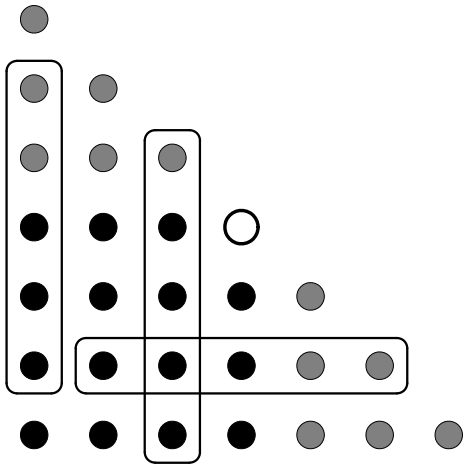
Algebraically Solvable Problems

Describing Polynomials as Equivalent to Explicit Solutions



Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften
der Fakultät für Mathematik und Physik
der Eberhard-Karls-Universität Tübingen

vorgelegt von
Uwe Schauz
aus Heidenheim

2007

Tag der mündlichen Prüfung:	16. Juli 2007
Dekan:	Prof. Dr. N. Schopohl
1. Berichterstatter:	Prof. Dr. C. Hering
2. Berichterstatter:	Prof. Dr. W. Knapp

Acknowledgment

An dieser Stelle möchte ich meinem Doktorvater Professor Dr. Christoph Hering, der mich zur Ausarbeitung des vorliegenden Teils meiner Forschungen überredet hat, für seine erfahrenen Ratschläge und seine Unterstützung herzlich danken.

Besonders möchte ich mich auch bei Andreas Krebs und Christoph Behle für hilfreiche Gespräche über Algorithmen bedanken.

Die immer hilfsbereite Alexandra Kallia und der freundliche Michael Harrison haben zahllose „Sprachfääler“ korrigiert, auch ihnen sei gedankt.

Dank geht auch an Matthias Grüninger, Oliver Burger, meinen Bruder Detlef Schauz und Prof. Dr. Ulf Schlotterbeck für ihre generelle Hilfsbereitschaft im weiteren Umfeld dieser Arbeit.

Und „last but not least“ gilt mein Dank meinen Eltern, die sich leider immer die falschen Sorgen machen. Aber trotzdem:

Vielen Dank!

Contents

Introduction in German (Zusammenfassung) 9

Introduction in English 13

1 Notation and constants 17

2 Interpolation polynomials and inversion formulas 23

3 Coefficient formulas – the main results 31

4 First applications and the application principles 37

5 The matrix polynomial – another application 41

6 Algebraic solvable existence problems: Describing polynomials as equivalent to explicit solutions 45

7 The Combinatorial Nullstellensatz or how to modify polynomials 49

8 A sharpening of Warning's Theorem – a further application 53

9 Results over $\mathbb{Z}$, $\mathbb{Z}_m$ and other generalizations 63

10 How to find nonvanishing points, numerical aspects 67

11 Mr. Paint and Mrs. Rubber, a coloration game 71

References 79

Index 83

Introduction in German (Zusammenfassung)

In Kürze: Die direkteste und beste Art, ein Existenzproblem zu lösen, besteht darin, eine explizite Lösung anzugeben. Ist dies nicht möglich, so kann man sich nach einer algebraischen Lösung, also einem beschreibenden Polynom mit gewissen Eigenschaften wie z.B. niedrigem Totalgrad, umsehen. Wir zeigen, dass die Existenz einer algebraischen Lösung äquivalent ist zur Existenz einer expliziten Lösung des Problems. Wobei wir unter einem „Problem“ alles verstehen, was eine Menge $\mathcal{S}$ und eine Teilmenge $\mathcal{S}_{\text{triv}} \subseteq \mathcal{S}$ „besitzt“, deren Elemente man „Lösungen“ bzw. „triviale Lösungen“ nennt.

Diese Äquivalenz basiert auf Alon und Tarsis kombinatorischem Nullstellensatz, für den wir eine verschärfte und verallgemeinerte Fassung (eine Koeffizientenformel) und einige nützliche Korollare, einschließlich einer Verallgemeinerung von Olsons Theorem, vorstellen. Die Verschärfung erlaubt auch (gewichtet) quantitative Rückschlüsse über die Lösungen eines Problems. Sie ist ursprünglich ein Resultat über Polynome und liefert Informationen über die polynomiale Abbildung $P|_{\mathfrak{X}}$, wenn nur unvollständige Informationen über das Polynom P gegeben sind. All das hat zu tun mit Interpolationspolynomen auf endlichen „Rastern“ $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathcal{R}^n$ über kommutativen Ringen $\mathcal{R}$.

Wir geben verschiedene Beispiele, wie man algebraische Lösungen finden und die Koeffizientenformel (kombinatorischer Nullstellensatz) anwenden kann. Diese Beispiele stammen hauptsächlich aus der Graphentheorie und der kombinatorischen Zahlentheorie. Der Chevalley-Warning Satz ist eine weitere Anwendung.

Wir wenden unsere Koeffizientenformel auf das Matrizenpolynom, eine Verallgemeinerung des Graphenpolynoms, an und erhalten eine Permanentenformel. Diese Formel ist eine vereinheitlichende Verallgemeinerung und Verschärfung von:

1. Rysers Permanentenformel.
2. Alons Permanentenlemma.
3. Alon und Tarsis Theorem über Orientierungen und Färbungen von Graphen.

In Kombination mit der Vigneron-Ellingham-Goddyn Eigenschaft planarer n-regulärer Graphen enthält sie außerdem, als kleine Spezialfälle:

4. Scheims Formel für die Anzahl der Kantenfärbungen derartiger Graphen mit n Farben.
5. Ellingham und Goddyns teilweise Bestätigung der Listenfärbungsvermutung.

In einer weiteren Anwendung verschärfen wir Warnings klassisches Resultat über die Anzahl simultaner Nullstellen von Systemen von Polynomen über endlichen Körpern.

Wir diskutieren die numerischen Aspekte und präsentieren zwei Algorithmen mit polynomialer Laufzeit, die Nichtnullstellen von Polynomen finden. Einen dieser Algorithmen erhalten wir als Gewinnstrategie zu einem neuen Färbungsspiel für Polynome (und Graphen). Dies führt auch zu einem rein kombinatorischen Beweis des Satzes von Alon und Tarsi (Punkt 3 oben).

$\mathfrak{X}$ $P|_{\mathfrak{X}}$ d_j P_d

Im Detail: Interpolationspolynome $P = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta$ über endlichen „Rastern“ $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathbb{F}^n$ sind nicht eindeutig bestimmt (durch die zu interpolierende Abbildung $P|_{\mathfrak{X}}\colon x \mapsto P(x)$). Man könnte die partiellen Grade beschränken, um die Eindeutigkeit zu erzwingen. Wenn wir nur den Totalgrad durch $\deg(P) \le d_1 + \cdots + d_n$ mit $d_j := |\mathfrak{X}_j| - 1$ beschränken, so sind die Polynome P noch nicht eindeutig bestimmt, aber sie sind teilweise eindeutig. Es gibt einen (und im Allgemeinen nur einen) Koeffizienten in $P = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta$, der eindeutig bestimmt ist, nämlich P_d mit $d := (d_1, \ldots, d_n)$. Wir beweisen dies in 3.3, indem wir eine Formel für diesen Koeffizienten angeben. Unsere Koeffizientenformel enthält Alon and Tarsis (zweiten) kombinatorischen Nullstellensatz [Al2, Theorem 1.2], [Al3]:

$$P_d \neq 0 \quad\Longrightarrow\quad P|_{\mathfrak{X}} \not\equiv 0 \ . \tag{1}$$

Dieses unscheinbare Resultat und seine Korollare 3.4, 3.5 und 9.4 sind erstaunlich flexibel in der Anwendung. In den meisten Anwendungen wollen wir die Existenz eines Punktes $x \in \mathfrak{X}$ mit $P(x) \neq 0$ nachweisen. Solch ein Punkt x steht dann z.B. für eine Färbung, einen Graphen oder ein geometrisches oder zahlentheoretisches Objekt mit speziellen Eigenschaften. Im einfachsten Fall haben wir die folgende Korrespondenz:

$$\begin{array}{rcl} \mathfrak{X} & \longleftrightarrow & \text{Klasse von Objekten} \\ x & \longleftrightarrow & \text{Objekt} \\ P(x) \neq 0 & \longleftrightarrow & \text{“Objekt ist interessant (eine Lösung).”} \\ P|_{\mathfrak{X}} \not\equiv 0 & \longleftrightarrow & \text{“Es existiert ein interessantes Objekt (eine Lösung).”} \end{array} \tag{2}$$

Dies soll erklären, warum wir an der Beziehung zwischen P und $P|_{\mathfrak{X}}$ interessiert sind. Normalerweise haben wir dabei nur unvollständige Informationen über P vorliegen und versuchen daraus Informationen über die polynomiale Abbildung $P|_{\mathfrak{X}}$ zu gewinnen. Wenn es z.B. eine triviale Lösung x_0

gibt, dann wissen wir $P(x_0) \neq 0$, und zusammen mit $\deg(P) < d_1 + \ldots + d_n$ stellt dies (nach 3.4) bereits genügend Information über P dar, um eine weitere (nicht triviale) Lösung $x \neq x_0$ zu garantieren: $P(x) \neq 0$. Der andere wichtige Fall liegt vor, wenn keine triviale Lösung existiert, wir aber wissen, dass $P_d \neq 0$ und $deg(P) \leq d_1 + \ldots + d_n$. In diesem Fall folgt $P|_{\mathfrak{X}} \not\equiv 0$ aus (1) oben oder mit unserem Hauptresultat 3.3. In manchen weiteren Fällen mag auch Satz 3.2, der auf dem allgemeineren Konzept der d-führenden Koeffizienten aus Definition 3.1 basiert, anwendbar sein.

Wir nehmen in Kapitel 4 einige der Anwendungsbeispiele aus [Al2] auf, um diese Methoden und den erzielten Fortschritt vorzuführen. In Kapitel 5 wenden wir unsere Resultate auf das Matrizenpolynom, eine Verallgemeinerung des Graphenpolynoms, an und erhalten eine Permanentenformel. Diese Formel ist eine vereinheitlichende Verallgemeinerung und Verschärfung verschiedener bekannter Resultate über Permanenten und Graphenfärbungen (die fünf Punkte oben).

Wir zeigen in 6.5, dass es theoretisch immer möglich ist, die Lösungen eines gegebenen Problems $\mathcal{P}$ (Definition 6.1) durch Elemente x in einem geeigneten Raster $\mathfrak{X}$ darzustellen und Polynome P mit Zusatzeigenschaften (z.B. $P_d \neq 0$ wie in (1) oben) zu finden, die das Problem beschreiben:

$$P(x) \neq 0 \quad \Longleftrightarrow \quad \text{“}x \text{ repräsentiert eine Lösung von } \mathcal{P}\text{.”} \tag{3}$$

Wir nennen derartige Polynome P algebraische Lösungen von $\mathcal{P}$, da ihre Existenz die Existenz einer nicht trivialen Lösung des Problem $\mathcal{P}$ nach sich zieht.

Die Kapitel 4, 5 und 8 enthalten verschiedene Beispiele algebraischer Lösungen. Algebraische Lösungen sind besonders einfach zu finden, wenn das Problem genau eine triviale Lösung besitzt. Basierend auf Korollar 3.4 müssen wir in diesem Fall nur ein beschreibendes Polynom P mit Totalgrad $\deg(P) < d_1 + \ldots + d_n$ finden. Vage gesprochen garantiert Korollar 3.4, dass jedes nicht zu komplexe Problem – in dem Sinne, dass es nicht zu viele Multiplikationen bei der Konstruktion von P erfordert – nicht genau eine (die triviale) Lösung besitzt.

In Kapitel 7 geben wir eine geringfügige Verallgemeinerung des (ersten) kombinatorischen Nullstellensatzes, eines verschärften Spezialfalls des Hilbertschen Nullstellensatzes, an und diskutieren Alons ursprüngliche Beweismethode. In Kapitel 3 benutzten wir eine andere Methode, um unser Hauptergebnis zu verifizieren.

Die Modifikationsmethoden aus Kapitel 7 und die Permanente von Matrizenpolynomen, wie sie in Kapitel 5 eingeführt wurde, nutzend, studieren

wir in Kapitel 8 die Verteilung der verschiedenen möglichen Funktionswerte $P(x)$ polynomialer Abbildungen $x \longmapsto P(x)$ auf dem speziellen Raster $\mathfrak{X} := \mathbb{F}_p^n$. Als Korollar erhalten wir eine Verschärfung eines klassischen Resultats von Warning über die Anzahl simultaner Nullstellen von Systemen von Polynomen über endlichen Körpern. Die Verschärfung sagt uns etwas über die Verteilung der Nullstellen in dem Raum $\mathbb{F}_p^n$. Mit Hilfe von Lemma 8.6 können diese Ergebnisse auch auf Polynomabbildungen über beliebigen endlichen Körper $\mathbb{F}_{p^k}$ angewandt werden.

Kapitel 9 enthält weitere Verallgemeinerungen und Resultate über den ganzen Zahlen $\mathbb{Z}$ und über $\mathbb{Z}/m\mathbb{Z}$. Korollar 9.2 ist eine überraschende Variante des wichtigen Korollars 3.4, die ganz ohne Gradbeschränkungen auskommt. Die Version 9.4 von Korollar 3.5 ist eine Verallgemeinerung von Olsons Theorem.

In Kapitel 10 präsentieren wir einen schnellen und einfachen Algorithmus, der Nichtnullstellen von Polynomen findet. Um ihn anzuwenden, muss man das Polynom P zuerst in das gekürzte Polynom $P/\mathfrak{X}$ mit partiellen Graden $\deg_j(P) \leq d_j$, wie es in Kapitel 7 beschrieben wurde, überführen. Diese Transformation $P \rightsquigarrow P/\mathfrak{X}$ kann für viele wichtige Raster $\mathfrak{X}$ sehr schnell ausgeführt werden, benötigt in manchen, weniger speziellen Fällen aber exponentielle Laufzeit.

Das nachfolgende Kapitel 11 führt zu einem Algorithmus, der die Transformation $P \rightsquigarrow P/\mathfrak{X}$ vermeidet, aber nur über sogenannten Farbrastern $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \{T_1, T_2, \dots\}^n$ anwendbar ist, die aus Unbestimmten T_j gebildet sind. Er wird als Gewinnstrategie zu einem neuen Färbungsspiel für Polynome (und Graphen) hergeleitet. Das Spiel von Mr. Paint und Mrs. Rubber führt auch zu einer geringfügigen Verallgemeinerung des graphentheoretischen Begriffs „Listenfärbung“ und einer entsprechenden Verallgemeinerung des kombinatorischen Nullstellensatzes 3.3 (ii) über Farbrastern. Es führt weiter zu einem rein kombinatorischen Beweis des Satzes von Alon und Tarsi 5.5 (ii), wie er von den beiden gesucht wurde.

Die meisten unserer Resultate gelten über Integritätsringen, und diese Bedingung kann sogar noch etwas abgeschwächt werden (siehe 2.7 für die Definition nullteilerfreier Raster). Im wichtigen Fall der Booleschen Raster $\mathfrak{X} = \{0,1\}^n$ gelten sie über beliebigen kommutativen Ringen $\mathcal{R}$. Unsere Ergebnisse basieren auf den Interpolationsformeln in Kapitel 2, die die Konstanten und Definitionen aus Kapitel 1 nutzen.

Für Neulinge in diesem Gebiet könnte es eine gute Idee sein, mit Kapitel 4 zu beginnen, um sich einen ersten Eindruck zu verschaffen.

Introduction

In short: The main result of this paper is a coefficient formula that sharpens and generalizes Alon and Tarsi's Combinatorial Nullstellensatz. On its own, it is a result about polynomials, providing some information about the polynomial map $P|_{\mathfrak{X}}$ when only incomplete information about the polynomial P is given.

In a very general working frame, the grid points $x \in \mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n$ which do not vanish under an algebraic solution – a certain describing polynomial P – correspond to the explicit solutions of a problem. As a consequence of the coefficient formula, we prove that the existence of an algebraic solution is equivalent to the existence of a nontrivial solution to a problem. By a problem, we mean everything that "owns" both, a set $\mathcal{S}$, which may be called the *set of solutions*; and a subset $\mathcal{S}_{\text{triv}} \subseteq \mathcal{S}$, the *set of trivial solutions*.

We give several examples on how to find algebraic solutions, and on how to apply our coefficient formula. These examples are mainly from graph theory and combinatorial number theory, but we also prove several versions of Chevalley and Warning's Theorem, including a generalization of Olson's Theorem, as examples and useful corollaries.

We obtain a permanent formula by applying our coefficient formula to the matrix polynomial, which is a generalization of the graph polynomial. This formula is an integrative generalization and sharpening of:

1. Ryser's permanent formula.
2. Alon's Permanent Lemma.
3. Alon and Tarsi's Theorem about orientations and colorings of graphs.

Furthermore, in combination with the Vigneron-Ellingham-Goddyn property of planar n-regular graphs, the formula contains as very special cases:

4. Scheim's formula for the number of edge n-colorings of such graphs.
5. Ellingham and Goddyn's partial answer to the list coloring conjecture.

In a further application of our coefficient formula, we prove a sharpening of Warning's classical result about the number of simultaneous zeros of systems of polynomial equations over finite fields.

We discuss the numerical aspects of using algebraic solutions to find explicit solutions, and present two polynomial-time algorithms that find nonzeros of polynomials. One of these algorithms is derived as a winning strategy of a new coloration game for polynomials (and graphs). It also satisfies a request by Alon and Tarsi for a purely combinatorial proof of their theorem about orientations and colorings of graphs (point 3 above).

$\mathfrak{X}$ $P|_{\mathfrak{X}}$ d_j P_d

More detailed: Interpolation polynomials $P = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta$ on finite "grids" $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathbb{F}^n$ are not uniquely determined by the interpolated maps $P|_{\mathfrak{X}}\colon x \mapsto P(x)$. One could restrict the partial degrees to force the uniqueness. If we only restrict the total degree to $\deg(P) \leq d_1 + \cdots + d_n$, where $d_j := |\mathfrak{X}_j| - 1$, the interpolation polynomials P are still not uniquely determined, but they are partially unique. That is to say, there is one (and in general only one) coefficient in $P = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta$ that is uniquely determined, namely P_d with $d := (d_1, \ldots, d_n)$. We prove this in Theorem 3.3 by giving a formula for this coefficient. Our coefficient formula contains Alon and Tarsi's Combinatorial Nullstellensatz [Al2, Th. 1.2], [Al3]:

$$P_d \neq 0 \quad \Longrightarrow \quad P|_{\mathfrak{X}} \not\equiv 0 \ . \tag{4}$$

This insignificant-looking result, along with Theorem 3.3 and its corollaries 3.4, 3.5 and 9.4, are astonishingly flexible in application. In most applications, we want to prove the existence of a point $x \in \mathfrak{X}$ such that $P(x) \neq 0$. Such a point x then may represent a coloring, a graph or a geometric or number-theoretic object with special properties. In the simplest case we will have the following correspondence:

$$\begin{array}{rcl} \mathfrak{X} & \longleftrightarrow & \text{Class of Objects} \\ x & \longleftrightarrow & \text{Object} \\ P(x) \neq 0 & \longleftrightarrow & \text{"Object is interesting (a solution)."} \\ P|_{\mathfrak{X}} \not\equiv 0 & \longleftrightarrow & \text{"There exists an interesting object (a solution)."} \end{array} \tag{5}$$

This explains why we are interested in the connection between P and $P|_{\mathfrak{X}}$: In general, we try to retrieve information about the polynomial map $P|_{\mathfrak{X}}$ using incomplete information about P. One important possibility is if there is (exactly) one trivial solution x_0 to a problem, so that we have the information that $P(x_0) \neq 0$. If, in this situation, we further know that $\deg(P) < d_1 + \ldots + d_n$, then Corollary 3.4 already assures us that there is a second (nontrivial) solution x, i.e., an $x \neq x_0$ in $\mathfrak{X}$ such that $P(x) \neq 0$. The other important possibility is that we do not have any trivial solutions at all, but we know that $P_d \neq 0$ and $deg(P) \leq d_1 + \ldots + d_n$. In this case, $P|_{\mathfrak{X}} \not\equiv 0$ follows from (4) above or from our main result, Theorem 3.3. In other cases, we may instead apply Theorem 3.2, which is based on the more general concept from Definition 3.1 of d-leading coefficients.

In Section 4, we demonstrate how the most examples from [Al2] follow easily from our coefficient formula and its corollaries. The new, quantitative

version 3.3 (i) of the Combinatorial Nullstellensatz is, for example, used in Section 5, where we apply it to the matrix polynomial – a generalization of the graph polynomial – to obtain a permanent formula. This formula is a generalization and sharpening of several known results about permanents and graph colorings (see the five points above). We briefly describe how these results are included in our permanent formula.

We show in Theorem 6.5 that it is theoretically always possible, both, to represent the solutions of a given problem $\mathcal{P}$ (see Definition 6.1) through some elements x in some grid $\mathfrak{X}$, and to find a polynomial P, with certain properties (e.g., $P_d \neq 0$ as in (4) above), that describes the problem:

$$P(x) \neq 0 \quad \Longleftrightarrow \quad \text{“}x \text{ represents a solution of } \mathcal{P}\text{.”} \tag{6}$$

We call such a polynomial P an *algebraic solution* of $\mathcal{P}$, as its existence guarantees the existence of a nontrivial solution to the problem $\mathcal{P}$.

Sections 4, 5 and 8 contain several examples of algebraic solutions. Algebraic solutions are particularly easy to find if the problems possess exactly one trivial solution: due to Corollary 3.4, we just have to find a describing polynomial P with degree $\deg(P) < d_1 + \ldots + d_n$ in this case. Loosely speaking, Corollary 3.4 guarantees that every problem which is not too complex, in the sense that it does not require too many multiplications in the construction of P, does not possess exactly one (the trivial) solution.

In Section 7 we give a slight generalization of the (first) Combinatorial Nullstellensatz – a sharpened specialization of Hilbert's Nullstellensatz – and a discussion of Alon's original proving techniques. Note that, in Section 3 we used an approach different from Alon's to verify our main result. However, we will show that Alon and Tarsi's so-called polynomial method can easily be combined with interpolation formulas, such as our inversion formula 2.8, to reach this goal.

In Section 8, we use the modification techniques of Section 7 and the δ-permanent introduced in Section 5 to study the distribution of the different possible values $P(x)$ of polynomial maps $x \longmapsto P(x)$ on the special grid $\mathfrak{X} := \mathbb{F}_p^n$. As a corollary, we obtain a sharpening of Warning's classical result about the number of simultaneous zeros of systems of polynomial equations over finite fields. This sharpening tells us something about the distribution of the zeros in the space $\mathbb{F}_p^n$. Using Lemma 8.6, we may apply these results to polynomial maps over arbitrary finite fields $\mathbb{F}_{p^k}$, as well.

Section 9 contains further generalizations and results over the integers $\mathbb{Z}$ and over $\mathbb{Z}/m\mathbb{Z}$. Corollary 9.2 is a surprising relative to the important

Corollary 3.4, one which works without any degree restrictions. Theorem 9.4, a version of Corollary 3.5, is a generalization of Olson's Theorem.

In Section 10 we present a very simple and fast algorithm that finds nonzeros of polynomials. To apply it, one first has to transform the given polynomial P into the trimmed polynomial $P/\mathfrak{X}$ with partial degrees $\deg_j(P) \leq d_j$, as described in Section 7. This transformation $P \rightsquigarrow P/\mathfrak{X}$ can be done very fast for the most frequently occurring grids $\mathfrak{X}$, but in some less special cases may take exponential time.

Section 11 leads to an algorithm that avoids the transformation $P \rightsquigarrow P/\mathfrak{X}$, but works only for so-called color grids $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \{T_1, T_2, \dots\}^n$ that are constructed from indeterminacies T_j. The algorithm is derived as a winning strategy to a new coloration game for polynomials (and graphs). This game of Mr. Paint and Mrs. Rubber also leads to a slight generalization of the graph-theoretic term "list coloring," and, in the case of color grids, to a corresponding generalization of the Combinatorial Nullstellensatz (our 3.3 (*ii*)). It leads further to a purely combinatorial proof of Alon and Tarsi's Theorem about orientations and colorings of graphs (our 5.5 (*ii*)).

Most of our results hold over integral domains, though this condition has been weakened in this paper for the shake of greater generality (see 2.7 for the definition of integral grids). In the important case of the Boolean grid $\mathfrak{X} = \{0, 1\}^n$, our results hold over arbitrary commutative rings $\mathcal{R}$. Our coefficient formulas are based on the interpolation formulas in Section 2, where we generalize known expressions for interpolation polynomials over fields to commutative rings $\mathcal{R}$. We frequently use the constants and definitions from Section 1.

For newcomers in this field, it might be a good idea to start with Section 4 to get a first impression.

The various parts of this dissertation will be published in the Electronic Journal of Combinatorics.

1 Notation and constants

$\mathcal{R}$ is always a commutative ring with $1 \neq 0$. $\mathcal{R}$

$\mathbb{F}_{p^k}$ denotes the field with p^k elements (p prime) and $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. $\mathbb{F}_{p^k}$, $\mathbb{Z}_m$

We write $p \lfloor n$ (or $n \rfloor p$) for "p *divides* n" and abbreviate $\mathcal{S}\backslash s := \mathcal{S}\backslash\{s\}$. $p \lfloor n$, $\mathcal{S}\backslash s$

For $n \in \mathbb{N} := \{0, 1, 2, \dots\}$ we set: $\mathbb{N}$

$(n] = (0, n] := \{1, 2, \dots, n\}$, $(n]$

$[n) = [0, n) := \{0, 1, \dots, n-1\}$, $[n)$

$[n] = [0, n] := \{0, 1, \dots, n\}$. (Note that $0 \in [n]$.) $[n]$

For statements $\mathcal{A}$ the "Kronecker query" $?_{(\mathcal{A})}$ is defined by:

$$?_{(\mathcal{A})} := \begin{cases} 0 & \text{if } \mathcal{A} \text{ is false,} \\ 1 & \text{if } \mathcal{A} \text{ is true.} \end{cases} \qquad ?_{(\mathcal{A})}$$

For finite tuples (and maps) $d = (d_j)_{j\in J}$ and sets Γ we define:

$\Pi d := \prod_{j\in J} d_j$, $\Pi\Gamma := \prod_{\gamma\in\Gamma} \gamma$ and Πd, $\Pi\Gamma$

$\Sigma d := \sum_{j\in J} d_j$, $\Sigma\Gamma := \sum_{\gamma\in\Gamma} \gamma$. Σd, $\Sigma\Gamma$

For maps $y, z\colon \mathfrak{X} \longrightarrow \mathcal{R}$ with finite domain we identify the map $y\colon x \longmapsto y(x)$ with the tuple $(y(x))_{x\in\mathfrak{X}} \in \mathcal{R}^{\mathfrak{X}}$. Consequently, the product with matrices $\Psi = (\psi_{\delta,x}) \in \mathcal{R}^{D\times\mathfrak{X}}$ is given by $\Psi y := \big(\sum_{x\in\mathfrak{X}} \psi_{\delta,x}\, y(x)\big)_{\delta\in D} \in \mathcal{R}^D$. y, Ψy

yz stands for the pointwise product, $(yz)(x) := y(x)z(x)$. If nothing else is said, y^{-1} is also defined pointwise, $y^{-1}(x) := y(x)^{-1}$, if $y(x)$ is invertible for all $x \in \mathfrak{X}$. We define $\operatorname{supp}(y) := \{\, x \in \mathfrak{X} \mid y(x) \neq 0 \,\}$. yz, y^{-1}, $\operatorname{supp}(y)$

The tensor product $\bigotimes_{j\in(n]} y_j$ of maps $y_j\colon \mathfrak{X}_j \longrightarrow \mathcal{R}$ is a map from $\mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n$ to $\mathcal{R}$ and is defined by $(\bigotimes_{j\in(n]} y_j)(x) := \prod_{j\in(n]} y_j(x_j)$. $\otimes$

Hence, the tensor product of tuples $a^j := (a^j_{x_j})_{x_j\in\mathfrak{X}_j}$, $j \in (n]$, is the tuple $\bigotimes_{j\in(n]} a^j = \big(\prod_{j\in(n]} a^j_{x_j}\big)_{x\in\mathfrak{X}_1\times\cdots\times\mathfrak{X}_n}$.

The tensor product of matrices $\Psi^j = (\psi^j_{\delta_j,x_j})_{\substack{\delta_j\in D_j \\ x_j\in\mathfrak{X}_j}}$, $j \in (n]$, is the matrix $\bigotimes_{j\in(n]} \Psi^j = \big(\prod_{j\in(n]} \psi^j_{\delta_j,x_j}\big)_{\substack{\delta\in D_1\times\cdots\times D_n \\ x\in\mathfrak{X}_1\times\cdots\times\mathfrak{X}_n}}$.

Tensor product and matrix-tuple multiplication go well together:

$$\begin{aligned} \Big(\bigotimes_{j\in(n]} \Psi^j\Big) \bigotimes_{j\in(n]} a^j &= \Big(\prod_{j\in(n]} \psi^j_{\delta_j,x_j}\Big)_{\substack{\delta\in D \\ x\in\mathfrak{X}}} \Big(\prod_{j\in(n]} a^j_{x_j}\Big)_{x\in\mathfrak{X}} = \Big(\sum_{x\in\mathfrak{X}} \prod_{j\in(n]} \psi^j_{\delta_j,x_j} a^j_{x_j}\Big)_{\delta\in D} \\ &= \Big(\prod_{j\in(n]} \sum_{x_j\in\mathfrak{X}_j} \psi^j_{\delta_j,x_j} a^j_{x_j}\Big)_{\delta\in D} = \bigotimes_{j\in(n]} \Big(\sum_{x_j\in\mathfrak{X}_j} \psi^j_{\delta_j,x_j} a^j_{x_j}\Big)_{\delta_j\in D_j} = \bigotimes_{j\in(n]} (\Psi^j a^j)\,. \end{aligned} \tag{7}$$

In the whole paper we work over Cartesian products $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n$ of subsets $\mathfrak{X}_j \subseteq \mathcal{R}$ of size $d_j + 1 := |\mathfrak{X}_j| < \infty$. We define:

Definition 1.1 (d-grids $\mathfrak{X}$).

$\mathfrak{X}, [d]$
$d = d(\mathfrak{X})$

For all $j \in (n]$ we define:	In n dimensions we define:
$\mathfrak{X}_j \subseteq \mathcal{R}$ is always a finite set $\neq \varnothing$.	$\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathcal{R}^n$ is a *d-grid* if
$\boxed{d_j = d_j(\mathfrak{X}_j) := \lvert\mathfrak{X}_j\rvert - 1}$ and	$d = d(\mathfrak{X}) := (d_1, \ldots, d_n)$.
$[d_j] := \{0, 1, \ldots, d_j\}$.	$[d] := [d_1] \times \cdots \times [d_n]$ is a d-grid in $\mathbb{Z}^n$.

The following function $N\colon \mathfrak{X} \longrightarrow \mathcal{R}$ will be used throughout the whole paper. The $\psi_{\delta,x}$ are the coefficients of the Lagrange polynomials $L_{\mathfrak{X},x}$, as we will see in 1.3. We define:

Definition 1.2 ($N_{\mathfrak{X}}$, $\Psi_{\mathfrak{X}}$, $L_{\mathfrak{X},x}$ and e_x).
Let $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathcal{R}^n$ be a d-grid, i.e., $d_j = |\mathfrak{X}_j| - 1$ for all $j \in (n]$.

e_x, $L_{\mathfrak{X},x}$
N, Ψ

For $x \in \mathfrak{X}_j$ and $\delta \in [d_j]$ we set:	For $x \in \mathfrak{X}$ and $\delta \in [d]$ we set:
$e_x^j\colon \mathfrak{X}_j \to \mathcal{R}$, $\quad e_x^j(\tilde{x}) := ?_{(\tilde{x}=x)}$.	$e_x := \bigotimes_{j\in(n]} e_{x_j}^j = (\tilde{x} \mapsto ?_{(\tilde{x}=x)})$.
$L_{\mathfrak{X}_j \setminus x}(X) := \prod_{\hat{x}\in\mathfrak{X}_j\setminus x}(X - \hat{x})$.	$L_{\mathfrak{X},x}(X_1, \ldots, X_n) := \prod_j L_{\mathfrak{X}_j\setminus x_j}(X_j)$.
$N_j = N_{\mathfrak{X}_j}\colon \mathfrak{X}_j \longrightarrow \mathcal{R}$ is defined by:	$N = N_{\mathfrak{X}}\colon \mathfrak{X} \longrightarrow \mathcal{R}$ is defined by:
$\boxed{N_j(x) := L_{\mathfrak{X}_j\setminus x}(x)}$.	$\boxed{N := \bigotimes_{j\in(n]} N_j = \big(x \mapsto L_{\mathfrak{X},x}(x)\big)}$.
$\Psi^j := (\psi^j_{\delta,x})_{\substack{\delta\in[d_j]\\ x\in\mathfrak{X}_j}}$ with $\psi^j_{\delta,x} := \sum_{\substack{\Gamma\subseteq\mathfrak{X}_j\setminus x\\ \lvert\Gamma\rvert = d_j-\delta}} \Pi(-\Gamma)$ and in particular $\psi^j_{d_j,x} = 1$. (8)	$\Psi = (\psi_{\delta,x})_{\substack{\delta\in[d]\\ x\in\mathfrak{X}}} := \bigotimes_{j\in(n]} \Psi^j$ i.e. $\psi_{\delta,x} := \prod_{j\in(n]} \psi^j_{\delta_j,x_j}$ and in particular $\psi_{d,x} = 1$. (9)

We use multiindex notation for polynomials, i.e., $X^{(\delta_1,\dots,\delta_n)} := X_1^{\delta_1}\cdots X_n^{\delta_n}$ and we define $P_\delta = (P)_\delta$ to be the coefficient of X^δ in the standard expansion of $P \in \mathcal{R}[X] := \mathcal{R}[X_1,\dots,X_n]$. That means $P = P(X) = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta$ and $(X^\varepsilon)_\delta = ?_{(\delta=\varepsilon)}$. $X^{(\delta_1,\dots,\delta_n)}$ $P_\delta = (P)_\delta$ $\mathcal{R}[X]$

Conversely, for tuples $P = (P_\delta)_{\delta\in\mathcal{D}} \in \mathcal{R}^{\mathcal{D}}$, we set $P(X) := \sum_{\delta\in\mathcal{D}} P_\delta X^\delta$. In this way we identify the set of tuples $\mathcal{R}^{[d]} = \mathcal{R}^{[d_1]\times\cdots\times[d_n]}$ with $\mathcal{R}[X^{\le d}]$, the set of polynomials $P = \sum_{\delta\le d} P_\delta X^\delta$ with restricted partial degrees $\deg_j(P) \le d_j$. It will be clear from the context whether we view P as a tuple (P_δ) in $\mathcal{R}^{[d]}$, a map $[d] \longrightarrow \mathcal{R}$ or a polynomial $P(X)$ in $\mathcal{R}[X^{\le d}]$. $P(X)|_{\mathfrak{X}}$ stands for the map $\mathfrak{X} \longrightarrow \mathcal{R}$, $x \longmapsto P(x)$. $P(X)$ $\mathcal{R}^{[d]}$ $\mathcal{R}[X^{\le d}]$ $P(X)|_{\mathfrak{X}}$

We have introduced the following four related or identified objects:

Maps:	Tuples:	Polynomials:	Polynomial Maps:
$\delta \mapsto P_\delta$,	$P = (P_\delta)$	$P(X) = \sum P_\delta X^\delta$	$P(X)|_{\mathfrak{X}}\colon x \mapsto P(x)$,
$[d] \to \mathcal{R}$	$\in \mathcal{R}^{[d]}$	$\in \mathcal{R}[X^{\le d}]$	$\mathfrak{X} \to \mathcal{R}$

(10)

With these definitions we get the following important formula:

Lemma 1.3 (Lagrange polynomials)**.**

$$\boxed{(\Psi e_x)(X) := \sum_{\delta\in[d]} \psi_{\delta,x} X^\delta = \prod_{j\in(n]} \prod_{\hat{x}_j\in\mathfrak{X}_j\setminus x_j} (X_j - \hat{x}_j) =: L_{\mathfrak{X},x}} \ .$$

Proof. We start with the one-dimensional case. Assume $x \in \mathfrak{X}_j$, then

$$\begin{aligned}
(\Psi^j e_x^j)(X_j) &= \big(\sum_{\delta\in[d_j]} \psi^j_{\delta,x} X_j^\delta\big) \\
&= \sum_{\delta\in[d_j]} \sum_{\substack{\Gamma\subseteq\mathfrak{X}_j\setminus x \\ |\Gamma|=d_j-\delta}} X_j^\delta\, \Pi(-\Gamma) \\
&= \sum_{\hat{\Gamma}\subseteq\mathfrak{X}_j\setminus x} X_j^{|(\mathfrak{X}_j\setminus x)\setminus\hat{\Gamma}|}\, \Pi(-\hat{\Gamma}) \\
&= \prod_{\hat{x}\in\mathfrak{X}_j\setminus x} (X_j - \hat{x}) \ .
\end{aligned} \tag{11}$$

In n dimensions and for $x \in \mathfrak{X}$ we conclude:

$$\begin{aligned}(\Psi e_x)(X) &= \Big(\big(\bigotimes_j \Psi^j\big) \bigotimes_j e^j_{x_j} \Big)(X) \\ &\overset{(7)}{=} \Big(\bigotimes_j \big(\Psi^j e^j_{x_j}\big) \Big)(X) \\ &= \prod\nolimits_j \big((\Psi^j e^j_{x_j})(X_j) \big) \\ &\overset{(11)}{=} \prod_{j\in(n]} \prod_{\hat{x}_j \in \mathfrak{X}_j \setminus x_j} (X_j - \hat{x}_j) \ .\end{aligned} \tag{12}$$

□

We further provide the following specializations of the ubiquitous function $N \in \mathcal{R}^{\mathfrak{X}},\ N(x) = \prod_{j\in(n]} N_j(x_j)$:

Lemma 1.4. *Let* $E_l := \{\, c \in \mathcal{R} \mid c^l = 1 \,\}$ *denote the set of the* l^{th} *roots of unity in* $\mathcal{R}$ *. For* $x \in \mathfrak{X}_j \subseteq \mathcal{R}$ *hold:*

(i) If $\mathfrak{X}_j = E_{d_j+1}$ *(* $|E_{d_j+1}| = d_j + 1$ *) and if* $\mathcal{R}$ *is an integral domain:*
$$N_j(x) \ = \ (d_j+1)\, x^{-1} \ .$$

(ii) If $\mathfrak{X}_j \uplus \{0\}$ *is a finite subfield of* $\mathcal{R}$ *:*
$$N_j(x) \ = \ -x^{-1} \ .$$

(iii) If $\mathfrak{X}_j = E_{d_j} \uplus \{0\}$ *(* $|E_{d_j}| = d_j$ *) and if* $\mathcal{R}$ *is an integral domain:*
$$N_j(x) \ = \ \begin{cases} d_j 1 & \text{for } x \neq 0\,, \\ -1 & \text{for } x = 0\,. \end{cases}$$

(iv) If $\mathfrak{X}_j$ *is a finite subfield of* $\mathcal{R}$ *:*
$$N_j(x) \ = \ -1 \ .$$

(v) If $\mathfrak{X}_j = \{0, 1, \ldots, d_j\} \subseteq \mathbb{Z}$ *:*
$$N_j(x) \ = \ (-1)^{d_j+x}\, d_j!\, \tbinom{d_j}{x}^{-1}.$$

(vi) For $\alpha \in \mathcal{R}$ *we have:*
$$N_{\mathfrak{X}_j+\alpha}(x+\alpha) \ = \ N_{\mathfrak{X}_j}(x) \ .$$

Proof. For finite subsets $\mathcal{D} \subseteq \mathcal{R}$ we define

$$L_{\mathcal{D}}(X) := \prod_{\hat{x}\in\mathcal{D}} (X - \hat{x}) \ . \tag{13}$$

It is well-known that, if E_l contains l elements and lies in an integral domain,

$$L_{E_l}(X) \ = \ \prod_{\hat{x}\in E_l} (X - \hat{x}) \ = \ X^l - 1 \ = \ (X-1)(X^{l-1} + \cdots + X^0) \ . \tag{14}$$

Thus

$$L_{E_l\setminus 1}(1) \,=\, \frac{\prod_{\hat{x}\in E_l}(X-\hat{x})}{X-1}\,\Big|_{X=1} = \,\frac{X^l-1}{X-1}\,\Big|_{X=1} = \,X^{l-1}+\cdots+X^0\,\Big|_{X=1} = \,l1\;. \tag{15}$$

Using this, we get for $x \in E_l$

$$L_{E_l\setminus x}(x) \,=\, L_{x(E_l\setminus 1)}(x) \,=\, \prod_{\hat{x}\in E_l\setminus 1}(x-x\hat{x}) \,=\, x^{l-1}L_{E_l\setminus 1}(1) \,=\, lx^{-1}\;. \tag{16}$$

This gives (i) with $l = |\mathfrak{X}_j| = d_j + 1$.

Part (ii) follows from part (i) in the case $\mathfrak{X}_j \,=\, F_{p^k}\backslash 0 \,=\, E_{p^k-1}$, as $d_j + 1 = |\mathfrak{X}_j| = (p^k - 1) \equiv -1 \pmod p$ in this case.

To get $N_j(x) = L_{\{0\}\uplus E_l\setminus x}(x)$ with $x \neq 0$ in part (iii) and part (iv) we multiply Equation (16) with $x - 0$ and use $l = |\mathfrak{X}_j| - 1 = d_j$ for part (iii) and $l = |\mathfrak{X}_j| - 1 = p^k - 1 \equiv -1 \pmod p$ for part (iv). For $x = 0$ we obtain in part (iii) and part (iv)

$$N_j(0) \,=\, L_{E_l}(0) \,=\, \prod_{\hat{x}\in E_l}(-\hat{x}) \,=\, -\prod_{\hat{x}\in E_l\setminus\{1,-1\}}(-\hat{x}) \,=\, -1 \;\;, \tag{17}$$

since each subset $\{\hat{x}, \hat{x}^{-1}\} \subseteq E_l \setminus \{1, -1\}$ contributes $(-\hat{x})\,(-\hat{x}^{-1}) = 1$ to the product – as $\hat{x} \neq \hat{x}^{-1}$, since $\hat{x}^2 - 1 = 0$ holds only for $\hat{x} = \pm 1$ – and $E_l \setminus \{1, -1\}$ is partitioned by such subsets. This completes the proofs of (iii) and (iv).

We now turn to part (v):

$$N_j(x) \,=\, \Big(\prod_{0\le\hat{x}<x}(x-\hat{x})\Big)\prod_{x<\hat{x}\le d_j}(x-\hat{x}) \,=\, x!\,(d_j-x)!\,(-1)^{d_j-x} \,=\, (-1)^{d_j+x}\,d_j!\binom{d_j}{x}^{-1}. \tag{18}$$

Part (vi) is trivial. □

2 Interpolation polynomials and inversion formulas

This section may be skipped at a first reading; the only things you need from here to understand the rest of the paper are: firstly, the fact that grids $\mathfrak{X} \subseteq \mathcal{R}^n$ over integral domains R are always *integral grids*; and, secondly, the inversion formula 2.8, which is, in this case, just the well-known interpolation formula for polynomials applied to polynomial maps $P|_{\mathfrak{X}}$. The rest of this section is concerned with providing some generality that is not really used in the applications of this paper.

We have to investigate the canonical homomorphism $\varphi\colon P \longmapsto P|_{\mathfrak{X}}$ that maps polynomials P to polynomial maps $P|_{\mathfrak{X}}\colon x \mapsto P(x)$ on a fixed d-grid $\mathfrak{X} \subseteq \mathcal{R}^n$. As the monic polynomial $L_j = L_{\mathfrak{X}_j}(X_j) := \prod_{\hat{x}\in\mathfrak{X}_j}(X_j - \hat{x})$ maps all elements of $\mathfrak{X}_j$ to 0, we may replace each given polynomial P by any other polynomial of the form $P + \sum_{j\in(n]} H_j L_j$ without changing its image $P|_{\mathfrak{X}}$. By applying such modifications, we may assume that P has partial degrees $\deg_j(P) \le |\mathfrak{X}_j| - 1 = d_j$ (see Example 7.1 for an illustration of this method). Hence the image of φ does not change if we regard φ as a map on $\mathcal{R}[X^{\le d}]$ (which we identify with $\mathcal{R}^{[d]}$ by $P \mapsto (P_\delta)_{\delta\in[d]}$). The resulting map

$$\varphi\colon \mathcal{R}[X^{\le d}] = \mathcal{R}^{[d]} \longrightarrow \mathcal{R}^{\mathfrak{X}},\ P \longmapsto P|_{\mathfrak{X}} := (x \mapsto P(x)) \tag{19}$$

is in the most important cases an isomorphism or at least a monomorphism, as we will see. In general, however, the situation is much more complicated:

Example 2.1. Over $\mathcal{R} = \mathbb{Z}_6 := \mathbb{Z}/6\mathbb{Z}$ we have $X^3|_{\mathbb{Z}_6} = X|_{\mathbb{Z}_6}$ and $3X^2|_{\mathbb{Z}_6} = 3X|_{\mathbb{Z}_6}$, so that each polynomial map $\mathfrak{X} := \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ can be represented by a polynomial of the form $aX^2 + bX + c$, with $a \in \{0, 1, -1\}$. Hence the corresponding $3 \cdot 6^2$ distinct maps are the only maps out of the 6^6 maps from $\mathfrak{X} = \mathbb{Z}_6$ to $\mathbb{Z}_6$ that can be represented by polynomials at all[1]. This simple example shows also that the kernel $\ker(\varphi)$ may look very complicated even in just one dimension.

In which situations does $\varphi\colon P \longmapsto P|_{\mathfrak{X}}$ become an isomorphism, or equivalently, when does its representing matrix Φ possess an inverse? Over com-

[1] In [MuSt] a system of polynomials in $\mathbb{Z}_m[X_1, \ldots, X_n]$ is given that represent all polynomial maps $\mathbb{Z}_m^n \to \mathbb{Z}_m$ and the number of all such maps is determined. In [Sp] it is shown that the Newton algorithm can be used to determine interpolation polynomials, if they exist. The "divided differences" in this algorithm are, like the interpolation polynomials themselves, not uniquely determined over arbitrary commutative rings, and exist if and only if interpolation polynomials exist.

mutative rings $\mathcal{R}$, square matrices $\Phi \in \mathcal{R}^{m\times m}$ with nonvanishing determi-
Adj(Φ) nant do not have an inverse, in general. However, there is the matrix $\mathrm{Adj}(\Phi)$ – the adjoint or cofactor matrix – that comes close to being an inverse:

$$\Phi\,\mathrm{Adj}(\Phi) \;=\; \mathrm{Adj}(\Phi)\Phi \;=\; \det(\Phi) I_m \;. \tag{20}$$

Φ In our concrete situation, where $\Phi \in \mathcal{R}^{\mathfrak{X}\times[d]}$ is the matrix of φ (a tensor
Ψ product of Vandermonde matrices), we work with Ψ (from Definition 1.2) instead of the adjoint matrix $\mathrm{Adj}(\Phi)$. Ψ comes closer than $\mathrm{Adj}(\Phi)$ to being a right inverse of Φ. The following theorem shows that

$$\Phi\Psi \;=\; \big(N(x)\,?_{(\tilde{x}=x)}\big)_{\tilde{x},x\in\mathfrak{X}} \;, \tag{21}$$

and the entries $N(x)$ of this diagonal matrix divide the entries $\det(\Phi)$ of $\Phi\,\mathrm{Adj}(\Phi)$, so that $\Phi\Psi$ is actually closer than $\Phi\,\mathrm{Adj}(\Phi)$ to the unity matrix (provided we identify the column indices $x \in \mathfrak{X}$ and row indices $\delta \in [d]$ in some way with the numbers $1, 2, \ldots, |\mathfrak{X}| = |[d]|$, in order to make $\det(\Phi)$ and $\mathrm{Adj}(\Phi)$ defined).

Φ, φ However, we used the matrix $\Phi \in \mathcal{R}^{\mathfrak{X}\times[d]}$ of $\varphi\colon P \longmapsto P|_{\mathfrak{X}}$ here just to explain the role of Ψ. In what follows, we do not use it any more; rather, we prefer notations with "φ" or "$|_{\mathfrak{X}}$." For maps/tuples $y \in \mathcal{R}^{\mathfrak{X}}$, we write
(Ψy)(X) $(\Psi y)(X) \in \mathcal{R}[X^{\leq d}]$, as already defined, for the polynomial whose coefficients form the tuple $\Psi y \in \mathcal{R}^{[d]}$, i.e., $(\Psi y)(X) = \Psi y$ by identification. We have:

Theorem 2.2 (Interpolation)**.** *For maps* $y\colon \mathfrak{X} \longrightarrow \mathcal{R}$,

$$\boxed{(\Psi y)(X)|_{\mathfrak{X}} \;=\; Ny} \;.$$

Proof. As both sides of the equation are linear in y, it suffices to prove the equation for the maps $y = e_{\tilde{x}}$, where $\tilde{x}$ ranges over $\mathfrak{X}$. Now we see that, at each point $x \in \mathfrak{X}$, we actually have

$$(\Psi e_{\tilde{x}})(X)|_{\mathfrak{X}}(x) \;\overset{1.3}{=}\; L_{\mathfrak{X},\tilde{x}}(x) \;=\; N(x)\,?_{(x=\tilde{x})} \;=\; (Ne_{\tilde{x}})(x) \;. \tag{22}$$

□

With this theorem, we are able to characterize the situations in which $\varphi\colon P \longmapsto P|_{\mathfrak{X}}$ is an isomorphism:

Equivalence and Definition 2.3 (Division grids)**.** *We call a d-grid* $\mathfrak{X} \subseteq \mathcal{R}^n$ *a* division grid *(over* $\mathcal{R}$ *) if it has the following equivalent properties:*

(i) For all $j \in (n]$ *and all* $x, \tilde{x} \in \mathfrak{X}_j$ *with* $x \neq \tilde{x}$, $x - \tilde{x}$ *is invertible.*

(ii) $N = N_{\mathfrak{X}}$ *is pointwise invertible, i.e., for all* $x \in \mathfrak{X}$, $N(x)$ *is invertible.*

(iii) ΠN *is invertible.*

(iv) $\varphi\colon \mathcal{R}[X^{\leq d}] = \mathcal{R}^{[d]} \longrightarrow \mathcal{R}^{\mathfrak{X}}$ *is bijective.*

Proof. The equivalence of (i),(ii) and (iii) follows from the Definition 1.2 of N, the definition $\Pi N = \prod_{x\in\mathfrak{X}} N(x)$ and the associativity and commutativity of $\mathcal{R}$.

Assuming (ii), it follows from Theorem 2.2 that $y \longmapsto (\Psi(N^{-1}y))(X)$ is a right inverse of $\varphi\colon P \longmapsto P|_{\mathfrak{X}}$:

$$y \longmapsto (\Psi(N^{-1}y))(X) \overset{\varphi}{\longmapsto} N(N^{-1}y) = y \ . \tag{23}$$

It is even a two-sided inverse, since square matrices Φ over a commutative ring $\mathcal{R}$ are invertible from both sides if they are invertible at all (since $\Phi \operatorname{Adj}(\Phi) = \det(\Phi)\mathbf{1}$). This gives (iv).

Now assume (iv) holds; then for all $x \in \mathfrak{X}$,

$$\big(\psi_{\delta,x}\big)_{\delta\in[d]} \ = \ \Psi e_x \overset{2.2}{=} \varphi^{-1}(Ne_x) \ = \ N(x)\,\varphi^{-1}(e_x) \ , \tag{24}$$

and in particular,

$$1 \overset{(9)}{=} \psi_{d,x} \ = \ N(x)\,\big(\varphi^{-1}(e_x)\big)_d \ . \tag{25}$$

Thus the $N(x)$ are invertible and that is (ii). □

If $\varphi\colon \mathcal{R}[X^{\leq d}] \longrightarrow \mathcal{R}^{\mathfrak{X}}$ is an isomorphism, then $\varphi^{-1}(y)$ is the unique polynomial in $\mathcal{R}[X^{\leq d}]$ that interpolates a given map $y \in \mathcal{R}^{\mathfrak{X}}$, so that, by Theorem 2.2, it has to be the polynomial $\Psi(N^{-1}y) \in \mathcal{R}^{[d]} = \mathcal{R}[X^{\leq d}]$. This yields the following result: φ^{-1}

Theorem 2.4 (Interpolation formula)**.** *Let* $\mathfrak{X}$ *be a division grid (e.g., if* $\mathcal{R}$ *is a field or if* $\mathfrak{X}$ *is the* Boolean grid $\{0,1\}^n$ *). For* $y \in \mathcal{R}^{\mathfrak{X}}$,

$$\boxed{\varphi^{-1}(y) \ = \ \Psi(N^{-1}y)} \ .$$

This theorem can be found in [Da, Theorem 2.5.2], but just for fields $\mathcal{R}$ and in a different representation (with $\varphi^{-1}(y)$ as a determinant).

Additionally, if $\mathfrak{X}$ is not a division grid, we may apply the canonical localization homomorphism

π
$\mathcal{S}, \mathcal{R}_N$

$$\pi\colon \mathcal{R} \longrightarrow \mathcal{R}_N := \mathcal{S}^{-1}\mathcal{R}\ ,\ \ r \longmapsto r^\pi := \tfrac{r}{1} \quad \text{with} \quad \mathcal{S} := \{\, (\Pi N)^m \mid m \in \mathbb{N} \,\}\ , \tag{26}$$

and exert our theorems in this situation. As π and $\mathcal{R}_N$ have the universal property with respect to the invertibility of $(\Pi N)^\pi$ in $\mathcal{R}_N$ (as required in 2.3(*iii*)), π and $\mathcal{R}_N$ are the best choices. This means specifically that if $(\Pi N)^\pi$ is not invertible in the codomain $\mathcal{R}_N$ of π, then no other homomorphism π' has this property, either. In general, π does not have this property itself: By definition,

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \ :\Longleftrightarrow\ \ \exists\, s \in \mathcal{S}\colon\ s\, r_1 s_2 = s\, r_2 s_1\ , \tag{27}$$

$\ker(\pi)$ and hence

$$\ker(\pi) = \{\, r \in \mathcal{R} \mid \exists\, m \in \mathbb{N}\colon (\Pi N)^m\, r = 0 \,\}\ , \tag{28}$$

so that $(\Pi N)^\pi = 0$ is possible. Localization works in the following situation:

Equivalence and Definition 2.5 (Affine grids)**.** *We call a d-grid* $\mathfrak{X} \subseteq \mathcal{R}^n$ affine *(over* $\mathcal{R}$*) if it has the following equivalent properties:*

(i) ΠN *is not nilpotent.*

(ii) $\pi \neq 0$*.*

(iii) $(\Pi N)^\pi$ *is invertible in* $\mathcal{R}_N$*.*

(iv) $\pi \neq 0$ *is injective on the* $\mathfrak{X}_j$
$\mathfrak{x}^\pi$ *and hence induces a bijection* $\mathfrak{X} \longrightarrow \mathfrak{X}^\pi := \mathfrak{X}_1^\pi \times \cdots \times \mathfrak{X}_n^\pi$*.*

Proof. (*ii*) is equivalent to $1^\pi \neq 0$, and this means that $s1 \neq 0$ for all s in the multiplicative system $\mathcal{S} = \{\, (\Pi N)^m \mid m \in \mathbb{N} \,\}$; thus $(i) \Longleftrightarrow (ii)$.

$(\Pi N)^\pi \frac{1}{\Pi N} = \frac{1}{1}$ is the unity in $\mathcal{R}_N$, provided $\frac{1}{1} = 1^\pi \neq 0$; therefor $(ii) \Longrightarrow (iii)$.

If (*iii*) holds then $(\Pi N)^\pi$ and its factors $(x_j - \tilde{x}_j)^\pi$ do not vanish; thus $(iii) \Longrightarrow (iv)$.

Finally, the implication $(iv) \Longrightarrow (ii)$ is trivial. □

If $\mathfrak{X} \subseteq \mathcal{R}^n$ is affine, then $\mathfrak{X}^\pi := \mathfrak{X}_1^\pi \times \cdots \times \mathfrak{X}_n^\pi \subseteq \mathcal{R}_N^n$ is a division d-grid over $\mathcal{R}_N$ by 2.5 (iv), 2.5 (iii) and 2.3 (iii). Now, Theorem 2.4 applied to $y := P^\pi|_{\mathfrak{X}^\pi}$ with $P^\pi = \sum_{\delta\in[d]} P_\delta^\pi X^\delta$ yields $\mathfrak{X}^\pi$ P^π

$$P^\pi \;=\; \Psi_{\mathfrak{X}^\pi}\big((N_{\mathfrak{X}^\pi})^{-1}(P^\pi|_{\mathfrak{X}^\pi})\big)\;, \tag{29}$$

along with the associated constants $N_{\mathfrak{X}^\pi} \in \mathcal{R}_N^{\mathfrak{X}^\pi}$ and $\Psi_{\mathfrak{X}^\pi} \in \mathcal{R}_N^{[d]\times\mathfrak{X}^\pi}$ of $\mathfrak{X}^\pi$.

With componentwise application of π to $P|_{\mathfrak{X}}$, $N \in \mathcal{R}^{\mathfrak{X}}$ and $\Psi \in \mathcal{R}^{[d]\times\mathfrak{X}}$ (i.e. $(P|_{\mathfrak{X}})^\pi$, $N^\pi \in \mathcal{R}_N^{\mathfrak{X}}$ and $\Psi^\pi \in \mathcal{R}_N^{[d]\times\mathfrak{X}}$), we obtain: N^π, Ψ^π

Theorem 2.6 (Inversion formula)**.** *Let $\mathfrak{X}$ be affine (e.g., if $\mathcal{R}$ does not possess nilpotent elements). For $P \in \mathcal{R}[X^{\le d}] = \mathcal{R}^{[d]}$,*

$$\boxed{P^\pi \;=\; \Psi^\pi\big((N^\pi)^{-1}(P|_{\mathfrak{X}})^\pi\big)}\;.$$

If π is injective on its whole domain $\mathcal{R}$ then $\mathcal{R}$ is a subring of $\mathcal{R}_N$ and we may omit π in formula 2.6. In fact, we will see that this is precisely when when φ is injective, as seen in the following characterization:

Equivalence and Definition 2.7 (Integral grids)**.** *We call a d-grid $\mathfrak{X} \subseteq \mathcal{R}^n$* integral *(over $\mathcal{R}$) if it has the following, equivalent properties:*

(i) For all $j \in (n]$ and all $x, \tilde{x} \in \mathfrak{X}_j$ with $x \neq \tilde{x}$, $x - \tilde{x}$ is not a zero divisor.

(ii) For all $x \in \mathfrak{X}$, $N(x)$ is not a zero divisor.

(iii) ΠN is not a zero divisor.

(iv) π is injective ($\mathcal{R} \subseteq \mathcal{R}_N$).

(v) $\varphi\colon \mathcal{R}[X^{\le d}] = \mathcal{R}^{[d]} \longrightarrow \mathcal{R}^{\mathfrak{X}}$ is injective.

Proof. The equivalence of (i),(ii) and (iii) follows from the Definition 1.2 of N, the definition $\Pi N = \prod_{x\in\mathfrak{X}} N(x)$ and the associativity and commutativity of $\mathcal{R}$.

As already mentioned, $\ker(\pi) = \{\, r \in \mathcal{R} \;\mid\; \exists\, m \in \mathbb{N}\colon (\Pi N)^m r = 0 \,\}$, so that $(iii) \Longrightarrow (iv)$.

If (iv) holds, then ΠN is invertible in $\mathcal{R}_N$. By Equivalence 2.3, it follows that $\varphi\colon \mathcal{R}_N[X^{\le d}] \longrightarrow \mathcal{R}_N^{\mathfrak{X}}$ is bijective, so that $(iv) \Longrightarrow (v)$.

Now suppose that (ii) does not hold, so that there are a point $x \in \mathfrak{X}$ and a constant $M \in \mathcal{R}\backslash 0$ with

$$MN(x) \,=\, 0\ . \tag{30}$$

Then

$$P \,:=\, \Psi(Me_x) \,\neq\, 0\ , \tag{31}$$

as

$$P_d \,=\, M(\Psi(e_x))_d \,=\, M\psi_{d,x} \overset{(9)}{=} M \,\neq\, 0\ . \tag{32}$$

However,

$$\varphi(P) \overset{2.2}{=} NMe_x \,=\, MN(x)e_x \,\equiv\, 0\ , \tag{33}$$

so that (v) does not hold, either. Thus $(v) \Longrightarrow (ii)$. □

Any integral grid $\mathfrak{X}$ over $\mathcal{R}$ is, in fact, a division grid over $\mathcal{R}_N \supseteq \mathcal{R}$, since ΠN becomes invertible in $\mathcal{R}_N$. Formula 2.4 applied to $y := P|_{\mathfrak{X}}$ yields the following specialization of 2.6:

Theorem 2.8 (Inversion formula)**.** *Let $\mathfrak{X}$ be integral (e.g., if $\mathcal{R}$ is an integral domain). For $P \in \mathcal{R}[X^{\leq d}] = \mathcal{R}^{[d]}$,*

$$\boxed{P \,=\, \Psi(N^{-1}P|_{\mathfrak{X}})}\ .$$

From the case $P = 1$, we see that $N^{-1}P|_{\mathfrak{X}}$ inside this formula does not lie in $\mathcal{R}^{\mathfrak{X}}$ in general. This also shows that, in general, the maps of the form Ny, with $y \in \mathcal{R}^{\mathfrak{X}}$, in Theorem 2.2 are not the only maps that can be represented by polynomials over $\mathcal{R}$, i.e., $\{\, Ny \mid y \in \mathcal{R}^{\mathfrak{X}} \,\} \subsetneq \mathrm{Im}(\varphi)$. However, the maps of the form Ny are exactly the linear combinations of Lagrange's polynomial maps $Ne_x = L_{\mathfrak{X},x}|_{\mathfrak{X}}$ over the grid $\mathfrak{X}$; and if we view, a bit more generally, Lagrange polynomials $L_{\tilde{\mathfrak{X}},x}$ over subgrids $\tilde{\mathfrak{X}} = \tilde{\mathfrak{X}}_1 \times \cdots \times \tilde{\mathfrak{X}}_n \subseteq \mathfrak{X}$, then the maps of the form $L_{\tilde{\mathfrak{X}},x}|_{\mathfrak{X}}$ span $\mathrm{Im}(\varphi)$, as one can easily show.

On the other hand, in general, $\mathrm{Im}(\varphi) \subsetneq \mathcal{R}^{\mathfrak{X}}$, so that not every map $y \in \mathcal{R}^{\mathfrak{X}}$ can be interpolated over $\mathcal{R}$. If $\mathfrak{X}$ is integral, then interpolation polynomials exist over the bigger ring $\mathcal{R}_N$. The univariate polynomials $\binom{X}{k} := \frac{X(X-1)\cdots(X-k+1)}{k!}$, for example, describe integer-valued maps (on the whole domain $\mathbb{Z}$), but do not lie in $\mathbb{Z}[X]$. More information about such "overall" integer-valued polynomials over quotient fields can be found, for example, in [CCF] and [CCS], and in the literature cited there.

The reader might find it interesting that the principle of inclusion and exclusion follows from Theorem 2.8 as a special case:

Proposition 2.9 (Principle of inclusion and exclusion)**.**
Let $\mathfrak{X} := \{0,1\}^n = [d]$ *and* $x \in \mathfrak{X}$*; then* $x^\delta = ?_{(\delta \leq x)}$ *for all* $\delta \in [d]$*. Thus, for arbitrary* $P = (P_\delta) \in \mathcal{R}^{[d]} = \mathcal{R}[X^{\leq d}]$*,*

$$P(x) \;=\; \sum\nolimits_{\delta \leq x} P_\delta \;. \tag{34}$$

Formula 2.8 is the Möbius inversion to Equation (34)*:*

$$\begin{aligned} P_\delta \quad &\overset{2.8}{=} \quad \sum_{x \in [d]} \psi_{\delta,x} N^{-1}(x) P(x) \\ &\overset{1.2}{=} \quad \sum_{x \in [d]} \big[\prod_{j \in (n]} ?_{(x_j \leq \delta_j)} \, (-1)^{1-\delta_j} \big] \big[\prod_{j \in (n]} (-1)^{1-x_j} \big] P(x) \\ &= \quad \sum\nolimits_{x \leq \delta} (-1)^{\Sigma(\delta - x)} P(x) \;. \end{aligned} \tag{35}$$

3 Coefficient formulas – the main results

The applications in this paper do not start with a map $y \in \mathcal{R}^{\mathfrak{X}}$ that has to be interpolated by a polynomial P. Rather, we start with a polynomial P, or with some information about a polynomial $P \in \mathcal{R}[X]$, which describes the very map $y := P|_{\mathfrak{X}}$ that we would like to understand. Normally, we will not have complete information about P, so that we do not usually know all coefficients P_δ of P. However, there may be a coefficient P_δ in $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta$ that, on its one, allows conclusions about the map $P|_{\mathfrak{X}}$. We define (see also figure 1 below):

Definition 3.1. Let $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathcal{R}[X]$ be a polynomial. We call a multiindex $\varepsilon \le d \in \mathbb{N}^n$ *d-leading* in P if for each monomial X^δ in P, i.e., each δ with $P_\delta \neq 0$, holds either

- (case 1) $\delta = \varepsilon$; *or*
- (case 2) there is a $j \in (n]$ such that $\delta_j \neq \varepsilon_j$ but $\delta_j \le d_j$.

Note that the multiindex d is d-leading in polynomials P with $\deg(P) \le \Sigma d$. In this situation, case 2 reduces to "there is a $j \in (n]$ such that $\delta_j < d_j$," and, as $\Sigma\delta \le \Sigma d$ for all X^δ in P, we can conclude:

$$\text{"not case 2"} \implies \delta \ge d \implies \delta = d \implies \text{"case 1"} . \tag{36}$$

Thus d really is d-leading in P (see also figure 2 on page 50). Of course, if all partial degrees are restricted by $\deg_j(P) \le d_j$ then all multiindices $\delta \le d$ are d-leading. Figure 1 (below) shows a nontrivial example $P \in \mathcal{R}[X_1, X_2]$. The monomials X^δ of P ($P_\delta \neq 0$), and the $2^n - 1 = 3$ "forbidden areas" of each of the two d-leading multiindices, are marked.

In what follows, we examine how the preconditions of the inversion formula 2.8 may be weakened. It turns out that formula 2.8 holds without further degree restrictions for the d-leading coefficients P_ε of P. The following theorem is a generalization and a sharpening of Alon and Tarsi's (second) Combinatorial Nullstellensatz [Al2, Theorem 1.2]:

Theorem 3.2 (Coefficient formula)**.** *Let $\mathfrak{X}$ be an integral d-grid. For each polynomial $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathcal{R}[X]$ with d-leading multiindex $\varepsilon \le d \in \mathbb{N}^n$,*

(i) $\boxed{P_\varepsilon = (\Psi(N^{-1}P|_{\mathfrak{X}}))_\varepsilon}$ $\quad (= \sum_{x \in \mathfrak{X}} \psi_{\varepsilon,x}\, N(x)^{-1} P(x)\ ),$ *and*

(ii) $\boxed{P_\varepsilon \neq 0 \implies P|_{\mathfrak{X}} \not\equiv 0}$.

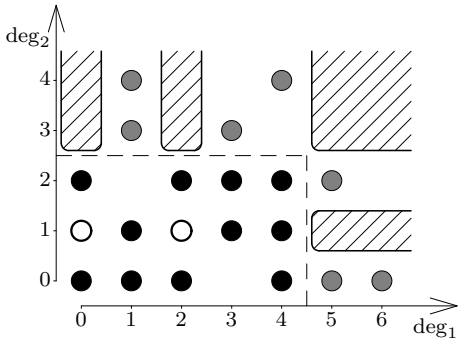


Figure 1: Monomials of a polynomial P with $(4,2)$-leading multiindices $(0,1)$ and $(2,1)$.

Proof. In our first proof we use the tensor product property (7) and the linearity of the map $P \mapsto (\Psi(N^{-1}P|_{\mathfrak{X}}))_\varepsilon$ to reduce the problem to the one-dimensional case. The one-dimensional case is covered by the inversion formula 2.8 . Another proof, following Alon and Tarsi's polynomial method, is described in Section 7 .

Since both sides of the Equation (i) are linear in P it suffices to prove $(X^\delta)_\varepsilon = (\Psi(N^{-1}X^\delta|_{\mathfrak{X}}))_\varepsilon$ in the both cases of Definition 3.1 . In each case,

$$\begin{aligned}
\Big(\Psi(N^{-1}X^\delta|_{\mathfrak{X}})\Big)_\varepsilon &= \Big(\Psi\Big(\big(\bigotimes\nolimits_j N_j^{-1}\big)\bigotimes\nolimits_j (X_j^{\delta_j}|_{\mathfrak{X}_j})\Big)\Big)_\varepsilon \\
&= \Big(\big(\bigotimes\nolimits_j \Psi^j\big)\bigotimes\nolimits_j (N_j^{-1}X_j^{\delta_j}|_{\mathfrak{X}_j})\Big)_\varepsilon \\
&\overset{(7)}{=} \Big(\bigotimes\nolimits_j \big(\Psi^j(N_j^{-1}X_j^{\delta_j}|_{\mathfrak{X}_j})\big)\Big)_\varepsilon \\
&= \prod_{j\in(n]} \Big(\Psi^j(N_j^{-1}X_j^{\delta_j}|_{\mathfrak{X}_j})\Big)_{\varepsilon_j} \ .
\end{aligned} \tag{37}$$

Using the one-dimensional case of the inversion formula 2.8 we also derive

$$\Big(\Psi^j(N_j^{-1}X_j^{\delta_j}|_{\mathfrak{X}_j})\Big)_{\varepsilon_j} = (X_j^{\delta_j})_{\varepsilon_j} = ?_{(\delta_j=\varepsilon_j)} \qquad \text{for all } j\in(n] \text{ with } \delta_j \le d_j \ . \tag{38}$$

Thus in case 1 ($\forall\, j \in (n]\colon\ \delta_j = \varepsilon_j \le d_j$) ,

$$\Big(\Psi(N^{-1}X^\delta|_{\mathfrak{X}})\Big)_\varepsilon = 1 = (X^\delta)_\varepsilon \ . \tag{39}$$

And in case 2 ($\exists\, j \in (n]\colon\ \varepsilon_j \ne \delta_j \le d_j$) ,

$$\Big(\Psi(N^{-1}X^\delta|_{\mathfrak{X}})\Big)_\varepsilon = 0 = (X^\delta)_\varepsilon \ . \tag{40}$$

□

Note that the one-dimensional case of Theorem 3.2 (ii) is nothing more then the well-known fact that polynomials $P(X_1) \neq 0$ of degree at most d_1 have at most d_1 roots.

With the remark after Definition 3.1, and the knowledge that $\psi_{d,x} \overset{(9)}{=} 1$ for all $x \in \mathfrak{X}$, we get our main result as an immediate consequence of Theorem 3.2:

Theorem 3.3 (Coefficient formula)**.** *Let $\mathfrak{X}$ be an integral d-grid. For each polynomial $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathcal{R}[X]$ of total degree $\deg(P) \leq \Sigma d$,*

(i) $\boxed{P_d \,=\, \Sigma(N^{-1}P|_{\mathfrak{X}})}$ $\quad (= \sum_{x \in \mathfrak{X}} N(x)^{-1}P(x)\,),$ *and*

(ii) $\boxed{P_d \neq 0 \implies P|_{\mathfrak{X}} \not\equiv 0}$.

This main theorem looks simpler then the more general Theorem 3.2, and you do not have to know the concept of d-leading coefficients to understand it. Furthermore, the applications in this paper do not really make use of the generality in Theorem 3.2. However, we tried to provide as much generality as possible, and it is of course interesting to understand the role of the degree restriction in Theorem 3.3. The most important part of this results, the implication in Theorem 3.3 (ii), which is known as Combinatorial Nullstellensatz was already proven in [Al2, Theorem 1.2], for integral domains. Note that $P_d = 0$ whenever $\deg(P) < \Sigma d$, so that the implication seems to become useless in this situation. However, one may modify P, or use smaller sets $\mathfrak{X}_j$ (and hence smaller d_j), and apply the implication then. So, if $P_\delta \neq 0$ for a $\delta \leq d$ with $\Sigma\delta = \deg(P)$ then it still follows that $P|_{\mathfrak{X}} \not\equiv 0$. De facto, such δ are d-leading.

If, on the other hand, $\deg(P) = \Sigma d$, then P_d is, in general, the only coefficient that allows conclusions on $P|_{\mathfrak{X}}$ as in 3.3 (ii), how the modification methods of Section 7 show. More precisely, if we do not have further information about the d-grid $\mathfrak{X}$, then the d-leading coefficients are the only coefficients that allow such conclusions. For special grids $\mathfrak{X}$, however, there may be some other coefficients P_δ with this property, e.g., P_0 in the case $0 = (0, \ldots, 0) \in \mathfrak{X}$.

Note further that for special grids $\mathfrak{X}$, the degree restriction in 3.3 may be weakened slightly. If, for example, $\mathfrak{X} = \mathbb{F}_q^n$, then the restriction $\deg(P) \leq \Sigma d + q - 2$ suffices; see the footnote on page 50 for an explanation.

The following corollary is a consequence of the simple fact that vanishing sums (the case $P_d = 0$ in Theorem 3.3 (i)) do not have exactly one nonvan-

ishing summand. It is very useful if a problem possesses exactly one trivial solution: if we are able to describe the problem by a polynomial of low degree, we just have to check the degree, and Corollary 3.4 guarantees a second (in this case, nontrivial) solution. There are many elegant applications of this; for some examples see Section 4. We will work out a general working frame in Section 6. We have:

Corollary 3.4. *Let $\mathfrak{X}$ be an integral d-grid. For polynomials P of degree $\deg(P) < \Sigma d$ (or, more generally, for polynomials with vanishing d-leading coefficient $P_d = 0$),*

$$\boxed{\left|\{\, x \in \mathfrak{X} \;:\; P(x) \neq 0 \,\}\right| \neq 1} \; .$$

If the grid $\mathfrak{X}$ has a special structure – for example, if $\mathfrak{X} \subseteq \mathbb{R}_{>0}^{\;n}$ – this corollary may also hold for polynomials P with vanishing d-leading coefficient $P_\varepsilon = 0$ for some $\varepsilon \neq d$. The simple idea for the proof of this, which uses Theorem 3.2 instead of Theorem 3.3, leads to the modified conclusion that

$$\left|\{\, x \in \mathfrak{X} \;:\; \psi_{\varepsilon,x} P(x) \neq 0 \,\}\right| \neq 1 \; . \tag{41}$$

Note further that the one-dimensional case of Corollary 3.4 is just a reformulation of the well-known fact that polynomials $P(X_1)$ of degree less than d_1 do not have $d_1 = |\mathfrak{X}_1| - 1$ roots, except if $P = 0$.

The example $P = 2X_1 + 2 \in \mathbb{Z}_4[X_1]$, $\mathfrak{X} = \{0, 1, -1\}$ shows that Corollary 3.4 does not hold over arbitrary grids. However, if $\mathfrak{X} = \mathbb{Z}_m^{\;n} =: \mathcal{R}^n$ with m not prime, the grid $\mathfrak{X}$ is not integral; yet assertion 3.4 holds anyway. Astonishingly, in this case the degree condition can be dropped, too. We will see this in Corollary 9.2.

We also present another proof of Corollary 3.4 that uses only the weaker part (ii) of Theorem 3.2, to demonstrate that the well-known Combinatorial Nullstellensatz, our Theorem 3.3 (ii), would suffice for the proof of the main part of the corollary:

Proof. Suppose P has exactly one nonzero $x_0 \in \mathfrak{X}$. Then

$$Q \;:=\; P - P(x_0) N^{-1}(x_0) L_{\mathfrak{X},x_0} \;\in\; \mathcal{R}[X] \tag{42}$$

vanishes on the whole grid $\mathfrak{X}$, but possesses the nonvanishing and d-leading coefficient

$$Q_d \;=\; -P(x_0) N^{-1}(x_0) \;\neq\; 0 \; , \tag{43}$$

in contradiction to Theorem 3.2 (ii). □

A further useful corollary, and a version of Chevalley and Warning's classical result – Theorem 4.3 in this paper – is the following result (see also Corollary 8.5 for a sharpening of Warning's Theorem, and Theorem 9.4 for a similar result over $\mathbb{Z}_{p^k}$):

Corollary 3.5. *Let* $\mathfrak{X} \subseteq \mathbb{F}_{p^k}^n$ *be a d-grid and* $P_1, \ldots, P_m \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$. *If* $(p^k - 1) \sum_{i \in (m]} \deg(P_i) < \Sigma d$, *then*

$$\boxed{\left|\left\{ x \in \mathfrak{X} \mid P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1} \ .$$

Proof. Define

$$P := \prod_{i \in (m]} (1 - P_i^{p^k - 1}) \ ; \tag{44}$$

then for points $x = (x_1, \ldots, x_n)$,

$$P(x) \neq 0 \iff \forall\, i \in (m] \colon P_i(x) = 0 \ , \tag{45}$$

and hence

$$\left|\left\{ x \in \mathfrak{X} \mid P_1(x) = \cdots = P_m(x) = 0 \right\}\right| = \left|\left\{ x \in \mathfrak{X} \mid P(x) \neq 0 \right\}\right| \overset{3.4}{\neq} 1 \ , \tag{46}$$

since

$$\deg(P) \leq \sum_{i \in (m]} (p^k - 1) \deg(P_i) < \Sigma d \ . \tag{47}$$

□

4 First applications and the application principles

In this section we present some short and elegant examples of how our theorems may be applied. They are all well-known, but we wanted to have some examples to demonstrate the huge flexibility of these methods. This flexibility will also be emphasized through the general working frame described in Section 6, for which the applications of this section may serve as examples. Alon used them already in [Al2] to demonstrate the usage of implication 3.3 (*ii*); whereas we prove them by application of Theorem 3.3 (*i*), and the corollaries 3.4 and 3.5, an approach which is – in most cases – more straightforward and more elegant. The main advantage of the coefficient formula 3.3 (*i*) can be seen in the proof of Theorem 4.3, where the implication 3.3 (*ii*) does not suffice to give a proof of the full theorem. Section 5 will contain another application that puts the new quantitative aspect of coefficient formula 3.3 into the spotlight.

Our first example was originally proven in [AFK]:

Theorem 4.1. *Every loopless* 4*-regular multigraph plus one edge* $G = (V, E \uplus \{e_0\})$ *contains a nontrivial* 3*-regular subgraph.*

See [AFK2] and [MoZi] for further similar results. The additional edge e_0 in our version is necessary as the example of a triangle with doubled edges shows.

We give a comprehensive proof in order to outline the principles:

Proof. Of course, the empty graph $(\varnothing, \varnothing)$ is a (trivial) 3-regular subgraph. So there is one "solution," and we just have to show that there is not exactly one "solution." This is where Corollary 3.5 comes in. Systems of polynomials of low degree do not have exactly one common zero. Thus, if the 3-regular subgraphs correspond to the common zeros of such a system of polynomials we know that there has to be a second (nontrivial) "solution."

The subgraphs without isolated vertices can be identified with the subsets S of the set of all edges $\bar{E} := E \uplus \{e_0\}$. Now, an edge $e \in \bar{E}$ may or may not lie in a subgraph $S \subseteq \bar{E}$. We represent these two possibilities by the numbers 1 and 0 in $\mathfrak{X}_e := \{0, 1\}$ (the first step in the algebraization), we define

$$\chi(S) := \big(?_{(e \in S)}\big)_{e \in \bar{E}} \in \mathfrak{X} := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}} \ . \tag{48}$$

With this representation, the subgraphs S correspond to the points $x = (x_e)$

of the Boolean grid $\mathfrak{X} := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}}$; and it is easy to see that the polynomials

$$P_v := \sum_{e \ni v} X_e \in \mathbb{F}_3[\, X_e \mid e \in \bar{E}\,] \quad \text{for all } v \in V \tag{49}$$

do the job, i.e., they have sufficient low degrees and the common zeros $x \in \mathfrak{X}$ correspond to the 3-regular subgraphs. To see this, we have to check for each vertex $v \in V$ the number $\big|\{\, e \ni v \mid x_e = 1\,\}\big| \leq 5$ of edges e connected to v that are "selected" by a common zero $x \in \mathfrak{X} = \{0,1\}^{\bar{E}}$:

$$P_v(x) = 0 \iff \sum_{e \ni v} x_e = 0 \iff \big|\{\, e \ni v \mid x_e = 1\,\}\big| \in \{0,3\}\ . \tag{50}$$

Furthermore, we have to check the degree condition of Corollary 3.5, and that is where we need the additional edge e_0:

$$(3^1 - 1) \sum_{v \in V} \deg(P_v) = 2|V| = |E| < |\bar{E}| = \Sigma d(\mathfrak{X})\ . \tag{51}$$

By Corollary 3.5, the trivial graph $\varnothing \subseteq \bar{E}$ ($x = 0$) cannot be the only 3-regular subgraph. □

The following simple, geometric result was proven by Alon and Füredi in [AlFü], and answers a question by Komjáth. Our proof uses Corollary 3.4:

Theorem 4.2. *Let $H_1, H_2, \ldots, H_m$ be affine hyperplanes in $\mathbb{F}^n$ ($\mathbb{F}$ a field) that cover all vertices of the unit cube $\mathfrak{X} := \{0,1\}^n$ except one, then $m \geq n$.*

Proof. Let $\sum_{j \in (n]} a_{i,j} X_j = b_i$ be an equation defining H_i, and set

$$P := \prod_{i \in (m]} \sum_{j \in (n]} (a_{i,j} X_j - b_i) \in \mathbb{F}[X_1, \ldots, X_n]\ ; \tag{52}$$

then for points $x = (x_1, \ldots, x_n)$;

$$P(x) \neq 0 \iff \big(\forall\, i \in (m]\colon \sum_{j \in (n]} a_{i,j} x_j \neq b_i\ \big) \iff x \notin \bigcup_{j \in (m]} H_j\ . \tag{53}$$

If we now suppose $m < n$, then it follows that

$$\deg(P) \leq m < n = \Sigma d(\mathfrak{X})\ , \tag{54}$$

and hence,

$$\big|\mathfrak{X} \setminus \textstyle\bigcup_{j \in (m]} H_j\big| = \big|\{\, x \in \mathfrak{X} \mid P(x) \neq 0\,\}\big| \overset{3.4}{\neq} 1\ . \tag{55}$$

This means that there is not one unique uncovered point x in $\mathfrak{X} = \{0,1\}^n$ – $m < n$ hyperplanes are not enough to achieve that. □

Our next example is a classical result of Chevalley and Warning that goes back to a conjecture of Dickson and Artin. There are a lot of different sharpenings to it; see [MSCK], the Corollaries 3.5 and 8.5 and Theorem 9.4 . In the proof of the classical version, presented below, we do not use the Boolean grid $\{0,1\}^n$, as in the last two examples. We also have to use Theorem 3.3 (i) instead of its corollaries. What remains the same from the proof of the closely related Corollary 3.5 is that we have to translate a system of equations into a single inequality:

Theorem 4.3. *Let p be a prime and $P_1, P_2, \ldots, P_m \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$.*

If $\sum_{i\in(m]} \deg(P_i) < n$, then

$$p \;\Big\lfloor\; \big|\{\, x \in \mathbb{F}_{p^k}^n \;\big|\; P_1(x) = \cdots = P_m(x) = 0 \,\}\big| \;\;,$$

and hence the P_i do not have one unique common zero x .

Proof. Define

$$P \;:=\; \prod_{i\in(m]} (1 - P_i^{p^k-1}) \;\; ; \tag{56}$$

then

$$P(x) \;=\; \begin{cases} 1 & \text{if } P_1(x) = \cdots = P_m(x) = 0\,, \\ 0 & \text{otherwise} \end{cases} \qquad \text{for all } x \in F_{p^k}{}^n, \tag{57}$$

thus, with $\mathfrak{X} := \mathbb{F}_{p^k}^n$,

$$\Big|\Big\{x \in \mathbb{F}_{p^k}^n \;\Big|\; P_1(x) = \cdots = P_m(x) = 0\Big\}\Big| \cdot 1 \;=\; \sum_{x\in\mathfrak{X}} P(x) \overset{3.3}{\underset{1.4}{=}} (-1)^n\,(P)_{d(\mathfrak{X})} \overset{(59)}{=} 0 \;\;, \tag{58}$$

where the last two equalities hold as

$$\deg(P) \;\le\; (p^k-1) \sum_{i\in(m]} \deg(P_i) \;<\; (p^k-1)\,n \;=\; \Sigma d(\mathfrak{X}) \;\; . \tag{59}$$

□

The Cauchy-Davenport Theorem is another classical result. It was first proven by Cauchy in 1813, and has many applications in additive number theory. The proof of this result is as simple as the last ones, but here we use the coefficient formula 3.3 (i) in the other direction – we know the polynomial map $P|_{\mathfrak{X}}$, and use it to determine the coefficient P_d :

Theorem 4.4. *If p is a prime, and A and B are two nonempty subsets of $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$, then*

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

Proof. We assume $|A+B| \leq |A|+|B|-2$, and must prove $|A+B| \geq p$.

Define

$$P := \prod_{c\in A+B} (X_1+X_2-c) \in \mathbb{Z}_p[X_1,X_2]\ , \tag{60}$$

set

$$\mathfrak{X}_1 := A\ , \tag{61}$$

and choose a subset

$$\varnothing \neq \mathfrak{X}_2 \subseteq B \tag{62}$$

of size

$$|\mathfrak{X}_2| = |A+B|-|A|+2 \quad (\ \leq |B|\ )\ . \tag{63}$$

Now

$$P|_{\mathfrak{X}_1\times\mathfrak{X}_2} \equiv 0\ , \tag{64}$$

and

$$\deg(P) = |A+B| = |\mathfrak{X}_1|+|\mathfrak{X}_2|-2 = d_1(\mathfrak{X}_1)+d_2(\mathfrak{X}_2)\ , \tag{65}$$

so that

$$\tbinom{|A+B|}{d_1}\cdot 1 = P_{(d_1,|A+B|-d_1)} = P_d \overset{3.3}{=} \sum_{x\in\mathfrak{X}_1\times\mathfrak{X}_2} 0 = 0 \in \mathbb{Z}_p\ . \tag{66}$$

Hence

$$p \bigm\lfloor \tbinom{|A+B|}{d_1}\ , \tag{67}$$

and it follows that

$$|A+B| \geq p\ . \tag{68}$$

□

There are some further number-theoretic applications, for example, Erdős, Ginzburg and Ziv's Theorem, which also can be found in [Al2].

5 The matrix polynomial – another application

In this section we apply our results to the matrix polynomial $\Pi(AX)$, a generalization of the graph polynomial (see also [AlTa2] or [Ya]).

We always assume $A = (a_{i,j}) \in \mathcal{R}^{m\times n}$, and the product of this matrix with the tuple $X := (X_1, \ldots, X_n) \in \mathcal{R}[X]^n$ is $AX := (\sum_{j\in(m]} a_{ij}X_j)_{i\in(n]}$. Now, $\Pi(AX)$ is defined in accordance with the definition of Π in Section 1, as follows: $A,\ X$ AX

Definition 5.1 (Matrix polynomial)**.** The *matrix polynomial* to the matrix $A = (a_{i,j}) \in \mathcal{R}^{m\times n}$ is given by $\Pi(AX)$

$$\Pi(AX) \ := \ \prod_{i\in(n]} \sum_{j\in(m]} a_{ij}X_j \ \in \mathcal{R}[X] \ .$$

It turns out that the coefficients of the matrix polynomial are some kind of permanents:

Definition 5.2 (δ-permanent)**.** For $\delta \in \mathbb{N}^n$ we define the *δ-permanent* of $A = (a_{i,j}) \in \mathcal{R}^{m\times n}$ through $\mathrm{per}_\delta(A)$

$$\mathrm{per}_\delta(A) \ := \sum_{\substack{\sigma:\ (m]\to(n] \\ |\sigma^{-1}|=\delta}} \pi_A(\sigma) \ ,$$

where $\pi_A(\sigma)$

$$\pi_A(\sigma) \ := \prod_{i\in(n]} a_{i,\sigma(i)} \quad \text{and} \quad |\sigma^{-1}| \ := \ \big(|\sigma^{-1}(j)|\big)_{j\in(n]} \ . \qquad |\sigma^{-1}|$$

Obviously, $\mathrm{per}_\delta(A) = 0$ if $\Sigma\delta \neq m$. If $m = n$ then $\mathrm{per} := \mathrm{per}_{(1,1,\ldots,1)}$ is the usual permanent; and, in the general situation, it is easy to see that per

$$\big(\textstyle\prod_{j\in(n]} \delta_j!\big)\ \mathrm{per}_\delta(A) \ = \ \mathrm{per}(A\langle|\delta\rangle), \tag{69}$$

where $A\langle|\delta\rangle$ is a matrix that contains the j^{th} column of A exactly δ_j times. But note that $\mathrm{per}_\delta(A)$ is, in general, not determined by $\mathrm{per}(A\langle|\delta\rangle)$. If, for example, $(\prod_{j\in(n]} \delta_j!)\, 1 = 0$ in $\mathcal{R}$, the δ-permanent $\mathrm{per}_\delta(A)$ may take arbitrary values, while $\mathrm{per}(A\langle|\delta\rangle) = 0$. $A\langle|\delta\rangle$

As an immediate consequence of the definitions, we have

Lemma 5.3.

$$\boxed{\Pi(AX) \ = \ \textstyle\sum_{\delta\in\mathbb{N}^n} \mathrm{per}_\delta(A)\, X^\delta} \ .$$

The next theorem now easily follows from our main result, Theorem 3.3 . It is an integrative generalization of Alon's Permanent Lemma [Al2, Section 8], and of Ryser's permanent formula [BrRy, p.200], which follow as the special cases:

- $m = n\,,\ d = (1, 1, \ldots, 1)$ *of the following 5.4 (ii) over fields,*
- $m = n\,,\ d = (1, 1, \ldots, 1)\,,\ \mathfrak{X} = \{0, 1\}^n\,,\ b = (0, 0, \ldots, 0)$ *of 5.4 (i) over fields.*

We already proved a slightly weaker version for $\mathfrak{X} \subseteq \mathbb{N}^n \subseteq \mathcal{R}^n$ in [Scha, 1.14 & 1.15]. This proof was based on Ryser's formula, and is a little more technical. [Scha, 1.10] is the special case $\mathfrak{X} = [d] \subseteq \mathbb{N}^n \subseteq \mathcal{R}^n$, but you will have to use $1.4\,(v)$ to see this. For some additional tricks over fields of characteristic $p > 0$, see [DeV]. We have:

A **Theorem 5.4** (Permanent formula)**.** *Suppose* $A = (a_{ij}) \in \mathcal{R}^{m\times n}$ *and* $b = (b_i) \in \mathcal{R}^m$ *are given, and let* $\mathfrak{X} \subseteq \mathcal{R}^n$ *be an integral d-grid. If* $m \leq \Sigma d$ *, then*

(i) $\boxed{\operatorname{per}_d(A) \;=\; \sum\nolimits_{x\in\mathfrak{X}} N(x)^{-1}\,\Pi(Ax - b)}$, *and*

(ii) $\boxed{\operatorname{per}_d(A) \neq 0 \quad\Longrightarrow\quad \exists\, x \in \mathfrak{X}\colon\ (Ax)_1 \neq b_1\,,\ \ldots\,,\ (Ax)_m \neq b_m}$.

Proof. Part (i) follows from Theorem 3.3, as $\deg\big(\Pi(AX - b)\big) = m \leq \Sigma d$, and $\big(\Pi(AX - b)\big)_d = \big(\Pi(AX)\big)_d \overset{5.3}{=} \operatorname{per}_d(A)$. Part (ii) is a simple consequence of part (i). □

We call an element $x \in \mathcal{R}^m$ with $(Ax)_1 \neq 0\,,\ \ldots\,,\ (Ax)_m \neq 0$ a
σ (correct) *coloring* of A , and a map $\sigma\colon [m] \longrightarrow [n]$ with $\pi_A(\sigma) \neq 0$ and $|\sigma^{-1}| = \delta$ is a *δ-orientation* of A . With this terminology, Theorem 5.4 describes a connection between the orientations and the colorings of A , and it is not too difficult to see that this is a sharpening and a generalization of Alon and Tarsi's Theorem about colorings and orientations of graphs in [AlTa]. That is because, in virtue of the embedding $\vec{G} \longmapsto A(\vec{G})$ described in (70) below, oriented graphs form a subset of the set of matrices, if $-1 \neq 1$ in $\mathcal{R}$. The resulting sharpening 5.5 of the Alon-Tarsi Theorem contains Scheim's formula for the number of edge r-colorings of a planar r-regular graph as a permanent and Ellingham and Goddyn's partial solution of the list coloring conjecture. We briefly elaborate on this; for even more detail, see [Scha], where we described this for grids $\mathfrak{X} \subseteq \mathbb{N}^n \subseteq \mathcal{R}^n$, and where we pointed out

that many other graph-theoretic theorems may be formulated for matrices, too.

Let $\vec{G} = (V, E, \rightarrow, \leftarrow)$ be a *oriented multigraph* with *vertex set* V, *edge set* E and *defining orientations* $\rightarrow\colon E \longrightarrow V$, $e \longmapsto e^{\rightarrow}$ and $\leftarrow\colon e \longmapsto e^{\leftarrow}$. $\vec{G}$ shall be *loopless*, so that $e^{\rightarrow} \neq e^{\leftarrow}$ for all $e \in E$. We write $v \in e$ instead of $v \in \{e^{\rightarrow}, e^{\leftarrow}\}$ and define the *incidence matrix* $A(\vec{G})$ of $\vec{G}$ by

$\vec{G}$, $e^{\rightarrow}$ — $\rightarrow$, $\leftarrow$ — $v \in e$ — $A(\vec{G})$

$$A(\vec{G}) := (a_{e,v}) \in \mathcal{R}^{E\times V}, \text{ where } a_{e,v} := ?_{(e^{\rightarrow}=v)} - ?_{(e^{\leftarrow}=v)} \in \{-1, 0, 1\} \ . \quad (70)$$

With this definition, the *orientations* $\sigma\colon E \ni e \longmapsto e^{\sigma} \in e$ and the *colorings* $x\colon V \longrightarrow \mathcal{R}$ of $\vec{G}$ are exactly the orientations and the colorings of $A(\vec{G})$ as defined above. The orientations σ of $A(\vec{G})$ have the special property $\pi_{A(\vec{G})}(\sigma) = \pm 1$. According to this, we say that an orientation σ of $\vec{G}$ is *even/odd* if $e^{\sigma} \neq e^{\rightarrow}$ (i.e., $e^{\sigma} = e^{\leftarrow}$) holds for even/odd many edges $e \in E$. We write $DE_\delta \,/\, DO_\delta$ for the set of even/odd orientations σ of $\vec{G}$ with $|\sigma^{-1}| = \delta \in \mathbb{N}^V$. With this notation we have:

DE_δ — DO_δ

Corollary 5.5. *Let $\vec{G} = (V, E, \rightarrow, \leftarrow)$ be a loopless, directed multigraph and $\mathfrak{X} \subseteq \mathcal{R}^V$ be an integral d-grid; where $d = (d_v) \in \mathbb{N}^V$, and $d_v = |\mathfrak{X}_v| - 1$ for all $v \in V$. If $|E| \leq \Sigma d$, then*

(i) $$|DE_d| - |DO_d| \ = \ \mathrm{per}_d(A(\vec{G})) \ = \ \sum\nolimits_{x\in\mathfrak{X}} N(x)^{-1} \prod\nolimits_{e\in E} \big(x_{e^{\rightarrow}} - x_{e^{\leftarrow}}\big) \ ,$$

(ii) $$|DE_d| \neq |DO_d| \implies \exists\, x \in \mathfrak{X}\colon \forall\, e \in E\colon \ x_{e^{\rightarrow}} \neq x_{e^{\leftarrow}} \ (x \text{ is coloring}).$$

Furthermore, it is not so hard to see that, if $EE \,/\, EO$ is the set of even/odd Eulerian subgraphs of $\vec{G}$, and $\delta := |{\rightarrow}^{-1}|$, we have $|DE_\delta| = |EE|$ and $|DO_\delta| = |EO|$; see also [Scha, 2.6].

EE, EO

Note that even though Corollary 5.5 looks a little simpler than [Scha, 1.14 & 2.4], there is some complexity hidden in the symbol $N(x)$. If the "lists" $\mathfrak{X}_v$ ($\mathfrak{X} = \prod_{v\in V} \mathfrak{X}_v$) are all equal, this becomes less complex. Further, if the graph $\vec{G}$ is the line graph of a r-regular graph, so that its vertex colorings are the edge colorings of the r-regular graph, then the whole right side becomes very simple. The summands are then – up to a constant factor – equal to ± 1; or to 0, if $x = (x_v)_{v\in V}$ is not a correct coloring. The corresponding specialization of equation 5.5 (i) was already obtained in [ElGo] and [Sch].

If in addition $\vec{G}$ is planar this formula becomes even simpler, so that the whole right side is – up to a constant factor – the number of edge r-colorings of the r-regular graph. Scheim [Sch] proved this specialization in his approach to the four color problem for 3-regular graphs using a result of Vigneron [Vig].

However, with Ellingham and Goddyn's generalization [ElGo, Theorem 3.1] of Vigneron's result, this specialization also follows in the r-regular case.

As the left side of our equation does not depend on the choice of the d-grid $\mathfrak{X}$, the right side does not depend on it, either. In our special case, where the right side is the number of r-colorings of the line graph of a planar r-regular graph, this means that if there are colorings to equal lists $\mathfrak{X}_v$ of size r (e.g., $\mathfrak{X} = [r)^V$), then there are also colorings to arbitrary lists $\mathfrak{X}_v$ of size $|\mathfrak{X}_v| = r$ – which is just Ellingham and Goddyn's confirmation of the list coloring conjecture for planar r-regular edge r-colorable multigraphs [ElGo].

6 Algebraic solvable existence problems: Describing polynomials as equivalent to explicit solutions

In this section we describe a general working frame to Theorem 3.3 (*ii*) and Corollary 3.4, as it may be used in existence proofs, such as those of 3.5, 4.2 or 5.4 (*ii*) . We call the polynomials defined in the equations (44) and (52) or the matrix polynomial $\Pi(AX)$ in our last example, algebraic solutions, and show that such algebraic solutions may be seen as equivalent to explicit solutions. We show that the existence of algebraic solutions, and of nontrivial explicit solutions are equivalent. To make this more exact, we have to introduce some definitions. Our definition of problems should not merely reflect common usage. In fact, the generality gained through an exaggerated extension of the term "problem" through abstraction is desirable.

Definition 6.1 (Problem)**.** A *problem* $\mathcal{P}$ is a pair $(\mathcal{S}, \mathcal{S}_{\text{triv}})$ consisting of a set $\mathcal{S}$, which we call its set of *solutions*; and a subset $\mathcal{S}_{\text{triv}} \subseteq \mathcal{S}$, which we call its set of *trivial solutions*. $\mathcal{P}$ $(\mathcal{S}, \mathcal{S}_{\text{triv}})$

In example 4.1, the set of solutions $\mathcal{S}$ consists of the 3-regular subgraphs and $\mathcal{S}_{\text{triv}} = \{(\varnothing, \varnothing)\}$. These are exact definitions, but it does not mean that we know if there are nontrivial solutions, i.e., if $\mathcal{S} \neq \mathcal{S}_{\text{triv}}$. The set $\mathcal{S}$ is well defined, but we do not know what it looks like; indeed, that is the actual problem.

To apply our theory about polynomials in such general situations, we have to bring in grids $\mathfrak{X}$ in some way. For that, we define impressions:

Definition 6.2 (Impression)**.** A triple $(\mathcal{R}, \mathfrak{X}, \chi)$ is a *impression* of $\mathcal{P}$ if $\mathcal{R}$ is a commutative ring with $1 \neq 0$, if $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathcal{R}^n$ is a finite integral grid (for some $n \in \mathbb{N}$) and if $\chi \colon \mathcal{S} \longrightarrow \mathfrak{X}$ is a map. $(\mathcal{R}, \mathfrak{X}, \chi)$

As the set $\mathcal{S}$ of solutions is usually unknown, one may ask how the map $\chi \colon \mathcal{S} \longrightarrow \mathfrak{X}$ can be defined. The answer is that we usually, define χ on a bigger domain at first, as in Equation (48) in example 4.1 . Then the unknown set of solutions $\mathcal{S}$ (more precisely, its image $\chi(\mathcal{S})$) is indirectly described:

Definition 6.3 (Describing polynomial)**.** A polynomial $P \in \mathcal{R}[X_1, \ldots, X_n]$ is a *describing polynomial* of $\mathcal{P}$ over $(\mathcal{R}, \mathfrak{X}, \chi)$ if

$$\chi(\mathcal{S}) \;=\; \operatorname{supp}(P|_{\mathfrak{X}}) \;.$$

The diagram (5) in the introduction shows a schematic illustration of our concept in the case $\mathcal{S}_{\text{triv}} = \varnothing$. The next question is how it might be possible to reveal the existence of nontrivial solutions using some knowledge about a describing polynomial P, and how to find such an appropriate P. In view of our results from Section 3, we give the following definition:

Definition 6.4 (Algebraic solutions)**.** A describing polynomial P is an *algebraic solution* (over $(\mathcal{R}, \mathfrak{X}, \chi)$) of a problem of the form $\mathcal{P} = (\mathcal{S}, \varnothing)$ if it fulfills

$$deg(P) \leq \Sigma d(\mathfrak{X}) \qquad \text{and} \qquad P_{d(\mathfrak{X})} \neq 0 \ .$$

It is an *algebraic solution* of a problem $\mathcal{P} = (\mathcal{S}, \mathcal{S}_{\text{triv}})$ with $\mathcal{S}_{\text{triv}} \neq \varnothing$ if it fulfills

$$\deg(P) < \Sigma d(\mathfrak{X}) \quad \text{and} \quad \sum_{x \in \chi(\mathcal{S}_{\text{triv}})} N(x)^{-1} P(x) \neq 0 \quad (\text{e.g., if } |\chi(\mathcal{S}_{\text{triv}})| = 1\,).$$

The bad news is that now, we do not have a general recipe for how to find algebraic solutions that indicate the solvability of problems. However, we have seen that there are several combinatorial problems that are algebraically solvable in an obvious way. The construction of algebraic solutions in these examples follows more or less the same simple pattern, and that constructive approach is the big advantage. Algebraic solutions are easy to construct if the problem is not too complex in the sense that the construction does not require too many multiplications. In many cases algebraic solutions can be formulated for whole classes of problems, e.g., for all extended 4-regular graphs in example 4.1, where the final algebraic solution was hidden in Corollary 3.5; however, we may have no idea about how explicit solutions (for whole classes of problems) can be found or presented.

If an algebraic solution is found, we can apply Theorem 3.3 , Corollary 3.4 or the following theorem, which also shows that algebraic solutions always exist, provided there are nontrivial solutions in the first place.

Theorem 6.5. *Let $\mathcal{P} = (\mathcal{S}, \mathcal{S}_{\text{triv}})$ be a problem. The following properties are equivalent:*

(i) There exists a nontrivial solution of $\mathcal{P}$; i.e., $\mathcal{S} \neq \mathcal{S}_{\text{triv}}$.

(ii) There exists an algebraic solution of $\mathcal{P}$ over an impression $(\mathcal{R}, \mathfrak{X}, \chi)$.

(iii) There exist algebraic solutions of $\mathcal{P}$ over each impression $(\mathcal{R}, \mathfrak{X}, \chi)$ that fulfills either

– $|\mathcal{R}| > 2$ *and* $\mathcal{S} \neq \mathcal{S}_{\text{triv}} \Rightarrow \chi(\mathcal{S}) \neq \chi(\mathcal{S}_{\text{triv}})$
(e.g., if χ is injective or if $\mathcal{S}_{\text{triv}} = \varnothing$); or

– $|\mathcal{R}| = 2$ *and* $|\chi(\mathcal{S})| + 1 \equiv |\chi(\mathcal{S}_{\text{triv}})| \equiv ?_{(\mathcal{S}_{\text{triv}} \neq \varnothing)} \pmod 2$.

Proof. First, assume (ii), and let P be an algebraic solution. We want to show that (i) holds. For $\mathcal{S}_{\text{triv}} = \varnothing$, this follows from Theorem 3.3 (ii). For $\mathcal{S}_{\text{triv}} \neq \varnothing$, we have

$$0 \;=\; P_d \overset{3.3}{=} \Sigma(N^{-1}P|_{\mathfrak{X}}) \;=\; \sum_{x \in \chi(\mathcal{S}_{\text{triv}})} N(x)^{-1}P(x) \;+\; \sum_{x \in \chi(\mathcal{S}) \setminus \chi(\mathcal{S}_{\text{triv}})} N(x)^{-1}P(x) \;, \tag{71}$$

where the first sum over $\chi(\mathcal{S}_{\text{triv}})$ does not vanish. Hence, the second sum over the set $\chi(\mathcal{S}) \setminus \chi(\mathcal{S}_{\text{triv}})$ does not vanish, either. Thus $\chi(\mathcal{S}) \setminus \chi(\mathcal{S}_{\text{triv}}) \neq \varnothing$, and $\mathcal{S} \neq \mathcal{S}_{\text{triv}}$ follows.

To prove $(i) \Longrightarrow (iii)$ for $\mathcal{S}_{\text{triv}} = \varnothing$, assume (i), and define a map $y\colon \mathfrak{X} \longrightarrow \mathcal{R}$ such that $\operatorname{supp}(y) = \chi(\mathcal{S})$ and $\Sigma y \neq 0$. (In the case $|\mathcal{R}| = 2$, we need $|\chi(\mathcal{S})| \equiv 1 \pmod 2$ to make this possible.) The interpolation polynomial $P := (\Psi y)(X)$ to the map Ny described in Theorem 2.2 now has degree $deg(P) \leq \Sigma d$, and fulfills

$$\operatorname{supp}(P|_{\mathfrak{X}}) \overset{2.2}{=} \operatorname{supp}(y) \;=\; \chi(\mathcal{S}) \tag{72}$$

and

$$P_d \overset{3.3}{=} \Sigma(N^{-1}P|_{\mathfrak{X}}) \overset{2.2}{=} \Sigma y \;\neq\; 0 \;. \tag{73}$$

To prove $(i) \Longrightarrow (iii)$ for $\mathcal{S}_{\text{triv}} \neq \varnothing$, assume (i), and define a map $y\colon \mathfrak{X} \longrightarrow \mathcal{R}$ such that $\operatorname{supp}(y) = \chi(\mathcal{S})$, $\sum_{x \in \chi(\mathcal{S}_{\text{triv}})} y(x) \neq 0$ and $\Sigma y = 0$. (In the case $|\mathcal{R}| = 2$, we need $|\chi(\mathcal{S})| + 1 \equiv |\chi(\mathcal{S}_{\text{triv}})| \equiv 1 \pmod 2$ to make this possible.) Now, the polynomial $P := (\Psi y)(X)$ has partial degrees $\deg_j(P) \leq d_j$, and total degree $deg(P) < \Sigma d$, as

$$P_d \overset{3.3}{=} \Sigma(N^{-1}P|_{\mathfrak{X}}) \overset{2.2}{=} \Sigma y \;=\; 0 \;. \tag{74}$$

It satisfies

$$\operatorname{supp}(P|_{\mathfrak{X}}) \overset{2.2}{=} \operatorname{supp}(y) \;=\; \chi(\mathcal{S}) \tag{75}$$

and

$$\sum_{x \in \chi(\mathcal{S}_{\text{triv}})} N(x)^{-1}P(x) \overset{2.2}{=} \sum_{x \in \chi(\mathcal{S}_{\text{triv}})} y \;\neq\; 0 \;. \tag{76}$$

Finally, to show $(iii) \Longrightarrow (ii)$, we only have to prove that there exists an impression $(\mathcal{R}, \mathfrak{X}, \chi)$ as described in (iii). This is clear, as we may define χ

by setting

$$\chi(s) := \begin{cases} x_{\text{triv}} & \text{for } s \in \mathcal{S}_{\text{triv}} \,, \\ x_{\text{good}} & \text{for } s \in \mathcal{S} \setminus \mathcal{S}_{\text{triv}} \,, \end{cases} \tag{77}$$

where x_{triv} and x_{good} are two distinct, arbitrary elements in some suitable grid $\mathfrak{X}$. □

The arguments in this proof also show that the restrictions to the impression $(\mathcal{R}, \mathfrak{X}, \chi)$ in part (iii) are really necessary. If, for example, we had $|\mathcal{R}| = 2$, $\mathcal{S}_{\text{triv}} = \varnothing$ and $|\chi(\mathcal{S})| \equiv 0 \pmod 2$, then $P_d = 0$, and the problem would not be algebraically solvable with respect to the impression $(\mathcal{R}, \mathfrak{X}, \chi)$.

7 The Combinatorial Nullstellensatz or how to modify polynomials

In this section, we describe a sharpening of a specialization of Hilbert's Nullstellensatz (see e.g. [DuFo]), the so-called (first) Combinatorial Nullstellensatz. This theorem, and the modification methods behind it, can be used in another proof of the coefficient formulas in Section 3.

We start with an example that illustrates the underlying modification method of this section. It also shows that the coefficient P_d in Theorem 3.3 is, in general, the only coefficient that is uniquely determined by $P|_{\mathfrak{X}}$:

Example 7.1. Let $P \in \mathbb{C}[X_1, X_2]$ (i.e., $\mathcal{R} := \mathbb{C}$ and $n := 2$), and define for $j = 1, 2$:

$$L_j \;:=\; \frac{X_j^5 - 1}{X_j - 1} \;=\; X_j^4 + X_j^3 + X_j^2 + X_j^1 + X_j^0 \;, \tag{78}$$

$$\mathfrak{X}_j \;:=\; \{x \in \mathbb{C} \mid L_j(x) = 0\} \;=\; \{x_1, x_2, x_3, x_4\} \;, \quad \text{where } x_k := e^{\frac{k}{5} 2\pi\sqrt{-1}} \;. \tag{79}$$

Then $d = d(\mathfrak{X}) = (3, 3)$. Now, for $\varepsilon \in \mathbb{N}^2$, the polynomial $X^\varepsilon L_1$ (and $X^\varepsilon L_2$) vanishes on $\mathfrak{X}$. Therefore, the modified polynomial

$$P' \;:=\; P + c\, X^\varepsilon L_1 \;, \quad \text{where} \quad c \in \mathcal{R}\backslash 0 \;, \tag{80}$$

fulfills

$$P'|_{\mathfrak{X}} \;=\; P|_{\mathfrak{X}} \;; \tag{81}$$

but the coefficients $P_{\varepsilon+(0,0)}$, $P_{\varepsilon+(1,0)}$, $P_{\varepsilon+(2,0)}$, $P_{\varepsilon+(3,0)}$ and $P_{\varepsilon+(4,0)}$ have changed:

$$P'_{\varepsilon+(i,0)} \;=\; P_{\varepsilon+(i,0)} + c \;\neq\; P_{\varepsilon+(i,0)} \quad \text{for} \quad i = 0, 1, 2, 3, 4 \;. \tag{82}$$

In this way we may modify P without changing the map $P|_{\mathfrak{X}}$.

Now, suppose $\deg(P) \leq \Sigma d = 3 + 3$. Figure 2 illustrates that all coefficients P_δ with $\delta \leq \Sigma d$ – except P_d – can be modified without losing the condition $\deg P \leq \Sigma d$, so that they are not uniquely determined by $P|_{\mathfrak{X}}$. If we try to modify $P_d = P_{(3,3)}$ – for example, by adding $c\, X^{(0,3)} L_1$ (or $c\, X^{(3,0)} L_2$) – we realize that

$$\deg(X^{(0,3)} L_1) \;=\; \deg(X^{(0,7)}) \;=\; 7 \;>\; 3 + 3 \;=\; \Sigma d \;, \tag{83}$$

and $\deg(P') > \Sigma d$ would follow. The coefficient P_d cannot be modified in this way.

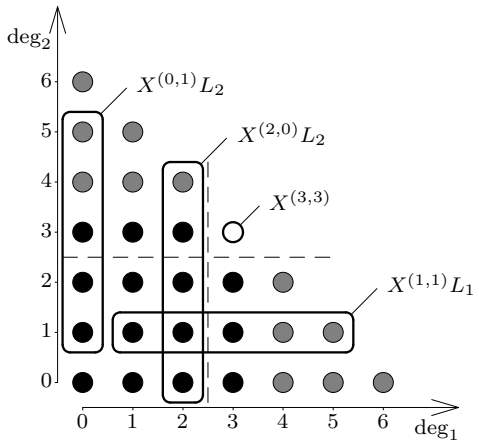


Figure 2: Monomials of degree $\leq 3+3$.

This example can also be used to illustrate a second proof of Theorem 3.3 (and Theorem 3.2):

L_j By successive modifications, as above, with

$$L_j = L_{\mathfrak{X}_j}(X_j) := \prod_{\hat{x}\in\mathfrak{X}_j} (X_j - \hat{x}) \tag{84}$$

in the general case, it is possible to wrangle P into a *trimmed* polynomial $P/\mathfrak{X}$ with the properties

$P/\mathfrak{X}$

$$P/\mathfrak{X}|_{\mathfrak{X}} = P|_{\mathfrak{X}} \qquad \text{and} \qquad \deg_j(P/\mathfrak{X}) \leq d_j \quad \text{for } j = 1,\ldots,n\,. \tag{85}$$

By 2.7(v), $P/\mathfrak{X}$ is uniquely determined if $\mathfrak{X}$ is an integral d-grid (e.g., $P/\{x\} = P(x)$). If $\deg(P) \leq \Sigma d$, then it is obviously possible to leave the coefficient P_d unchanged during the modification[2]. Therefore we get

$$P_d = (P/\mathfrak{X})_d \overset{2.8}{=} (\Psi(N^{-1}P/\mathfrak{X}|_{\mathfrak{X}}))_d = (\Psi(N^{-1}P|_{\mathfrak{X}}))_d \overset{(9)}{=} \Sigma(N^{-1}P|_{\mathfrak{X}}) \;; \tag{86}$$

and Theorem 3.3 follows immediately.

Theorem 3.2 can also be proven the same way by using the following, obvious generalization (Lemma 7.2) of the first equation in (86). Furthermore, we want to mention at this point that the proof above (and the following lemma) may work for some other coefficients P_δ as well if the $L_j = L_{\mathfrak{X}_j}(X_j)$

[2]At this point the degree restriction $\deg(P) \leq \Sigma d$ may be weakened slightly if the grid $\mathfrak{X}$ – and hence the L_j – have a special structure. If, e.g., $L_j = X_j^{k+1} - 1$ (or $L_j = X_j^{k+1} - X_j$) for all $j \in (n]$, then $\deg(P) \leq \Sigma d + k$ $[= (n+1)k]$ (respectively $\deg(P) \leq \Sigma d + k - 1$) suffices.

have a special structure, e.g., $L_j = X^{d_j} - 1$. Of course it works for P_0 if $0 = (0, \ldots, 0) \in \mathfrak{X}$, since all L_j lack a constant term in this case. Without further information about the grid $\mathfrak{X}$, we "carry through" only the d-leading coefficients:

Lemma 7.2. *Let $\mathfrak{X}$ be a d-grid. For each polynomial $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathcal{R}[X]$ with d-leading multiindex $\varepsilon \leq d \in \mathbb{N}^n$ (e.g., if $\Sigma\varepsilon = \deg(P)$),*

$$\boxed{(P/\mathfrak{X})_\varepsilon = P_\varepsilon} \ .$$

If we take a closer look at the modification methods above, we see that the difference $P - P/\mathfrak{X}$ can be written as

$$P - P/\mathfrak{X} \ = \ \sum_{j \in (n]} H_j L_j \ , \tag{87}$$

with some $H_j \in \mathcal{R}[X]$ of degree $\deg(H_j) \leq \deg(P) - \deg(L_j)$.

If $P|_{\mathfrak{X}} \equiv 0$, then $P/\mathfrak{X} = 0$ by the uniqueness of the trimmed polynomial, and (87) yields $P = \sum_{j \in (n]} H_j L_j$. This was proven for integral rings in [Al2, Theorem 1.1]. More formally, we have:

Theorem 7.3 (Combinatorial Nullstellensatz)**.** *Let $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \mathcal{R}^n$ be an integral grid with associated polynomials $L_j := \prod_{\hat{x} \in \mathfrak{X}_j} (X_j - \hat{x})$.*
For any polynomial $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathcal{R}[X]$, the following are equivalent:

(i) $P|_{\mathfrak{X}} \equiv 0$.

(ii) $P/\mathfrak{X} = 0$.

(iii) $P = \sum_{j \in (n]} H_j L_j \in \mathcal{R}[X]$
for some polynomials H_j over a ring extension of $\mathcal{R}$.

(iv) $P = \sum_{j \in (n]} H_j L_j$
for some $H_j \in \mathcal{R}[X]$ of degree $\deg(H_j) \leq \deg(P) - |\mathfrak{X}_j|$.

Proof. We already have seen that the implications $(i) \Longrightarrow (ii) \Longrightarrow (iv)$ hold; and the implications $(iv) \Longrightarrow (iii) \Longrightarrow (i)$ are trivial. □

The implication " $(i) \Longrightarrow (iv)$ " states that polynomials P with $P|_{\mathfrak{X}} \equiv 0$ may be written as $\sum_{j\in(n]} H_j L_j$. In other words, P lies in the ideal spanned by the polynomials L_j . As we do not know *a priori* that this ideal is a radical ideal, Hilbert's Nullstellensatz would only provide $P^k = \sum_{j\in(n]} H_j L_j$ for some $k \geq 1$, and without degree restrictions for the H_j (provided $\mathcal{R}$ is an algebraically closed field). Alon suggested calling the stronger (with respect to the special polynomials L_j) result "Combinatorial Nullstellensatz." He used it to prove the implication (ii) in the coefficient formula 3.3 [Al2, Theorem 1.2] and recycled the phrase "Combinatorial Nullstellensatz" for the implication 3.3 (ii).

8 A sharpening of Warning's Theorem – a further application

In this section, we investigate the distribution of the different possible values of polynomial maps $x \longmapsto P(x)$ on the grid $\mathfrak{X} := \mathbb{F}_p^n$ by using affine linear subspaces $v + U$ of $\mathfrak{X}$ considered as a vector space over $\mathbb{F}_p$ (Theorem 8.4). This leads to a sharpening (Corollary 8.5) of Warning's classical result [Schm] about the number of simultaneous zeros of systems of polynomial equations over finite fields. We formulated this, and the other results of this section, for prime fields $\mathbb{F}_p$; but they may also be applied to arbitrary finite fields $\mathbb{F}_{p^k}$ by using Lemma 8.6. $v + U$

We will use the notation $P/\mathfrak{X}$ of (85) in Section 7 for the trimmed polynomial; and the notation per_δ for the δ-permanent, defined in 5.2. We know that for matrices $A = (a_{i,j}) \in \mathcal{R}^{m\times n}$ and for $\delta \in \mathbb{N}^n$, $P/\mathfrak{X}$, per_δ

$$A \;\longmapsto\; \mathrm{per}_\delta(A) := \sum_{\substack{\sigma\colon [m]\to[n] \\ |\sigma^{-1}|=\delta}} \pi_A(\sigma) \quad \text{is multilinear in the rows of } A\,. \tag{88}$$

This is clear because the maps $A \longmapsto \pi_A(\sigma)$ (defined in 5.2) are multilinear. The notation $A\langle k|\rangle$, with $k \in \mathbb{N}$, stands for a matrix that contains each row of A exactly k times. We have some nice roles for the δ-permanent of such matrices with multiple rows: π_A, $A\langle k|\rangle$

Lemma 8.1. *Let $\mathcal{R}$ be an integral ring of characteristic p. For matrices $A = (a_{i,j}) \in \mathcal{R}^{m\times n}$ and tuples $\delta = (\delta_j) \in [p^h)^n$ hold:*

(i) If A contains p^h identical rows, then

$$\mathrm{per}_\delta(A) \;=\; 0\;. \tag{89}$$

(ii) If A' is obtained from A by adding a multiple of one row to another, then

$$\mathrm{per}_\delta(A'\langle p^h - 1|\rangle) \;=\; \mathrm{per}_\delta(A\langle p^h - 1|\rangle)\;. \tag{90}$$

(iii) If $\mathrm{rank}(A) < m$, then

$$\mathrm{per}_\delta(A\langle p^h - 1|\rangle) \;=\; 0\;. \tag{91}$$

Proof. To prove (i), we may suppose that the first p^h rows of A coincide. Let $\tau\colon (m] \to (m]$ be the cyclic permutation of these rows: $\tau = (1, 2, \ldots, p^h)$. For each map $\sigma\colon (m] \to (n]$ with $|\sigma^{-1}| := \big(|\sigma^{-1}(j)|\big)_{j\in(n]} = \delta$, the maps of the form $\sigma \circ \tau^i\colon (m] \to (n]$ also have the property $|\sigma^{-1}| = \delta$, and

$$\pi_A(\sigma') \,=\, \pi_A(\sigma'') \quad \text{for each two } \sigma', \sigma'' \in \bar\sigma \,:=\, \{\, \sigma \circ \tau^i \;\mid\; 0 \le i < p^h \,\}\,. \tag{92}$$

We use this, to partition the summation range in the definition of per_δ, in order to bundle equal summands. As we explain below, for each σ,

$$p \,\big\lfloor\, |\bar\sigma| \;, \quad \text{i.e.,} \quad |\bar\sigma|\, 1 \,=\, 0 \;, \tag{93}$$

and hence

$$\sum_{\sigma'\in\bar\sigma} \pi_A(\sigma') \,=\, 0 \;. \tag{94}$$

It follows that indeed

$$\mathrm{per}_\delta(A) \;:=\; \sum_{\sigma\colon |\sigma^{-1}|=\delta} \pi_A(\sigma) \;=\; \sum_{\bar\sigma\colon |\sigma^{-1}|=\delta} \;\sum_{\sigma'\in\bar\sigma} \pi_A(\sigma') \;=\; \sum_{\bar\sigma\colon |\sigma^{-1}|=\delta} 0 \;=\; 0 \;. \tag{95}$$

The used statement (93) holds, since the least integer $i \ge 1$ with

$$\sigma \circ \tau^i \,=\, \sigma \tag{96}$$

is a multiple of p. Otherwise,

$$1 \,=\, \gcd(i, p^h) \,=\, \alpha i + \beta p^h \quad \text{with some } \alpha, \beta \in \mathbb{Z} \;, \tag{97}$$

and hence

$$\sigma \circ \tau^1 \;=\; \sigma \circ \tau^{\alpha i + \beta p^h} \;=\; \sigma \circ (\tau^i)^\alpha \circ \mathrm{Id}^\beta \overset{(96)}{=} \sigma \;, \tag{98}$$

which would mean that σ is constant on all p^h points of $(p^h]$, i.e.,

$$|\sigma^{-1}(\sigma(1))| \,\ge\, p^h \;, \tag{99}$$

and that contradicts

$$|\sigma^{-1}| = \delta \in [p^h)^n \;. \tag{100}$$

Part (ii) follows through repeated applications of part (i), using the multilinearity (88).

The last part (iii) follows from part (ii) and the well known fact that matrices $A \in \mathbb{F}_p^{m\times n}$ with $\mathrm{rank}(A) < m$ can be transformed by elementary row operations into a matrix with a zero row. □

The following, nontrivial lemma is the basis of the results in this section:

Lemma 8.2. *Let* $\mathcal{R}$ *be an integral ring with* $\mathbb{F}_p \subseteq \mathcal{R}$ *. Assume that* $r \in (n]$ *, and define* $\Delta_r := \{\, \delta \in [p)^n \mid \Sigma\delta = r(p-1) \,\}$ *. To each* $0 \neq \lambda = (\lambda_\delta) \in \mathcal{R}^{\Delta_r}$, Δ_r
there is a matrix $A = (a_{i,j}) \in \mathbb{F}_p^{r \times n}$ *of rank* r *such that*

$$\sum\nolimits_{\delta \in \Delta_r} \lambda_\delta \operatorname{per}_\delta(A\langle p-1|\rangle) \;\neq\; 0 \;\; .$$

Proof. As $\lambda \neq 0$, there is a $d \in \Delta_r$ with

$$\lambda_d \;\neq\; 0 \;\; . \tag{101}$$

Set $j_0 := 1$, and define $j_i \in (n]$ for all $i \in (r]$ as the least number with

$$\sum_{j \in (j_i]} d_j \;\geq\; (p-1)\, i \;\; . \tag{102}$$

Set

$$a''_{i,j} \;:=\; ?_{(j_{i-1} \leq j \leq j_i)} \;\; , \quad A'' := (a''_{i,j})_{\substack{i \in (r] \\ j \in (n]}} \quad \text{and} \quad a''_{i,*} := (a''_{i,j})_{j \in (n]} \in \mathbb{F}_p^{1 \times n} \;\; . \tag{103}$$

We want to show that

$$\operatorname{per}_d(A''\langle p-1|\rangle) \neq 0 \;\; . \tag{104}$$

To see this, realize that there is just one unique partition

$$d \;=\; d^1 + d^2 + \cdots + d^r \tag{105}$$

of the tuple $d = (d_j) \in \Delta_r \subseteq [p)^n$ into tuples $d^i = (d^i_j) \in [p)^n$ with the properties

$$j_{i-1} \;\leq\; \operatorname{supp}(d^i) \;\leq\; j_i \;\; , \tag{106}$$

i.e.,

$$a''_{i,j} \neq 0 \quad \text{for all } j \in \operatorname{supp}(d^i) \;\; , \tag{107}$$

and

$$d^i_1 + d^i_2 + \cdots + d^i_n \;=\; p-1 \;\; . \tag{108}$$

Here, the last equation means that each of the unique $d^i = (d^i_1, \ldots, d^i_n)$ is itself a partition of $p-1$, so that the multinomial coefficients $\binom{p-1}{d^i} := \binom{p-1}{d^i_1, \ldots, d^i_n}$ are well-defined. From the uniqueness of the d^i follows

$$\operatorname{per}_d(A''\langle p-1|\rangle) \;=\; \prod_{i \in (r]} \operatorname{per}_{d^i}\big(a''_{i,*}\langle p-1|\rangle\big) \;=\; \prod_{i \in (r]} \binom{p-1}{d^i} 1 \;\neq\; 0 \;\; , \tag{109}$$

since

$$\binom{p-1}{d^i} \;=\; \tfrac{(p-1)!}{\prod_{j\in(n]}\, d_j^i!} \;\not\equiv\; p \quad \text{for all } \; i \in (r]\,. \tag{110}$$

Now set

$$A' := (a''_{i,j}\, X_j)_{\substack{i\in(r]\\ j\in(n]}} \;\in\; \mathbb{F}_p[X]^{r\times n} \tag{111}$$

and

$$P(X) \;:=\; \sum_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A'\langle p-1|\rangle) \;\in\; \mathbb{F}_p[X]\;. \tag{112}$$

Then

$$\deg(P) \;\leq\; r(p-1) \;=\; \Sigma d \tag{113}$$

and

$$P_d\, X^d \;=\; \lambda_d \operatorname{per}_d(A'\langle p-1|\rangle) \;=\; \lambda_d \operatorname{per}_d(A''\langle p-1|\rangle)\, X^d \;\neq\; 0\;. \tag{114}$$

Hence by Theorem 3.3 (ii), there is a $x \in \mathbb{F}_p^n$ such that, for

$$A := (a''_{i,j}\, x_j) \;\in\; \mathbb{F}_p^{r\times n}\;, \tag{115}$$

it follows that

$$0 \;\neq\; P(x) \;=\; \textstyle\sum_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A\langle p-1|\rangle)\;. \tag{116}$$

In this the matrix A necessarily has rank r by Lemma 8.1 (iii). □

Now we are able to construct our main tool:

Lemma 8.3. *Let $r \in [n]$ and an $\mathbb{F}_p$-subspace $U \leq \mathbb{F}_p^n$ of dimension $\dim(U) = n - r$ be given.*

1_{v+U} *There is a system (in general, not unique) of polynomials $1_{v+U} \in \mathbb{F}_p[X_1,\ldots,X_n]$ – corresponding to the affine subspaces $v+U$ of $\mathbb{F}_p^n$ – such that for each $v \in \mathbb{F}_p^n$:*

(i) $1_{v+U}(x) \;=\; ?_{(x\in v+U)}$ *for all $x \in \mathbb{F}_p^n$; and*

(ii) $\deg(1_{v+U}) \;\leq\; r(p-1)$ *; and*

Δ_r *(iii)* $(1_{v+U})_\delta \;=\; (1_U)_\delta$ *for all $\delta \in \Delta_r := \{\, \delta \in [p)^n \;\mid\; \Sigma\delta = r(p-1)\,\}$.*

Let $0 \neq \lambda = (\lambda_\delta) \in \mathbb{F}_p^{\Delta_r}$; then the subspace U (and the polynomials 1_{v+U}) may be chosen in such a way that, in addition,

(iv) $\textstyle\sum_{\delta\in\Delta_r} \lambda_\delta (1_U)_\delta \;\neq\; 0\,.$

Proof. Let

$$\sum_{j\in(n]} a_{i,j}X_j \;=\; 0 \;\;,\quad i=1,\ldots,r \tag{117}$$

be a system of equations defining U; then the polynomials

$$1_{v+U} \;:=\; \prod_{i\in(r]} \Big(1-\Big(\sum_{j\in(n]}\big(a_{i,j}(X_j-v_j)\big)\Big)^{p-1}\Big) \;\in\; \mathbb{F}_p[X] \tag{118}$$

fulfill the conditions (i), (ii) and (iii).

Part (iv) holds for $r=0$. For $r>0$, we have to find a matrix $A=(a_{i,j})\in\mathbb{F}_p^{r\times n}$ of rank r such that the polynomial $1_U=1_{0+U}$ defined by (118) fulfills the inequality in part (iv); the searched $(n-r)$-dimensional subspace U is then given through Equation (117) using this same matrix A. For $\delta\in\Delta_r$, we have

$$\begin{aligned}(1_U)_\delta \;&=\; (-1)^r\big((\Pi(AX))^{p-1}\big)_\delta \\ &=\; (-1)^r\big(\Pi(A\langle p-1|\rangle X)\big)_\delta \overset{5.3}{=} (-1)^r\operatorname{per}_\delta(A\langle p-1|\rangle)\;\;,\end{aligned} \tag{119}$$

and we thus obtain (iv) if we choose A by Lemma 8.2:

$$\sum_{\delta\in\Delta_r}\lambda_\delta(1_U)_\delta \;=\; (-1)^r\sum_{\delta\in\Delta_r}\lambda_\delta\operatorname{per}_\delta(A\langle p-1|\rangle) \overset{8.2}{\neq} 0\;. \tag{120}$$

□

The following, main result of this section now tells us something about the distribution of the different possible values $P(x)$ of polynomial maps $x\longmapsto P(x)$ on the special grid $\mathfrak{X}:=\mathbb{F}_p^n$. Again, $U\leq\mathbb{F}_p^n$ means that U is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_p^n$. $U\leq\mathbb{F}_p^n$

Theorem 8.4. *Let $\mathcal{R}$ be an integral ring with $\mathbb{F}_p\subseteq\mathcal{R}$. For $\mathfrak{X}:=\mathbb{F}_p^n$ and $P\in\mathcal{R}[X]$ hold:*

(i) If $P|_{\mathfrak{X}}\not\equiv 0$, then there exists a subspace $U\leq\mathbb{F}_p^n$ with
$\dim(U)=\lceil\frac{\deg(P/\mathfrak{X})}{(p-1)}\rceil$ *such that, for all $v\in\mathbb{F}_p^n$,* $\boxed{P|_{v+U}\;\not\equiv\;0\;.}$

(ii) If $P|_{\mathfrak{X}}\not\equiv 0$ and $p-1\,\big\lfloor\,\deg(P/\mathfrak{X})$, then there exists an $U\leq\mathbb{F}_p^n$ with
$\dim(U)=\frac{\deg(P/\mathfrak{X})}{(p-1)}$ *such that* $\boxed{\Sigma(P|_U)\;\neq\;0\;.}$

(iii) For all $U\leq\mathbb{F}_p^n$ with $\dim(U)>\frac{\deg(P/\mathfrak{X})}{(p-1)}$, $\boxed{\Sigma(P|_U)\;=\;0\;.}$

(iv) For all $U\leq\mathbb{F}_p^n$ with $\dim(U)\geq\frac{\deg(P/\mathfrak{X})}{(p-1)}$
and all $v\in\mathbb{F}_p^n$, $\boxed{\Sigma(P|_{v+U})\;=\;\Sigma(P|_U)\;.}$

Proof. To prove part (i), let X^μ be a monomial in $P/\mathfrak{X}$ ($\mu \leq d(\mathfrak{X})$) of maximal degree. We set

$$r := \left\lfloor \frac{\Sigma d(\mathfrak{X}) - \Sigma\mu}{(p-1)} \right\rfloor = n - \left\lceil \frac{\Sigma\mu}{(p-1)} \right\rceil \in \mathbb{Z} \tag{121}$$

and

$$\Delta_r := \{ \delta' \in [p)^n \mid \Sigma\delta' = r(p-1) \} . \tag{122}$$

Choose a $\delta \in \Delta_r$ with

$$\delta \leq d(\mathfrak{X}) - \mu , \tag{123}$$

and set

$$\bar{d} := \mu + \delta . \tag{124}$$

Define $\lambda = (\lambda_{\delta'}) \in \mathbb{F}_p^{\Delta_r}$ by setting

$$\lambda_{\delta'} := P_{\bar{d}-\delta'} \quad (= 0 \text{ if } \bar{d} - \delta' \not\geq 0) . \tag{125}$$

Note that

$$\lambda \neq 0 \quad \text{as} \quad \lambda_\delta = P_\mu \neq 0 . \tag{126}$$

Now, for each $v \in \mathbb{F}_p^n$, the monomial $X^{\bar{d}}$ occurs in

$$Q := (P/\mathfrak{X})\, 1_{v+U} , \tag{127}$$

where $U = U_\lambda$ and the 1_{v+U} are as in Lemma 8.3 (iv). That is so, since only the monomials of maximal degree from $P/\mathfrak{X}$ and from 1_{v+U} may contribute something to the coefficient $Q_{\bar{d}}$, so that

$$Q_{\bar{d}} = \sum_{\delta' \in \Delta_r} (P/\mathfrak{X})_{\bar{d}-\delta'} (1_{v+U})_{\delta'} \overset{8.3}{=} \sum_{\delta' \in \Delta_r} \lambda_{\delta'} (1_U)_{\delta'} \overset{8.3}{\neq} 0 . \tag{128}$$

It follows that

$$Q|_{\mathfrak{X}} \overset{3.2}{\not\equiv} 0 \quad \text{and so} \quad P|_{v+U} \not\equiv 0 . \tag{129}$$

The proofs of the parts (ii),(iii) and (iv) work almost identically. Since $N \equiv (-1)^n$ (by Lemma 1.4 (iv)), we obtain the following equation, which can be used instead of the conclusion (129):

$$\Sigma(P|_{v+U}) = \Sigma(P/\mathfrak{X}|_{v+U}) = \Sigma(Q|_{\mathfrak{X}}) \overset{3.3}{=} (-1)^n Q_d . \tag{130}$$

Part (ii) follows from the equations (128) and (130) as $d = \bar{d}$ in this case.

As we do not need property 8.3 (iv) (and the resulting Inequality (128)) in the proof of parts (iii) and (iv), we may take Equation (127) with an arbitrary $U \leq \mathbb{F}_p^n$ to define Q. Part (iii) follows now from $\Sigma d > \deg(Q)$, and hence $Q_d = 0$. Part (iv) follows, as Q_d does not depend on v (8.3 (iii)). □

As a corollary, we obtain the following sharpening of Warning's classical result [Schm] (the second inequality below) about the number of simultaneous zeros of systems of polynomial equations over finite fields; see also Corollary 3.5 and the Theorems 4.3 and 9.4. The sharpening tells us something about the distribution of the simultaneous zeros in the space $\mathbb{F}_p^n$.

Corollary 8.5. *Let* $P_1, \ldots, P_m \in \mathbb{F}_p[X]$, *and denote the set of simultaneous zeros by* $\mathcal{V} := \{\, x \in \mathbb{F}_p^n \mid P_1(x) = \cdots = P_m(x) = 0 \,\}$.

If $\mathcal{V} \neq \varnothing$, *then there exists a linear subspace* $U \leq \mathbb{F}_p^n$ *of dimension* $\dim(U) \leq \sum_{i\in(m]} \deg(P_i)$ *such that, for all* $v \in \mathbb{F}_p^n$,

$$\boxed{\mathcal{V} \cap (v+U) \neq \varnothing \ ,}$$

so that in particular,

$$\boxed{|\mathcal{V}| \geq p^{n-\sum_i \deg(P_i)} \ .}$$

For all subspaces $U \leq \mathbb{F}_p^n$ *of dimension* $\dim(U) \geq \sum_{i\in(m]} \deg(P_i)$ *and all* $v \in \mathbb{F}_p^n$,

$$\boxed{\big|\mathcal{V} \cap (v+U)\big| \equiv \big|\mathcal{V} \cap U\big| \pmod p \ .}$$

Proof. Define

$$P := \prod_{i\in(m]} (1 - P_i^{p-1}) \ ; \tag{131}$$

then for each $x \in \mathbb{F}_p^n$,

$$x \in \operatorname{supp}(P) \iff P(x) \neq 0 \iff P_1(x) = \cdots = P_m(x) = 0 \iff x \in \mathcal{V} \ . \tag{132}$$

By Theorem 8.4 (i), there is a subspace $U \leq \mathbb{F}_p^n$ with

$$\dim(U) \ = \ \left\lceil \tfrac{\deg(P/\mathfrak{X})}{(p-1)} \right\rceil \ \leq \ \sum\nolimits_i \deg(P_i) \ , \tag{133}$$

and

$$\varnothing \ \neq \ \operatorname{supp}(P|_{v+U}) \ = \ \operatorname{supp}(P) \cap (v+U) \ = \ \mathcal{V} \cap (v+U) \quad \text{for all } v \in \mathbb{F}_p^n. \tag{134}$$

The lower bond for $|\mathcal{V}|$ follows immediately. The remainder of the corollary follows from Theorem 8.4 (iv), since

$$P(x) \in \{0,1\} \quad \text{for all } x \in \mathbb{F}_p^n \, . \tag{135}$$

□

Our sharpening could suggest that, for any subset $\tilde{\mathcal{V}} \subseteq \mathbb{F}_p^n$ with at least p^{n-m} elements, there is a subspace $U \leq \mathbb{F}_p^n$ of dimension m such that

$$\tilde{\mathcal{V}} \cap (v+U) \neq \varnothing \quad \text{for all } v \in \mathbb{F}_p^n . \tag{136}$$

This is not the case. If, for example, $p = 5$, $n = 2$ and $m = 1$, then any subset $\tilde{\mathcal{V}} := \{ (0,0), (0,1), (1,0), (2,2), (a,b) \} \subseteq \mathbb{F}_5^2$ of $5 = p^{n-m}$ points does not have this property. To any subspace $U \leq \mathbb{F}_p^n$ of dimension 1, there is a $v' \in \mathbb{F}_5^2$ such that $v'+U$ contains two of the "first" four elements of $\tilde{\mathcal{V}}$, so that there must be another $v \in \mathbb{F}_5^2$ with $\tilde{\mathcal{V}} \cap (v+U) = \varnothing$. In other words, the first (and the last) property of the sets $\mathcal{V}$ of simultaneous zeros in Corollary 8.5, is something special.

We formulated all our results in this section for prime fields $\mathbb{F}_p$, but we may also apply them to arbitrary finite fields $\mathbb{F}_{p^k}$ by using the following lemma. It is based on elementary techniques from field theory which were used in a similar way in [Ba, Prop. 3.3] and [MoMo, Lemma 1].

Lemma 8.6. *Let $\alpha \in \mathbb{F}_{p^k}$ be a primitive element of the extension $\mathbb{F}_{p^k} \supseteq \mathbb{F}_p$, $\mathbb{F}_{p^k} = \mathbb{F}_p(\alpha)$. For each $x = (x_j) \in \mathfrak{X} := \mathbb{F}_{p^k}^{(n]}$, let $\bar{x} = (\bar{x}_{i,j}) \in \bar{\mathfrak{X}} := \mathbb{F}_p^{[k)\times(n]}$ be the unique point with $x_j = \bar{x}_{0,j}\alpha^0 + \cdots + \bar{x}_{k-1,j}\alpha^{k-1}$ for all $j \in (n]$, so that $x \longmapsto \bar{x}$ is a bijection $\mathfrak{X} \longrightarrow \bar{\mathfrak{X}}$.*

For each polynomial $P \in \mathbb{F}_{p^k}[X]$ with $X = (X_j)_{j\in(n]}$, there is a polynomial $\bar{P} \in \mathbb{F}_p[\bar{X}]$ with $\bar{X} = (X_{i,j})_{(i,j)\in[k)\times(n]}$ of degree $\deg(\bar{P}) \leq k \deg(P)$ such that, for all $x \in \mathfrak{X}$,

$$\boxed{\bar{P}(\bar{x}) = \mathcal{N}(P(x))} ,$$

where $\mathcal{N} \colon \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$ is the norm of the field extension $\mathbb{F}_{p^k} \supseteq \mathbb{F}_p$.

Proof. Let $A \in \mathbb{F}_p^{[k)\times[k)}$ be the companion matrix of the minimal polynomial f_α of α. We may identify $\mathbb{F}_p[A]$ with $\mathbb{F}_{p^k}$ and A with α. In this way $\mathbb{F}_{p^k}$ is a $\mathbb{F}_p$-vector space with basis $A^0, \ldots, A^{k-1}$ and a subfield of the matrix ring $\mathbb{F}_p^{[k)\times[k)}$. The norm $\mathcal{N}$ of the extension $\mathbb{F}_p(A) \supseteq \mathbb{F}_p$ is given by the determinant det. (See, e.g., [DuFo] for more information about the norm and field extensions.) Now define

$$\tilde{P}(\bar{X}) = (\tilde{P}_{i,j}(\bar{X})) \in \mathbb{F}_p[A][\bar{X}] \subseteq \mathbb{F}_p^{[k)\times[k)}[\bar{X}] \subseteq \mathbb{F}_p[\bar{X}]^{[k)\times[k)} \tag{137}$$

by

$$\tilde{P}(\bar{X}) := P\big((X_{0,j}A^0 + \ldots + X_{k-1,j}A^{k-1})_{j\in(n]} \big) . \tag{138}$$

The entries $\tilde{P}_{i,j}(\bar{X})$ of this matrix have degree at most $\deg(P)$, so that

$$\bar{P}(\bar{X}) := \det(\tilde{P}(\bar{X})) \tag{139}$$

has degree at most $k\deg(P)$, and

$$\bar{P}(\bar{x}) = \det\Big(P\Big((\bar{x}_{0,j}A^0 + \ldots + \bar{x}_{k-1,j}A^{k-1})_{j\in(n]}\Big)\Big) = \mathcal{N}(P(x)) \ . \tag{140}$$

□

The degree restriction $\deg(\bar{P}) \leq k\deg(P)$ in this lemma can be sharpened using the so-called p-weight degree $w_p(P)$ of P. See [MoMo] for the simple idea behind this improvement, and for the definition of w_p.

9 Results over $\mathbb{Z}$, $\mathbb{Z}_m$ and other generalizations

There are several ways to generalize the coefficient formulas 3.3 and 3.2. This section will address some of those.

If a grid $\mathfrak{X}$ is just affine but we want to use Theorem 3.3, we may apply the homomorphism $\pi\colon r \mapsto \frac{r}{1}$ from $\mathcal{R}$ to the localization $\mathcal{R}_N$, exactly as in Theorem 2.6. In particular, this leads to the implications: π

$$P_d = 1 \implies P_d^\pi \neq 0 \implies P|_{\mathfrak{X}} \not\equiv 0 \ . \tag{141}$$

It may also be that there is an integral grid $\hat{\mathfrak{X}}$ over a ring $\hat{\mathcal{R}}$, and a homomorphism $\hat{\mathcal{R}} \longrightarrow \mathcal{R}$ that induces a map from $\hat{\mathfrak{X}}$ into $\mathfrak{X}$. Our results may then be applied to a preimage $\hat{P} \in \hat{\mathcal{R}}[X]$ of $P \in \mathcal{R}[X]$. This leads to results about P on not necessarily integral or affine grids $\mathfrak{X}$. If, for example, $\mathcal{R} = \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ and $\hat{\mathcal{R}} = \mathbb{Z}$, we may read the following formula 9.1 modulo m (note that it contains only integer coefficients). $\mathbb{Z}_m$

Theorem 9.1. *Assume* $P \in \mathbb{Z}[X]$ *and* $\mathfrak{X} = [d] := [d_1] \times \cdots \times [d_n]$. *If* $\deg(P) \leq \Sigma d$, *then*

$$\boxed{(-1)^{\Sigma d} \big[\prod_{j\in(n]}(d_j!)\big]\, P_d \ = \ \sum_{x\in\mathfrak{X}} \big[\prod_{j\in(n]}(-1)^{x_j}\tbinom{d_j}{x_j}\big]\, P(x)} \ .$$

Proof. This follows from Theorem 3.3 and Lemma 1.4 (v). □

With this theorem we get the following special version of Corollary 3.4, which works perfectly well without a degree condition. (See [MuSt] and [Sp] for more information about polynomial maps $\mathbb{Z}_m^{\,n} \to \mathbb{Z}_m$.)

Corollary 9.2. *Let* $P \in \mathbb{Z}_m[X]$, *and set* $\mathfrak{X} := \mathbb{Z}_m^{\,n}$, *which we identify with* $[m)^n \subseteq \mathbb{Z}^n$. *If* m *is not prime, and* $(m,n) \neq (4,1)$, *then:*

(i) $\boxed{\big|\{\, x \in \mathfrak{X} \ \big|\ P(x) \neq 0 \,\}\big| \ \neq \ 1}$.

(ii) $\boxed{P_0 \neq 0 \implies \exists\, x \in \mathfrak{X}\backslash 0 : \big[\prod_{j\in(n]} \tbinom{m-1}{x_j}\big]\, P(x) \neq 0 \implies P|_{\mathfrak{X}\backslash 0} \not\equiv 0}$.

(iii) $\boxed{0 \ = \ \sum\nolimits_{x\in\mathfrak{X}} \big[\prod_{j\in(n]}(-1)^{x_j}\tbinom{m-1}{x_j}\big]\, P(x)}$.

Proof. Suppose there is an $\hat{x} \in \mathfrak{X} = \mathbb{Z}_m^{\,n}$ with $P(\hat{x}) \neq 0$. By applying the substitutions $X_j = X_j + \hat{x}_j$, we may assume $0 \neq P(0) = P_0$; and part (i) follows from the implication (ii).

Part (ii) follows from (iii), as the summand $[\prod_{j\in(n]}(-1)^0\binom{m-1}{0}]P(0) = P_0$ cannot be the only nonvanishing summand in the vanishing sum.

To prove part (iii), we may assume that P has partial degrees $\deg_j(P) \leq d_j = d_j(\mathfrak{X})$. This is so, as the monic polynomial $L_j := \prod_{x\in\mathfrak{X}_j}(X_j - x)$ maps $\mathfrak{X}_j$ to 0, so that we may replace P with any polynomial of the form $P + \sum_{j\in(n]} H_j L_j$ without changing its image $P|_{\mathfrak{X}}$ (see the Example 7.1 and (85) for an illustration of this method). Now let $\hat{P} \in \mathbb{Z}[X]$ be such that

$$P \;=\; \hat{P} + m\mathbb{Z}[X] \;\in\; \mathbb{Z}[X]/m\mathbb{Z}[X] \;=\; \mathbb{Z}_m[X] \qquad \text{and} \qquad deg_j(\hat{P}) \;\leq\; d_j \;. \quad (142)$$

We only have to show that $m \,\big\lfloor\, (m-1)!^{\,n}$, so that the left side of Equation 9.1, applied to $\hat{P}$, vanishes modulo m, in the relevant case $d_1, \ldots, d_n = m-1$:

If $m \neq 4$ and $m = m_1 m_2$, with $m_1 < m_2 < m$, then $m \,\big\lfloor\, (m-1)!$.

If $m \neq 4$ and $m = p^2$, with $p > 2$, then
$p < 2p < m$, and hence $m \,\big\lfloor\, p\,(2p) \,\big\lfloor\, (m-1)!$.

If $m = 4$ and $n \geq 2$, then $m = 2^2 \,\big\lfloor\, 3!^{\,2} \,\big\lfloor\, (m-1)!^{\,n}$. □

The examples $X^3 + X + 2$ and $X^3 - 2X^2 - X + 2 \in \mathbb{Z}_4[X]$ show that the very special case $(m, n) = (4, 1)$ in 9.2 is really an exception. As one can show, these two examples are the only exceptions to assertion (i) that fulfill the additional normalization conditions $\deg(P) \leq 3$, $P_3 \neq -1$ and that the nonvanishing point is the zero ($P(x) \neq 0 \;\Leftrightarrow\; x = 0$).

We also present another version of Corollary 3.5. For this, we will need the following specialization of [AFK2, Lemma A.2]:

Lemma 9.3. *Let $p \in \mathbb{N}$ be prime, $k > 0$ and $c = c(p^k) := \sum_{i\in[k)}(p^i - 1)$. For $y \in \mathbb{Z}$,*

(i) $p^c \,\Big\lfloor\, \displaystyle\prod_{0<\hat{y}<p^k} (y - \hat{y})$, *and*

(ii) $p^{c+1} \not\Big\lfloor\, \displaystyle\prod_{0<\hat{y}<p^k} (y - \hat{y}) \quad\Longleftrightarrow\quad p^k \,\big\lfloor\, y$.

For completeness, we present the relatively short proof:

Proof. For each $j \in (k]$ there are exactly p^{k-j} numbers among the p^k consecutive integers $y\,,\ y-1\,,\ \ldots\,,\ y-(p^k-1)$ that are dividable by p^j. Thus:

If $p^k \bigm\lfloor y$, then exactly $p^{k-j}-1$ of the factors $y-\hat{y}$ $(0<\hat{y}<p^k)$ are dividable by p^j.

If $p^k \not\bigm\lfloor y$, then at least $p^{k-j}-1$ of these factors are dividable by p^j; and in the case $j=k$, strictly more than $p^{k-j}-1=0$ are multiples of $p^j=p^k$.

It follows:

If $p^k \bigm\lfloor y$, then $p^c \bigm\lfloor \prod_{0<\hat{y}<p^k}(y-\hat{y})$, but $p^{c+1} \not\bigm\lfloor \prod_{0<\hat{y}<p^k}(y-\hat{y})$.

If $p^k \not\bigm\lfloor y$, then $p^{c+1} \bigm\lfloor \prod_{0<\hat{y}<p^k}(y-\hat{y})$. □

The following version of Corollary 3.5 (see also Theorem 4.3 and Corollary 8.5) reduces to Olson's Theorem [AFK2, Theorem 2.1], if we set $\mathfrak{X} := \{0,1\}^n$ and if $\deg(P_1) = \cdots = \deg(P_m) = 1$. Olson's Theorem can be used, for example, to prove generalizations of Theorem 4.1 about regular subgraphs, such as those in [AFK2]. Here we view, more generally, arbitrary polynomials and arbitrary *p-integral* grids – i.e., grids $\mathfrak{X} \subseteq \mathbb{Z}^n$ with the property:

$$\text{For all } j \in (n] \text{ and all } x, \tilde{x} \in \mathfrak{X}_j \text{ with } x \neq \tilde{x}, \quad p \not\bigm\lfloor x-\tilde{x}\ . \tag{143}$$

We have:

Theorem 9.4. *Let $p \in \mathbb{N}$ be a prime and $\mathfrak{X} \subseteq \mathbb{Z}^n$ a p-integral d-grid. For polynomials $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$, and numbers $k_1, \ldots, k_m > 0$ small enough so that $\sum_{i\in(m]}(p^{k_i}-1)\deg(P_i) < \Sigma d$,*

$$\boxed{\left|\left\{\, x \in \mathfrak{X} \;\mid\; \forall\, i \in (m]\colon\ p^{k_i} \bigm\lfloor P_i(x)\ \right\}\right| \ \neq\ 1}\ .$$

Proof. Set

$$c := \sum_{i\in(m]} c_i \quad \text{where} \quad c_i = c(p^{k_i}) := \sum_{j\in[k_i)} (p^j-1)\ , \tag{144}$$

define

$$P := \prod_{i\in(m]} \prod_{0<\hat{y}<p^{k_i}} (P_i-\hat{y}) \ \in \mathbb{Z}[X] \tag{145}$$

and let

$$\bar{P} := P + p^{c+1}\mathbb{Z}[X] \ \in \mathbb{Z}[X]/p^{c+1}\mathbb{Z}[X] = \mathbb{Z}_{p^{c+1}}[X]\ . \tag{146}$$

For points $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, set

$$\bar{x} \;:=\; (x_1 + p^{c+1}\mathbb{Z}\,, \ldots,\; x_n + p^{c+1}\mathbb{Z}) \;\in\; (\mathbb{Z}_{p^{c+1}})^n \;; \tag{147}$$

then

$$\bar{\mathfrak{X}} \;:=\; \{\, \bar{x} \;\mid\; x \in \mathfrak{X} \,\} \;\subseteq\; (\mathbb{Z}_{p^{c+1}})^n \tag{148}$$

is an integral d-grid, and $x \longmapsto \bar{x}$ induces a bijection from $\mathfrak{X}$ to $\bar{\mathfrak{X}}$. Now it follows that

$$\begin{aligned} \bar{P}(\bar{x}) \neq 0 \quad &\iff \quad p^{c+1} \nmid P(x) \\ &\overset{9.3\,(i)}{\iff} \quad \forall\, i\colon\; p^{c_i+1} \nmid \prod_{0<\hat{y}<p^{k_i}} (P_i(x) - \hat{y}) \\ &\overset{9.3\,(ii)}{\iff} \quad \forall\, i\colon\; p^{k_i} \,\big\lfloor\, P_i(x) \;, \end{aligned} \tag{149}$$

and since

$$\deg(\bar{P}) \;\leq\; \deg(P) \;\leq\; \sum_{i\in(m]} (p^{k_i} - 1)\deg(P_i) \;<\; \Sigma d \;, \tag{150}$$

we obtain

$$\Big|\big\{\, x \in \mathfrak{X} \;\mid\; \forall\, i \in (m]\colon\; p^{k_i} \,\big\lfloor\, P_i(x) \,\big\}\Big| \;=\; \Big|\big\{\, \bar{x} \in \bar{\mathfrak{X}} \;\mid\; \bar{P}(\bar{x}) \neq 0 \,\big\}\Big| \overset{3.4}{\neq} 1 \;. \tag{151}$$

□

Our result can be generalized further, in the obvious way, by using [AFK2, Lemma A.2], instead of our Lemma 9.3. However, the result would look a bit more technical.

10 How to find nonvanishing points, numerical aspects

If $\mathfrak{X}$ is an integral d-grid, and if $deg(P) \leq \Sigma d$ and $P_d \neq 0$, we know by Theorem 3.3 that there is a nonvanishing point x of $P \in \mathcal{R}[X] = \mathcal{R}[X_1, \ldots, X_n]$ in $\mathfrak{X}$; but how can such a point $x \in \mathfrak{X}$ be found? Of course, the naive brut-force method would be simple; but is there a polynomial-time algorithm? Alon pointed out the importance of such an algorithm in [Al4].

It turns out that finding nonzeros is, for the most important types of grids $\mathfrak{X}$, much simpler than finding zeros. One possibility is to use the modification methods of Section 7 to transform P into the trimmed polynomial $P/\mathfrak{X}$ with partial degrees $\deg_j(P/\mathfrak{X}) \leq d_j$ (and $P/\mathfrak{X} \neq 0$, as $(P/\mathfrak{X})_d \overset{7.2}{=} P_d \neq 0$) and apply the simple and fast algorithm presented below to it. This method also works for polynomials of arbitrary degree, provided they have a nonvanishing point $x \in \mathfrak{X}$, so that $P/\mathfrak{X} \neq 0$ (Theorem 7.3).

The described transformation $P \rightsquigarrow P/\mathfrak{X}$ is easily performed for the most important, Boolean grid $\mathfrak{X} = \{0,1\}^n$, though it is also very simple if the $\mathfrak{X}_j$ are fields or multiplicative groups of fields. The set $E_l := \{\, c \in \mathbb{C} \mid c^l = 1 \,\}$ of l^{th} roots of unity in the complex numbers $\mathcal{R} = \mathbb{C}$ may also be of interest. In all these cases the polynomials $L_j = L_{\mathfrak{X}_j}(X_j) \overset{(84)}{:=} \prod_{\hat{x} \in \mathfrak{X}_j}(X_j - \hat{x})$ used to perform the transformation $P \rightsquigarrow P/\mathfrak{X}$ contain only two monomials, and the transformation $P \rightsquigarrow P/\mathfrak{X}$ can be done in cubic time. In the general case, however, the trimmed polynomial $P/\mathfrak{X}$ may contain many more monomials then the original polynomial P, so that we generally need an exponential amount of space – and hence exponential time – to store all coefficients of $P/\mathfrak{X}$. (See, e.g., [CLRS] for an introduction to algorithms.)

If the polynomial $P \neq 0$ is already trimmed, the following cubic time algorithm can be applied. (There are 2 nested loops, and the evaluation in line 8 takes linear time.) It finds nonzeros of polynomials $0 \neq P \in \mathcal{R}[X^{\leq d}]$ in integral d-grids $\mathfrak{X}$, which are guaranteed by 2.7(v):

Algorithm 1: NONZERO-FINDER

Input: A finite set J, a tuple $d \in \mathbb{N}^J$,
an integral d-grid $\mathfrak{X} = \prod_{j \in J} \mathfrak{X}_j$ (i.e., $|\mathfrak{X}_j| = d_j + 1$)
and a nonvanishing polynomial
$0 \neq P = \sum_{\delta \in \mathbb{N}^J} P_\delta X^\delta \in \mathcal{R}[X_J] := \mathcal{R}[X_j \mid j \in J]$
with partial degrees $\deg_j(P) \leq d_j$.

Output: A nonvanishing point $x = (x_j) \in \mathfrak{X}$ of P ($P(x) \neq 0$).

```
1  begin
2    while J ≠ ∅ do
3      choose a new j ∈ J   ♯ X_j will be substituted.
4      J ← J\j
5      repeat
6        choose a new x_j ∈ 𝔛_j   ♯ A blind guess.
7        𝔛_j ← 𝔛_j\x_j
8      until P|_{X_j=x_j} ≠ 0
9      P ← P|_{X_j=x_j}
       ♯ This final x_j is one coordinate of the output.
10   endw
11 end
```

Proof. The algorithm terminates, as we may view P at each stage of the procedure as a polynomial in just one variable X_j; and polynomials $P \neq 0$ in one variable X_j of degree at most d_j always possess a nonvanishing point x_j in $\mathfrak{X}_j$, if $\mathfrak{X}_j$ with $|\mathfrak{X}_j| = d_j + 1$ is integral $(2.7(v))$. Thus the condition in line 8 will eventually be fulfilled for at least one $x_j \in \mathfrak{X}_j$. □

With slight modifications, this algorithm can also be used to find all nonvanishing points; or just a second one, as guaranteed by Corollary 3.4. Furthermore, as most of our results are based on Theorem 3.3 and Corollary 3.4, this approach also provides numerical solutions to the existence statements of our other results. However, these derived algorithms may have exponential running time. Solving a set of multivariate polynomial equations over a finite field is, in general, an NP-complete problem [GaJo]. See [DGS] for an algorithm that finds simultaneous zeros to systems of polynomial equations over finite fields. A brief summary of algorithms for solving multivariate polynomial equations can be found there, too.

Of course, our method can also be used to find graph colorings, and even those with a minimal number of colors. As our algorithm is very fast, this may be a little astonishing at first glance, but note that computing the graph polynomial $\Pi(A(\vec{G})X)$ (Definition 5.1 and (70)) needs, in general, exponential time.

Another open problem is that of what can be done if the grid $\mathfrak{X}$ does not have a simple structure, so that the transformation $P \rightsquigarrow P/\mathfrak{X}$ is very complicated and time-consuming. Is there a way to avoid the transformation $P \rightsquigarrow P/\mathfrak{X}$, and compute nonzeros directly from P, without computing $P/\mathfrak{X}$ first? In the next section, we give a positive answer to this question in the case of so-called color d-grids $\mathfrak{X}$.

11 Mr. Paint and Mrs. Rubber, a coloration game

If we are interested in graph colorings and the graph polynomial $\Pi(A(\vec{G})X)$ (Definition 5.1 and (70)), then we may take arbitrary elements as colors. If we take symbolic variables T_i as colors, i.e., $\mathfrak{X} \subseteq \{T_1, T_2, \dots\}^n$, and work over the extension $\mathcal{R}[T_1, T_2, \dots]$, things become easier, when we evaluate $P(x)$, as the multiplications are easier to carry out. In addition, as the T_i are independent transcendentals over $\mathcal{R}$, we also may focus on one homogeneous component $\check{P}$ of $P \in \mathcal{R}[X]$, as in view of degree considerations,

$$\check{P}(x) \neq 0 \implies P(x) \neq 0 \qquad \text{for all } x \in \mathfrak{X} \subseteq \{T_1, T_2, \dots\}^n . \tag{152}$$

In what follows, we discuss this special type of nonvanishing point $x \in \{T_1, T_2, \dots\}^n$ which we call a *coloring*, and we describe a coloring game for polynomials. This leads us to a new approach to Alon's second Combinatorial Nullstellensatz (our Theorem 3.3 (*ii*)). We deduce a new proof and a slight generalization of this important result in the case of colorings. This version works, in view of (152), without any degree restrictions. Its proof is formulated as a winning strategy for the second player in our game. The winning strategy leads also to a coloration algorithm. This algorithm computes nonzeros x in color grids $\mathfrak{X}$ (Definition 11.1 below) directly from P without computing $P/\mathfrak{X}$ first as announced in the last section. It has polynomial running time. We define:

Definition 11.1 (Colors)**.** We call the symbolic variables $T_1, T_2, \dots$ *colors*, and each point $x \in \{T_1, T_2, \dots\}^n$ with $P(x) \neq 0$ a *coloration* of $P \in \mathcal{R}[X]$. d-grids $\mathfrak{X}$ that are made up with colors $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \{T_1, T_2, \dots\}^n$ are called *color d-grids*.

The game of Mr. Paint and Mr. Paint is now defined as follows:

Game 11.2 (Mr. Paint and Mrs. Rubber)**.** *Let $J = J_1$ be a finite set and $\mathcal{R} = \mathcal{R}_1$ a commutative ring. Let $P = P_1 \neq 0$ be a polynomial in $\mathcal{R}[X_J] := \mathcal{R}[\, X_j \mid j \in J\,]$ (usually $J := (n)$, in which case $\mathcal{R}[X_J] = \mathcal{R}[X]$). Lay on each index $j \in J$ a stack S_j of erasers.* X_J

The game of Mr. Paint and Mrs. Rubber works as follows:

1P: Mr. Paint starts, chooses a subset $\varnothing \neq \check{J}_1 \subseteq J_1$, and substitutes the color T_1 for the variables X_j satisfying $j \in \check{J}_1$.

$1R$: *Mrs. Rubber may use – and hereby use up – for each "colored" variable* X_j *(i.e., each index* $j \in \check{J}_1$ *) one eraser from* S_j *(if* $S_j \neq \varnothing$ *) to revoke the substitution for* X_j *. What remains if she recovers all* X_j *with* $j \in \hat{J}_1$ *for some* $\hat{J}_1 \subseteq \check{J}_1$ *is a polynomial* $P_2 \in \mathcal{R}_2[X_{J_2}]$ *with* $\mathcal{R}_2 := \mathcal{R}_1[T_1]$ *and* $J_2 := J_1 \setminus (\check{J}_1 \setminus \hat{J}_1) \subseteq J_1$ *in which all variables* X_j *with* $j \in \check{J}_1 \setminus \hat{J}_1 = J_1 \setminus J_2$ *are replaced by* T_1 *. It is the job of Mrs. Rubber to ensure that* $P_2 \neq 0$ *by means of her choice of* $\hat{J}_1 \subseteq \{\, j \in \check{J}_1 \mid S_j \neq \varnothing \,\}$ *.*

$2P$: *Mr. Paint chooses another subset* $\varnothing \neq \check{J}_2 \subseteq J_2$ *of "uncolored indices" and substitutes* T_2 *for all* X_j *with* $j \in \check{J}_2$ *in* P_2 *.*

$2R$: *Mrs. Rubber again may have to use (up) some erasers to ensure that the remaining polynomial* $P_3 \in \mathcal{R}_3[X_{J_3}] := (\mathcal{R}_2[T_2])[X_{J_3}]$ *does not vanish,* $P_3 \neq 0$ *.*

$\vdots$ $\vdots$

End: The game ends when one player cannot move any more, and hence loses.

Mrs. Rubber cannot move if she does not have enough erasers any more to ensure the nonvanishing of the polynomial.

Mr. Paint loses if all variables X_j *have already been replaced, but the polynomial does not vanish. In this case,* P_1 *has been properly colored with indeterminacies* $T_1, T_2, \ldots$ *.*

Definition 11.3. If there is a winning strategy for Mrs. Rubber, and if the stacks of erasers S_j have sizes d_j, we say that $P \in \mathcal{R}[X_J]$ is *d-correctable*, where $d := (d_j)_{j \in J}$.

If $\check{J} \subseteq J$, and there is a winning strategy for Mrs. Rubber provided that Mr. Paint chooses $\check{J}_1 := \check{J}$ in his first move $1P$ (abbreviated $1P = \check{J}$), we say that $P \in \mathcal{R}[X_J]$ is *d-correctable when* $1P = \check{J}$.

$1P = \check{J}$

It is easy to see that each d-correctable polynomial P possesses a coloration x in every color d-grid $\mathfrak{X} = \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \subseteq \{T_1, T_2, \ldots\}^n$, a "list coloring" with respect to the "color lists" $\mathfrak{X}_j$. To obtain such a coloring $x \in \mathfrak{X}$ as a by-product of the playing, we have to fix the strategy of Mr. Paint as follows:

In the i^{th} move of Mr. Paint (iP), let him choose $\check{J}_i := \{\, j \in J_i \mid T_i \in \mathfrak{X}_j \,\}$ (and use T_i as color for the corresponding variables X_j with $j \in \check{J}_i$).

(153)

These sets $\check{J}_i$ may be empty, but only finitely often; and that is not really a problem, as such rounds may be skipped. The game terminates before the sequence of the $\check{J}_i$ can become constantly "zero," since the number of erasers at each X_j is limited by d_j , and Mr. Paint has up to $|\mathfrak{X}_j| = d_j + 1$ tries for this variable. So, indeed, as intended by Mr. Paint's "considerateness" (153), the resulting coloration x (when Mrs. Rubber plays a winning strategy) lies in $\mathfrak{X}$.

Summarizing, we can say that correctability is stronger than "list colorability," i.e., d-correctability implies the existence of a coloring $x \in \mathfrak{X}$ in any color d-grid $\mathfrak{X} \subseteq \{T_1, T_2, \dots\}^n$. This is particularly interesting if we view it as a statement about graphs, where a graph G is d-correctable if its graph polynomial $\Pi(A(\vec{G})X)$ has this property. (See Definition 5.1 and (70) for the meaning of $\Pi(A(\vec{G})X)$; $\vec{G}$ denotes G together with an arbitrarily chosen orientation $\rightarrow$ of G). However, even on the level of polynomials, we do not know of an example that shows the strictness of this statement, i.e., a polynomial P that is d-list colorable but not d-correctable. Conversely, we can prove that Alon and Tarsi's second Combinatorial Nullstellensatz 3.3 (ii) – applied to color grids $\mathfrak{X} \subseteq \{T_1, T_2, \dots\}^n$ – also holds for correctability. Their result about list colorings of graphs, Theorem 5.5 (ii), holds consequently for correctability, too. To prove this sharpening, we will need the following lemma :

Lemma 11.4. *Let $P = \sum_{\delta \in \mathbb{N}^J} P_\delta X^\delta \in \mathcal{R}[X_J]$, $d \in \mathbb{N}^J$, $\check{J} \subseteq J$, $j \in \check{J}$, $e_j := (?_{(i=j)})_{i \in J}$ and $d + \mathbb{N}^{\check{J}} := \{\, \delta \geq d \mid \delta|_{J \setminus \check{J}} = d|_{J \setminus \check{J}} \,\} \subseteq \mathbb{N}^J$; then:*

(i) $$d + \mathbb{N}^{\check{J}} \;=\; d + e_j + \mathbb{N}^{\check{J}} \;\uplus\; d + \mathbb{N}^{\check{J} \setminus j} \quad .$$

(ii) $$\sum_{\delta \in d + \mathbb{N}^{\check{J}}} P_\delta \;=\; \sum_{\delta \in d + e_j + \mathbb{N}^{\check{J}}} P_\delta \;+\; \sum_{\delta \in d + \mathbb{N}^{\check{J} \setminus j}} P_\delta \quad .$$

(iii) $$\sum_{\delta \in d + e_j + \mathbb{N}^{\check{J}}} P_\delta \neq 0 \;\Longrightarrow\; \sum_{\delta \in d + \mathbb{N}^{\check{J}}} P_\delta \neq 0 \;\vee\; \sum_{\delta \in d + \mathbb{N}^{\check{J} \setminus j}} P_\delta \neq 0 \quad .$$

(iv) $$\sum_{\delta \in d + \mathbb{N}^{\check{J}}} P_\delta \neq 0 \;\Longrightarrow\; \left\{ \begin{array}{l} \text{There is a } \hat{d} \leq d \text{ and a } \hat{J} \subseteq \check{J} \text{ such that} \\ \hat{d}|_{\hat{J}} \equiv 0 \;,\quad \hat{d}|_{\check{J} \setminus \hat{J}} < d|_{\check{J} \setminus \hat{J}} \;,\quad \displaystyle\sum_{\delta \in \hat{d} + \mathbb{N}^{\hat{J}}} P_\delta \neq 0 \;. \end{array} \right.$$

Proof. Part (i) is trivial; and obviously $(i) \implies (ii) \implies (iii)$. In order to prove (iv), we may use (iii) to produce sequences

$$d =: d^0 \gneq d^1 \gneq \cdots \gneq d^t \geq 0 \qquad \text{and} \qquad \check{J} =: \check{J}_0 \supseteq \check{J}_1 \supseteq \cdots \supseteq \check{J}_t \tag{154}$$

with the property

$$\sum_{\delta \in d^i + \mathbb{N}^{\check{J}_i}} P_\delta \neq 0 \qquad \text{for all } i \in [t]\,. \tag{155}$$

Note that $d^t|_{\check{J}_t} \equiv 0$ if and only if the sequences (154) cannot be extended any more through application of (iii); so that in this case part (iv) holds, if we set $\hat{d} := d^t$ and $\hat{J} := \check{J}_t$. □

With this, the second Combinatorial Nullstellensatz 3.3 (ii) can be sharpened for color grids $\mathfrak{X} \subseteq \{T_1, T_2, \dots\}^n$. Without degree restrictions, we have:

Theorem 11.5 (Winning strategy)**.** *Let* $P = \sum_{\delta \in \mathbb{N}^J} P_\delta X^\delta \in \mathcal{R}[X_J]$ *and* $d \in \mathbb{N}^J$*; then*

$$\boxed{P_d \neq 0 \implies P \text{ is } d\text{-correctable.}}$$

More generally, for $\check{J} \subseteq J$ *and* $d + \mathbb{N}^{\check{J}} := \{\, \delta \geq d \mid \delta|_{J\setminus\check{J}} = d|_{J\setminus\check{J}} \,\}$*;*

$$\boxed{\textstyle\sum_{\delta \in d + \mathbb{N}^{\check{J}}} P_\delta \neq 0 \implies P \text{ is } d\text{-correctable when } 1P = \check{J}.}$$

Proof. We present a winning strategy for Mrs. Rubber in the case $P_d \neq 0$; apart from a slight modification at the beginning, this strategy also works in the second case of our theorem. In our winning strategy, we allow Mrs. Rubber to replace, at any stage, the present polynomial P_i by an homogeneous component of P_i. Mr. Paint will not complain about this, since in view of the contrapositive to the implication (152), the chance of Mrs. Rubber's success will not increase. In particular, we may suppose that $P_1 = P$ is already homogeneous (with $P_d \neq 0$). We also may allow Mrs. Rubber to throw some of here erasers away.

Now, suppose that the game has reached the i^{th} round, so that the initial polynomial $P_1 = P$ has become $P_i \in \mathcal{R}_i[X_{J_i}]$. Furthermore, suppose that Mrs. Rubber has left d^i_j erasers at each $j \in J_i$, and that she has managed to ensure

$$(P_i)_{d^i} \neq 0\ . \tag{156}$$

Suppose further that she has managed, to make P_i homogeneous (of degree $\deg(P_i) = \Sigma d^i$).

Now Mr. Paint makes his i^{th} move:

iP: Mr. Paint chooses a subset $\varnothing \neq \check{J}_i \subseteq J_i$, and substitutes T_i for all variables X_j with $j \in \check{J}_i$ in P_i (in short, $iP = \check{J}_i$). If $J_i = \varnothing$ already, the game ends here: Mr. Paint is defeated, and Mrs. Rubber wins.

Mrs. Rubber watches exactly what Mr. Paint is doing, and in the very moment when he has chosen the set $\check{J}_i \subseteq J_i$ but has not yet performed the substitution, she applies the algorithm behind 11.4 (iv) to P_i. That is possible, since

$$\sum_{\delta \in d^i + \mathbb{N}^{\check{J}_i}} (P_i)_\delta \;=\; (P_i)_{d^i} \overset{(156)}{\neq} 0 \;, \tag{157}$$

as P_i is homogeneous of degree $\deg(P_i) = \Sigma d^i$. She obtains a subset $\hat{J}_i \subseteq \check{J}_i$, and a tuple $\hat{d}^i \leq d^i$ as in 11.4 (iv), and memorizes them.

Now, after Mr. Paint's substitution, Mrs. Rubber makes her i^{th} move in the following way, which is always possible, so that the game does not stop when it is her turn and she indeed does not lose:

iR: Mrs. Rubber uses here erasers on all variables X_j with $j \in \check{J}_i \setminus \hat{J}_i$, and perhaps throws away some of the erasers such that $\hat{d}^i_j$ erasers remain at each $j \in J_i$. The other variables X_j with $j \in \hat{J}_i$ in the polynomials P_i stay replaced by T_i. The resulting polynomial

$$P_{i+1} \;\in\; \mathcal{R}_{i+1}[X_{J_{i+1}}] \quad \text{with} \quad \mathcal{R}_{i+1} := \mathcal{R}_i[T_i] \quad \text{and} \quad J_{i+1} := J_i \setminus \hat{J}_i \tag{158}$$

does not vanish:

$$P_{i+1} \;\neq\; 0 \;. \tag{159}$$

Moreover,

$$(P_{i+1})_{d^{i+1}} \;\neq\; 0 \quad \text{for} \quad d^{i+1} := \hat{d}^i|_{J_{i+1}} \tag{160}$$

as

$$(P_{i+1})_{d^{i+1}}|_{T_i=1} \;=\; \big(P_i \,\big|_{\substack{X_j=1 \\ j \in \hat{J}_i}}\big)_{d^{i+1}} \overset{\hat{d}^i|_{\hat{J}_i} \equiv 0}{=} \sum_{\delta \in \hat{d}^i + \mathbb{N}^{\hat{J}_i}} (P_i)_\delta \overset{11.4(iv)}{\neq} 0 \;. \tag{161}$$

These properties remain true if Mrs. Rubber finally replaces $P_{i+1} \in \mathcal{R}_{i+1}[X_{J_{i+1}}]$ by the homogeneous component of P_{i+1} that contains $(P_{i+1})_{d^{i+1}} X^{d^{i+1}}$.

The homogeneous polynomial P_{i+1} and the reduced stacks S_j of size $d_j^{i+1} = \hat{d}_j^i$ ($j \in J_{i+1}$) will be passed to the next round. After finite time $t \in \mathbb{N}$, the set J_t will be empty, Mr. Paint cannot move, and Mrs. Rubber's strategy succeeds. □

For clarity, we present this winning strategy in combination with the fixed (through (153)) strategy of Mr. Paint (which leads to "list colorings" $x \in \mathfrak{X}$) as an algorithm in pseudo-code. This algorithm is, in contrast to the algorithm presented in the last section, self explanatory. Its proof of correctness is not based on our results. You can observe the "induction hypothesis" $P_d \neq 0$ (respectively, $\sum_{\delta \in d+\mathbb{N}^J} P_\delta \neq 0$) through the whole procedure; it never gets lost. The final P_d, when $J = \varnothing$ and hence $d = ()$, is then still nonvanishing, i.e., $P_{()} \neq 0$. This value $P_{()} \neq 0$ would be the value $P_{\text{Input}}(x)$ of the original input polynomial P_{Input} at the computed tuple $x = (x_j)$, if we had not replaced the original P_{Input} several times by one of its homogeneous components in line 4. In this case, $P_{\text{Input}}(x) = P_{()} \neq 0$ would not be zero, and x would indeed be a coloring. However, in view of observation (152), the replacements in line 4 do not matter, so that x is actually a coloring of the input polynomial.

Algorithm 2: Mr. Paint and Mrs. Rubber

Input: A finite set J, a tuple $d \in \mathbb{N}^J$,
a color d-grid $\mathfrak{X} = \prod_{j\in J} \mathfrak{X}_j \subseteq \{T_1, T_2, \dots\}^J$ (i.e., $|\mathfrak{X}_j| = d_j + 1$),
a polynomial $P = \sum_{\delta\in\mathbb{N}^J} P_\delta X^\delta \in \mathcal{R}[X_J] := \mathcal{R}[X_j \mid j \in J]$
with $P_d \neq 0$ over a commutative ring R.

Output: A coloration $x = (x_j) \in \mathfrak{X}$ of P ($P(x) \neq 0$).

```
1  begin
2      i ← 0   ♯ T_{i+1} = T_1 is the first color.
3      while J ≠ ∅ do
4          Replace P by the homogeneous component of P that contains X^d.
               ♯ (152)
           ♯ Σ_{δ∈d+ℕ^J} P_δ = P_d ≠ 0 for any J̌ ⊆ J .
5          i ← i + 1   ♯ Take next color T_i .
6          J̌ ← { j ∈ J ¦ T_i ∈ 𝔛_j }   ♯ as in (153).
>7         while J̌ ≠ ∅ do
8              choose a new j ∈ J̌   ♯ X_j is proposed for coloration.
9              while d_j ≠ 0 do
10                 d_j ← d_j − 1   ♯ Take a rubber. Shell we use or scrap it?
11                 if Σ_{δ∈d+ℕ^J} P_δ = 0 then
12                     J̌ ← J̌\j   ♯ Erase the coloration proposal for X_j .
                       ♯ Σ_{δ∈d+ℕ^J} P_δ ≠ 0 by 11.4(iii).
13                     return to >7
14                 endif
15             endw
               ♯ Σ_{δ∈d+ℕ^J} P_δ ≠ 0 and d_j = 0 .
16             J̌ ← J̌\j
               ♯ Σ_{δ∈d+ℕ^J} Q_δ ≠ 0 with Q := P|_{X_j=1} .
17             P ← P|_{X_j=T_i}
18             J ← J\j
19             d ← d|_J
20             R ← R[T_i]   ♯ Again P ∈ R[X_J] .
               ♯ Σ_{δ∈d+ℕ^J} P_δ ≠ 0 , as this holds even for Q above.
21             x_j ← T_i   ♯ One coordinate of the output.
22         endw
           ♯ Again, P_d = Σ_{δ∈d+ℕ^∅} P_δ ≠ 0 .
23     endw
       ♯ P_() = P_d ≠ 0  ⟹(152)  ‘‘x is a coloring’’ (explained on page 76).
24 end
```

It is not hard to see that this algorithm has running time $O(\eta^4)$, where η is the input length. There are three nested loops, and the evaluation in the most critical line, line 11, takes linear time. (See, e.g., [CLRS] for an introduction to algorithms and the O-notation.)

When applied to the graph polynomial $\Pi(A(\vec{G})X)$ (see Definition 5.1 and (70)) of an arbitrarily oriented graph $\vec{G}$, this algorithm produces graph colorings, as dose the algorithm of the last section. If we are interested in list colorings of graphs, this algorithm could be faster then the algorithm in the last section, as it avoids the computation of $P/\mathfrak{X}$, which could be space- and time-consuming for complicated grids $\mathfrak{X}$. However, as already mentioned, computing the graph polynomial ($\vec{G} \rightsquigarrow \Pi(A(\vec{G})X)$) needs exponential time, in general.

Our algorithm (and its proof of correctness) can be specialized to the graph-theoretic situation, and all algebraic terms, such as "polynomial," can be replaced by graph-theoretic expressions, e.g., certain sets of orientations. What remains is a purely combinatorial proof of Alon and Tarsi's Theorem 5.5 (*ii*). Alon and Tarsi asked already in [AlTa] for such a proof, and this was also mentioned in [JeTo, p. 217].

References

[Al] N. Alon: Restricted colorings of graphs.
In "Surveys in combinatorics, 1993", London Math. Soc. Lecture Notes Ser. 187, Cambridge Univ. Press, Cambridge 1993, 1-33.

[Al2] N. Alon: Combinatorial Nullstellensatz.
Combin. Probab. Comput. 8, No. 1-2 (1999), 7-29.

[Al3] N. Alon: Discrete Mathematics: Methods and Challenges.
Proc. of the International Congress of Mathematicians (ICM), Beijing 2002, China, Higher Education Press (2003), 119-135.

[Al4] N. Alon: Algebraic and probabilistic methods in discrete mathematics.
Geom. Funct. Anal. 2000, Special Volume, Part II, 455-470.

[AFK] N. Alon, S. Friedland, G. Kalai:
Every 4-regular graph plus an edge contains a 3-regular subgraph.
J. Combin. Theory Ser. B 37 (1984), 92-93.

[AFK2] N. Alon, S. Friedland, G. Kalai:
Regular subgraphs of almost regular graphs.
J. Combin. Theory Ser. B 37 (1984), 79-91.

[AlFü] N. Alon, Z. Füredi: Covering the cube by affine hyperplans.
European J. Combinatorics 14 (1993), 79-83.

[AlTa] N. Alon, M. Tarsi: Colorings and orientations of graphs.
Combinatorica 12 (1992), 125-134.

[AlTa2] N. Alon, M. Tarsi: A nowhere-zero point in linear mappings.
Combinatorica 9 (1989), 393-395.

[ApHa] K. I. Appel, W. Haken, J. Koch: Every planar map is four colorable.
Illinois J. Math. 21 (1977), 429-567.

[Ba] D. A. M. Barrington:
Some problems involving Razborov-Smolensky polynomials.
Boolean Function Complexity, ed. M. S. Patterson, London Math. Soc. Lecture Note Series 169, Cambridge University Press 1992a, 109-128.

[BrRy] R. A. Brualdi, H. J. Ryser: Combinatorial matrix theory.
Cambridge University Press, Cambridge 1991.

[CCF] P. J. Cahen, J. L. Chabert, S. Frisch: Interpolation domains.
J. Algebra 225 (2000), 794–803.

[CCS] J. L. Chabert, S. T. Chapman, W. W. Smith:
The Skolem Property in rings of integer-valued polynomials.
Proceedings of the American Mathematical Society, Vol. 126 No. 11 (1998), 3151-3159.

[CLRS] T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein:
Introduction to Algorithms. *MIT Press. Cambridge 2001.*

[Da] P. J. Davis: Interpolation and approximation.
Dover Books on Advanced Mathematics. New York 1975.

[DeV] M. DeVos: Matrix choosability.
J. Combin. Theory Ser. A 90 (2000), 197-209.

[Di] R. Diestel: Graph theory. *Springer, Berlin 2000.*

[DGS] J. Ding, J. E. Gower, D. S. Schmidt:
Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field. *Cryptology ePrint Archive, Report 2006/038, 2006.* http://eprint.iacr.org/.

[DuFo] D. S. Dummit, R. M. Foote: Abstract Algebra.
John Wiley and Sons, Inc. 2004.

[ElGo] M. N. Ellingham, L. Goddyn:
List edge colourings of some 1-factorable multigraphs.
Combinatorica 16 (1996), 343-352.

[GaJo] M. R. Garey, D. S. Johnson: Computers and intractability, a guide to the theory of NP-completeness. *W. H. Freeman, 1979.*

[JeTo] T. R. Jensen,B. Toft: Graph coloring problems.
Wiley, New York 1995.

[Minc] H. Minc: Permanents. *Addison-Wesley, London 1978.*

[MSCK] O. Moreno, K. W. Shum, F. N. Castro, P. V. Kumar:
Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications. *Proc. London Math. Soc. (3) 88 (2004), 545-564.*

[MoMo] O. Moreno, C. J. Moreno:
Improvements of the Chevalley-Warning and the Ax-Katz Theorems.
American Journal of Mathematics,Vol. 117, No. 1, (1995), 241-244.

[MoZi] O. Moreno, V. A. Zinoviev:
Tree-regular subgraphs of four-regular graphs.
European J. Combinatorics 19, No. 3, (1998), 369-373.

[MuSt] G. Mullen, H. Stevens: Polynomial functions (mod m).
Acta Math. Hung. 44 (1984), 237-241.

[Scha] U. Schauz: Colorings and orientations of matrices and graphs.
The Electronic Journal of Combinatorics 13 (2006), #R61.

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

[Schm] W. M. Schmidt: Equations over finite fields.
Lecture Notes in Math., Vol. 536, Springer, Berlin and New York 1976.

[Sp] R. Spira: Polynomial interpolation over commutative rings.
Amer. Math. Monthly 75 (1968), 638–640.

[Vig] L. Vigneron: Remarques sur les réseaux cubiques de classe 3 associés au problème des quatre couleurs.
C. R. Acad. Sci. Paris T. 223 (1946), 770-772.

[Ya] Yu Yang: The permanent rank of a matrix.
J. Combin. Theory Ser. A 85(2) (1999), 237-242.

Index

$?_{(\mathcal{A})}$, Π , Σ , $\operatorname{supp}(y)$, $\bigotimes$, 17
$n \rfloor p$, $(n]$, $[n)$, $[n]$, 17
$\mathcal{R}$, $\mathbb{Z}_m$, $\mathbb{F}_{p^k}$, $\mathbb{N}$, 17
$\mathfrak{X}$, $[d]$, d , N , Ψ , $L_{\mathfrak{X},x}$, e_x , 18
$P/\mathfrak{X}$, $L_j = L_{\mathfrak{X}_j}$, 50
P_δ , $P(X)$, $P|_{\mathfrak{X}} = P(X)|_{\mathfrak{X}}$, 19
φ , $\mathcal{R}[X^{\leq d}]$, $\mathcal{R}^{[d]}$, $\mathcal{R}^{\mathfrak{X}}$, 23
π , $\mathcal{S}$, $\mathcal{R}_N$, 26
$A\langle k|\rangle$, 53
$A\langle|\delta\rangle$, $\Pi(AX)$, $\operatorname{per}_\delta$, $\pi_{\mathcal{A}}$, $|\sigma^{-1}|$, 41
$A(\vec{G})$, $\vec{G}$, $\rightarrow$, DE_δ , EE , 43
$\mathcal{P}$, $\mathcal{S}$, $\mathcal{S}_{\text{triv}}$, χ , 45
$\mathbf{1}_{v+U}$, Δ_r , 56
T_i , X_J , 71
$1P = \check{J}$, 72

δ-orientation, 42
δ-permanent, 41
d-correctable, 72
d-grid, 18
d-leading, 31

algebraic solution, 46

coefficient formula, 31, 33
color, 71
coloring, 42
Combinatorial Nullstellensatz, 51
correctable, 73

describing polynomial, 45

grid, 18
  affine, 26
  Boolean, 25
  color, 71
  division, 25
  integral, 27
  p-integral, 65

impression, 45
inclusion and exclusion, 29
interpolation, 24
interpolation formula, 25
inversion formula, 27, 28

Lagrange polynomial, 19
list colorable, 73

matrix polynomial, 41
modification method, 49
Mr. Paint and Mrs. Rubber, 71

nonvanishing point, 67
nonzero, 67

orientation, 42

permanent, 41
permanent formula, 42
Permanent Lemma, 42
problem, 45

solution, 45

theorem
  about cube coverings, 38
  about polyn. maps on $\mathbb{F}_p^n$, 57
  about second nonzeros, 34, 63
  about subgraphs, 37
  of Alon and Füredi, 38
  of Alon and Tarsi, 43
  of Cauchy and Davenport, 39
  of Chevalley and Warning, 35, 39
  of Olson, 65
  of Scheim, 43
  of Warning, 59
trimmed polynomial, 50

winning strategy, 74