Combinatorial Nullstellensatz modulo prime powers and the Parity Argument

László Varga[*]

Institute of Mathematics
Eötvös Loránd University
Budapest, Hungary

LVarga@cs.elte.hu

Submitted: Feb 19, 2014; Accepted: Nov 18, 2014; Published: Nov 27, 2014
Mathematics Subject Classifications: 11B75

Abstract

We present new generalizations of Olson's theorem and of a consequence of Alon's Combinatorial Nullstellensatz. These enable us to extend some of their combinatorial applications with conditions modulo primes to conditions modulo prime powers. We analyze computational search problems corresponding to these kinds of combinatorial questions and we prove that the problem of finding degree-constrained subgraphs modulo 2^d such as 2^d-divisible subgraphs and the search problem corresponding to the Combinatorial Nullstellensatz over $\mathbb{F}_2$ belong to the complexity class Polynomial Parity Argument (PPA).

Keywords: Combinatorial Nullstellensatz; Olson's theorem; PPA

1 Introduction

In this paper, we are interested in combinatorial and computational problems in connection with Alon's Combinatorial Nullstellensatz [1] which is a landmark theorem in algebraic combinatorics.

Theorem 1 (Combinatorial Nullstellensatz, Alon, [1]). *Let $\mathbb{F}$ be an arbitrary field, and let $f \in \mathbb{F}[x_1, \dots x_m]$ be an m-variable polynomial. Suppose that the degree of f is $\sum_{j=1}^{m} t_j$, where each t_j is a nonnegative integer, and that the coefficient of $\prod_{j=1}^{m} x_j^{t_j}$ is nonzero. Then, if $S_1, S_2, \dots, S_m$ are subsets of $\mathbb{F}$ with $|S_j| > t_j$ for all $j = 1, \dots, m$, then there exists $\mathbf{s} = (s_1, s_2, \dots, s_m) \in S_1 \times S_2 \times \dots \times S_m$ such that $f(\mathbf{s}) \neq 0$.*

[*] Supported by Hungarian Scientific Research Fund - OTKA, K109240.

The following corollary is often used implicitly in applications, see [1].

Corollary 2. *Let p be an arbitrary prime. Let us be given some m-variable polynomials $f_1, f_2, \ldots, f_n$ over $\mathbb{F}_p$ with no constant terms and $Q_1, Q_2, \ldots, Q_n \subseteq \mathbb{F}_p$ such that $0 \in Q_i$ for all i. If*

$$m > \sum_{i=1}^{n} \deg(f_i) \cdot |\mathbb{F}_p \backslash Q_i|,$$

then there exists a vector $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that $f_i(\mathbf{x}) \in Q_i$ for all i.

Proof. Let $f(\mathbf{x}) = \prod_{i=1}^{n} \prod_{q \notin Q_i} (q - f_i(\mathbf{x})) - c \cdot \prod_{j=1}^{m} (1 - x_j)$ over $\mathbb{F}_p$, where $c = \prod_{i=1}^{n} \prod_{q \notin Q_i} q$. It is easy to check that $\deg(f) = m > \sum_{i=1}^{n} \deg(f_i) \cdot |\mathbb{F}_p \backslash Q_i|$ and for a vector $\mathbf{x} \in \{0,1\}^m$, $f(\mathbf{x}) \neq 0$ if and only if $\mathbf{0} \neq \mathbf{x}$ and $f_i(\mathbf{x}) \in Q_i$ for all i. Then, with setting $S_i = \{0,1\}$ for all i, the Combinatorial Nullstellensatz implies the statement. □

The goal of this paper is to give similar theorems for problems modulo arbitrary prime powers: we prove that if the number m of variables is sufficiently large, the corollary also holds modulo arbitrary prime powers. We develop a general method for the Combinatorial Nullstellensatz-type proofs, where the polynomials are modulo prime powers instead of primes. As an application, we extend the following theorem of Olson [2] and its generalization by Alon, Friedland and Kalai [3].

Let us be given a prime p, nonnegative integers $d_1 \geqslant d_2 \geqslant \ldots \geqslant d_n$ and sets $Q_1, Q_2, \ldots, Q_n$ such that each of them contains zero and $Q_i \subseteq \mathbb{Z}_{p^{d_i}}$ for every $i = 1, \ldots, n$. Let us denote $(d_1, d_2, \ldots, d_n)$ by $\mathbf{d}$ and $(Q_1, Q_2, \ldots, Q_n)$ by $\mathbf{Q}$.

Alon et al. [3] ask to determine the minimum value $F(\mathbf{d}, \mathbf{Q})$ such that for every $m > F(\mathbf{d}, \mathbf{Q})$ and for arbitrary integers a_{ij} $(i = 1, \ldots, n, j = 1, \ldots, m)$ there exists a nonempty subset $J \subseteq \{1, 2, \ldots, m\}$ that fulfills the following condition:

$$\sum_{j \in J} a_{ij} \equiv q_i \pmod{p^{d_i}} \quad \text{for some } q_i \in Q_i \text{ for every } i = 1, \ldots, n. \qquad (\clubsuit)$$

Using this terminology, we can easily formulate Olson's theorem and its extension by Alon et al. as follows:

Theorem 3 (Olson, [2])**.** *$F(\mathbf{d}, \mathbf{Q}) = \sum_{i=1}^{n} \left(p^{d_i} - 1\right)$, if $\{0\} = Q_i$ for all i.*

Theorem 4 (Alon, Friedland, Kalai, [3])**.** *$F(\mathbf{d}, \mathbf{Q}) \leqslant \sum_{i=1}^{n} \left(p^{d_i} - card_p(Q_i)\right)$ where $card_p(Q)$ denotes the number of distinct elements in Q modulo p.*

Whereas Theorem 4 does not seem to be a strong estimation because of $card_p(Q) \leqslant p$, no better estimation has been known thus far.

It is worth noting that for $d_1 = d_2 = \cdots = d_n = 1$, Theorem 3 and Theorem 4 immediately follow from Corollary 2: for $f_i(\mathbf{x}) = \sum_{j=1}^{m} a_{ij} x_j$, there exists a vector $\mathbf{0} \neq \mathbf{s} \in \{0,1\}^m$ such that $f_i(\mathbf{s}) \in Q_i$ for all i. Consequently, $J = \{j : s_j = 1\}$ fulfills the condition ($\clubsuit$).

Motivated by these questions, in this paper, we give analogous theorems modulo arbitrary prime powers instead of primes, extending Corollary 2, and give improved bounds on $F(\mathbf{d}, \mathbf{Q})$.

It is also worth noting that Brink [9] gave another extension of Corollary 2 and Olson's theorem in a slightly different way. His theorem also deals with arbitrary prime powers, however, the variables are restricted to sets where the elements are pairwise incongruent modulo p. In contrast, our results allow one variable, the right hand side of the polynomial, to be restricted to arbitrary set, and the other variables remain to be restricted to the set $\{0, 1\}$.

1.1 Complexity aspects

As an application of Olson's theorem, Alon, Friedland and Kalai [3] discussed the following extremal graph theoretic question. Given a prime power p^d and an integer n, the problem is to determine the smallest value of m such that for every graph on n vertices and m edges, there exists a nonempty p^d-divisible subgraph, that is, a nonempty subset of edges such that the number of edges incident to every vertex is divisible by p^d. Conversely, determine the maximum number of edges a graph can have without containing a nonempty p^d-divisible subgraph. The exact answer was given in [3], see Theorem 21.

A natural question is to determine the computational complexity of finding such a subgraph if the graph has sufficiently large number of edges. For the case $p^d = 2$, the problem is equivalent to finding a cycle in a graph. In this case, there exists a polynomial time algorithm, but the problem is open in all other cases.

Due to various applications of the Combinatorial Nullstellensatz, it is also a natural question to determine the computational complexity of the corresponding search problem. An open question by West [5] is about the complexity of the Combinatorial Nullstellensatz over $\mathbb{F}_2 = \{0, 1\}$. He conjectures that the corresponding search problem belongs to the complexity class Polynomial Parity Argument (PPA) defined by Papadimitriou [4]. This complexity class contains such computational search problems that the existence of a solution can be proved by so-called parity argument: *Every finite graph has an even number of odd-degree nodes.* In this paper, we verify his conjecture.

2 Main results

Now we present the first main result of this paper: the extension of Corollary 2 for arbitrary prime powers. This theorem also implies Theorem 3 and Theorem 4.

Definition 5. Let $h(x)$ be an integer-valued polynomial in $\mathbb{Q}[x]$ such that $h(0)$ is not divisible by p. We say that $B \subseteq \mathbb{Z}_{p^d}$ is covered by a set of such integer-valued polynomials $\mathcal{H}$ if for every $b \in B$, we have $p \mid h(b)$ for at least one $h \in \mathcal{H}$. The price of the set B is defined as

$$\mathit{price}(B) = \min\{\sum_{h \in \mathcal{H}} \deg(h) : B \text{ is covered by } \mathcal{H}, \text{ such that for all } h \in \mathcal{H}, p \nmid h(0)\}.$$

Theorem 6. *Suppose that there are given some m-variable polynomials $f_1, f_2, \dots, f_n$ over $\mathbb{Z}$ without constant terms and some sets $Q_1, Q_2, \dots, Q_n$ such that $Q_i \subseteq \mathbb{Z}_{p^{d_i}}$ and $0 \in Q_i$ for all i. If*

$$m > \sum_{i=1}^{n} \deg(f_i) \cdot price(\mathbb{Z}_{p^{d_i}} \backslash Q_i)$$

then exists a $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that

$$f_i(\mathbf{x}) \equiv q_i \pmod{p^{d_i}} \quad \text{for some } q_i \in Q_i \text{ for all } i.$$

We will prove this theorem in Section 3. It is easy to check that Theorem 6 implies Corollary 2: let $d = 1$, so $0 \in Q \subseteq \mathbb{F}_p$. Then, $\{h(x) = x - q : q \notin Q\}$ covers $\mathbb{F}_p \backslash Q$ with price $|\mathbb{F}_p \backslash Q|$.

Theorem 3 and Theorem 4 will follow from Theorem 6 via the following general estimation for $F(\mathbf{d}, \mathbf{Q})$ which we will prove in Section 4.

Theorem 7. *$F(\mathbf{d}, \mathbf{Q}) \leqslant \sum_{i=1}^{n} price(\mathbb{Z}_{p^{d_i}} \backslash Q_i)$.*

In Section 4, we will give a general and constructive bound for *price*(B), which gives a strictly stronger estimation for $F(\mathbf{d}, \mathbf{Q})$ than that one in Theorem 4. We also show a wide class where this estimation is tight.

In the rest of the paper, we analyze the related computational questions. In Section 6, we will prove that the 2^d-divisible subgraph problem belongs to the complexity class Polynomial Parity Argument (PPA). We reduce the 2^d-divisible subgraph problem to the search problem of the Combinatorial Nullstellensatz over $\mathbb{F}_2$ and in Section 5, we verify West's conjecture: the search problem of the Combinatorial Nullstellensatz over $\mathbb{F}_2$ is also in PPA, if the polynomial is given in a general form such as in most of the applications. In Section 7, we focus on degree-constrained subgraphs modulo prime powers, and we will prove an analogous theorem for Shirazi-Verstraëte theorem [7].

3 The proof of Theorem 6

The proof of Theorem 6 presented here is similar to the proof of Theorem 4 in [3]. Alon et al. used a similar polynomial to the one in Equation (1), however, they used only the special construction of Equation (2) instead of arbitrary polynomials. Now we extend it to arbitrary integer-valued polynomials h and we can use more than one polynomial at the same time.

We apply the following corollary of Gregory-Newton formula for integer-valued polynomials, see e.g. [6].

Theorem 8. *Let $h(x)$ be an integer-valued polynomial in $\mathbb{Q}[x]$, namely, for every integer T, $h(T)$ is an integer. Then, $h(x)$ can be written as $\sum_{r=0}^{d} \alpha_r \binom{x}{r}$ where $\alpha_r \in \mathbb{Z}$.*

In the following abstract definitions, one can think of the polynomial f as the 'true meaning' of the problem such as f_i in Corollary 2, and one can think of the polynomial h as the covering polynomial in Definition 5.

The key idea is in the following observation. Although $h(x)$ may have non-integral coefficients, we can construct a polynomial $\Psi^h(f)$ over $\mathbb{Z}$ that satisfies the equality $\Psi^h(f)(\mathbf{s}) = h(f(\mathbf{s}))$, if $\mathbf{s} = (s_1, s_2, \ldots, s_m) \in \{0,1\}^m$. Since $\Psi^h(f)$ have integral coefficients, it can be considered over $\mathbb{F}_p$, so some information over $\mathbb{Z}$ – and hence, modulo p^d – can be encoded over $\mathbb{F}_p$.

Definition 9. Let $f = \sum_{i=1}^{k} p_i$ be a polynomial over $\mathbb{Z}$, where each p_i is a monomial with coefficient 1. Let $\Psi_r(f) \in \mathbb{Z}[x_1, \ldots, x_m]$ be the following polynomial:

$$\Psi_r(f) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant k} p_{i_1} p_{i_2} \ldots p_{i_r}.$$

The degree of the constructed polynomial $\Psi_r(f)$ is at most $r \cdot \deg(f)$. It is worth noting that if $\mathbf{s} = (s_1, s_2, \ldots, s_m) \in \{0,1\}^m$, then the possible values of $p_i(\mathbf{s})$ are 0 and 1, so if the number of p_is such that $p_i(\mathbf{s}) = 1$ is c, then the number of terms in $\Psi_r(f)$ that are 1 at $\mathbf{s}$ is precisely $\binom{c}{r}$.

Definition 10. Let $f = \sum_{i=1}^{k} p_i$ be a polynomial over $\mathbb{Z}$ as above. Let $h(x) = \sum_{r=0}^{d} \alpha_r \binom{x}{r}$ be an integer-valued polynomial in $\mathbb{Q}[x]$ where $\alpha_r \in \mathbb{Z}$. Let $\Psi^h(f) \in \mathbb{Z}[x_1, \ldots, x_m]$ be the following polynomial:

$$\Psi^h(f) = \sum_{r=0}^{d} \alpha_r \Psi_r(f).$$

Note that, $\deg(\Psi^h(f)) \leqslant deg(h) \cdot \deg(f)$. In the following lemma, we can obtain the benefit of these definitions: $h(f(\mathbf{x}))$ can be written as a polynomial with integer coefficients.

Lemma 11. *Let $f = \sum_{i=1}^{k} p_i$ be a polynomial over $\mathbb{Z}$ as above. Let $h(x) = \sum_{r=0}^{d} \alpha_r \binom{x}{r}$ be an integer-valued polynomial as above. Further, let $\mathbf{s} = (s_1, s_2, \ldots, s_m) \in \{0,1\}^m$.*

Then,

$$\Psi^h(f)(\mathbf{s}) = h(f(\mathbf{s})).$$

Proof. Let $c = f(\mathbf{s})$. Then, the number of terms in $\Psi_r(f)$ that are 1 at $\mathbf{s}$ is precisely $\binom{c}{r}$, the other terms are 0. So

$$\Psi^h(f)(\mathbf{s}) = \sum_{r=0}^{d} \alpha_r \Psi_r(f)(\mathbf{s}) = \sum_{r=0}^{d} \alpha_r \binom{c}{r} = h(c) = h(f(\mathbf{s})).$$

□

Now we are ready to prove Theorem 6.

Proof of Theorem 6. To simplify the notation, let C_i be the complementary set of Q_i, that is, $\mathbb{Z}_{p^{d_i}} \backslash Q_i$. Due to the definitions, there exists a set of polynomials $\mathcal{H}_i$ which covers C_i with the total degree $price(C_i)$. Let us consider the following polynomial in $\mathbb{F}_p[x_1, \ldots, x_m]$:

$$f(\mathbf{x}) = \prod_{i=1}^{n} \prod_{h \in \mathcal{H}_i} \Psi^h(f_i(\mathbf{x})) - c \cdot \prod_{j=1}^{m} (1 - x_j), \tag{1}$$

where c is a nonzero constant to be defined later.

The degree of the first part of the polynomial is at most $\sum_{i=1}^{n}\big(\deg(f_i)\cdot\sum_{h\in\mathcal{H}_i} deg(h)\big) = \sum_{i=1}^{n}\deg(f_i)\cdot price(C_i) < m$, so the degree of the polynomial f is m, and the coefficient of $x_1x_2\dots x_m$ is $-c\cdot(-1)^m \neq 0$.

If $\mathbf{x}=\mathbf{0}$, then the first part is nonzero, because $h(0)$ is not divisible by p for every $h\in\mathcal{H}_i$. Let c be the value of the first part at $\mathbf{0}$. So, $f(\mathbf{0}) = c - c = 0$. Let $t_j = 1, S_j = \{0,1\}$. Then, the conditions of Combinatorial Nullstellensatz hold, so there exists an $\mathbf{s}\in\{0,1\}^m$ such that $f(\mathbf{s})\neq 0$. For this $\mathbf{s}\in\{0,1\}^m$, at least one component of $\mathbf{s}$ is 1 due to $f(\mathbf{0})=0$, so the second part of the polynomial f is zero.

For the sake of contradiction, suppose that $f_i(\mathbf{s})\in C_i$. Since $\mathcal{H}_i$ covers C_i, there exists an integer-valued polynomial $h\in\mathcal{H}_i$ such that $p|f_i(\mathbf{s})$. This means that the first part of the polynomial f is also zero at vector $\mathbf{s}$, so $f(\mathbf{s})=0$, and this is a contradiction.

So,

$$f_i(\mathbf{s}) \equiv q_i \pmod{p^{d_i}} \quad \text{for some } q_i\in Q_i \text{ for every } i=1,\dots,n,$$

completing the proof. □

4 The generalization of Olson's theorem: estimation for $\boldsymbol{F}(\mathrm{d},\mathrm{Q})$

Let us now derive Theorem 7 from Theorem 6.

Proof of Theorem 7. Let $f_i(x_1,\dots,x_m) = \sum_{j=1}^{m} a_{ij}x_j$ and $m > \sum_{i=1}^{n} price(\mathbb{Z}_{p^{d_i}}\backslash Q_i)$. Applying Theorem 6, there exists a vector $\mathbf{0}\neq\mathbf{s}\in\{0,1\}^m$ such that

$$f_i(\mathbf{s}) \equiv q_i \pmod{p^{d_i}} \quad \text{for some } q_i\in Q_i \text{ for every } i=1,\dots,n.$$

Let $J=\{j : s_j = 1\}$. Then,

$$\sum_{j\in J} a_{ij} = f_i(\mathbf{x}) \equiv q_i \pmod{p^{d_i}} \quad \text{for some } q_i\in Q_i \text{ for every } i=1,\dots,n.$$

Hence, $F(\mathbf{d},\mathbf{Q}) \leqslant \sum_{i=1}^{n} price(\mathbb{Z}_{p^{d_i}}\backslash Q_i)$. □

We are ready to show that Theorem 7 implies Theorem 4 and its special case, Theorem 3.

Let d be arbitrary, and $0\in Q'\subseteq\mathbb{Z}_{p^d}$ be a set of distinct integers modulo p. Then, let

$$h(T) := \frac{1}{p^\delta}\prod_{q\notin Q'}(T-q), \text{ where } \delta = \sum_{r=0}^{d-1}(p^r-1). \tag{2}$$

For every integer T, in the product $\prod_{q\notin Q'}(T-q)$, at least $p^{d-r}-1$ numbers are divisible by p^r for every $1\leqslant r\leqslant d$. Hence $h(T)$ is an integer-valued polynomial. Further, $h(T)$ is not divisible by p if and only if no factor is divisible by p^d. So $h(T)$ is divisible by p if and only if $T \equiv q \pmod{p^d}$ for some $q \notin Q'$. Hence, $h(0)$ is not divisible by p and $h(T)$ covers $\mathbb{Z}_{p^d} \backslash Q'$ with price $deg(h) = p^d - |Q'|$.

This implies that if $0 \in Q$ is an arbitrary subset of $\mathbb{Z}_{p^d}$, $price(\mathbb{Z}_{p^d} \backslash Q) \leqslant p^d - card_p(Q)$, so Theorem 4 follows from Theorem 7.

Furthermore, Theorem 7 enables to obtain strictly stronger bounds than the one in Theorem 4 via the following general constructive estimation on $price(B)$.

Definition 12. For set B of integers modulo p, let $\kappa(B) = |B|$. For any $d > 1$ and for set B of integers modulo p^d, let us define k as the cardinality of the set $\{b \in B : b \text{ is divisible by } p^{d-1}\}$ and $\hat{B}$ as the set of such residues modulo p^{d-1} that appear in B more than k times. Then, let $\kappa(B) = k \cdot p^{d-1} + \kappa(\hat{B})$.

The following definition for κ is equivalent to the above one. It gives a way to compute the value of $\kappa(B)$. Let B be a set of integers modulo p^d. Now, we define integers $k_{d-1}, \dots, k_0$ and sets $B_d, \dots, B_1$ such that B_r is a set of integers modulo p^r. Let $B_d = B$ and

$$k_{d-1} = |\{b \in B : b \text{ is divisible by } p^{d-1}\}|.$$

Then, for $r = d-1, \dots, 2, 1$, if B_{r+1} is given, let B_r be the set of such residues modulo p^r that appear in B_{r+1} more than k_r times and let $k_{r-1} = |\{b \in B_r : b \text{ is divisible by } p^{r-1}\}|$. Then, $\kappa(B) = \sum_{r=0}^{d-1} k_r \cdot p^r$.

Example 13. Let $p^d = 5^3 = 125$ and

$$B = \{1, 2, 5, 6, 12, 20, 40, 42, 50, 51, 52, 56, 69, 70, 87, 95, 100, 101, 102, 112\}.$$

Then, $k_2 = 2$, because two integers in B are divisible by 25 (50 and 100). Then, $B_2 = \{1, 2, 12, 20\}$. For instance, $20 \in B_2$, because $20 \equiv 70 \equiv 95$ are in B_3, but $6 \notin B_2$, because only $6 \equiv 56$ are in B_3. So on, $k_1 = 1$, $B_1 = \{2\}$, and $k_0 = 1$. Hence, $\kappa(B) = 2 \cdot 25 + 1 \cdot 5 + 1 \cdot 1 = 56$.

Theorem 14. *With the above definition, $price(B) \leqslant \kappa(B)$ holds.*

Proof. As the first step, we construct a polynomial that covers a complete p^r-residue system modulo p^{r+1} with price p^r.

Let $q_1, q_2, \dots, q_{p^r}$ be a complete p^r-residue system and let

$$h(T) := \frac{1}{p^\delta} \prod_{i=1}^{p^r} (T - q_i), \text{ where } \delta = \sum_{j=0}^{r-1} p^j.$$

For every integer T, the integers $T - q_1, T - q_2, \dots, T - q_{p^r}$ also form a complete residue system modulo p^r, so in the product $\prod_{i=1}^{p^r} (T - q_i)$, p^{r-j} factors are divisible by p^j for every $1 \leqslant j \leqslant r$. Hence, the product is divisible by p^δ and $h(T)$ is an integer-valued polynomial.

Further, $h(T)$ is divisible by p if and only if the factor which is divisible by p^r is also divisible by p^{r+1}. This means $T \equiv q_i \pmod{p^{r+1}}$ for some i, that is, $h(T)$ covers $q_1, q_2, \dots, q_{p^r}$ modulo p^{r+1}, precisely, it covers the set

$$\{q \in \mathbb{Z}_{p^d} : q \equiv q_i \pmod{p^{r+1}} \text{ for some } i\}$$

with price p^r.

Then, by Definition 12, the statement immediately follows: one can cover the integers that are divisible by p^{d-1} with k such conditions. These conditions also covers other residues k times, so such residues are not covered by the conditions that appear more than k times. These remaining residues are in $\hat{B}$ modulo p^{d-1} and they can be covered with $\kappa(\hat{B})$. □

4.1 A special case when Theorem 7 is tight

Here we show a special case when the theorem is tight. This statement shows a wide class where Theorem 7 and hence Theorem 6 give tight estimation. In general, tightness is not yet known. This result also shows cases when Theorem 4 gives strictly weaker estimation than the one in Theorem 7.

Definition 15. Let R be a subset of $\{0, 1, \ldots, d-1\}$. Let us define the set $\Omega \subseteq \mathbb{Z}_{p^d}$ by the following property: $c \in \Omega$ if and only if $c^{(r)} = 0$ for every $r \in R$ in the $c^{(d-1)} \ldots c^{(1)}c^{(0)}$ form of c in base p. We call Ω the R-zero set modulo p^d. Let $\sigma(R) = (p-1)\sum_{r \in R} p^r$.

Theorem 16. *Let R_i be an arbitrary subset of $\{0, 1, \ldots, d_i - 1\}$ and denote the R_i-zero set modulo p^{d_i} by Ω_i. Then, $F(\mathbf{d}, \mathbf{\Omega}) = \sum_{i=1}^{n} \sigma(R_i)$.*

Proof. We show that $\sigma(R) = \kappa(\mathbb{Z}_{p^d} \backslash \Omega)$ and hence $F(\mathbf{d}, \mathbf{\Omega}) \leqslant \sum_{i=1}^{n} \sigma(R_i)$ by Theorem 7 and Theorem 14.

The proof is by induction on d. Let $B = \mathbb{Z}_{p^d} \backslash \Omega$. Further, let $d' = d - 1$ and let Ω' be the $R' = R \backslash \{d-1\}$-zero set modulo $p^{d'}$ and $B' = \mathbb{Z}_{p^{d'}} \backslash \Omega'$. By induction, $\sigma(R') = \kappa(B')$.

If $d - 1 \notin R$, then $k = |\{b \in B : b \text{ is divisible by } p^{d-1}\}| = 0$, and $\hat{B} = B'$. Then $\kappa(B) = 0 + \kappa(B') = \sigma(R') = \sigma(R)$.

If $d - 1 \in R$, then $k = |\{b \in B : b \text{ is divisible by } p^{d-1}\}| = p - 1$ and $\hat{B} = B'$. Then $\kappa(B) = (p-1) \cdot p^{d-1} + \kappa(B') = (p-1) \cdot p^{d-1} + \sigma(R') = \sigma(R)$.

Moreover, these bounds are tight: $F(\mathbf{d}, \mathbf{\Omega}) = \sum_{i=1}^{n} \sigma(R_i)$, because if $m = \sum_{i=1}^{n} \sigma(R_i)$, then there exists integers a_{ij} such that the proper nontrivial subset does not exist. Let a_{ij} be -1 if $\sum_{l=1}^{i-1} \sigma(R_l) < j \leqslant \sum_{l=1}^{i} \sigma(R_l)$, and zero otherwise. However, in the range $-p^{d_i}, \ldots, 0$, the largest integer of the R_i-zero sets modulo p^{d_i} is

$$\sum_{r \notin R_i} (p-1) \cdot p^r = p^{d_i} - 1 - \sum_{r \in R_i} (p-1) \cdot p^r = p^{d_i} - 1 - \sigma(R_i) \equiv -\sigma(R_i) - 1 \pmod{p^{d_i}}$$

and $-\sigma(R_i) \leqslant \sum_{j \in J} a_{ij} \leqslant 0$, hence, no nonempty subset exists that fulfills the condition ($\clubsuit$). □

5 Complexity aspects of the Combinatorial Nullstellensatz

Due to various applications of the Combinatorial Nullstellensatz, it is a natural and important question to determine the computational complexity of the corresponding search problem. Now, we study the complexity of the Combinatorial Nullstellensatz over $\mathbb{F}_2$. It is worth noting that if $t_i = 0$ for some indices, then we could choose $|S_i| = 1$, so in an appropriate vector $(s_1, s_2, \ldots, s_m)$, we have to choose the only element of S_i to s_i and therefore, we could replace x_i by the only element of S_i in f. Hence, we may assume that $S_i = \mathbb{F}_2$ for every index i and the problem is finding a vector $(s_1, s_2, \ldots, s_m) \in \mathbb{F}_2^m$ such that $f(s_1, s_2, \ldots s_m) \neq 0$.

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

It is easy to check that the problem belongs to P if the polynomial is given explicitly as the sum of monomials. First, we can replace the term $x_{i_1}^{t_{i_1}} x_{i_2}^{t_{i_2}} \ldots x_{i_k}^{t_{i_k}}$ by $x_{i_1} x_{i_2} \ldots x_{i_k}$, because these are equal due to the fact $0^t = 0, 1^t = 1$ in $\mathbb{F}_2$. Substitute 0 and 1 to x_1: let $g(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$ and $h(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$. If in f the coefficient of $x_2 x_3 \ldots x_m$ is nonzero, then in g the coefficient of $x_2 x_3 \ldots x_m$ will be also nonzero. If it is zero, in h the coefficient of $x_2 x_3 \ldots x_m$ will be nonzero. Then, substitute 0 and 1 to x_2 and in one of them the coefficient of $x_3 x_4 \ldots x_m$ will be nonzero, and so on. Finally, we obtain a constant nonzero polynomial, and this means that for this substitution $\mathbf{s} \in \mathbb{F}_2^m$, $f(\mathbf{s}) \neq 0$ holds. It is worth noting that a similar polynomial time algorithm can be obtained over arbitrary finite field, if the polynomial is given explicitly.

However, if the polynomial is given as the sum of products of polynomials (such as in most of the applications), the problem is not known to be solvable in polynomial time. Furthermore, the existence of an efficient general algorithm for this case would imply that there cannot be any one-way permutations [10].

An open question in [5] is about the complexity of the Combinatorial Nullstellensatz conjecturing that the problem over $\mathbb{F}_2$ belongs to the class Polynomial Parity Argument (PPA) defined by Papadimitriou [4].

In this section, we verify this conjecture: we prove that the Combinatorial Nullstellensatz over $\mathbb{F}_2$ is in PPA if the polynomial is given as the sum of products of polynomials. Consequently, the applications given in Sections 6 and 7 also belong to PPA.

Roughly speaking, the class PPA is a subclass of the semantic class TFNP, the set of all total search problems. A search problem is called *total* if the corresponding decision problem is trivial, that is, for every feasible input, there exists a solution. A total problem is usually equipped with a mathematical proof showing that it belongs to TFNP, so the problems can be classified based on their proof styles. The complexity class PPA is the class of all search problems whose totality is proved using the parity argument: *Every finite graph has an even number of odd-degree nodes.*

It is worth noting that the class TFNP coincides with the set of search variants of NP $\cap$ coNP problems [11], so the class PPA is between the the set of search variants of P and NP.

The class PPA can be defined with a canonical complete problem, the End Of The Line. Hence, a computational search problem is in PPA if and only if it is reducible to the problem End Of The Line.

In this problem, we are given a graph $G = (V, E)$ on exponentially many nodes. It can be assumed that each node has an unique code from Σ^n, that is $V \subseteq \Sigma^n$. The edges of the graph are described by a polynomial time algorithm in n. This polynomial time pairing function is the following.

For an undirected graph $G = (V, E)$, the function $\phi : V \times V \to V \cup \{*\}$ is called a *pairing function*, if it satisfies the following conditions: if vw is not an edge of G, let $\phi(v, w) = *$. Otherwise, it outputs a node $w' = \phi(v, w)$ such that w' is also connected to v and $\phi(v, \phi(v, w)) = w$ holds. Furthermore, for every v, at most one such node w exists with property $\phi(v, w) = w$.

It means that ϕ pairs up the neighbours of an input node v: for an even-degree node v, it pairs its neighbours completely, and for an odd-degree node v, ϕ pairs all but one neighbours. The task is to find an odd-degree node v and a node w such that $\phi(v, w) = w$. This node w verifies that v is an odd-degree node.

The problem End Of The Line can be defined as follows.

End of the Line.

Input: an undirected finite graph $G = (V, E)$ in the above way. The edges of the graph is described by a polynomial time pairing function. Furthermore, a node ε is given which has odd number of edges and a node δ which shows it: $\phi(\varepsilon, \delta) = \delta$.

Find: another node v which has odd number of edges and a node w which give the certificate $\phi(v, w) = w$.

In order to prove problems belonging to PPA, we give reductions to the problem End Of The Line.

It is worth noting that this problem is computationally equivalent to the problem in which the nodes have at most two neighbours, a node of degree one is given and the task is to find another node which has exactly one incident edge. (Instead of the polynomial time pairing function, a polynomial time algorithm is given which outputs the neighbours of an input node.) It is easy to see that this is an easier problem, however, Papadimitriou showed that they are computationally equivalent.

In [4], Papadimtriou shows that the following computational problem Chévalley MOD 2 belongs to the class PPA. The required vector exists due to Chévalley's following theorem.

Theorem 17 (Chévalley)**.** *Let $\mathbb{F}$ be a finite field with characteristic p. Let $p_1, p_2, \ldots, p_n$ be polynomials in m variables over $\mathbb{F}$. Suppose that $\sum_{i=1}^{n} \deg(p_i) < m$. Then, the number of common solutions of the polynomial equation system $p_i(x_1, \ldots, x_m) = 0$ $(i = 1 \ldots n)$ is divisible by p. In particular, if there is a solution, there exists another.*

Chévalley MOD 2.

Input: polynomials $p_1, p_2, \ldots, p_n$ in $\mathbb{F}_2[x_1, \ldots x_m]$ such that

$$\sum_{i=1}^{n} \deg(p_i) < m.$$

Also, we are given a root $(c_1, c_2, \ldots, c_m) \in \mathbb{F}_2^m$ of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$.

Find: another root of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$.

Using Theorem 18 and that Chévalley's theorem can be proved via a reduction to the Combinatorial Nullstellensatz, see [1], one can give an alternative proof for the PPA membership of Chévalley MOD 2. Originally, this reduction motivates West's question [5] about the complexity of the Combinatorial Nullstellensatz.

Now, let us define the following computational problem. Note that the required vector exists due to the Combinatorial Nullstellensatz.

Combinatorial Nullstellensatz over $\mathbb{F}_2$.

Input: a polynomial f in m variables in a general form

$$f = \sum_{i=1}^{k} \left(\prod_{j=1}^{m_i} p_{ij} \right),$$

where p_{ij} is an explicitly given polynomial in $\mathbb{F}_2[x_1, \ldots x_m]$, k, m_i and the number of monomials of p_{ij} is polynomially bounded in m. Suppose that $\sum_{j=1}^{m_i} \deg(p_{ij}) \leqslant m$ for all i and there is a polynomial time pairing function which can pair up all but one terms $x_1 x_2 \ldots x_m$ to prove that the degree of f is m and the coefficient of $x_1 x_2 \ldots x_m$ is nonzero.

Find: a vector $(s_1, s_2, \ldots, s_m) \in \mathbb{F}_2^m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

Theorem 18. *The* Combinatorial Nullstellensatz over $\mathbb{F}_2$ *is polynomially reducible to* End of the Line. *Consequently, The* Combinatorial Nullstellensatz over $\mathbb{F}_2$ *is in PPA.*

The proof of Theorem 18 is similar to the proof for PPA membership of Chévalley MOD 2. Our construction is based on that proof, nevertheless, we need a new key idea about the upper-level pairing function which pairs up blocks whose value at 1 for the substitution $\mathbf{x}$.

We construct a graph, the nodes correspond to the vectors and the terms. The nodes with odd degree correspond to the vectors $\mathbf{x}$ such that $f(\mathbf{x}) \neq 0$ and an extra node w. As we mentioned, we have to present a pairing function. It can be done easily at the terms, but it is more complicated at the vectors. The main idea here is the following.

We call the polynomials $\prod_{j=1}^{m_i} p_{ij}$ as the blocks of the input polynomial f. Each term is the product of monomials from the given polynomials of a block, so each term in the ith block can be represented by an $(m_i + 1)$-tuple of integers: $(i, a_{i,1}, \dots, a_{i,m_i})$. The first coordinate shows the block the term belongs to, and the other coordinates show the monomials the term is product of: it is the product of $a_{i,j}$th monomials of p_{ij}. (Note that the same term might have more than one occurrence and these occurrences are represented by different tuples.) In the next proof, we will pair up these tuples.

Remark 19. In a standard PPA-type problem definition it is required that the assumptions of the problem should be in NP. If the input is feasible, we have to return a solution, but if the input is infeasible, we have to return a polynomial certificate of infeasibility.

It is easy to check that the assumptions in the definition of the Combinatorial Nullstellensatz over $\mathbb{F}_2$ are in NP. In the case of an infeasible input, we can give the following certificate: the index i such that $\sum_{j=1}^{m_i} \deg(p_{ij}) > n$ or two occurrences of the term $x_1 x_2 \dots x_m$ for which the polynomial time pairing function fails.

Proof of Theorem 18. We shall construct a graph Γ whose odd-degree nodes precisely correspond to appropriate vectors $\mathbf{s}$ such that $f(\mathbf{s}) \neq 0$ and furthermore, we add an extra node w: the standard leaf.

The graph is bipartite. The nodes on one side are all the vectors in $\mathbb{F}_2^m$ and the extra node w. The nodes of the other side are the terms of the polynomial $f = \sum_{i=1}^{k} \left(\prod_{j=1}^{m_i} p_{ij} \right)$. Each term is represented in the above way as an $(m_i + 1)$-tuple of integers.

There is an edge between vector $\mathbf{x}$ and term t if and only if $t(\mathbf{x}) = 1$, and there is an edge between the extra node w and the term t if and only if $t(\mathbf{x}) = x_1 x_2 \dots x_m$.

It is easy to see that for a vector $\mathbf{x}$, $f(\mathbf{x}) \neq 0$ holds if and only if its degree is odd. The extra node w also has an odd degree because the coefficient of $x_1 x_2 \dots x_m$ is nonzero due to the assumptions.

All nodes in the other side have even degree. In Γ, the degree of each term $t(\mathbf{x}) = x_1 x_2 \dots x_m$ is precisely 2, because it is connected only to the vector $(1, 1, \dots, 1)$ and to the extra w node. Let t be any other term, and let x_l be a variable not appearing in t. Then, if t is connected to $(s_1, s_2, \dots, 0, \dots, s_m)$, it is also connected to $(s_1, s_2, \dots, 1, \dots, s_m)$, so the degree of these nodes are even.

Therefore, odd-degree nodes are precisely the vectors $\mathbf{s}$ such that $f(\mathbf{s}) \neq 0$ and the extra node w.

However, the nodes of this graph have exponentially large degrees, and therefore we must exhibit a pairing function between the edges incident to a node.

For a node corresponding to the term $t(\mathbf{x}) \neq x_1 x_2 \dots x_m$, we pair up the vector $\mathbf{x}$ for which $t(\mathbf{x}) = 1$ to $(x_1, x_2, \dots, 1 - x_l, \dots x_m)$ where x_l is such a variable which does not appear in t. (We choose the smallest such index l.) The degree of nodes corresponding to terms $x_1 x_2 \dots x_m$ in this side is only 2, its edges can be simply paired up.

For such node corresponding to a vector $\mathbf{x}$ that $f(\mathbf{x}) = 0$ holds, we should pair up the terms such that $t(\mathbf{x}) = 1$. Suppose that term t is represented by $(i, a_{i1}, \ldots, a_{ij}, \ldots, a_{i,m_i})$.

Denote its block by $g = \prod_{j=1}^{m_i} p_{ij}$. If $g(\mathbf{x}) = 0$, then there is an index j such that $p_{ij}(\mathbf{x}) = 0$. Pick the smallest such j. There is an even number of monomials of p_{ij} such that $p_{ij}(\mathbf{x}) = 1$. We pair these monomials by a pairing function ϕ_i. Then the mate of term $(i, a_{i1}, \ldots, a_{ij}, \ldots, a_{i,m_i})$ is $(i, a_{i1}, \ldots, \phi_i(a_{ij}), \ldots, a_{i,m_i})$.

It is a more complicated case when $g(\mathbf{x}) = 1$. Since $f(\mathbf{x}) = 0$, there is an even number of indices l, such that $\left(\prod_{j=1}^{m_l} p_{lj}\right)$ is 1 at $\mathbf{x}$. We pair these blocks by a pairing function ϕ. So, for i and every $j = 1, \ldots, m_i$, p_{ij} is 1 at $\mathbf{x}$, and we can pair all but one monomials of p_{ij} with $p_{ij}(\mathbf{x}) = 1$ by a pairing function ϕ_{ij}. One of them does not have a mate, denote its index by ω_{ij}. If $a_{ij} = \omega_{ij}$ for all indices j, then we define its mate to be $(\phi(i), \omega_{\phi(i),1}, \ldots, \omega_{\phi(i),m_{\phi(i)}})$. Otherwise there is an index j such that $a_{ij} \neq \omega_{ij}$. Pick the smallest such j. Then the mate of $(i, a_{i1}, \ldots, a_{i,m_i})$ is defined as $(i, a_{i1}, \ldots, \phi_{ij}(a_{ij}), \ldots, a_{i,m_i})$.

Observe that this gives a bijection and a correct pairing function.

For such node corresponding to a vector $\mathbf{x}$ that $f(\mathbf{x}) = 1$ holds, we should pair up all but one terms such that $t(\mathbf{x}) = 1$. If t is a term of such block $g = \prod_{j=1}^{m_i} p_{ij}$ that $g(\mathbf{x}) = 0$ holds, it can be paired up similarly to the previous case. If $g(\mathbf{x}) = 1$, we pair these blocks by a pairing function. One of them does not have a mate, denote its index by Ω. If g is not the block with index Ω, the pairing can be similar to the previous case. If g is the block with index Ω, we can pair up the terms similarly to the previous case, only the term t represented by $(\Omega, \omega_{\Omega 1}, \ldots, \omega_{\Omega, m_\Omega})$ does not have a mate. So we paired up all but one neighbours of the node corresponding to the vector $\mathbf{x}$.

Finally, we pair up the terms which are connected to the extra node w. These are the terms $x_1 x_2 \ldots x_m$. Due to the assumptions, there is a polynomial time pairing function which can pair up all but one terms $x_1 x_2 \ldots x_m$, so it can pair up the nodes which are connected to the extra node w.

We presented a polynomial algorithm that computes the mate of an edge out of a node, so the proof is complete. □

6 Complexity of finding divisible subgraphs

Alon, Friedland and Kalai proved the following corollary of the original Olson's Theorem 3 and using it in the case $p = 2$, they derived the result on p^d-divisible subgraphs (Theorem 21) mentioned in the Introduction. We present their proofs since they also show the reductions between the corresponding computational problems.

Corollary 20 ([3]). *Let n, m be positive integers and let p be a prime. Let $d_1 \geqslant d_2 \geqslant \ldots \geqslant d_n \geqslant 1$ positive integers and for $i = 1, \ldots, n, j = 1, \ldots, m$ let a_{ij} be an integer such that $\sum_{i=1}^{n} a_{ij}$ is divisible by p for every j index. If $m > p^{d_n - 1} - 1 + \sum_{i=1}^{n-1}(p^{d_i} - 1)$, then there is a subset $\emptyset \neq J \subseteq \{1, 2, \ldots, m\}$ such that $\sum_{j \in J} a_{ij}$ is divisible by p^{d_i} for every $i = 1, \ldots, n$.*

Proof in [3]. For $j = 1, \dots, m$, let $b_{ij} = a_{ij}$, if $i = 1, \dots, n-1$ and let $b_{nj} = \frac{1}{p}\left(\sum_{i=1}^{n} a_{ij}\right)$.

According to Olson's Theorem 3, there is an $\emptyset \neq J \subseteq \{1, 2, \dots, m\}$ such that $\sum_{j \in J} b_{ij}$ is divisible by p^{d_i} for every $i = 1, \dots, n-1$ and $\sum_{j \in J} b_{nj}$ is divisible by $p^{d_{n-1}}$ because $m > p^{d_n - 1} - 1 + \sum_{i=1}^{n-1}(p^{d_i} - 1)$.

However, $\sum_{j \in J} b_{nj} = \sum_{j \in J} \frac{1}{p}\left(\sum_{i=1}^{n} a_{ij}\right)$ is divisible by $p^{d_{n-1}}$, so $\sum_{j \in J}\left(\sum_{i=1}^{n} a_{ij}\right)$ is divisible by p^{d_n}. Because of $d_1 \geqslant d_2 \geqslant \dots \geqslant d_n \geqslant 1$, $\sum_{j \in J} b_{ij} = \sum_{j \in J} a_{ij}$ is divisible by p^{d_n} for every $i = 1, \dots, n-1$, hence $\sum_{j \in J} a_{nj}$ should be divisible by p^{d_n} and we are done. □

Theorem 21 (Alon, Friedland, Kalai, [3])**.** *For the maximum number of edges of a graph G on n vertices that contains no nontrivial p^d-divisible subgraph,*

$$f(n, p^d) = \begin{cases} (p^d - 1) \cdot n & \text{if } p \text{ is an odd prime.} \\ (2^d - 1) \cdot n - 2^{d-1} & \text{if } p = 2 \end{cases}$$

Proof in [3]. Here, we only prove the direction $\leqslant$ of the equality. In [3], Alon et al. showed by examples that these bounds are tight.

Denote the number of edges of G by m. Let $a_{ij} = 1$ if and only if the j^{th} edge is incident to the i^{th} vertex, as usual. (That is, $((a_{ij}))$ is the incidence matrix of G.)

For an odd prime p, suppose $m > (p^d - 1) \cdot n$. According to Olson's Theorem 3 with $d_1 = d_2 = \dots = d_n = d$, there is a nonempty subset J of edges such that $\sum_{j \in J} a_{ij}$ is divisible by p^d for every i, so there is nontrivial p^d-divisible subgraph.

For $p = 2$, suppose $m > (2^d - 1) \cdot n - 2^{d-1} = (n-1) \cdot (2^d - 1) + (2^{d-1} - 1)$. According to Corollary 20 with $d_1 = d_2 = \dots = d_n = d$, there is a nonempty subset J of edges such that $\sum_{j \in J} a_{ij}$ is divisible by p^d for every i, so there is nontrivial p^d-divisible subgraph. The conditions of corollary hold, because $\sum_{i=1}^{n} a_{ij} = 2$ for every index j. □

Let us now define the computational problems corresponding to the above theorems. The existence of the solutions is guaranteed by Theorem 21, Theorem 3 and Corollary 20, respectively.

2^d-DIVISIBLE SUBGRAPH.

Input: a positive integer d and a graph $G = (V, E)$, where $|V| = n$, $|E| = m$ and $m > n \cdot (2^d - 1) - 2^{d-1}$ holds.

Find: a 2^d-divisible subgraph, that is, an $\emptyset \neq F \subseteq E$ such that for every $v \in V$, the number of incident edges of F is divisible by 2^d.

OLSON MOD 2^d.

Input: a positive integer d, the integers n and m such that $m > n \cdot (2^d - 1)$ and given integers a_{ij} $(i = 1, \dots, n, j = 1, \dots, m)$.

Find: a $\emptyset \neq J \subseteq \{1, 2, \dots, m\}$ such that $\sum_{j \in J} a_{ij}$ is divisible by 2^d for every i.

Even-Sum Olson MOD 2^d.

Input: a positive integer d, the integers n and m such that $m > n \cdot (2^d - 1) - 2^{d-1}$ and given integers a_{ij} $(i = 1, \dots, n, j = 1, \dots, m)$ such that $2 \mid \sum_{i=1}^{n} a_{ij}$.

Find: a $\emptyset \neq J \subseteq \{1, 2, \dots, m\}$ such that $\sum_{j \in J} a_{ij}$ is divisible by 2^d for every i.

As we have seen in the previous sections, Olson's theorem can be proved via the Combinatorial Nullstellensatz. It implies the following propositions.

Theorem 22. Olson MOD 2^d *and* Even-Sum Olson MOD 2^d *are polynomially reducible to the* Combinatorial Nullstellensatz over $\mathbb{F}_2$. *Consequently, they are in PPA.*

Proof. In the proof of Theorem 7 and Theorem 6, we construct a polynomial f in m variables over $\mathbb{F}_2$ such that $\deg(f) = m$ and the coefficient of $\prod_{j=1}^{m} x_j$ is nonzero. Such vectors $\mathbf{s}$ that satisfy $f(\mathbf{s}) \neq 0$ precisely correspond to the subsets $\emptyset \neq J \subseteq \{1, 2, \dots, m\}$ such that $\sum_{j \in J} a_{ij}$ is divisible by 2^d for every i.

We only have to check that this reduction is a polynomial reduction. In the proofs the size of the constructed polynomial is $O(2^d \cdot d \cdot n + m)$, which can be bounded $O(nm \log(m))$ due to condition $m > n \cdot (2^d - 1)$, so the reduction is polynomial.

For reduction to the Combinatorial Nullstellensatz over $\mathbb{F}_2$, we have to present a pairing function which can pair up terms $x_1 x_2 \dots x_m$. Here it is obvious, because there is only one term $x_1 x_2 \dots x_m$.

Similarly, one can check that Even-Sum Olson MOD 2^d is also polynomially reducible to the Combinatorial Nullstellensatz over $\mathbb{F}_2$. □

The reduction in the proof of Theorem 21 immediately implies the following.

Theorem 23. 2^d-divisible subgraph *is polynomially reducible to* Even-Sum Olson MOD 2^d. *Consequently,* 2^d-divisible subgraph *is in PPA.*

7 Degree-constrained subgraphs: Louigi's problem

In Louigi's problem, given are a graph $G = (V, E)$ and forbidden sets $F(v) \subseteq \mathbb{N}$ for every $v \in V$. By an F-avoiding subgraph we mean a subgraph $\emptyset \neq E' \subseteq E$ such that for every $v \in V$ the number of incident edges of E' is not in $F(v)$. Shirazi and Verstraëte [7] proved the following theorem. We give a new proof using our techniques.

Theorem 24 (Shirazi, Verstraëte [7])**.** *If* $0 \notin F(v)$ *for all* $v \in V$ *and* $\sum_{v \in V} |F(v)| < |E|$, *then there exists a nontrivial* F*-avoiding subgraph.*

Proof. Let p be a prime greater than the maximum degree in G. For the node $v_i \in V$, let $Q_i = \mathbb{Z}_p \backslash F(v_i)$ and $a_{ij} = 1$ if the node v_i is incident to the edge $e_j \in E$, and 0 otherwise. Due to the conditions, $\sum_{v_i \in V} \mathit{price}(\mathbb{Z}_p \backslash Q_i) = \sum_{v_i \in V} |\mathbb{Z}_p \backslash Q_i| = \sum_{v \in V} |F(v)| < |E|$, so according to Theorem 7, there exists a subset J, which corresponds to a nontrivial F-avoiding subgraph. □

Note that, in [7], the authors also proved their theorem via the Combinatorial Nullstellensatz, but in a different way via polynomials over $\mathbb{R}$.

One may ask a version of Louigi's problem modulo prime powers: given are a prime power p^d, a graph $G = (V, E)$ and forbidden sets modulo p^d: $F(v) \subseteq \mathbb{Z}_{p^d}$ for every $v \in V$. By an F-avoiding subgraph modulo p^d we mean a subgraph $\emptyset \neq E' \subseteq E$ such that for every $v \in V$ the number of incident edges of E' is not congruent to any number in $F(v)$ modulo p^d. We can show the following.

Theorem 25. *If $0 \notin F(v)$ for all $v \in V$ and $\sum_{v \in V} \mathit{price}(F(v)) < |E|$, then there exists a nontrivial F-avoiding subgraph modulo p^d.*

Proof. Similarly to the proof above, for the node $v_i \in V$, let $Q_i = \mathbb{Z}_{p^d} \backslash F(v_i)$ and $a_{ij} = 1$ if the node v_i is incident to the edge $e_j \in E$, and 0 otherwise. Due to the conditions, $\sum_{v_i \in V} \mathit{price}(\mathbb{Z}_p \backslash Q_i) = \sum_{v \in V} \mathit{price}(F(v)) < |E|$, so according to Theorem 7, there exists a subset J, which corresponds to a nontrivial F-avoiding subgraph modulo p^d. □

Frank et al. [8] gave a polynomial time combinatorial algorithm for finding an F-avoiding subgraph as in Theorem 24. For F-avoiding subgraph modulo 2^d, one can show that the search problem belongs to PPA.

Let us define the corresponding computational problem. The existence of a solution is guaranteed by Theorem 25.

Degree-constrained subgraph modulo 2^d.

Input: a positive integer d, a graph $G = (V, E)$, subsets $F(v) \subseteq \mathbb{Z}_{p^d}$ such that $\sum_{v \in V} \mathit{price}(F(v)) < |E|$.

Find: a nontrivial F-avoiding subgraph modulo 2^d.

Similarly to the proofs of Theorems 22, 23, the proofs of Theorems 25, 7, 6 imply the following.

Theorem 26. Degree-constrained subgraph modulo 2^d *is polynomially reducible to* Combinatorial Nullstellensatz over $\mathbb{F}_2$. *Consequently, the problem* Degree-constrained subgraph modulo 2^d *is in PPA.*

Acknowledgments

I am grateful to László Végh for his extremely helpful remarks and valuable suggestions. Also, I would like to thank the anonymous referee for providing constructive comments.

References

[1] N. Alon: *Combinatorial Nullstellensatz*. Combinatorics, Probability and Computing, 8, 1999, pp. 7-29.

[2] J. E. Olson: *A combinatorial problem on finite Abelian groups, I.* Journal of Number Theory, Vol. 1, Issue 1, January 1969, pp. 8-10.

[3] N. Alon, S. Friedland, G. Kalai: *Regular subgraphs of almost regular graphs*. Journal of Combinatorial Theory, Series B Vol. 37, Issue 1, August 1984, pp. 79-91.

[4] C. H. Papadimitriou: *On the Complexity of the Parity Argument and Other Inefficient Proofs of Existence*. Journal of Computer and System Sciences Vol. 48, Issue 3, June 1994, pp. 498-532.

[5] D. B. West: *Research Experiences for Graduate Students in Combinatorics (Open Problem Collection)* http://www.math.uiuc.edu/~west/regs/combnull.html

[6] P-J. Cahen, J-L. Chabert: *Integer-valued Polynomials*. Mathematical Surveys and Monographs 48, Providence, RI: American Mathematical Society 1997.

[7] H. Shirazi, J. Verstraëte: *A note on polynomials and f-factors of graphs*. Electronic J. of Combinatorics, 15, 2008, N22.

[8] A. Frank, L. C. Lau, J. Szabó: *A note on degree-constrained subgraphs*. Discrete Mathematics, 2008, 308.12, pp. 2647-2648.

[9] D. Brink: *Chevalley's theorem with restricted variables*. Combinatorica 2011, 31.1, pp. 127-130.

[10] N. Alon: *Discrete Mathematics: methods and challenges*. Proc. of the International Congress of Mathematicians, Beijing 2002, China, Higher Education Press 2003, pp. 119-135.

[11] C. H. Papadimitriou, N. Meggido: *On total functions, existence theorems and computational complexity*. Theoretical Computer Science, Vol. 81, Issue 2, 30 April 1991, pp. 317-324.