*** *(nd-k-colouring) iff for any edge $e = \{u, v\}$ the corresponding sets $S(v)$ and $S(u)$ of the endpoints are different, or symbolically*

$$\forall\{v, u\} \in E : S(v) \neq S(u)$$

The smallest integer k such that there exists a neighbour set distinguishing edge-k-colouring of the graph G is called the ***neighbour set distinguishing chromatic index****, denoted by $\chi'_{nd}(G)$.*

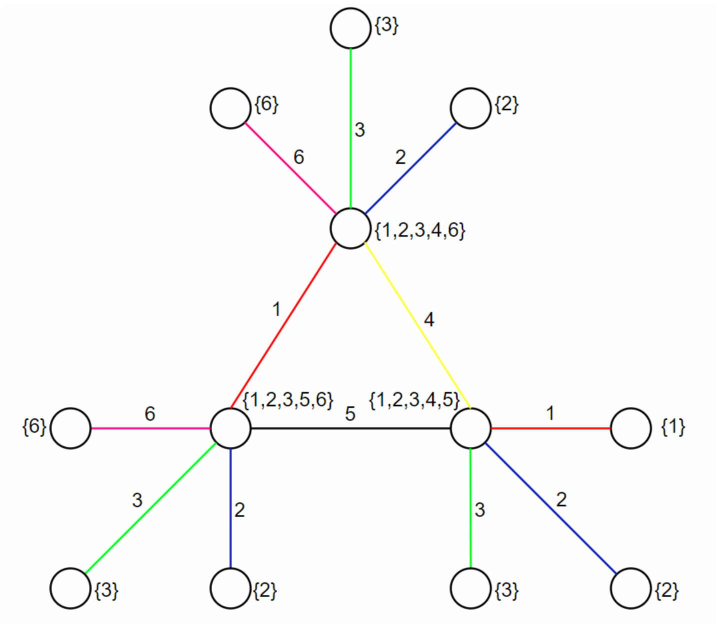

Figure 5: A neighbour set distinguishing colouring.

We might also wish for the sums over neighbour-sets of adjacent vertices to be distinguishable, in which case we get neighbour sum distinguishing colourings.

Def 4.9 *[10] (Neighbour sum distinguishing colouring)*
Let $G = (V, E)$ be a graph, let k be a positive integer, let $c\colon E \to [k]$ be a proper edge-k-colouring, and let $S(v) \subseteq E$ be the set of edges incident to a vertex $v \in V$. We call the edge-k-colouring c ***neighbour sum distinguishing*** *(nsd-k-colouring) iff for any edge the sums of the colours of the incident edges of the endpoints are different, or*

$$\forall \{u, v\} \in E : \sum_{e_v \in S(v)} c(e_v) \neq \sum_{e_u \in S(u)} c(e_u)$$

The smallest integer k such that there exists a nsd-k-colouring of the graph G is called the ***neighbour sum distinguishing chromatic index****, denoted by $\chi'_{\sum}(G)$.*

Examples for both a nd-k-colouring and a nsd-k-colouring can be found in Figures 5 and 6 respectively.

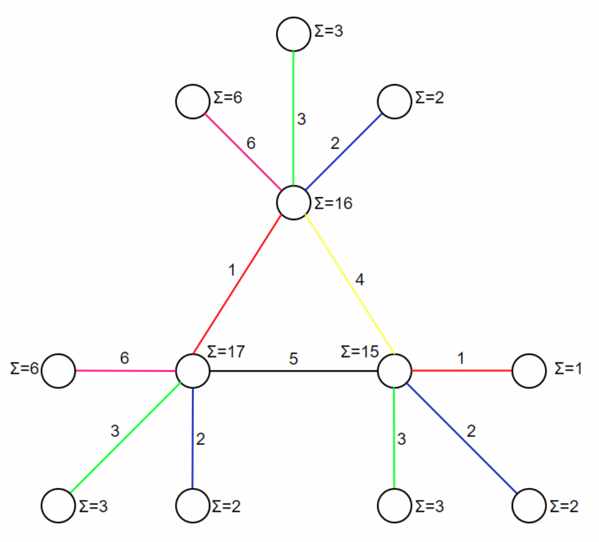

Figure 6: A neighbour sum distinguishing colouring.

There is a conjecture from 2002 by Z. Zhang, L. Liu, and J. Wang [11], which proposes that for every graph that has at least 6 vertices and no isolated edges, the neighbour set distinguishing chromatic index $\chi'_{nd}(G)$ is smaller than the maximum degree of the graph plus 3, or symbolically $\chi'_{nd}(G) \leq \Delta(G) + 2$.

Combining both edge and vertex colourings of a graph we get total colourings. That is a colouring of both the vertices and edges of a graph in such a way that no adjacent edges or vertices have the same colour. An example is also given in Figure 7.

Def 4.10 *[12] (Total colouring)*
*Let $G = (V, E)$ be a graph where $V \cap E = \emptyset$, and let $k \in \mathbb{N}$. We call a colouring $c\colon V \cup E \to [k]$ a **total k-colouring** iff it satisfies the properties*

1) $\forall e = \{u, v\} \in E \quad c(u) \neq c(v)$
(adjacent vertices have different colours),
2) $\forall v \in V \quad \forall e \in E : v \in e \Rightarrow c(v) \neq c(e)$
(a vertex and its incident edges have different colours),
3) $\forall e, e' \in E \quad e \cap e' \neq \emptyset \Rightarrow c(e) \neq c(e')$
(adjacent edges have different colours).

We can now look at colourings that in addition to distinguishing neighbouring edge sets also take into consideration the vertices themselves. We get the total neighbour set distinguishing colourings. An example can be seen in Figure 8.

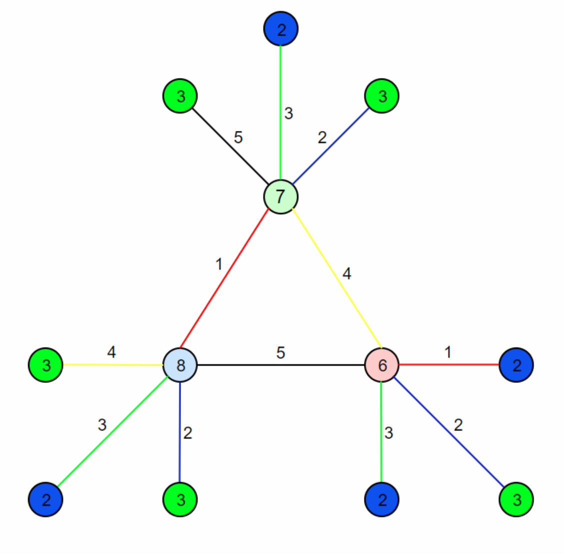

Figure 7: A total colouring.

Def 4.11 *[12] (Total neighbour set distinguishing colouring)*
Let $G = (V, E)$ be a graph where $V \cap E = \emptyset$, and let k be a positive integer. Let $c\colon V \cup E \to [k]$ be an total k-colouring, and let $S\colon V \to [k]$,

$$S(v) := (\{c(e) \mid e \in E \text{ s.t. } v \in e\} \cup \{c(v)\}) \subseteq [k]$$

be the set of colours $c(e)$ of the edges incident to a vertex $v \in V$ and the colour $c(v)$ of the vertex v.
*We call the total k-colouring of a graph **total neighbour set distinguishing** (total nd-k-colouring) iff for any edge $\{u, v\} \in E$ the sets $S(v)$ and $S(u)$ corresponding to the endpoints are different, or*

$$\forall \{u, v\} \in E : S(v) \neq S(u)$$

*The smallest integer k such that there exists a total nd-k-colouring of G is called the **total neighbour set distinguishing chromatic number**, denoted by $\chi''_{nd}(G)$.*

Repeating the process of summing the sets we get total neighbour sum distinguishing colourings. An example is given in Figure 9.

Def 4.12 *[12] (Total neighbour sum distinguishing colouring)*
*Let us have $G, k, c,$ and S as before. We call the total k-colouring of a graph **total neighbour sum distinguishing** (total nsd-k-colouring) iff for any edge $\{u, v\} \in E$ the sums of the colours in $S(v)$ and $S(u)$ of the endpoints are different, or*

$$\forall \{u, v\} \in E : \sum_{x \in S(v)} x \neq \sum_{y \in S(u)} y$$

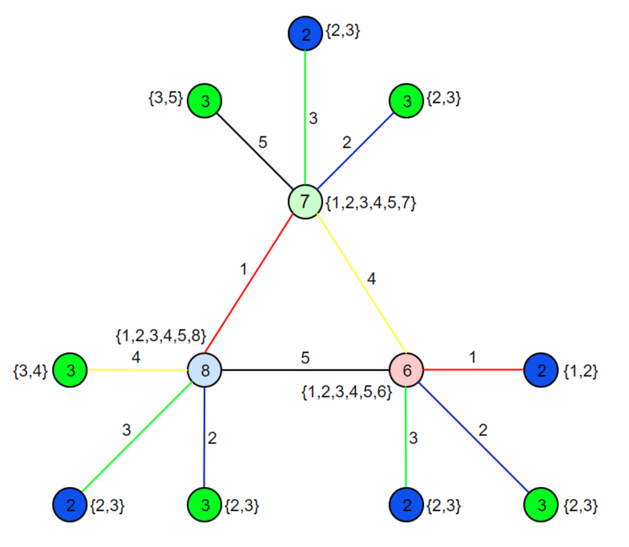

Figure 8: A total neighbour set distinguishing colouring.

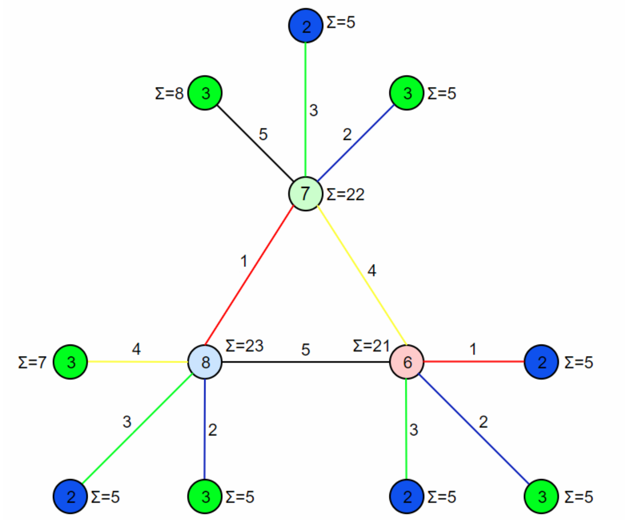

Figure 9: A total neighbour sum distinguishing colouring.

The smallest integer k such that there exists a total nsd-k-colouring of G is called the ***total neighbour sum distinguishing chromatic number****, denoted by* $\chi''_{\sum}(G)$.

We can also define, following the same construction, neighbour sum distinguishing total choosability of a graph $(\mathrm{ch}''_{\sum}(G))$ and neighbour set distinguishing total choosability of a graph ($\mathrm{ch}''_{nd}(G)$). Examples are given in Figures 10 and 11.

Def 4.13 *[12] (Total neighbour set distinguishing choosability)*
Let $G = (V, E)$ be a graph where $V \cap E = \emptyset$, let k be a positive integer. Let $S\colon V \cup E \to \mathbb{N}^k$ be a function assigning a set of k positive integers to each vertex and edge. We call a graph ***total neighbour set distinguishing k-choosable*** *(total nd-k-choosable) iff for every possible assignment S of sets of positive integers to the edges and vertices such that $\forall x \in V \cup E \quad |S(x)| = k$, there exists a total nd-k-colouring $c\colon V \cup E \to [k]$ such that $\forall x \in V \cup E \quad c(x) \in S(x)$. Or symbolically:*

$$\begin{aligned}
&G \textit{ is total nd-k-choosable} \Leftrightarrow \\
&\qquad\qquad \forall S\colon V \cup E \to \mathbb{N}^k \ \textit{s.t.}\ (\forall x \in V \cup E : |S(x)| = k), \\
&\qquad\qquad \exists c\colon V \cup E \to [k] \ \textit{s.t.}\ (\forall x \in V \cup E : c(x) \in S(x)), \ \textit{and} \\
&\qquad\qquad c \textit{ is a total nd-k-colouring.}
\end{aligned}$$

The smallest integer k, for which any specified collection of such lists there exists a neighbour set distinguishing colouring using colours from $S(x)$ for each $x \in V \cup E$, is called ***the neighbour set distinguishing total choosabilty*** *of G, denoted by $\mathrm{ch}''_{nd}(G)$.*

Def 4.14 *[12] (Total neighbour sum distinguishing choosability)*
Let us have G, k, and S as before. We call a graph ***total neighbour sum distinguishing k-choosable*** *(total nsd-k-choosable) iff for every possible assignment S of sets of positive integers to the edges and vertices such that $\forall x \in V \cup E \quad |S(x)| = k$, there exists a total nsd-k-colouring $c\colon V \cup E \to [k]$ such that $\forall x \in V \cup E \quad c(x) \in S(x)$. Or symbolically:*

$$\begin{aligned}
&G \textit{ is total nsd-k-choosable} \Leftrightarrow \\
&\qquad\qquad \forall S\colon V \cup E \to \mathbb{N}^k \ \textit{s.t.}\ (\forall x \in V \cup E : |L(x)| = k), \\
&\qquad\qquad \exists c\colon V \cup E \to [k] \ \textit{s.t.}\ (\forall x \in V \cup E : c(x) \in S(x)), \ \textit{and} \\
&\qquad\qquad c \textit{ is a total nsd-k-colouring.}
\end{aligned}$$

The smallest integer k, for which any specified collection of such lists there exists a neighbour sum distinguishing colouring using colours from $S(x)$ for each $x \in V \cup E$, is called ***the neighbour sum distinguishing total choosabilty*** *of G, denoted by $\mathrm{ch}''_{\sum}(G)$.*

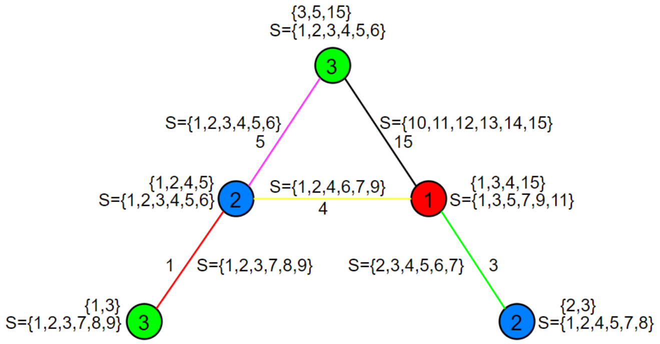

Figure 10: Total neigbour set distinguishing choosability.

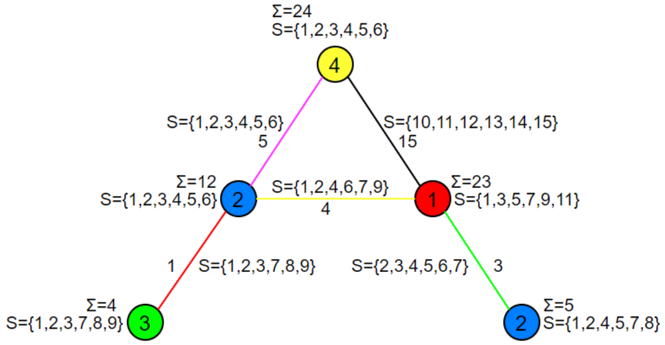

Figure 11: Total neigbour sum distinguishing choosability

4.1.3 Graph Labellings

Let us now assume that all vertices of a graph $G = (V, E)$ have labels attached to them that are arbitrary elements from a set S. We then have a mapping $f : V \to S$, which we call a **vertex-labelling** of the graph G. In the same way we can define an **edge-labelling** $f : E \to S$ of G. In most cases the set S is taken to be equal to $[k]$ for some positive integer k.

The reader might have heard of magic squares, where the sum of each row and each column is the same. An analogue also exists for edge-labelled graphs. If the sum of the edge-labels around each vertex is the same, then we get a magic labelling. More interestingly though, if the sum of the labels is different for all vertices, we call the labelling antimagic.

Def 4.15 *[13] (Antimagic labelling)*
Let $G = (V, E)$ be graph with $|E| = m, |V| = n$. Let $f : E \to [m]$ be an injective (in fact, bijective) edge-labelling, and let $L(v) \subseteq E$ be the set of labels on edges

incident to a vertex $v \in V$. We call f an ***antimagic labelling*** *iff $\forall u, v \in V$ such that $u \neq v$ it holds that $\sum_{e \in L(v)} e \neq \sum_{e' \in L(u)} e'$.*
We call the graph G antimagic iff there exists an antimagic labelling for G.

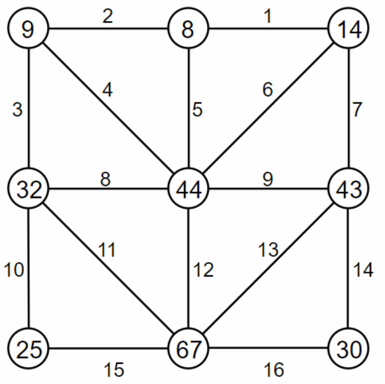

Figure 12: An antimagic graph

The reader may also think of antimagic labellings as neighbour sum distinguishing colourings, where all of the vertices have to have different sums, not just the adjacent ones. An example of an antimagic graph can be seen in Figure 12.

Note that in the definition we restricted the labels to the set $[m]$. If we allow the labels to be from the set $[m+k]$ while keeping all the other conditions, we would call the labelling a **k-antimagic** labelling (In short: k-AM).

Taking into account the vertices themselves, we get something similiar to total neighbour sum distinguishing colourings.

Def 4.16 *[13] ((ω, k)-antimagic labelling)*
*Let $G = (V, E)$ be graph with $|E| = m, |V| = n$. Let k be a non-negative integer. Let $f \colon E \to [m+k]$ be an injective edge-labelling. Let $\omega : V \to \mathbb{R}$ be a vertex-labelling from the set of real numbers, and let $L'(v) \subseteq E \cup \{v\}$ be the set of labels on the edges incident to a vertex $v \in V$ and the label on v. We call ω and f together a (ω, k)-**antimagic labelling** (in short: (ω, k)-AM) iff $\forall u, v \in V$ such that $u \neq v$ it holds that $\sum_{x \in L'(v)} x \neq \sum_{y \in L'(u)} y$.*
We call the graph G (ω, k)-antimagic iff there exists an (ω, k)-antimagic labelling for G.

Clearly the (0,0)-AM labelling (with ω being the 0-function) is equivalent to the 0-AM labelling and also to the normal antimagic labelling. An example of a (1,0)-AM graph (with $\omega(v) = 1 \quad \forall v \in V$ being the constant 1-function) is in Figure 13.

It was conjectured by N. Hartsfield and G. Ringel in 1990 [14] that every connected graph that is not the K_2 graph, is antimagic.

In addition to antimagic labellings there are also lucky labellings, which come from labelling only the vertices. (See example in Figure 14.)

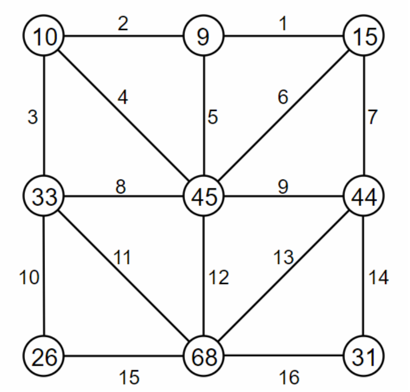

Figure 13: A (1,0)-antimagic graph

Def 4.17 *[15] (Lucky labelling)*
Let $G = (V, E)$ be graph. Let $f\colon V \to \mathbb{N}$ be a vertex-labelling, and let $S(v)$ be the sum of labels of vertices adjacent to the vertex $v \in V$. We call f a ***lucky labelling*** *iff*

$$\forall \{u, v\} \in E : S(u) \neq S(v)$$

We call the smallest positive interger k such that there exists a lucky labelling $f\colon V \to [k]$ the ***lucky number*** *of G, denoted $\eta(G)$.*
We call the graph G lucky iff there exists a lucky labelling for G.

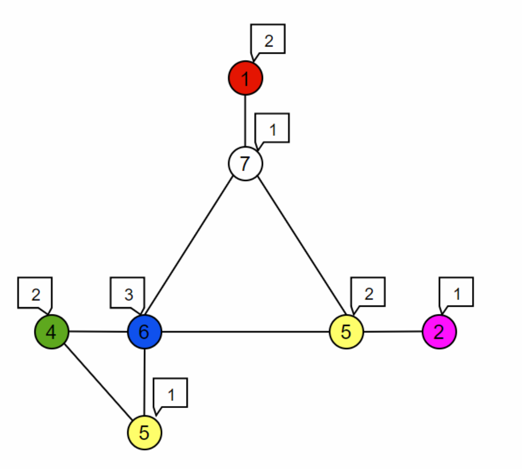

Figure 14: A lucky labelling.

Now we have a multitude of colourings and the smallest numbers of colours needed for them to exist for a given graph G.

- **The chromatic number** $\chi(G)$ for a proper vertex colouring
- **The choice number** $\mathrm{ch}(G)$ for k-choosability
- **The chromatic index** $\chi'(G)$ for a proper edge colouring
- **The list chromatic index** $ch'(G)$ for k-list-choosability
- **The neighbour set distinguishing chromatic index** $\chi'_{nd}(G)$ for a nd-k-colouring
- **The neighbour sum distinguishing chromatic index** $\chi'_{\sum}(G)$ for a nsd-k-colouring
- **The total neighbour set distinguishing chromatic number** $\chi''_{nd}(G)$ for a total nd-k-colouring
- **The total neighbour set distinguishing choice number** $\mathrm{ch}''_{nd}(G)$ for a total nd-k-choosability
- **The total neighbour sum distinguishing chromatic number** $\chi''_{\sum}(G)$ for a total nsd-k-colouring
- **The total neighbour sum distinguishing choice number** $\mathrm{ch}''_{\sum}(G)$ for a total nsd-k-choosability

We also have two notions for labellings.

- **The lucky number** $\eta(G)$ for a lucky labelling
- (ω, k)**-antimagic** graphs for antimagic labellings

Lastly we have three general notions.

- **The maximum degree** $\Delta(G)$
- **The average degree** $\mathrm{ad}(G)$
- **The maximum average degree** $\mathrm{mad}(G)$

Equipped with these notions, we can start looking at the applications of the Combinatorial Nullstellensatz.

4.2 Results in graph colourings

Most of the definitions in the previous section have arisen from attempts at proving The List Colouring Conjecture. [1] The conjectures proposes that for every graph, the chromatic index is equal to its list chromatic index, or symbolically $\forall G \quad \chi'(G) = ch'(G)$. While significant improvements have been made with achieving better bounds, the conjecture still remains an open problem.

Some researchers [10][12] approach this through neigbour-sum colourings. It is easy to check that if G is a normal graph (that is, if G does not have an isolated edge), then $\Delta(G) \leq \chi'(G) \leq \chi'_{nd}(G) \leq \chi'_{\sum}(G)$. Additionally, for total colorings it can be shown that $\chi''_{nd}(G) \leq \chi''_{\sum}(G)$. [10][12]

In 2014 L. H. Ding, G. H. Wang, and G. Y. Yan [12] proved the following bounds. In this theorem $\mathrm{col}(G)$ is the colouring number of a graph G, which is defined as the smallest integer k such that G has a vertex enumeration in which each vertex is preceded by fewer than k of its neighbours.

Theorem 4.1 *[12]*
Let G be a graph with at least 2 vertices. Then

$$\begin{aligned} \mathrm{ch}''_{\sum}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 1; \\ \mathrm{ch}''_{nd}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 1; \\ \chi''_{\sum}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 1. \end{aligned}$$

Furthermore, if G does not contain a component which is a regular subgraph of degree $\Delta(G)$, then

$$\begin{aligned} \mathrm{ch}''_{\sum}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 2; \\ \mathrm{ch}''_{nd}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 2; \\ \chi''_{\sum}(G) &\leq 2\Delta(G) + \mathrm{col}(G) - 2. \end{aligned}$$

A few years later, in 2018, L. H. Ding, X. W. Yu, and Y. P. Gao [10] extended the previous theorem.

Theorem 4.2 *[10]*
Let G be a normal graph with maximum degree $\Delta(G) \geq 5$ and maximum average degree $\mathrm{mad}(G) < 3 - \frac{2}{\Delta(G)}$. Then

$$\chi'_{\sum}(G) \leq \Delta(G) + 1.$$

Since $\chi'_{nd}(G) \leq \chi'_{\sum}(G)$, then it also holds that:

$$\chi'_{nd}(G) \leq \Delta(G) + 1.$$

In 2009 T. Bartnicki, J. Grytczuk, and S. Niwczyk [16] approached the List Colouring Conjecture from a slightly different angle and proved for several classes of graphs, including complete graphs, complete bipartite graphs, and trees (except K_2, which is a graph containing two vertices connected by a single edge), that they are weight colourable from the set $\{1, 2, 3\}$. Weight colourability is a combination of list-choosability and neighbour sum distinguishing colourings. It is defined as follows.

Def 4.18 *[16]*
Let $G = (V, E)$ be a finite graph and $L_e \subset \mathbb{R}$ be lists of real numbers assigned to each edge $e \in E$.

*We call a graph G **weight colourable** from the lists L_e iff there exists an edge weighting $w\colon E \to \cup_{e \in E} L_e$ such that for each edge $e, w(e) \in L_e$, and the* *sums of the weights of the incident edges of the endpoints of each edge are different, or symbolically, if $S(v)$ is the set of all edges incident to a vertex $v \in V$,*

$$\begin{aligned} &\exists w \colon E \to \cup_{e \in E} L_e \ s.t. \\ &\qquad\qquad\qquad \forall e \in E : w(e) \in L_e, \\ &\qquad\qquad\qquad \forall \{u,v\} \in E : \sum_{e_v \in S(v)} w(e_v) \neq \sum_{e_u \in S(u)} w(e_u) \end{aligned}$$

*Additionally, G is **k-weight choosable** iff it is weight colourable from any collection of lists of size k.*

In the same year, S. Czerwinski, J. Grytczuk and W. Zelazny [15] used the Combinatorial Nullstellensatz to prove that every orientable graph with a maximum out-degree of k, has a lucky number $\eta(G) \leq k+1$. A graph is called orientable iff it is possible to add directions to the edges in such a way that every vertex is reachable from every other vertex. Furthermore, they proved that every planar-bipartite graph has a lucky number $\eta(G) \leq 3$, and conjectured that $\eta(G) \leq \chi(G)$ for every graph. [15]

In the next two theorems about antimagic labellings, we use the term graph factorisation, which is defined as follows:

Def 4.19
*We say that a graph $G = (V, E)$ **admits an H-factor** iff there exists a spanning subgraph $G' := (V, E') \subseteq (V, E)$ of G (that is a subgraph of G that covers all the vertices of G) such that every connected component of G' is isomorphic to H. Furthermore, we call the partition of the edges of G into factors H an **H-factorisation of** G.*

Additionally, we denote the cycle of length $n \in \mathbb{N}$ as C_n, and a graph consisting of r pairwise disjoint n-cycles is denoted as C_n^r.

The results make significant steps towards the conjecture that every graph, other than K_2, is antimagic. In particular, D. Hefetz proved in 2005 [13] the following result.

Theorem 4.3 *[13]*
Let G be a graph on 3^k vertices, where $k \in \mathbb{N}$. If G admits a C_3-factor, then G is antimagic.

A few years later, in 2009, D. Hefetz along with A. Saluz and H. T. T. Tran [17] extended the proof to a more general result.

Theorem 4.4 *[17]*
Let G be a graph on $n = p^k$ vertices, where p is an odd prime and $k \in \mathbb{N}$. If G admits a C_p-factor, then it is antimagic.

The latest results by T. L. Wong; X. D. Zhu [18] look at (ω, k)-antimagic graphs. In particular, they prove the following two theorems.

Theorem 4.5 *[18]*
Let $G = (V, E)$ be a graph. If there exists a vertex $v \in V$ that is adjacent to all other vertices, then G is $(\omega, 2)$-antimagic for any weight function $\omega\colon V \to \mathbb{N}$.

Theorem 4.6 *[18]*
Let $G = (V, E)$ be a graph. If $|V| = p$, where p is a prime, and G has a Hamiltonian path, then G is $(\omega, 1)$-antimagic for any weight function $\omega\colon V \to \mathbb{N}$.

Most of the proofs of the theorems above rely on the Combinatorial Nullstellensatz and the following lemma.

Lemma 4.7 *[19]*
Let $P(x_1, x_2, \ldots, x_n) \in \mathbb{R}[x_1, x_2, \ldots, x_n]$, $n \in \mathbb{N}$, and $\{s_1, s_2, \ldots, s_n\} \in \mathbb{N}^n$. If $\deg(P) \leq s_1 + s_2 + \ldots + s_n$, then

$$\left(\frac{\partial}{\partial x_1}\right)^{s_1}\left(\frac{\partial}{\partial x_2}\right)^{s_2}\ldots\left(\frac{\partial}{\partial x_n}\right)^{s_n} P(x_1, x_2, \ldots, x_n)$$
$$= \sum_{x_1=0} s_1 \ldots \sum_{x_n=0} s_n (-1)^{s_1+x_1}\binom{s_1}{x_1}\ldots(-1)^{s_n+x_n}\binom{s_n}{x_n} P(x_1, x_2, \ldots, x_n).$$

The general idea for these proofs is to construct a polynomial P which has a non-zero evaluation if and only if the theorem in question holds, and simplify it by using Lemma 4.7, to a form where the coefficients of the monomials are easier to find. After proving that the coefficient of a monomial of degree $\deg(P)$ is not zero, the Combinatorial Nullstellensatz is used and the proof is completed.

It is also interesting to note that most of the proofs use iterated applications of the Combinatorial Nullstellensatz, mostly due to applying mathematical induction in the process.

For completeness, we will present a sketch of a proof for Theorem 4.4, as given by D. Hefetz, A. Saluz, and H. T. T. Tran [17]. We omit much of the technical details, to keep the proof readable and focused on the use of the Combinatorial Nullstellensatz. Additionally, we will mark "$(*)$" at places, where a more significant gap is left. The reader may refer to the original paper [17] for the details.

Proof of Theorem 4.4: [17]
Let p be an odd prime and $k \in \mathbb{N}$. Let $G = (V, E)$ be a graph with $V = \{0, 1, \ldots, n-1\}$, where $n = p^k$, such that it admits a C_p-factor $f = (V, E')$. Let $r = n/p$ denote the number of p-cycles in f. Since all the connected components of f have to be isomorphic to C_p, then $f \cong C_p^r$. Also note that as every p-cycle has exactly p edges and there are r of such cycles in f, then $|E'| = n$. Label the edges of $E \setminus E'$ arbitrarily using labels from $\{n+1, \ldots, |E|\}$. Let $w\colon V \to \mathbb{R}$ be a vertex-labeling from the set of real numbers. For every vertex $v \in V$, denote the sum of labels on the edges incident to v and the label of the vertex v as $\omega(v)$. It suffices to prove that the factor f is $(\omega, 0)$-antimagic for any vertex-labeling ω.$(*)$ Let

$$P_\omega(x_0, \ldots, x_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (x_{i_1} + x_{i_2} + \omega(i) - x_{j_1} - x_{j_2} - \omega(j)),$$

where x_{i_1}, x_{i_2} represent the edges of f that are incident with a vertex $i \in V$, and x_{j_1}, x_{j_2} represent the edges of f that are incident with a vertex $j \in V$. Note that since all the components of f are isomorphic to C_p then the degree of every vertex in f is two ($\deg(v) = 2 \quad \forall v \in V$). Let

$$Q_\omega(x_0, \ldots, x_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (x_i - x_j) P_\omega(x_0, \ldots, x_{n-1}).$$

The factor f is $(\omega, 0)$-antimagic if and only if there exists a vector $(a_0, \ldots, a_{n-1}) \in [n]^n$ such that $Q_\omega(a_0, \ldots, a_{n-1}) \neq 0$. By the Combinatorial Nullstellensatz it suffices to show that there exists a monomial $x_0^{n-1} \ldots x_{n-1}^{n-1}$ with a non-zero coefficient in the expansion of $Q_\omega(x_0, \ldots, x_{n-1})$.

Denote the coefficient of the monomial $x_0^{n-1} \ldots x_{n-1}^{n-1}$ with c, and note that c is equal to the coefficient of the same monomial in

$$Q_0(x_0, \ldots, x_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (x_i - x_j) P_0(x_0, \ldots, x_{n-1}),$$

where

$$P_0(x_0, \ldots, x_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (x_{i_1} + x_{i_2} - x_{j_1} - x_{j_2}).$$

By Lemma 4.7

$$\begin{aligned}
& c[(n-1)!]^n \\
& = \left(\frac{\partial}{\partial x_0}\right)^{n-1} \left(\frac{\partial}{\partial x_1}\right)^{n-1} \cdots \left(\frac{\partial}{\partial x_{n-1}}\right)^{n-1} Q_0(x_0, x_1, \ldots, x_{n-1}) \\
& = \sum_{x_0=0}^{n-1} \cdots \sum_{x_{n-1}=0}^{n-1} (-1)^{x_0+\ldots+x_{n-1}} \prod_{i=0}^{n-1} \binom{n-1}{x_i} Q_0(x_0, \ldots, x_{n-1}) \\
(*) & = (-1)^{\binom{n}{2}} \prod_{i=0}^{n-1} \binom{n-1}{i} \prod_{n-1 \geq i > j \geq 0} (i-j) \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) P_0(\sigma(0), \ldots, \sigma(n-1)),
\end{aligned}$$

where $\mathcal{S}_n$ is the set of permutations on n elements and $\operatorname{sgn}(\sigma)$ is the parity of the permutation. Therefore it is sufficient to prove that

$$\sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) P_0(\sigma(0), \ldots, \sigma(n-1)) \neq 0.$$

Let $H_n = \mathcal{S}_n / \operatorname{Aut}(C_p^r)$, where $\operatorname{Aut}(G)$ denotes the automorphism group of G, and let the period of $\sigma \in \mathcal{S}_n$, denoted by k_σ, be the smallest positive integer such that σ and $\sigma + k_\sigma$ both belong in the same element of H_n. Let id_n denote the identity element in $\mathcal{S}_n$.

Then it is possible to show that $(*)$

$$\sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) P_0(\sigma(0), \ldots, \sigma(n-1)) = (2p)^r r! \sum_{[\tau] \in H_n} \operatorname{sgn}(\tau) P_0(\tau(0), \ldots, \tau(n-1)),$$

where $[\tau]$ is an element (coset) of H_n, and τ is any representative of $[\tau]$.

For any $\pi \in \mathcal{S}_n$ let

$$S(\pi) := \frac{P_0(\pi(0), \dots, \pi(n-1))}{\prod_{n-1 \geq i > j \geq 0}(i-j)} \mod p.$$

Additionally, $S(\pi)$ is well defined.($*$) Therefore it suffices to prove that

$$\sum_{[\tau] \in H_n} \operatorname{sgn}(\tau) S(\tau) \neq 0 \mod p.$$

D. Hefetz, A. Saluz, and H. T. T. Tran go on to prove the following equalities: ($*$)

$$\begin{aligned}
&\sum_{[\tau] \in H_n} \operatorname{sgn}(\tau) S(\tau) = \sum_{[\tau] \in B_1} \operatorname{sgn}(\tau) S(\tau) + \sum_{[\tau] \in B_2} \operatorname{sgn}(\tau) S(\tau), \\
&\sum_{[\tau] \in B_1} \operatorname{sgn}(\tau) S(\tau) = 0 \mod p, \text{ and} \\
&\sum_{[\tau] \in B_2} \operatorname{sgn}(\tau) S(\tau) = \frac{p-1}{2} \operatorname{sgn}(id_p^r) S(id_p^r) \neq 0 \mod p,
\end{aligned}$$

where $B_1 := \{[\pi] \in H_n \colon p \mid k_\pi\}$ and $B_2 := \{[\pi] \in H_n \colon k_\pi = 1\}$. We now have the series of implications:

$$\begin{aligned}
&\sum_{[\tau] \in B_1} \operatorname{sgn}(\tau) S(\tau) = 0 \mod p, \text{ and } \sum_{[\tau] \in B_2} \operatorname{sgn}(\tau) S(\tau) \neq 0 \mod p \\
&\Rightarrow \sum_{[\tau] \in H_n} \operatorname{sgn}(\tau) S(\tau) \neq 0 \mod p \\
&\Rightarrow \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) P_0(\sigma(0), \dots, \sigma(n-1)) \neq 0 \\
&\Rightarrow c \neq 0 \\
&\Rightarrow \exists (a_0, \dots, a_{n-1}) \in [n]^n \text{ s.t. } \forall \omega \quad Q_\omega(a_0, \dots, a_{n-1}) \neq 0 \\
&\Leftrightarrow f \text{ is } (\omega, 0)\text{-antimagic for all } \omega \\
&\Rightarrow G \text{ is antimagic. } \square
\end{aligned}$$

It is apparent that proving these new results requires complex technicalities from their own field in addition to the Combinatorial Nullstellensatz, but nonetheless Alon's theorem has sparked novel ways of approaching proofs.

5 The Unique-Multiset and GM-MDS Conjectures

In addition to the results above, we will provide an outline for a possible proof, which utilizes the Combinatorial Nullstellensatz, to a combinatorial problem called the GM-MDS Conjecture. [20]

As with any conjecture, we should first give an overview of the background. The Unique-Multiset Conjecture stems from a conjecture about Maximum Distance Seprable (MDS) error-correcting codes (which also contain the well known Reed-Solomon error-correcting codes), called the GM-MDS Conjecture. [20] Notably, it has been shown by S. H. Dau, W. Song, and C. Yuen [20] that if the Unique-Multiset Conjecture holds, then the determinant of a certain matrix (which we will also define later) is not identically zero, from which it follows that the GM-MDS Conjecture holds.

While the The Unique-Multiset Conjecture remains an open problem, the GM-MDS Conjecture has been recently proven by Shachar Lovett [21]. The proof utilizes the polynomial method and namely the Schwartz–Zippel-DeMillo-Lipton lemma [22], which has many similiarities with the Combinatorial Nullstellensatz. This gives hope that it is possible to utilize similiar constructions to prove both the MDS Conjecture and the Unique-Multiset Conjecture using the Combinatorial Nullstellensatz.

The Unique-Multiset Conjecture can be stated as follows.

Conjecture 5.1 *[20] (The Unique-Multiset Conjecture)*
Let $Z_i = \{z_{i,1}, z_{i,2}, \dots, z_{i,k-1}\}$, $i \in [k]$ be subsets of $[n]$ consisting of $k-1$ elements each, such that they satisfy

$$|\cap_{i \in I} Z_i| \leq k - |I|,$$

for every nonempty subset $I \subseteq [k]$. Consider all permutations σ on k elements. For each permutation σ, consider all possible ways of selecting a $(\sigma(i)-1)$-element subset S_i of Z_i for each $i \in [k]$. If we take a multiset (A set that allows duplicate elements) union of these k subsets S_i, then there exists a multiset M that is unique among all possible selections of σ and the sets S_i.

In essence the assumption of the conjecture says that we need to have sets that do not intersect in too many places. The condition $|\cap_{i \in I} Z_i| \leq k - |I|$ means that for any two sets there must be an element in each set such that it is not also in the other set. Any three sets should have at least two elements each that are not simultaneously in the other two sets, and so on until for all k sets there must not be any elements that are contained in all sets.

It is clear that there are $k!$ permutations on k elements and for each permutation there are $\binom{k-1}{\sigma(i)-1}$ possible selections of subsets for each $i \in [k]$. Since a permutation simply reorders the k elements, then there are $\prod_{i=1}^{k} \binom{k-1}{i-1} = \prod_{i=1}^{k-1} \binom{k-1}{i} = \prod_{i=1}^{k-1} i^{2i-k}$ choices of the sets S_i for each permutation. From this we can see that there are $k! \prod_{i=1}^{k-1} i^{2i-k}$ ways of selecting the permutation and the subsets, and the same number of resulting multisets.

The conjecture itself proposes that no matter which sets Z_i are chosen, as long as the assumptions hold, there will be at least one multiset that appears exactly once among all the possible multisets.

The GM-MDS Conjecture, for which we will provide an outline of a possible proof, is stated as follows.

Conjecture 5.2 *[20] (GM-MDS Conjecture)*
Let $M = (m_{i,j})$ be a $k \times n$ binary matrix, such that

$$|\cap_{i\in I} \textit{supp}(M_i)| \geq n - k + |I|,$$

for every nonempty subset $I \subseteq [k]$, where $\textit{supp}(M_i) = \{j \mid 1 \leq j \leq n, \quad m_{i,j} \neq 0\}$ is the support of the i-th row of M. Then for every prime power $q \geq n+k-1$, there exists an $[n,k]_q$ MDS code that has a generator matrix $G = (g_{i,j})$ satisfying $g_{i,j} = 0$ whenever $m_{i,j} = 0$.

We will omit the definitions for the terms (like $[n,k]_q$ MDS code and a generator matrix) in the proposition of the conjecture, as they are not important in our proof. The reader may find out more about the MDS codes, error-correcting codes, and the related definitions and how the it relates to the Unique-Multiset Conjecture from the original article from S. H. Dau, W. Song, and C. Yuen [20] and from the book "The Theory of Error-Correcting Codes" by F.J. MacWilliams and N. J. A. Sloane [23].

It is however important to note the following result from S. H. Dau, W. Song, and C. Yuen [20].

Lemma 5.3 *[20]*
Let k, n be positive integers, such that $n \geq k+1$. Let q be a prime power, such that $q \geq n+k-1$.
Let $\mathbb{F}_q$ be the field of q elements, and $\alpha_1, \ldots, \alpha_n$ be n distinct elements in $\mathbb{F}_q$.
Let $Z_i = \{z_{(i,1)}, z_{(i,2)}, \ldots z_{(i,k-1)}\} \subset [n] \quad i \in [k]$, be $(k-1)$-element subsets of $[n]$, such that $|\cap_{i\in I} Z_i| \leq k - |I|$ for all $I \in \mathcal{P}([k]) \setminus \emptyset$. That is, let Z_i be sets as prescribed by the Unique-Multiset Conjecture.
Let $A = (a_{i,j})$ be a $k \times k$ matrix, such that

$$a_{i,j} = \begin{cases} (-1)^{k-j} \sum_{T\subseteq Z_i, |T|=k-j} \prod_{t\in T} \alpha_t, \text{ if } 1 \leq j < k, \\ 1, \text{ if } j = k. \end{cases}$$

If $\det(A)$ is not identically zero, then the GM-MDS Conjecture holds.

5.1 An example of the Unique-Multiset Conjecture

For a better understanding of the Unique-Multiset Conjecture, we present a short example with $k = 3$ and $n = 4$.

$$Z_1 = \{1,2\}, Z_2 = \{2,3\}, Z_3 = \{1,4\}.$$

Clearly all three of these sets are of size $k-1 = 2$. We can also check that these sets satisfy the condition $|\cap_{i\in I} Z_i| \leq k - |I|$ for all $I \in \mathcal{P}([k]) \setminus \emptyset$. Indeed, if $|I| = 1$, then $|Z_1| = |Z_2| = |Z_3| = k-1$. For the two element subsets, we can see that $|Z_i \cap Z_j| = 1 = k - |I| = 3 - 2$ for every $i, j \in [3], j \neq i$. And lastly if $I = \{1,2,3\}$, then $|Z_1 \cap Z_2 \cap Z_3| = 0$. Therefore these sets are as prescribed by the Unique-Multiset Conjecture.

On 3 elements there are 6 possible permutations. Let us label them as follows.

$$\sigma_1 = \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \sigma_2 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \sigma_3 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \sigma_4 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \sigma_5 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \sigma_6 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$$

Then we get the corresponding 12 multisets as in Table 1.

Table 1: Example of multisets generated by the Unique-Multiset Conjecture

	σ_1	σ_1	σ_2	σ_2	σ_3	σ_3	σ_4	σ_4	σ_5	σ_5	σ_6	σ_6
Z_1	$\{\}$	$\{\}$	$\{1\}$	$\{2\}$	$\{1,2\}$	$\{1,2\}$	$\{\}$	$\{\}$	$\{1\}$	$\{2\}$	$\{1,2\}$	$\{1,2\}$
Z_2	$\{2\}$	$\{3\}$	$\{2,3\}$	$\{2,3\}$	$\{\}$	$\{\}$	$\{2,3\}$	$\{2,3\}$	$\{\}$	$\{\}$	$\{2\}$	$\{3\}$
Z_3	$\{1,4\}$	$\{1,4\}$	$\{\}$	$\{\}$	$\{4\}$	$\{1\}$	$\{4\}$	$\{1\}$	$\{1,4\}$	$\{1,4\}$	$\{\}$	$\{\}$
Multiset	$\{1,2,4\}$	$\{1,3,4\}$	$\{1,2,3\}$	$\{2,2,3\}$	$\{1,2,4\}$	$\{1,1,2\}$	$\{2,3,4\}$	$\{1,2,3\}$	$\{1,1,4\}$	$\{1,2,4\}$	$\{1,2,2\}$	$\{1,2,3\}$

As conjectured, there exists a unique multiset. In fact, for this configuration of the sets Z_1, Z_2, Z_3, there are 6 multisets that are unique among all resulting multisets. These are the multisets $\{1,3,4\}, \{2,2,3\}, \{1,1,2\}, \{2,3,4\}, \{1,1,4\}$, and $\{1,2,2\}$.

As the matrix A that we defined in Lemma 5.3 is the key point in our proof, we will also give here an example of both the matrix A and its determinant.

$$\begin{aligned} A &= \begin{pmatrix} \sum_{T\subseteq\{1,2\},|T|=2} \prod_{t\in T} \alpha_{z_{(1,t)}} & (-1)\sum_{t=1}^{2} \alpha_{z_{(1,t)}} & 1 \\ \sum_{T\subseteq\{2,3\},|T|=2} \prod_{t\in T} \alpha_{z_{(2,t)}} & (-1)\sum_{t=1}^{2} \alpha_{z_{(2,t)}} & 1 \\ \sum_{T\subseteq\{1,4\},|T|=2} \prod_{t\in T} \alpha_{z_{(3,t)}} & (-1)\sum_{t=1}^{2} \alpha_{z_{(3,t)}} & 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1 \cdot \alpha_2 & (-1)(\alpha_1 + \alpha_2) & 1 \\ \alpha_2 \cdot \alpha_3 & (-1)(\alpha_2 + \alpha_3) & 1 \\ \alpha_1 \cdot \alpha_4 & (-1)(\alpha_1 + \alpha_4) & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned}\det(A) &= \begin{vmatrix} \alpha_1 \cdot \alpha_2 & (-1)(\alpha_1 + \alpha_2) & 1 \\ \alpha_2 \cdot \alpha_3 & (-1)(\alpha_2 + \alpha_3) & 1 \\ \alpha_1 \cdot \alpha_4 & (-1)(\alpha_1 + \alpha_4) & 1 \end{vmatrix} \\ &= -\alpha_1\alpha_2(\alpha_2 + \alpha_3) - \alpha_1\alpha_4(\alpha_1 + \alpha_2) - \alpha_2\alpha_3(\alpha_1 + \alpha_4) + \\ &\quad + \alpha_1\alpha_4(\alpha_2 + \alpha_3) + \alpha_1\alpha_2(\alpha_1 + \alpha_4) + \alpha_2\alpha_3(\alpha_1 + \alpha_2) \\ &= -\alpha_1^1\alpha_2^2\alpha_3^0\alpha_4^0 - \alpha_1^1\alpha_2^1\alpha_3^1\alpha_4^0 - \alpha_1^2\alpha_2^0\alpha_3^0\alpha_4^1 - \alpha_1^1\alpha_2^1\alpha_3^0\alpha_4^1 \\ &\quad - \alpha_1^1\alpha_2^1\alpha_3^1\alpha_4^0 - \alpha_1^0\alpha_2^1\alpha_3^1\alpha_4^1 + \alpha_1^1\alpha_2^1\alpha_3^0\alpha_4^1 + \alpha_1^1\alpha_2^0\alpha_3^1\alpha_4^1 \\ &\quad + \alpha_1^2\alpha_2^1\alpha_3^0\alpha_4^0 + \alpha_1^1\alpha_2^1\alpha_3^0\alpha_4^1 + \alpha_1^1\alpha_2^1\alpha_3^1\alpha_4^0 + \alpha_1^0\alpha_2^2\alpha_3^1\alpha_4^0\end{aligned}$$

Note the powers of the variables $\alpha_1, \dots, \alpha_4$ in the mononomials. They exactly describe the multisets we got previously, with $\alpha_1, \dots, \alpha_4$ corresponding to the multiset elements $1, \dots, 4$ respectively. For the monomial $-\alpha_1^1\alpha_2^2\alpha_3^0\alpha_4^0$ we have the corresponding multiset $\{1, 2, 2\}$, to the monomial $-\alpha_1^1\alpha_2^1\alpha_3^1\alpha_4^0$ corresponds the multiset $\{1, 2, 3\}$, and so on.

5.2 Outline of a possible proof of the GM-MDS Conjecture

As per Lemma 5.3 if $\det(A)$ is not identically zero, then the GM-MDS Conjecture holds. Therefore to prove the GM-MDS Conjecture, we want to show that $\det(A)$ can never be identically zero. For this we hope to use the Generalized Combinatorial Nullstellensatz (Theorem 2.4).

As given by Lemma 5.3, let k, n be positive integers such that $n \geq k+1$. Let q be a prime power such that $q \geq n+k-1$. Let $\mathbb{F}_q$ be a field of q elements, and $\alpha_1, \dots, \alpha_n$ be n distinct elements in $\mathbb{F}_q$. Let $Z_i = \{z_{(i,1)}, z_{(i,2)}, \dots z_{(i,k-1)}\} \subset [n] \quad i \in [k]$, be $(k-1)$-element subsets of $[n]$, such that $| \cap_{i \in I} Z_i| \leq k - |I|$ for all $I \in \mathcal{P}([k]) \setminus \{\emptyset\}$. That is, let Z_i be sets as prescribed by the Unique-Multiset Conjecture. Let $A = (a_{i,j})$ be a $k \times k$ matrix, given by

$$a_{i,j} = \begin{cases} (-1)^{k-j} \sum_{T \subseteq Z_i, |T| = k-j} \prod_{t \in T} \alpha_t, \text{ if } 1 \leq j < k, \\ 1, \text{ if } j = k. \end{cases}$$

Note that the highest degree of α_t in $a_{i,j}$ is at most 1 for every $t \in [n]$ and $i, j \in [k]$. [20] Writing out the last few columns of A, we get:

$$A = \begin{pmatrix} a_{1,1} & \cdots & \sum_{T \subseteq Z_1, |T|=2} \prod_{t \in T} \alpha_{z_{(1,t)}} & (-1) \sum_{t=1}^{k-1} \alpha_{z_{(1,t)}} & 1 \\ a_{2,1} & \cdots & \sum_{T \subseteq Z_2, |T|=2} \prod_{t \in T} \alpha_{z_{(2,t)}} & (-1) \sum_{t=1}^{k-1} \alpha_{z_{(2,t)}} & 1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{k,1} & \cdots & \sum_{T \subseteq Z_k, |T|=2} \prod_{t \in T} \alpha_{z_{(k,t)}} & (-1) \sum_{t=1}^{k-1} \alpha_{z_{(k,t)}} & 1 \end{pmatrix}$$

Let us now consider the determinant $\det(A)$. Note that $\det(A) \in \mathbb{F}_q[\alpha_1, \dots, \alpha_n]$ is a polynomial in n variables over the field $\mathbb{F}_q[\alpha_1, \dots, \alpha_n]$. Similiarly to selecting the sets that will be contained in a multiset in the Unique-Multiset Conjecture, the determinant of A is a sum over all possible permutations and all possible suitably-sized subsets of the sets Z_i. As a result, the determinant will be a sum of monomials in variables $\alpha_1, \ldots, \alpha_n$, with each monomial $\alpha_1^{p_1}\alpha_2^{p_2}\ldots\alpha_n^{p_n}$ corresponding to a multiset $\{\underbrace{11\ldots1}_{p_1}\underbrace{22\ldots2}_{p_2}\ldots\underbrace{nn\ldots n}_{p_n}\}$ given by the Unique-Multiset Conjecture. [20]

Note that by the definition of the determinant

$$\det(A) = \sum_{\sigma\in\mathcal{S}_k} \operatorname{sgn}(\sigma)\prod_{i=1}^{k} a_{i,\sigma(i)}$$

(where $\mathcal{S}_k$ is the symmetric permutation group on k elements and $\operatorname{sgn}(\sigma)$ is the sign of the permutation σ), and since we already established that highest degree for every α_t in every $a_{i,j}$ is 1, then the degree of every α_t in any given monomial in $\det(A)$ can be at most $k-1$ (it can not be k, since the rightmost column of A is a column of ones, which do not add to the total degree). This means that for every monomial $\alpha_1^{t_1}\alpha_2^{t_2}\ldots\alpha_n^{t_n}$ in $\det(A)$, it holds that $0 \leq t_i < k \quad \forall i \in [n]$. [20]

If we define $S_1 = S_2 = \ldots = S_n = \{\alpha_1, \ldots, \alpha_n\}$ as n subsets of $\mathbb{F}_q$ of size n, then we have most of the assumptions necessary to use the Generalized Combinatorial Nullstellensatz. In particular, we have:

- $\mathbb{F}_q$ is a field.
- $f(\alpha_1, \ldots, \alpha_n) = \det(A) \in \mathbb{F}_q[\alpha_1, \ldots, \alpha_n]$.
- $S_1, \ldots, S_n$ are subsets of $\mathbb{F}_q$ such that $|S_i| = n > k-1 \geq t_i \quad \forall i \in [n]$.

We are currently unable to prove that there always exists a monomial $\alpha_1^{t_1}\ldots\alpha_n^{t_n}$ in $\det(A)$ such that $(t_1, \ldots, t_n) \in \mathit{Supp}(\det(A))$. However, let us assume that such a monomial always exists.

If the Unique-Multiset Conjecture is true, then there is always a monomial in the determinant of A that has a coefficient equal to plus or minus one. From this it follows that the determinant of A is not identically zero. [20] As per Lemma 5.3, if $\det(A)$ is not identically zero, then the GM-MDS Conjecture holds.

Suppose then that the Unique-Multiset Conjecture is false. Then there are k, n, and the sets $Z_1, \ldots, Z_k$ as before, but there are no unique multisets.

Under the assumption that there exists a monomial $\alpha_1^{t_1}\ldots\alpha_n^{t_n}$ in $\det(A)$ such that $(t_1, \ldots, t_n) \in \mathit{Supp}(\det(A))$, we have all the necessary assumptions fulfilled for the Generalized Combinatorial Nullstellensatz. Therefore, there have to exist $(\alpha_1', \ldots, \alpha_n') \in S_1 \times \ldots \times S_n$ such that $\det(A) \neq 0$. Therefore, $\det(A)$ can not be identically zero, which implies that the GM-MDS Conjecture holds.

As all of the above relies on finding a monomial with a non-zero coefficient in $\det(A)$, which might turn out to be an insurmountable task, we will also provide a sketch of the structure of a proof of the Unique-Multiset Conjecture that does not rely on the matrix A.

Sketch of a possible proof of the Unique-Multiset Conjecture:
Let us have $k, n, q, \mathbb{F}_q$, and the sets $Z_1, \dots, Z_k$ as before.

Construct a polynomial $f = f(\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q[\alpha_1, \dots, \alpha_n]$ such that f evaluates to zero everywhere if and only if the Unique-Multiset Conjecture is false. That is equivalent to stating that there exists $(\alpha_1', \dots, \alpha_n') \in \mathbb{F}_q^n$ such that $f(\alpha_1', \dots, \alpha_n') \neq 0$ if and only if the conjecture is true. Additionally, the polynomial f should preferably be such that it is possible to find the coefficients of its monomials.

Assume that the Unique-Multiset Conjecture is false. Then $f(\alpha_1, \dots, \alpha_n) = 0$ for all values of $(\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$. By the Generalized Combinatorial Nullstellensatz, it would suffice to prove that there exists a monomial $\alpha_1^{t_1} \dots \alpha_n^{t_n}$ in f such that $t_i < q \quad \forall i \in [n]$ and $(t_1, \dots, t_n)$ is a maximal element in $Supp(f)$. Then there would exist $(\alpha_1', \dots, \alpha_n') \in \mathbb{F}_q^n$ such that $f(\alpha_1', \dots, \alpha_n') \neq 0$, which is a contradiction with f evaluating to zero everywhere. Therefore, the Unique-Multiset Conjecture is true, from which it follows that the GM-MDS Conjecture holds.

As S. Lovett [21] already proved the GM-MDS Conjecture by utilizing the Schwartz–Zippel-DeMillo-Lipton lemma [22], similiar constructions to the ones found in his proof could be useful in constructing the polynomial f needed to utilize the Generalized Combinatorial Nullstellsatz.

References

[1] N. Alon. (1999). *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing, Volume 8, Issue 1-2, [7:29].

[2] D. Hilbert. (1893). *Ueber die vollen Invariantensysteme*, Mathematische Annalen 42, [320:327].

[3] S. Jukna. (2001). *Extremal Combinatorics With Applications in Computer Science, Second Edition*, Springer-Verlag, [223:236]

[4] J. Matoušek, J. Nešetril. (2008). *Invitation to Discrete Mathematics, 2nd edition.*, Oxford University Press, [109:216].

[5] V. Laan. (01.05.2019). *ALGEBRA II, Kevad 2019, Loengukonspekt*, `https://courses.ms.ut.ee/MTMM.00.040/2019_spring/uploads/Main/kon.pdf`, [27:33].

[6] M. Lason. (2010). *A generalization of Combinatorial Nullstellensatz*, The Electronic Journal of Combinatorics 17.

[7] H. Chevalley, E. Warning. (1935). *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, Volume 11, Issue 1, [76:83].

[8] H. Davenport. (1935). *On the addition of residue classes*, The Journal of the London Mathematical Society, Volume 10, Issue 1, [30:32].

[9] N. Alon, Z. Füredi. (1993). *Covering the cube by affine hyperplanes*, European Journal of Combinatorics, Volume 14, Issue 2, [79:83].

[10] L. H. Ding, Y. P. Gao, X. W. Yu. (2018). *Neighbor sum distinguishing chromatic index of Sparse Graphs via the Combinatorial Nullstellensatz*, Acta Mathematicae Applicatae Sinica, English Series, Volume 34, Issue 1, [135:144].

[11] Z. Zhang, L. Liu, J. Wang. (2002). *Adjacent strong edge coloring of graphs*, Applied Mathematics Letters, Volume 15, Issue 5, [623:626].

[12] L. H. Ding, G. H. Wang, G. Y. Yan. (2014). *Neighbor sum distinguishing total colorings via the Combinatorial Nullstellensatz*, Science China Mathematics, Volume 57, issue 9, [1875:1882].

[13] D. Hefetz. (2005). *Anti-magic graphs via the Combinatorial NullStellenSatz*, Journal of Graph Theory, Volume 50, Issue 4, [263:272].

[14] N. Hartsfield, G. Ringel. (1990). *Pearls in Graph Theory, A Comprehensive Introduction*, Academic Press, Inc., Boston, [108:109].

[15] S. Czerwiński, J. Grytczuk, W. Żelazny. (2009). *Lucky labelings of graphs*, Information Processing Letters, Volume 109, Issue 18, [1078:1081].

[16] T. Bartnicki, J. Grytczuk, S. Niwczyk. (2008). *Weight choosability of graphs*, Journal of Graph Theory, Volume 60, Issue 3, [242:256].

[17] D. Hefetz, A. Saluz, H. T. T. Tran. (2010). *An application of the combinatorial Nullstellensatz to a graph labelling problem* , Journal of Graph Theory, Volume 65, Issue 1, [70:82].

[18] T. L. Wong, X. D. Zhu. (2012). *Antimagic labelling of vertex weighted graphs*, Journal of Graph Theory, Volume 70, Issue 3, [348:359].

[19] D. E. Scheim. (1974). *The number of edge 3-colorings of a planar cubic graph as a permanent*, Discrete Mathematics, Volume 8, Issue 4, [377:382].

[20] S. H. Dau, W Song, C. Yuen. (2014). *On the Existence of MDS Codes Over Small Fields With Constrained Generator Matrices*, IEEE International Symposium On Information Theory, [1787:1791].

[21] S. Lovett. (2018). *MDS matrices over small fields: A proof of the GM-MDS conjecture*, IEEE 59th Annual Symposium on Foundations of Computer Science, [194:199].

[22] R. A. Demillo, R. J. Lipton. (1978). *A probabilistic remark on algebraic program testing*, Information Processing Letters, Volume 7, Issue 4, [193:195].

[23] F.J. MacWilliams, N. J. A. Sloane. (1977) *The Theory of Error-Correcting Codes*, North-Holland Publishing Company.

Non-exclusive licence to reproduce thesis and make thesis public

I, Karl Hannes Veskus,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

"Combinatorial Nullstellensatz and its applications",

supervised by Ago-Erik Riet.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Karl Hannes Veskus
01/05/2019