On the Complexity of Hilbert Refutations for Partition

S. Margulies

Department of Mathematics, Pennsylvania State University, State College, PA

S. Onn

Industrial Engineering & Management, Technion - Israel Institute of Technology, Haifa, Israel

D.V. Pasechnik

School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

Abstract

Given a set of integers W, the PARTITION problem determines whether W can be divided into two disjoint subsets with equal sums. We model the PARTITION problem as a system of polynomial equations, and then investigate the complexity of a Hilbert's Nullstellensatz refutation, or certificate, that a given set of integers is not partitionable. We provide an explicit construction of a minimum-degree certificate, and then demonstrate that the PARTITION problem is equivalent to the determinant of a carefully constructed matrix called the partition matrix. In particular, we show that the determinant of the partition matrix is a polynomial that factors into an iteration over all possible partitions of W.

Key words: Hilbert's Nullstellensatz, linear algebra, partition

1. Introduction

The NP-complete problem PARTITION [12] is the question of deciding whether or not a given set of integers $W = \{w_1, \ldots, w_n\}$ can be broken into two sets, I and $W \setminus I$, such that the sums of the two sets are equal, or that $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$. Since it is widely believed that NP $\neq$ coNP, it is interesting to study various types of *refutations*, or certificates for the *non*-existence of a partition in a given set W.

In this paper, we study the certificates provided by Hilbert's Nullstellensatz (see [1, 2, 11, 18, 20] and references therein). Given an algebraically-closed field $\mathbb{K}$ and a set of

Email addresses: `margulies@math.psu.edu` (S. Margulies), `onn@ie.technion.ac.il` (S. Onn), `dima@ntu.edu.sg` (D.V. Pasechnik).

Preprint submitted to Elsevier *31 December 2013*

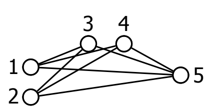
polynomials $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, Hilbert's Nullstellensatz states that the system of polynomial equations $f_1 = f_2 = \cdots = f_s = 0$ has *no* solution if and only if there exist polynomials $\beta_1, \ldots, \beta_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that $1 = \sum_{i=1}^{s} \beta_i f_i$. We measure the complexity of a given certificate in terms of the size of the β coefficients, since these are the unknowns we must discover in order to demonstrate the *non*-existence of a solution to $f_1 = f_2 = \cdots = f_s = 0$. Thus, we measure the degree of a Nullstellensatz certificate as $d = \max\{\deg(\beta_1), \ldots, \deg(\beta_s)\}$.

There is a well-known connection between Hilbert's Nullstellensatz and a particular sequence of linear algebra computations. These sequences have been studied from both a theoretical perspective [5, 11], and a computational perspective [9, 10]. When the polynomial ideal contains $x_i^2 - x_i$ for each variable (thus forcing the variety to contain only 0/1 points), these sequences have also been explored as algebraic proof systems [4, 6, 17, 21]. Additionally, D. Grigoriev demonstrates a linear lower bound for the knapsack problem in [13] (see also [14]), and Buss and Pitassi [5] show that a polynomial system loosely based upon the "pigeon-hole principle" requires a $\lfloor \log n \rfloor - 1$ Nullstellensatz degree certificate. However, when the system of polynomial equations $f_1, \ldots, f_s$ models an NP-complete problem, the degree d is likely to grow at least linearly with the size of the underlying NP-complete instance [19]. In other words, as long as P $\neq$ NP, the certificates should be hard to find (i.e., the size of the linear systems involved should be exponential in the size of the underlying instance), and as long as NP $\neq$ coNP, the certificates should be hard to verify (i.e., the certificates should contain an exponential number of monomials).

For example, consider the NP-complete problem of finding an independent set of size k in a graph G. Recall that an independent set is a set of pairwise non-adjacent vertices. This problem was modeled by Lovász [18] as a system of polynomial equations as follows:

$$\begin{aligned} x_i^2 - x_i = 0 \ , &\ \text{for every vertex } i \in V(G) \ , \\ x_i x_j = 0 \ , &\ \text{for every edge } (i,j) \in E(G) \ , \end{aligned} \qquad \text{and} \qquad -k + \sum_{i=1}^{n} x_i = 0 \ .$$

Clearly, this system of polynomial equations has a solution if and only the underlying graph G has an independent of size k. For example, consider the Turán graph $T(5,3)$. By inspection, we see that size of the largest independent set in $T(5,3)$ is two. Therefore, there is *no* independent set of size three, and using the connection between Hilbert's Nullstellensatz and linear algebra (described more thoroughly in Sec 3), the authors of [11] produce the following certificate:



Turán graph
$T(5,3)$

$$\left(\frac{1}{3}x_4 + \frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_3 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_4 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_2x_3 +$$
$$\left(\frac{1}{3}\right)x_2x_4 + \left(\frac{1}{3}\right)x_2x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_3x_5 + \left(\frac{1}{3}\right)x_4x_5 + \left(\frac{1}{3}x_2 + \frac{1}{6}\right)(x_1^2 - x_1) +$$
$$\left(\frac{1}{3}x_1 + \frac{1}{6}\right)(x_2^2 - x_2) + \left(\frac{1}{3}x_4 + \frac{1}{6}\right)(x_3^2 - x_3) + \left(\frac{1}{3}x_3 + \frac{1}{6}\right)(x_4^2 - x_4) + \left(\frac{1}{6}\right)(x_5^2 - x_5) +$$
$$\underbrace{\left(-\frac{1}{3}(x_1x_2 + x_3x_4) - \frac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5) - \frac{1}{3}\right)}_{\beta_1}(x_1 + x_2 + x_3 + x_4 + x_5 - 3) = 1 \ .$$

The combinatorial interpretation of this algebraic identity is unexpectedly clear: the size of the largest independent set is the degree of the Nullstellensatz certificate (i.e., the largest monomial x_1x_2 corresponds to the maximum independent set formed by vertices $\{1,2\}$), and the coefficient β_1 contains one monomial for each independent set in G. The combinatorial interpretation of these certificates is proven in [11] by De Loera et al. only in terms of monomials: the relationship between the numbers such as 1/3 and 1/6 and the independent sets of the underlying graph is not clear.

In this paper, we model the PARTITION problem as a system of polynomial equations, and then present a combinatorial interpretation of an associated minimum-degree Nullstellensatz certificate. However, the focus of our combinatorial interpretation is not only on the relationship between partitions and monomials, but also on the relationship between partitions and numeric coefficients (i.e., the numbers 1/3 and 1/6). In Section 2, we present an algebraic model of the partition problem and describe a minimum-degree Nullstellensatz certificate. In Section 3, we describe the connection between Hilbert's Nullstellensatz and linear algebra, leading to the construction of a *square* system of linear equations, forming what we call the *partition matrix*. In Section 4, we prove our main result: the determinant of the partition matrix represents a brute-force iteration over *all* the possible partitions of the set W, a polynomial we refer to as the *partition polynomial*.

We conclude our introduction with an example. Let $W = \{w_1, w_2, w_3, w_4\}$, and we see that the determinant of the associated *partition matrix* is as follows:

$$\det\left(\begin{bmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{bmatrix}\right) = \begin{array}{l} (w_1+w_2+w_3+w_4)(-w_1+w_2+w_3+w_4) \\ (w_1-w_2+w_3+w_4)(w_1+w_2-w_3+w_4) \\ (-w_1+w_2-w_3+w_4)(-w_1-w_2+w_3+w_4) \\ (w_1-w_2-w_3+w_4)(-w_1-w_2-w_3+w_4)\ . \end{array}$$

Thus, the determinant of the *partition matrix* is indeed a brute-force iteration over every possible partition of W: the *partition polynomial*.

2. Partitions and a System of Polynomial Equations

The PARTITION problem determines if a given set of integers $W = \{w_1, \ldots, w_n\}$ can be divided into two sets, I and $W \setminus I$ such that $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$. In this section, we describe a system of polynomial equations that models this question, and discuss the degree and monomials in an associated minimum-degree Nullstellensatz certificate.

Proposition 1. *Given a set of integers $W = \{w_1, \ldots, w_n\}$, the following system of polynomial equations*

$$x_i^2 - 1 = 0\ , \quad \textit{for } 1 \le i \le n\ , \qquad \textit{and} \quad \sum_{i=1}^{n} w_i x_i = 0\ .$$

has a solution if and only if there exists a partition of W into two sets, $I \subseteq W$ and $W \setminus I$, such that $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$.

Proof: The variables x_i can take on the values of ± 1. Thus, we relate partitions to solutions by placing integers w_i with $+1$ x_i values on one side of the partition and integers

w_i with -1 x_i values on the other. □

Let $[n]$ denote the set of integers $\{1,\ldots,n\}$ and let S_k^n denote the set of k-subsets of $[n]$. For $S \in S_k^n$, let x^S denote the corresponding square-free monomial of degree k in n variables. For example, given $S = \{1,3,4\} \subseteq [5]$, the corresponding monomial $x^S = x_1x_3x_4$. Additionally, let $S_k^{n\setminus i}$ denote the k-subsets of $[n] \setminus i$.

Theorem 2. *Given a set of non-partitionable integers $W = \{w_1,\ldots,w_n\}$ encoded as a system of polynomial equations according to Prop. 1, there exists a minimum-degree Nullstellensatz certificate for the* non-*existence of a partition of W as follows:*

$$1 = \sum_{i=1}^{n}\Big(\sum_{\substack{k \text{ even} \\ k\le n-1}}\sum_{S\in S_k^{n\setminus i}} c_{i,S}x^S\Big)(x_i^2-1) + \Big(\sum_{\substack{k \text{ odd} \\ k\le n}}\sum_{S\in S_k^{n}} b_S x^S\Big)\Big(\sum_{i=1}^{n} w_i x_i\Big) \ .$$

Moreover, every Nullstellensatz certificate for the system of equations defined by Prop. 1 contains one monomial for each of the odd parity subsets of each S_k^n, and one monomial for each of the even parity subsets of each $S_k^{n\setminus i}$.

Via Thm. 2, we see that the degree of the certificate is n for n odd, and $n-1$ for n even. Furthermore, by considering the monomials present in the certificate as identifying the integers present on *one* side of a partition, we see that the monomials represent a brute-force iteration over every possible partition of W. We note that we identify the constant terms $c_{i,\emptyset}$ with the case of placing every integer on one side of the partition and the empty set on the other. Thus, this result is similar to the independent set result (De Loera et al., [11]) reviewed in the introduction. However, in this paper, we are interested not only in a combinatorial interpretation of the monomials, but also in a combinatorial interpretation of the unknowns $c_{i,S}, b_S$.

The proof of Thm. 2 is virtually identical to the proof of the independent set result described in [11], with no new techniques or insights. The essential strategy of the proof is to consider an arbitrary minimum-degree Nullstellensatz certificate, and then "reduce" the certificate to a version containing only square-free monomials by adding and subtracting different polynomials from the certificate (or taking the monomials modulo the ideal). It is then possible to demonstrate that every square-free monomial representing a partition must be present in the certificate; otherwise, the certificate would require an infinite chain of higher and higher degree square-free monomials in order to simplify to 1. Since the technical details of this strategy were carefully presented in [11], we omit the formal proof here and simply state Thm. 2 as a result.

Example 1. *The set of integers $W = \{1,3,5,2\}$ is* not *partitionable. We encode this problem as a system of polynomial equations as follows:*

$$x_1^2-1=0\ ,\quad x_2^2-1=0\ ,\quad x_3^3-1=0\ ,\quad x_4^2-1=0\ ,\quad x_1+3x_2+5x_3+2x_4=0\ .$$

Since W is not *partitionable, this system of equations has* no *solution, and a Nullstel-*

lensatz certificate exists. Here is the minimum-degree certificate described by Thm. 2:

$$1 = \Big(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4\Big)(x_1^2 - 1) + \Big(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4\Big)(x_2^2 - 1) + \Big(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4\Big)(x_3^2 - 1) + \Big(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3\Big)(x_4^2 - 1) + \Big(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \mathbf{\frac{34}{693}}x_4 - \frac{842}{3465}x_1x_2x_3 + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4\Big)(x_1 + 3x_2 + 5x_3 + 2x_4) \ .$$

Note that the coefficient for $(x_1^2 - 1)$ contains only even degree monomials that do not *contain x_1 (similarly for $(x_2^2 - 1)$, etc.) and that the coefficient for $(x_1 + 3x_2 + 5x_3 + 2x_4)$ contains every possible odd degree monomial in four variables. The combinatorial interpretation of a number such as* 34/693 *is explicitly demonstrated in Ex. 7.* □

3. The Partition Matrix: Definition and Properties

In this section, we explore the well-known connection between Hilbert's Nullstellensatz and linear algebra, in terms of the minimum-degree certificate defined in Thm. 2:

$$1 = \sum_{i=1}^{n}\Big(\sum_{\substack{k \text{ even} \\ k \le n-1}} \sum_{S \in S_k^{n \setminus i}} c_{i,S}x^S\Big)(x_i^2 - 1) + \Big(\sum_{\substack{k \text{ odd} \\ k \le n}} \sum_{S \in S_k^n} b_S x^S\Big)\Big(\sum_{i=1}^{n} w_i x_i\Big) \ .$$

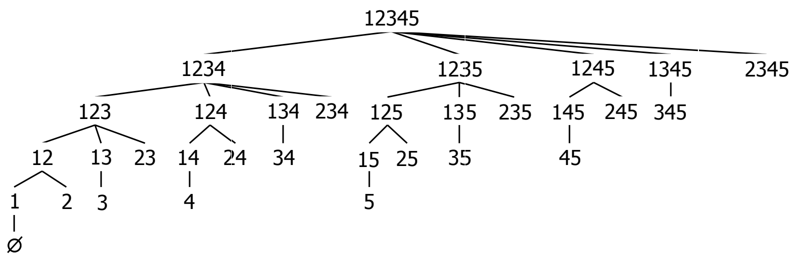
We begin by defining *graded reverse lexicographic order*. We then construct a $2^{n-1} \times 2^{n-1}$ square system of linear equations containing only the unknowns b. When ordered according to *graded reverse lexicographic order*, this square matrix is known as the *partition matrix*. We next prove a series of properties of the partition matrix (including symmetry), and conclude by expressing the partition matrix as the sum of a very specific set of permutation matrices. The properties of these permutation matrices allow for a simple and elegant proof of the main result in Section 4.

3.1. Graded Reverse Lexicographic Order as a Tree

Since we are dealing only with square-free monomials, we define *graded reverse lexicographic order* (denoted $\succeq_D$) as follows. Given $S \in S_k^n$, we represent S as a vector in $\{0,1\}^n$ (denoted v_S) by setting $v_S[i] = 1$ if $i \in S$ and $v_S[i] = 0$ otherwise. For example, let $S = \{2,3,7\} \in S_3^7$. Then $v_S = \{0,1,1,0,0,0,1\}$. Given distinct $S \in S_k^n$ and $S' \in S_{k'}^n$, then $S \succeq_D S'$ in two cases: 1) if $k > k'$, or 2) if $k = k'$ and the *right-most nonzero entry* of $v_S - v_{S'}$ is negative. For example, $\{2,3,4,5\} \succeq_D \{1,2,5\}$, and $\{2,3\} \succeq_D \{1,4\}$.

In order to prove specific properties of the partition matrix, we use a slightly less common, recursive definition of graded reverse lexicographic order. First, we order the $\binom{n}{n-1}$ subsets of $[n]$ in lexicographic order, creating sets $S_1, \ldots, S_n$. Next, the sets $S_1, \ldots, S_n$ are iterated, and for each S_i, the $\binom{n-1}{n-2}$ subsets of S_i are iterated in lexicographic order, etc.. This order is pictorially represented as a tree in Ex. 2.

Example 2. *Here we pictorially order the set of integers* [5] *according to* $\succeq_D$.



Using this tree, if two sets S, S' are from different levels in the tree with S higher than S', then $S \succeq_D S'$. For example, $\{1245\} \succeq_D \{234\}$. Additionally, if S, S' are from the same level in the tree but S appears further to the left than S', then $S \succeq_D S'$. For example, $\{23\} \succeq_D \{15\}$. Additionally, observe that if the even and odd cardinality subsets of $[5]$ are iterated in $\succeq_D$ order, then the following pairing of even and odd subsets occurs:

12345	123	124	134	234	125	135	235	145	245	345	1	2	3	4	5
1234	1235	1245	1345	2345	12	13	23	14	24	34	15	25	35	45	∅

Given a set S in the pairing diagram above, if $5 \in S$, then S is paired with $S \setminus 5$. If $5 \notin S$, then S is paired with $S \cup 5$. This observation is proven in general in Prop. 3.2. □

We refer to this tree as the *order tree* of $[n]$. If two sets S, S' are children of the same parent in the tree, we say that the sets are contained in the same *block*. For example, $\{1, 2, 3\}$ and $\{2, 3, 4\}$ are in the same block, but $\{2, 3, 4\}$ and $\{1, 2, 5\}$ are not.

3.2. The Partition Matrix

In this section, we demonstrate how to extract a $2^{n-1} \times 2^{n-1}$ matrix from the minimum-degree certificate of Thm. 2. We begin by considering the coefficients of $(x_i^2 - 1)$:

$$\Big(\sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{S \in S_k^{n \setminus i}} c_{i,S} x^S \Big) (x_i^2 - 1) \ .$$

We observe that each monomial $c_{i,S} x^S$ multiplies $(x_i^2 - 1)$, which implies that each $c_{i,S}$ appears in two equations (one corresponding to the monomial $x^S x_i^2$, and one corresponding to the monomial $-x^S$). Thus, the unknown $c_{i,S}$ appears in the first equation with a positive coefficient, and the second equation with a negative coefficient. This allows us to sum the two equations, and cancel the c unknowns in a cascading manner. For example, there is always one equation for the constant term:

$$-c_{1,\emptyset} - c_{2,\emptyset} - \cdots - c_{n,\emptyset} = 1 \ .$$

Notice that this equation sums to one, since the Nullstellensatz certificate simplifies to one. There is also always one equation for each x_i^2 monomial:

$$b_i w_i + c_{i,\emptyset} = 0 \ . \tag{1}$$

The $b_i w_i$ term appears in these equations since the product of

$$\Big(\sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{S \in S_k^n} b_S x^S \Big) \Big(w_1 x_1 + \cdots + w_n x_n \Big) \ ,$$

contributes the term $b_i x_i \cdot w_i x_i = b_i w_i x_i^2$, among others. Notice that Eq. 1 sums to zero, since every monomial other than the constant term must cancel in a Nullstellensatz certificate. This set of $n+1$ equations yields the following subsystem:

$$\begin{aligned} -c_{1,\emptyset} - c_{2,\emptyset} - \cdots - c_{n,\emptyset} &= 1 \ , \quad &&\text{(constant term)} \\ b_1 w_1 + c_{1,\emptyset} &= 0 \ , \quad &&(x_1^2) \\ \vdots \quad & \quad \vdots \\ b_n w_n + c_{n,\emptyset} &= 0 \ . \quad &&(x_n^2) \end{aligned}$$

Summing these $n+1$ equations together yields the following equation (in b only):

$$\sum_{i=1}^{n} b_i w_i = 1 \ .$$

In general, let $S \subseteq [n] \setminus i$ be an even cardinality subset, and consider the two monomials $x^S x_i^2$ and x^S. Then, the following $n-|S|+1$ equations are always present in the extracted linear system:

$$\begin{aligned} b_{S \cup i} w_i + c_{i,S} &= 0 \ , \qquad (x^S x_i^2) \ , \quad \text{for each } i \notin S \\ \sum_{j \in S} b_{S \setminus j} w_j - \sum_{i \notin S} c_{i,S} &= 0 \ , \qquad (x^S) \ . \end{aligned} \tag{2}$$

Summing up these $n-|S|+1$ equations together yields the following equation (in b only):

$$\sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j = 0 \ .$$

Definition 1. *Given a set of integers $W = \{w_1, \ldots, w_n\}$, the coefficient matrix of the following square system of linear equations*

$$\sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j = 0 \ , \quad \textit{for each } S \in \left(S_k^n \setminus \emptyset\right) \textit{ with } |S| \textit{ even}$$
$$\sum_{i=1}^{n} b_i w_i = 1 \ ,$$

defines a $2^{n-1} \times 2^{n-1}$ matrix with columns indexed by the unknowns b_S (corresponding to the 2^{n-1} odd cardinality subsets of $[n]$), and rows indexed by the sets S (corresponding to the 2^{n-1} even cardinality subsets of $[n]$, including $\emptyset$). This matrix is the partition matrix, *denoted by $\Pi(W)$, with rows and columns ordered by graded reverse lexicographic order.*

By studying Eq. 2, we see that each c unknown appears in exactly one equation along with exactly one b unknown. Thus, solving for the b unknowns *uniquely determines the entire certificate*, and determining whether or not a given set W is partitionable depends entirely on the *determinant of the partition matrix.*

Example 3. *Let $W = \{w_1, w_2, w_3\}$. Via Thm. 2, the Nullstellensatz certificate is:*

$$\begin{aligned} 1 = &(c_{1,\emptyset} + c_{1,\{23\}} x_2 x_3)(x_1^2 - 1) + (c_{2,\emptyset} + c_{2,\{13\}} x_1 x_3)(x_2^2 - 1) + (c_{3,\emptyset} + c_{3,\{12\}} x_1 x_2)(x_3^2 - 1) \\ &+ (b_1 x_1 + b_2 x_2 + b_3 x_3 + b_{123} x_1 x_2 x_3)(w_1 x_1 + w_2 x_2 + w_3 x_3) \ . \end{aligned}$$

If W is not partitionable, there must exist an assignment to the unknowns c and b such that the certificate simplifies to one. In other words, the following system of linear equations has a solution:

$$
\begin{array}{rrcrr}
(x_1^2) & c_{1,\emptyset} + b_1 w_1 = 0 \ , & & (x_2 x_3) & -c_{1,\{23\}} + b_2 w_3 + b_3 w_2 = 0 \ , \\
(x_2^2) & c_{2,\emptyset} + b_2 w_2 = 0 \ , & & (x_1 x_2 x_3^2) & c_{3,\{12\}} + b_{123} w_3 = 0 \ , \\
(x_3^2) & c_{3,\emptyset} + b_3 w_3 = 0 \ , & & (x_1 x_2^2 x_3) & c_{2,\{13\}} + b_{123} w_2 = 0 \ , \\
(x_1 x_2) & -c_{3,\{12\}} + b_1 w_2 + b_2 w_1 = 0 \ , & & (x_1^2 x_2 x_3) & c_{1,\{23\}} + b_{123} w_1 = 0 \ , \\
(x_1 x_3) & -c_{2,\{13\}} + b_1 w_3 + b_3 w_1 = 0 \ , & & (\textit{constant term}) & -c_{1,\emptyset} - c_{2,\emptyset} - c_{3,\emptyset} = 1 \ .
\end{array}
$$

Following the simplifications described above, we extract a square *system of linear equations that contain only the b unknowns from these equations:*

$$
\begin{array}{llll}
b_{123} w_3 + b_1 w_2 + b_2 w_1 = 0 \ , & S = \{1,2\} \ , & b_{123} w_2 + b_1 w_3 + b_3 w_1 = 0 \ , & S = \{1,3\} \ , \\
b_{123} w_1 + b_2 w_3 + b_3 w_2 = 0 \ , & S = \{2,3\} \ , & b_1 w_1 + b_2 w_2 + b_3 w_3 = 1 \ . & S = \emptyset \ .
\end{array}
$$

Ordering the columns as $\{b_{123}, b_1, b_2, b_3\}$, the partition matrix *is as follows:*

$$
\begin{array}{c}
\\ \{1,2\} \\ \{1,3\} \\ \{2,3\} \\ \emptyset
\end{array}
\begin{array}{c}
\begin{array}{cccc} b_{123} & b_1 & b_2 & b_3 \end{array} \\
\begin{bmatrix}
w_3 & w_2 & w_1 & 0 \\
w_2 & w_3 & 0 & w_1 \\
w_1 & 0 & w_3 & w_2 \\
0 & w_1 & w_2 & w_3
\end{bmatrix}
\end{array}
$$

As a preview of our main result, we note that the determinant of this matrix is

$$
(w_1 + w_2 + w_3)(-w_1 + w_2 + w_3)(w_1 - w_2 + w_3)(-w_1 - w_2 + w_3) \ ,
$$

which represents a brute-force iteration over all of the possible partitions of the set W. This will be formally defined as the partition polynomial *in Sec. 4.* □

For the duration of this section, we collect a few essential facts about the partition matrix $\Pi(W)$. We also provide a slightly larger example of the partition matrix to demonstrate these properties.

Example 4. *Given $W = \{w_1, \ldots, w_5\}$, here is the 16×16 partition matrix $\Pi(W)$.*

	12345	123	124	134	234	125	135	235	145	245	345	1	2	3	4	5
1234	w_5	w_4	w_3	w_2	w_1	0	0	0	0	0	0	0	0	0	0	0
1235	w_4	w_5	0	0	0	w_3	w_2	w_1	0	0	0	0	0	0	0	0
1245	w_3	0	w_5	0	0	w_4	0	0	w_2	w_1	0	0	0	0	0	0
1345	w_2	0	0	w_5	0	0	w_4	0	w_3	0	w_1	0	0	0	0	0
2345	w_1	0	0	0	w_5	0	0	w_4	0	w_3	w_2	0	0	0	0	0
12	0	w_3	w_4	0	0	w_5	0	0	0	0	0	w_2	w_1	0	0	0
13	0	w_2	0	w_4	0	0	w_5	0	0	0	0	w_3	0	w_1	0	0
23	0	w_1	0	0	w_4	0	0	w_5	0	0	0	0	w_3	w_2	0	0
14	0	0	w_2	w_3	0	0	0	0	w_5	0	0	w_4	0	0	w_1	0
24	0	0	w_1	0	w_3	0	0	0	0	w_5	0	0	w_4	0	w_2	0
34	0	0	0	w_1	w_2	0	0	0	0	0	w_5	0	0	w_4	w_3	0
15	0	0	0	0	0	w_2	w_3	0	w_4	0	0	w_5	0	0	0	w_1
25	0	0	0	0	0	w_1	0	w_3	0	w_4	0	0	w_5	0	0	w_2
35	0	0	0	0	0	0	w_1	w_2	0	0	w_4	0	0	w_5	0	w_3
45	0	0	0	0	0	0	0	0	w_1	w_2	w_3	0	0	0	w_5	w_4
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	w_1	w_2	w_3	w_4	w_5

□

Proposition 3. *Given $W = \{w_1, \dots, w_n\}$, the $2^{n-1} \times 2^{n-1}$ partition matrix $\Pi(W)$ has the following properties:*

(1) The entry w_i with $i = \{1, \dots, n\}$ appears exactly once in each row and column.
(2) If row i is indexed by set $S \subseteq [n]$ (with $|S|$ even), and $n \in S$, then column i is indexed by $S \setminus n$. If $n \notin S$, then column i is indexed by $S \cup n$.
(3) All diagonal entries of $\Pi(W)$ are equal to w_n.
(4) $\Pi(W)$ is symmetric.

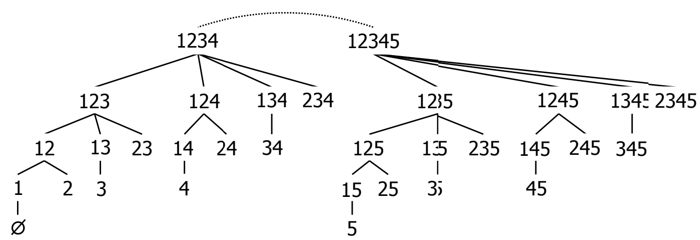
Proof of Prop. 3.1: After inspecting the equation defining the partition matrix

$$\sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j = 0 \ ,$$

where S represents an even cardinality subset of $[n]$, it is evident that each row contains exactly one entry for each w_i. To see that each column also contains exactly one entry w_i with $i = \{1, \dots, n\}$, consider the column indexed by unknown $b_{S'}$ where $S' \subseteq [n]$ with odd cardinality. Then, for each $j \in S'$, the row indexed by $S = S' \setminus j$ contains w_j. Additionally, for each $j \notin S'$, the row indexed by $S = S' \cup j$ also contains w_j. Thus, each row and column contains exactly one entry w_i for $i = \{1, \dots, n\}$. □

As an example of Prop. 3.2, note that row $\{12\}$ is paired with column $\{125\}$, and column $\{1\}$ is paired with row $\{15\}$ in Ex. 4.

Proof of Prop. 3.2: To prove this claim, suppose that we have the "order tree" T_{n-1} for the subsets of $[n-1]$. In order to create the order tree T_n for the subsets of $[n]$, we first copy T_{n-1} and add the integer n to each set, creating the tree $T_{n-1} \cup n$. We then join the node in $T_{n-1} \cup n$ indexed by $\{1 \cdots n\}$ to the node in T_{n-1} indexed $\{1 \cdots (n-1)\}$. The resulting tree is the order tree for T_n. For example,



Since no set in T_{n-1} contains the integer n and every set in $T_{n-1} \cup n$ contains n, it is easy to see that the even and odd sets are paired by inspecting how T_{n-1} overlays on top of $T_{n-1} \cup n$. Thus, the claim holds. □

Proof of Prop. 3.3: This result follows from the equations defining the partition matrix, and also Prop. 3.2, which defines the row-column pairing of the diagonal element. □

Proof of Prop. 3.4: Consider an arbitrary row i indexed by a set S_i, and let column i be indexed by the set b_i. In order to prove symmetry, we must show that row i is equal to column i. By Prop. 3.2, n is either in S_i or b_i, but not both. Without loss of generality, assume $n \in S_i$ and $b_i = S_i \setminus n$ (e.g. $S_i = \{15\}$ and $b_i = \{1\}$). Suppose $\big(\Pi(W)\big)_{ij} = w_{k_j}$ for $j < i$. We must show that $\big(\Pi(W)\big)_{ji} = w_{k_j}$. Since $j < i$, $k_j \notin S_i$, and column j is indexed by $b_j = S_i \cup k_j$ (e.g. in row $\{15\}$, w_2 appears in column $\{125\}$). Since $n \in (S_i \cup k_j)$, row j is indexed by $S_j = (S_i \cup k_j) \setminus n$ (e.g. $S_j = \{12\}$). Then, $S_j \setminus k_j = b_i$, and $\big(\Pi(W)\big)_{ji} = w_{k_j}$.

Suppose $i < j$, and $\big(\Pi(W)\big)_{ij}$ is again equal to w_{k_j}. Then $k_j \in S_i$, and column j is indexed by $b_j = S_i \setminus k_j$ and row j is indexed by $S_j = (S_i \setminus k_j) \setminus n$ (e.g., in row $\{15\}$, w_1 appears in column $\{1\}$). But then $S_j \cup k_j = b_i$, and $\big(\Pi(W)\big)_{ji} = w_{k_j}$.

A similar argument holds if $n \notin S_i$, but with the logic reversed. Since we have shown that $\big(\Pi(W)\big)_{ij} = \big(\Pi(W)\big)_{ji}$. we have shown that the matrix is symmetric. □

3.3. *The Partition Matrix as a Sum of Permutation Matrices*

We will now express the partition matrix in terms of a specific set of permutation matrices, and then prove a series of properties about these particular permutation matrices. Recall that the *symmetric difference* of two sets A and B (denoted as $A\Delta B$) is the set of elements which are in either set A or B but not in their intersection. For example, the symmetric difference $\{1,2,3\}\Delta\{3,4\} = \{1,2,4\}$. By Prop. 3.4, every w_k appears exactly once in each row and column. Therefore, we can express $\Pi(W)$ as follows.

Definition 2. Given $W = \{w_1, \ldots, w_n\}$ and the corresponding partition matrix $\Pi(W)$, let $\Pi_1, \ldots, \Pi_n \in \{0,1\}^{2^{n-1} \times 2^{n-1}}$ be permutation matrices such that

$$(\Pi_k)_{ij} = \begin{cases} 1 & \text{if } \big(\Pi(W)\big)_{ij} = w_k \ , \\ 0 & \text{otherwise .} \end{cases} , \qquad \text{where } 1 \leq i, j \leq 2^{n-1}.$$

By this definition, it is clear that

$$\Pi(W) = \sum_{k=1}^{n} w_k \Pi_k \ .$$

Example 5. *Let $W = \{w_1, \ldots, w_4\}$. Here we display the 8×8 partition matrix $\Pi(W)$, and the particular permutation matrix Π_3. For convenience, we highlight the w_3 entries appearing in $\Pi(W)$.*

$\Pi(W) =$

	123	124	134	234	1	2	3	4
1234	w_4	$\mathbf{w_3}$	w_2	w_1	0	0	0	0
12	$\mathbf{w_3}$	w_4	0	0	w_2	w_1	0	0
13	w_2	0	w_4	0	$\mathbf{w_3}$	0	w_1	0
23	w_1	0	0	w_4	0	$\mathbf{w_3}$	w_2	0
14	0	w_2	$\mathbf{w_3}$	0	w_4	0	0	w_1
24	0	w_1	0	$\mathbf{w_3}$	0	w_4	0	w_2
34	0	0	w_1	w_2	0	0	w_4	$\mathbf{w_3}$
∅	0	0	0	0	w_1	w_2	$\mathbf{w_3}$	w_4

, $\Pi_{\mathbf{3}} =$

	123	124	134	234	1	2	3	4
1234	0	**1**	0	0	0	0	0	0
12	**1**	0	0	0	0	0	0	0
13	0	0	0	0	**1**	0	0	0
23	0	0	0	0	0	**1**	0	0
14	0	0	**1**	0	0	0	0	0
24	0	0	0	**1**	0	0	0	0
34	0	0	0	0	0	0	0	**1**
∅	0	0	0	0	0	0	**1**	0

□

By Prop. 3.4, the matrix $\Pi(W)$ is symmetric. Therefore, each of the permutation matrices $\Pi_1, \ldots, \Pi_n$ is likewise symmetric, and the following proposition holds.

Proposition 4. *Given $W = \{w_1, \ldots, w_n\}$ and the corresponding permutation matrices $\Pi_1, \ldots, \Pi_n$, each of the following holds:*

(1) Π_n is the identity matrix ,
(2) For $k = 1, \ldots, n$, $\Pi_k^2 = I$ (the matrices are involutory*) ,*
(3) For $k = 1, \ldots, n-1$, Π_k has ± 1 eigenvalues, and Π_n has all $+1$ eigenvalues.
(4) For $k = 1, \ldots, n$, Π_k is diagonalizable, and

(5) $\Pi_k\Pi_l = \Pi_l\Pi_k$ *(the permutation matrices* Π_k *pairwise commute) .*

Example 6. *Given* $W = \{w_1, \ldots, w_5\}$*, here is the* 16×16 *partition matrix* $\Pi(W)$*. We will show that* $\big(\Pi_1\Pi_3\big)_{(\{23\},\{125\})} = 1 = \big(\Pi_3\Pi_1\big)_{(\{23\},\{125\})}$ *.*

	12345	123	124	134	234	125	135	235	145	245	345	1	2	3	4	5
1234	w_5	w_4	w_3	w_2	w_1	0	0	0	0	0	0	0	0	0	0	0
1235	w_4	w_5	0	0	0	$\mathbf{w_3}$	w_2	w_1	0	0	0	0	0	0	0	0
1245	w_3	0	w_5	0	0	w_4	0	0	w_2	w_1	0	0	0	0	0	0
1345	w_2	0	0	w_5	0	0	w_4	0	w_3	0	w_1	0	0	0	0	0
2345	w_1	0	0	0	w_5	0	0	w_4	0	w_3	w_2	0	0	0	0	0
12	0	w_3	w_4	0	0	w_5	0	0	0	0	0	w_2	w_1	0	0	0
13	0	w_2	0	w_4	0	0	w_5	0	0	0	0	w_3	0	w_1	0	0
23	0	$\mathbf{w_1}$	0	0	w_4	0	0	w_5	0	0	0	0	$\mathbf{w_3}$	w_2	0	0
14	0	0	w_2	w_3	0	0	0	0	w_5	0	0	w_4	0	0	w_1	0
24	0	0	w_1	0	w_3	0	0	0	0	w_5	0	0	w_4	0	w_2	0
34	0	0	0	w_1	w_2	0	0	0	0	0	w_5	0	0	w_4	w_3	0
15	0	0	0	0	0	w_2	w_3	0	w_4	0	0	w_5	0	0	0	w_1
25	0	0	0	0	0	$\mathbf{w_1}$	0	w_3	0	w_4	0	0	w_5	0	0	w_2
35	0	0	0	0	0	0	w_1	w_2	0	0	w_4	0	0	w_5	0	w_3
45	0	0	0	0	0	0	0	0	w_1	w_2	w_3	0	0	0	w_5	w_4
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	w_1	w_2	w_3	w_4	w_5

Observe that $\Pi_1\big(\{23\},\{123\}\big) = 1 = \Pi_3\big(\{1235\},\{125\}\big)$. Furthermore, observe that $\big(\{1235\},\{123\}\big)$ indexes a diagonal element since $\{1235\}\Delta\{5\} = \{123\}$ (by Prop. 3.2). For the commuted multiplication $\Pi_3\Pi_1$, observe that $\Pi_3\big(\{23\},\{2\}\big) = 1 = \Pi_1\big(\{25\},\{125\}\big)$. Furthermore, observe that $\big(\{25\},\{2\}\big)$ indexes a diagonal element since $\{25\}\Delta\{5\} = \{2\}$. This is the technique used to prove Prop. 4.5. □

Proof. Prop. 4.1 comes directly from the definition of the permutation matrices and Prop. 3.3. To see that the matrices are involutory (Prop. 4.2), recall that for any permutation matrix P, $PP^T = I$. In this case, since the matrices are symmetric, $\Pi_k = \Pi_k^T$, and thus $\Pi_k^2 = I$ follows. For Prop. 4.3, since the matrices Π_k are involutory, the minimal polynomial is $x^2 - 1$, and because the eigenvalues are roots of the minimal polynomial, the eigenvalues are clearly ± 1. Since $\Pi_n = I$, the eigenvalues of Π_n all clearly $+1$. For Prop. 4.4, we observe that this is proven in [15], Theorem 6, pg. 204.

Finally, we must show that the matrices pairwise commute. We will show that, given $k_1, k_2 \in \{1, \ldots, n\}$, $\Pi_{k_1}\Pi_{k_2} = \Pi_{k_2}\Pi_{k_1}$. Since every row/column of Π_k has exactly one non-zero entry, $\big(\Pi_{k_1}\Pi_{k_2}\big)_{ij} = 1$ only when the non-zero entries are located in the same row/column, respectively.

In particular, let S_i index the i-th row of $\Pi(W)$, and let S_j index the j-th column of $\Pi(W)$. For shorthand, we will denote $\big(\Pi_k\big)_{S_i,S_j}$ as $\big(\Pi_k\big)_{ij}$ with $1 \le i,j \le 2^{n-1}$. Then, the non-zero entries in row S_i of Π_{k_1} and column S_j in Π_{k_2} can be expressed as $\Pi_{k_1}\big(S_i, S_i\Delta k_1\big) = 1 = \Pi_{k_2}\big(S_j\Delta k_2, S_j\big)$ (relevant to the product $\Pi_{k_1}\Pi_{k_2}$), and the non-zero entries in row S_i of Π_{k_2} and column S_j in Π_{k_1} can be expressed as $\Pi_{k_2}\big(S_i, S_i\Delta k_2\big) = 1 = \Pi_{k_1}\big(S_j\Delta k_1, S_j\big)$ (relevant to the commuted product $\Pi_{k_2}\Pi_{k_1}$). This can be seen by recalling the definitions of both the partition matrix and permutation matrices. We observe that $\big(\Pi_{k_1}\Pi_{k_2}\big)_{ij} = 1$ if and only if $\{S_j\Delta k_2, S_i\Delta k_1\}$ indexes a diagonal entry, and $\left(\Pi_{k_2}\Pi_{k_1}\right)_{ij} = 1$ if and only if $\{S_j \Delta k_1, S_i \Delta k_2\}$ indexes a diagonal entry. Therefore, in order to show $\left(\Pi_{k_1}\Pi_{k_2}\right)_{ij} = \left(\Pi_{k_2}\Pi_{k_1}\right)_{ij}$, we simply observe that if $\{S_j \Delta k_2, S_i \Delta k_1\}$ indexes a diagonal entry, then $S_j \Delta k_2 \Delta n = S_i \Delta k_1$ (by Prop. 3.2). However, if $S_j \Delta k_2 \Delta n = S_i \Delta k_1$, then $S_j \Delta k_1 \Delta n = S_i \Delta k_2$, by the definition of the symmetric difference. Therefore, $\left(\Pi_{k_1}\Pi_{k_2}\right)_{ij} = \left(\Pi_{k_2}\Pi_{k_1}\right)_{ij}$, and the matrices pairwise commute. □

We pause to observe that the set of matrices $\{\Pi_1, \ldots, \Pi_n\}$ has now been shown to be a set of commuting, diagonalizable matrices. Recall that a set of matrices is *simultaneously diagonalizable* if there exists a single invertible matrix P such that $P^{-1}AP$ is a diagonal matrix for every A in the set. This allows us to recall the following well-known fact:

Proposition 5 ([16], pg. 64)**.** *A set (possibly infinite) of diagonalizable matrices is commuting if and only if it is simultaneously diagonalizable.*

Having gathered together a series of facts about the partition matrix and the associated permutation matrices, we now investigate the determinant of the partition matrix.

4. The Partition Matrix and Partition Polynomial

Given a square non-singular matrix A, Cramer's rule states that $Ax = b$ is solved by

$$x_i = \frac{\det(A|_b^i)}{\det(A)} \ ,$$

where $A|_b^i$ is the matrix A with the i-th column replaced with the right-hand side vector b. In Section 3, we extracted a $2^{n-1} \times 2^{n-1}$ square linear system from the general linear system constructed via the minimum-degree Nullstellensatz certificate described by Thm. 2. Here, we see by Cramer's rule that the unknowns within that certificate are ratios of two determinants. In this section, we show that the determinant of the partition matrix is equivalent to a brute-force iteration over all the partitions of W. Therefore, the denominator of any unknown in the certificate is a combinatorial representation of the partition problem.

We observe that, in general, the linear system $Ax = b$ may have a solution even if $\det(A) = 0$. However, in the case of the partition matrix, when we demonstrate that the $\det(A)$ is equal to the *partition polynomial*, we will be demonstrating that $Ax = b$ only has a solution in the case when $\det(A) \neq 0$.

Let $\{-1, 1\}^n$ be the set of all ± 1 bit strings of length n. For $S \in \{-1, 1\}^n$, let s_i denote the i-th bit in the string S.

Definition 3. *Given a set $W = \{w_1, \ldots, w_n\}$, let*

$$\prod_{S \in \{-1,1\}^{n-1}} \left(\left(\sum_{i=1}^{n-1} s_i w_i \right) + w_n \right)$$

be the partition polynomial *of W.*

For example, let $n = 5$, and $S \in \{-1, 1\}^4$ be $S =$ "-1,1,-1,-1". Then, S corresponds to the $-w_1 + w_2 - w_3 - w_4$, and denotes a partition of $W = \{w_1, \ldots, w_5\}$, with w_5 fixed on the "positive" side of the partition, and the other w_i sorted according to sign.

$-$	$+$
w_1	w_5
w_3	w_2
w_4	

If this arrangement of w_i is a partition of W, then $-w_1 + w_2 - w_3 - w_4 + \mathbf{w_5} = 0$. In this way, *any* bitstring $S \in \{-1, 1\}^{n-1}$ is equivalent to fixing w_n on the "positive" side of the partition, and then arranging the other w_i on the "positive/negative" side, according to sign. In this way, the partition polynomial represents an iteration over *every possible partition of* W, avoiding double-counting by permanently fixing w_n on the "positive" side. If the set W is partitionable, one of bitstrings S will define a factor of the partition polynomial that sums to zero. We will show that the determinant of the partition matrix is the partition polynomial: therefore, if the determinant of the partition matrix is zero, the linear system has *no* solution, and there is *no* Nullstellensatz certificate.

Example 7. *In Ex. 1, we presented an actual minimum-degree certificate for the non-partitionable set* $W = \{1, 3, 5, 2\}$ *. We observe that*

$$-51975 = (1+3+5+2)(-1+3+5+2)(1-3+5+2)(1+3-5+2)$$
$$(-1-3+5+2)(-1+3-5+2)(1-3-5+2)(-1-3-5+2)\ .$$

Via Cramer's rule, we see that the unknown b_4 *is equal to*

$$b_4 = \frac{-2550}{-51975} = \frac{34}{693}\ ,$$

which is indeed the value of unknown b_4 *as it appears in the certificate.* □

Example 8. *Here is the determinant of the* 8×8 *partition matrix* $Part_4$*:*

$$\det\left(\begin{bmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{bmatrix}\right) = \begin{array}{l} (w_1+w_2+w_3+w_4)(-w_1+w_2+w_3+w_4) \\ (w_1-w_2+w_3+w_4)(w_1+w_2-w_3+w_4) \\ (-w_1+w_2-w_3+w_4)(-w_1-w_2+w_3+w_4) \\ (w_1-w_2-w_3+w_4)(-w_1-w_2-w_3+w_4)\ . \end{array}$$

Theorem 6. *Given* $W = \{w_1, \ldots, w_n\}$*, the determinant of the partition matrix of* W *is the partition polynomial of* W*.*

Proof. Since $\Pi_1, \ldots, \Pi_n$ are a set of pairwise commuting diagonalizable matrices, via Prop. 5, they are also simultaneously diagonalizable. Let P be the $2^{n-1} \times 2^{n-1}$ matrix that simultaneously diagonalizes $\Pi_1, \dots, \Pi_n$. Then

$$
\begin{aligned}
P^{-1}\Pi(W)P &= P^{-1}\left(\sum_{k=1}^{n} w_k \Pi_k\right)P = \sum_{k=1}^{n} w_k P^{-1}\Pi_k P \\
&= \begin{bmatrix} \sum_{k=1}^{n} w_k \lambda_{k,1} & & & \\ & \sum_{k=1}^{n} w_k \lambda_{k,2} & & \\ & & \ddots & \\ & & & \sum_{k=1}^{n} w_k \lambda_{k,2^{n-1}} \end{bmatrix}
\end{aligned}
$$

where $\lambda_{k,1}, \dots, \lambda_{k,2^{n-1}} \in \{-1, 1\}$ are the eigenvalues of Π_k. Then, we see

$$
\begin{aligned}
\det\big(\Pi(W)\big) &= \det\big(P^{-1}\big)\det\big(\Pi(W)\big)\det(P) = \det\big(P^{-1}\Pi(W)P\big) \\
&= \prod_{j=1}^{2^{n-1}}\left(\sum_{k=1}^{n} w_k \lambda_{k,j}\right) .
\end{aligned}
$$

Therefore, we see that $\det\big(\Pi(W)\big)$ is a product of linear polynomials in w_k with coefficients ± 1, where the coefficient of w_n is always $+1$.

In order to complete the proof, we must now show that *every* linear polynomial of this form is present in the determinant (for example, for $n = 3$, the determinant is *not* $(w_1 - w_2 + w_3)^4$). Thus, consider any linear polynomial $\sum_{k=1}^{n} p_k w_k$ with $p_n = 1$ and $p_k = \pm 1, k = 1, \dots, n-1$, and assume this polynomial is *not* a factor of $\det\big(\Pi(W)\big)$.

In order to derive a contradiction, set $w_k = -p_k$ for $k = 1, \dots, n-1$, and $w_n = n-1$. Observe that $W = \{-p_1, -p_2, \dots, -p_{n-1}, n-1\}$ is partitionable, according to the sign pattern of the p_k:

$$
\sum_{p_k=+1} w_k - \sum_{p_k=-1} w_k = \sum_{k=1}^{n} p_k w_k = 0 .
$$

However, for every other assignment of $\lambda_n = 1, \lambda_k = \pm 1$, $\sum_{k=1}^{n} \lambda_k w_k \geq 1$. Since $\sum_{k=1}^{n} p_k w_k$ is *not* a factor of $\det\big(\Pi(W)\big)$, then $\det\big(\Pi(W)\big) \neq 0$ for this W. However, we can now construct a Nullstellensatz certificate of non-partitionability, even though W is partitionable, which is a contradiction. Since the linear factor was chosen at random, each of the 2^{n-1} linear polynomials $\sum_{k=1}^{n} p_k w_k, p_k = \pm 1, p_n = 1$ must appear as a factor of the determinant and

$$
\det\big(\Pi(W)\big) = \prod_{P \in \{-1,1\}^{n-1}}\left(\left(\sum_{k=1}^{n-1} p_k w_k\right) + w_n\right) = \text{the partition polynomial} . \qquad \square
$$

Remark 7. A short proof of Thm. 6 may also be derived using representation theory of finite groups, essentially, applying [7, Thm. 2], as follows. The $n-1$ non-identity permutation matrices $\Pi_1, \dots, \Pi_{n-1}$ giving $\Pi(W)$ in Definition 2 generate an elementary abelian 2-group $E_{2^{n-1}}$ of order 2^{n-1}. It can be shown that $E_{2^{n-1}}$ acts fixed-point-free, i.e. we have its regular representation. Thus, after the simultaneous diagonalization of the Π_j's, the diagonal entries of the transformed $\Pi(W)$ will be in 1-to-1 correspondence with the irreducible representations of $E_{2^{n-1}}$, which are encoded by the ± 1-signs assigned to $\Pi_1, \dots, \Pi_{n-1}$.

Acknowledgements

The authors would like to acknowledge the support of NSF DSS-0729251, NSF-CSSI-0926618, DSS-0240058, the Rice University VIGRE program, and the Defense Advanced Research Projects Agency under Award No. N66001-10-1-4040. Additionally, research on this projected was supported in part by a grant from the Israel Science Foundation and Singapore MOE Tier 2 Grant MOE2011-T2-1-090 (ARC 19/11). Finally, the authors thank the editors and anonymous referees for their time, energy and insight.

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, 8:7–29, 1992.

[2] N. Alon and S. Tarsi, Colorings and orientations of graphs, *Combinatorica*, 12:125–134, 1992.

[3] E. Babson, S. Onn and R.R. Thomas, The Hilbert zonotope and a polynomial time algorithm for universal Gröbner bases, *Advances in Applied Mathematics*, 30:529–544, 2003.

[4] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proc. London Math. Soc*, 73:1–26, 1996.

[5] S. Buss and T. Pitassi, Good degree bounds on Nullstellensatz refutations of the induction principle, *IEEE Conference on Computational Complexity*, 233–242, 1996.

[6] M. Clegg, J. Edmonds and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In 28th Ann. ACM Symp. on Theory of Computing, 174–183, 1996.

[7] K. Conrad. The origin of representation theory, *Enseign. Math. (2)*, 44(3-4):361–392, 1998

[8] D. Cox and J. Little and D. O'Shea, Ideals, Varieties and Algorithms, *Springer*, New York, 1998.

[9] J.A. De Loera, J. Lee, P.N. Malkin, S. Margulies, Computing Infeasibility Certificates for Combinatorial Problems through Hilbert's Nullstellensatz, *Journal of Symbolic Computation*, 46(11), pg. 1260-1283, 2011.

[10] J.A. De Loera, J. Lee, P.N. Malkin, S. Margulies, Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility, Interntl. Symposium on Symbolic and Algebraic Computation, ISSAC 2009.

[11] J. De Loera, J. Lee, S. Margulies and S. Onn, Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz, *Combinatorics, Probability and Computing*, 18:551–582, 2009.

[12] S. Garey and D. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, *W.H. Freeman and Company*, 1979.

[13] D.Grigoriev, Complexity of Positivstellensatz proofs for the knapsack. *Computational Complexity*, 10(2):139–154, 2001.

[14] D. Grigoriev, E.A. Hirsch and D.V. Pasechnik, Complexity of semi-algebraic proofs. *Moscow Mathematical Journal*, 2:647–679, 2002.

[15] K.M. Hoffman, R. Kunze, Linear Algebra (2nd Edition), *Prentice-Hall, Inc.*, 1971.

[16] R.A. Horn, C.R. Johnson, Matrix Analysis, *Cambridge University Press*, 2012.

[17] R. Impagliazzo, P. Pudlák and J. Sgall. Lower bounds for polynomial calculus and the Groebner basis algorithm. *Computational Complexity*, 8:127–144, 1999.
[18] L. Lovász, Stable sets and Polynomials, *Discrete Mathematics*, 124:137–153, 1994.
[19] S. Margulies, Computer Algebra, Combinatorics and Complexity Theory: Hilbert's Nullstellensatz and NP-complete problems. Ph.D. thesis, UC Davis, 2008.
[20] S. Onn, Nowhere-zero flow polynomials, *Journal of Combinatorial Theory Series A*, 108:205–215, 2004.
[21] A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.