Computational Aspects of the Combinatorial Nullstellensatz Method

Edinah K. Gnang*

March 15, 2014

Abstract

We discuss here some computational aspects of the Combinatorial Nullstellensatz argument. Our main result shows that the order of magnitude of the symmetry group associated with permutations of the variables in algebraic constraints, determines the performance of algorithms naturally deduced from Alon's Combinatorial Nullstellensatz arguments. Finally we present a primal-dual polynomial constructions for certifying the existence or the non-existence of solutions to combinatorial problems.

1 Introduction

It is well-known that systems of polynomial equations over algebraically closed fields provide concise encodings for classical NP-hard problems such as the subgraph isomorphism problem. In [A], Alon presents the Combinatorial Nullstellensatz method, a general unified algebraic framework for establishing the existence of solutions to numerous problems in combinatorics and combinatorial number theory. The Combinatorial Nullstellensatz argument has recently been subject to intense scrutiny in the literature. Lasoń in [La] proposed a generalization of Alon's original formulation of the Combinatorial Nullstellensatz by weakening the assumption on the degree of the nonvanishing leading monomial. Furthermore, several variations of the proof of the Combinatorial Nullstellensatz can be found in the literature [Mi, H, Ko].

In the concluding remarks of [A] Alon points out that the proofs presented in [A] are based on non-constructive algebraic arguments and thus supply no efficient procedure for solving the corresponding algorithmic problems. Alon further proceeded to raise the fundamental problem of determining whether or not it is possible to deduce from such arguments efficient procedures for solving the corresponding algorithmic problems. Following up on the fundamental problem raised by Alon, we remark that it is well-known that combinatorial problems formulated as systems of polynomial equations can be solved using standard tools in computational algebra such as Gröbner basis [B, CLO] and closely related methods as presented in [S]. Unfortunately a precise analysis of the performance of Gröbner basis approaches in relation to special instances of combinatorial problems remain unknown. In subsequent work [LMM, LMO, M, LHMO], the authors follow up on the fundamental problem raised in [A] by Alon and propose the Nullstellensatz Linear Algebra algorithmic framework. Their proposed algorithms, relies on the experimentally-observed low degrees of Hilbert's Nullstellensatz certificates polynomial encodings of special families of combinatorial problem instances. The research program developed in [LMM, LMO, LHMO] follows up on the natural connection between Hilbert's Nullstellensatz [K] and complexity theory. This connection was first pointed out by Lovasz in [Lo]. Margulies further developed this connection in [M], and established that the minimum-degree Nullstellensatz certificate for the non-existence of an independent set of size greater than the largest independent set in the graph is equal to the size of the largest independent set in the graph. Finally, in [LMM, LMO, M, LHMO] the authors suggest that algebraic formulations enable us to exploit sparsity structure of special families of combinatorial problems. The authors also suggest that symmetries with respect to permutations of the variables in the algebraic constraints could yield performance improvements for algorithms which derive Nullstellensatz certificates. This last suggestion by the authors that exploiting symmetries are helpful for

*School of Mathematics, Institute for Advanced Study. Email: gnang@ias.edu.

deriving Nullstellensatz certificates stems from the well-known role of symmetries for solving combinatorial problems [SSK, K].

Our main result establishes that the order of magnitude of the automorphism group of the constraints with respect to permutations of the variables, determines the performance of algorithms deduced from Alon's Combinatorial Nullstellensatz argument for NP-hard problems. We further show that the Combinatorial Nullstellensatz method yields a natural framework for a primal-dual certificates for the existence versus the non-existence of solutions to graph and subgraph isomorphism instances.

2 Preliminary.

The Hadamard product of two given column vectors $\mathbf{a},\ \mathbf{b} \in \mathbb{C}^{n\times 1}$ noted $\mathbf{a}\star\mathbf{b}$, corresponds to a column vector of the same dimensions whose entries correspond to the product of the corresponding entries of $\mathbf{a}$, and $\mathbf{b}$; we write

$$k-\text{th entry of } \mathbf{a}\star\mathbf{b} \text{ is } a_k b_k. \tag{1}$$

Let us recall here the familiar notation used for the vector product of $\mathbf{a},\ \mathbf{b} \in \mathbb{C}^{n\times 1}$ with background matrix the $n\times n$ matrix $\mathbf{M}$. We write

$$\langle \mathbf{a},\ \mathbf{b}\rangle_{\mathbf{M}} := \sum_{0\leq k_0,k_1<n} a_{k_0} m_{k_0,k_1} b_{k_1}, \tag{2}$$

in particular it follows that

$$\langle \mathbf{a},\ \mathbf{b}\rangle := \langle \mathbf{a},\ \mathbf{b}\rangle_{\mathbf{I}} = \sum_{0\leq k<n} a_k b_k\ . \tag{3}$$

It shall be convenient to adopt the notation convention

$$\mathbf{a}^{\star^{\alpha}} := \left((a_k)^{\alpha}\right)_{0\leq k<n} \tag{4}$$

Futhermore let ω_n the denote the primitive n-th root of unity expressed by

$$\omega_n = e^{\frac{2\pi i}{n}} \tag{5}$$

and

$$\Omega_n := \left\{(\omega_n)^k\right\}_{0\leq k<n}. \tag{6}$$

The Discrete Fourier Transform matrix $\mathbf{W}$ whose entries are specified as follows

$$\mathbf{W} := \left(w_{uv} = (\omega_n)^{u\cdot v}\right)_{0\leq u,v<n} \tag{7}$$

is such that

$$\mathbf{W}\cdot\mathbf{W}^{\dagger} = n\,\mathbf{I} = \mathbf{W}^{\dagger}\cdot\mathbf{W}. \tag{8}$$

We shall often denote the set of column vectors of the DFT matrix $\mathbf{W}$ by the set $\left\{\mathbf{w}^{\star^k}\right\}_{0\leq k<n}$, where

$$\mathbf{w} := \left(w_k = (\omega_n)^k\right)_{0\leq k<n}. \tag{9}$$

3 Overview of the Combinatorial Nullstellensatz

The Combinatorial Nullstellensatz first presented in [A] by Alon , corresponds to the following theorem.

Theorem (Combinatorial Nullstellensatz I **Alon 1999**): Let $\mathbb{F}$ be an arbitrary field, and let $f\in\mathbb{F}[\mathbf{x}]$ and $\{S_k\subset\mathbb{F}\}_{0\leq k<n}$ denote a collection of non-empty subsets of $\mathbb{F}$ and define $g_i(x_i)=\prod_{s\in S_i}(x_i-s)$. If f vanishes over all common zeros of the vector $\mathbf{g}=(g_i)_{0\leq i<n}\in(\mathbb{F}[\mathbf{x}])^n$ (that is; if $f(\mathbf{s})=0$ forall $\mathbf{s}\in S_0\times\cdots\times S_{n-1}$), then there is a vector $\mathbf{h}=(h_i)_{0\leq i<n}\in(\mathbb{F}[\mathbf{x}])^n$ satisfying the innequalities $\{\deg(h_i)\leq\deg(f)-\deg(g_i)\}_{0\leq i<n}$ such that

$$f(\mathbf{x}) = \langle \mathbf{h}(\mathbf{x}), \mathbf{g}(\mathbf{x})\rangle := \sum_{0\leq k<n} h_k(\mathbf{x})\ g_k(\mathbf{x}). \tag{10}$$

Moreover, if the polynomial f and the entries of $\mathbf{g}$ lie in $R[\mathbf{x}]$ for some subring R of $\mathbb{F}$ there are polynomials $\{h_i\}_{0\leq i<n} \subset R[\mathbf{x}]$ as above.

Consequently we can prove the following :

Theorem (Combinatorial Nullstellensatz II **Alon 1999**): Let $\mathbb{F}$ be an arbitrary field, and let $f \in \mathbb{F}[\mathbf{x}]$. Suppose $\deg(f)$ is $\sum_{0\leq i<n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\mathbf{x}^{\mathbf{t}}$ in f is nonzero. Then if $\{S_k \subset \mathbb{F}\}_{0\leq k<n}$ denotes a collection of non-empty subset of $\mathbb{F}$ with $|S_i| > t_i$, there are $\mathbf{s} \in S_0 \times \cdots \times S_{n-1}$ so that

$$f(\mathbf{s}) \neq 0. \tag{11}$$

Subsequently the following generalization of the Combinatorial Nullstellensatz was proposed by Lasoń in [La].

Theorem (Generalized Combinatorial Nullstellensatz **M. Lasoń 2013):** Let $f \in \mathbb{F}[\mathbf{x}]$. If $\mathbf{x}^{\mathbf{t}}$ is a non-vanishing monomial in f and $\mathbf{t}$ is maximal in $\mathrm{Supp}(f)$, then for any subsets $S_0, \ldots, S_{n-1}$ of $\mathbb{F}$ satisfying $|S_i| > t_i$, there are $\mathbf{s} \in S_0 \times \cdots \times S_{n-1}$ so that $f(\mathbf{s}) \neq 0$.

We present here for the sake of completeness a proof by contradiction of Alon's Combinatorial Nullstellensatz argument but we remark that alternative short and possibly more elegant proofs can be found in [A, Mi, La, Kou, H].

Proof : We recall that by the Lagrange interpolation formula, the coefficients of the polynomial $f \in \mathbb{F}[\mathbf{x}]$ of degree $\sum_{0\leq k<n}(-1+|S_k|)$ are determined by evalutions of f on the Cartesian product set $S_0 \times \cdots \times S_{n-1}$. More explicitly we have

$$f(\mathbf{x}) \equiv \sum_{\mathbf{r}\in S_0\times\cdots\times S_{n-1}} f(\mathbf{r}) \prod_{\{s_k\in S_k\setminus\{r_k\}\}_{0\leq k<n}} \left(\frac{x_k - s_k}{r_k - s_k}\right) \mod \left\{\prod_{s_i\in S_i}(x_i - s_i)\right\}_{0\leq i<n},$$

where the right hand side of the congruence identity corresponds to the minimal degree polynomial congruent to f. By hypothesis we assumed that the coefficient of the leading monomial $\prod_{0\leq k<n}(x_k)^{-1+|S_k|}$ term is non-zero, and incidentally if we have that

$$\forall\, \mathbf{r} \in S_0 \times \cdots \times S_{n-1},\ f(\mathbf{r}) = 0$$

it would follow that the polynomial $f(\mathbf{x})$ is congruent to the identically zero polynomial which would contradicts our assumption that the the coefficient of the leading monomial $\prod_{0\leq k<n}(x_k)^{-1+|S_k|}$ term is non-zero.□

3.1 A classical application

Alon's Combinatorial Nullstellensatz argument is classicaly used to prove the existence of integral coefficient Galois resolvent.
Theorem (Integral Galois resolvent) : For all vectors $\mathbf{r} \in \mathbb{C}$, such that

$$0 \neq \prod_{0\leq i<j<n} \langle (\mathbf{e}_i - \mathbf{e}_j), \mathbf{r}\rangle, \tag{12}$$

(where $\{\mathbf{e}_k\}_{0\leq k<n}$ denotes the column vectors of the identity matrix) there exist at least one vector $\mathbf{s} \in \left\{0, \cdots, \binom{n!}{2}\right\}^n$ for which the stabilizer subgroup of S_n associated with the linear form $\langle \mathbf{r}, \mathbf{s}\rangle$ is trivial.

Proof : Consider the polynomial

$$f_{\mathbf{r}}(\mathbf{x}) = \prod_{\substack{0\leq \text{Lex Order}(\mu) < \text{Lex Order}(\nu) < n! \\ (\mu,\nu)\in S_n\times S_n}} (\langle \mathbf{r}, \mathbf{P}_\mu \mathbf{x}\rangle - \langle \mathbf{r}, \mathbf{P}_\nu \mathbf{x}\rangle) \tag{13}$$

$$\Rightarrow f_{\mathbf{r}}\left(\mathbf{x}\right)=\sum_{\gamma\in S_{(n!)}}\mathrm{Sgn}\left(\gamma\right)\prod_{\substack{0\leq\mathrm{Lex\ Order}\left(\sigma\right)<n!\\ \sigma\in S_n}}\left\langle\mathbf{r},\,\mathbf{P}_{\sigma}\mathbf{x}\right\rangle^{\gamma(\mathrm{Lex\ Order}(\sigma))}, \tag{14}$$

where for an arbitrary $\sigma\in S_n$, the matrix $\mathbf{P}_{\sigma}$ denotes the permutation matrix

$$\mathbf{P}_{\sigma}=\sum_{0\leq k<n}\mathbf{e}_k\cdot\left(\mathbf{e}_{\sigma(k)}\right)^T, \tag{15}$$

and Lex Order(σ) denotes the lexicographical order number associated with σ. Incidentally, the leading monomial of $f_{\mathbf{r}}\left(\mathbf{x}\right)$ for some appropriately chosen monomial order is of the form

$$\left(\prod_{0\leq i<n}x_i\right)^{\binom{n!}{2}}, \tag{16}$$

and hence by the Combinatorial Nullstellensatz we have that

$$\forall\ \left\{A_k\subset\mathbb{C}\right\}_{0\leq k<n},\ \text{ with }\left\{\left|A_k\right|>\binom{n!}{2}\right\}_{0\leq k<n},\quad\exists\,\mathbf{a}\in A_0\times\cdots\times A_{n-1}\text{ s.t. }f_{\mathbf{r}}\left(\mathbf{a}\right)\neq 0 \tag{17}$$

and in particular

$$\exists\,\mathbf{s}\in\left\{0,\cdots,\binom{n!}{2}\right\}^n\text{ s.t. }f_{\mathbf{r}}\left(\mathbf{s}\right)\neq 0. \tag{18}$$

4 The Combinatorial Nullstellensatz method

4.1 Nullstellensatz approach to subgraph isomorphism

Given $n\times n$ adjacency matrices $\mathbf{A}$ and $\mathbf{B}$ associated with unweighted directed graphs G and H. We say that $G\supseteq H$ i.e. H is subisomorphic to G if the following matrix equality holds for some $n\times n$ matrix $\mathbf{P}$

$$\left\{\begin{array}{rcl}\left(\mathbf{P}^T\cdot\mathbf{A}\cdot\mathbf{P}\right)\star\mathbf{B}&=&\mathbf{B}\\ \mathbf{P}^T\cdot\mathbf{P}&=&\mathbf{I}\\ \mathbf{P}^{\star^2}&=&\mathbf{P}\end{array}\right., \tag{19}$$

where $\mathbf{M}\star\mathbf{N}$ denotes the entry-wise or Hadamard product of the matrices $\mathbf{M}$, $\mathbf{N}$ and furthermore the matrix $\mathbf{M}^{\star^k}$ denotes the matrix resulting from raising all non-zero entries of $\mathbf{M}$ to some integer power k. We now express the matrix constraints above as constraints over elements of the ring $\mathbb{C}[x_0,x_1]/\{(x_j)^n-1\}_{0\leq j<2}$. We recall that the adjacency polynomials for the input graphs whose vertices are labeled with roots of unity, are deduced from the adjacency matrices $\mathbf{A},\mathbf{B}\in\{0,1\}^{n\times n}$ as follows

$$A\left(x_0,\,x_1\right)=n^{-2}\sum_{0\leq k_0,\,k_1<n}\left\langle\mathbf{w}^{\star^{-k_0}},\,\mathbf{w}^{\star^{-k_1}}\right\rangle_{\mathbf{A}}\left(x_0\right)^{k_0}\left(x_1\right)^{k_1},$$

$$B\left(x_0,\,x_1\right)=n^{-2}\sum_{0\leq k_0,\,k_1<n}\left\langle\mathbf{w}^{\star^{-k_0}},\,\mathbf{w}^{\star^{-k_1}}\right\rangle_{\mathbf{B}}\left(x_0\right)^{k_0}\left(x_1\right)^{k_1},$$

Incidentally, the subgraph isomorphism constraints are reformulated as follows

$$B\left(x_0,\,x_1\right)=$$

$$B\left(x_0,\,x_1\right)A\left(\sum_{0\leq k_0<n}r_{k_0}\prod_{0\leq t_0\neq k_0<n}\left(\frac{x_0-e^{i\frac{2\pi t_0}{n}}}{e^{i\frac{2\pi k_0}{n}}-e^{i\frac{2\pi t_0}{n}}}\right),\sum_{0\leq k_1<n}r_{k_1}\prod_{0\leq t_1\neq k_1<n}\left(\frac{x_1-e^{i\frac{2\pi t_1}{n}}}{e^{i\frac{2\pi k_1}{n}}-e^{i\frac{2\pi t_1}{n}}}\right)\right) \tag{20}$$

$$\forall\, 0 < t < n, \quad 0 = \sum_{0 \leq j < n} (r_j)^t \text{ and } n = \sum_{0 \leq j < n} (r_j)^n \tag{21}$$

$$\forall\, 0 \leq j < 2, \quad (x_j)^n = 1 \tag{22}$$

Fortunately, the constraints may be more concisely expressed using a polynomial parametrization of permutations of roots of unity expressed by

$$p(x, \mathbf{r}) = \sum_{0 \leq k < n} r_k \prod_{0 \leq s \neq k < n} \left(\frac{x - e^{i\frac{2\pi}{n}s}}{e^{i\frac{2\pi}{n}k} - e^{i\frac{2\pi}{n}s}} \right) \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ x^n - 1 \end{array} \right\}. \tag{23}$$

The solution to the subgraph isomorphism problem is therefore completely determined by the existence of $\gamma \in S_n$ and $\mathbf{g}(\mathbf{x}, \mathbf{r}) \in (\mathbb{C}[\mathbf{x}, \mathbf{r}])^n$ such that for

$$\mathbf{P}_\gamma = \sum_{0 \leq k < n} \mathbf{e}_k \cdot \mathbf{e}_{\gamma(k)}^T$$

we have

$$\langle (\mathbf{r} - \mathbf{P}_\gamma \mathbf{w}), \mathbf{g}(\mathbf{x}, \mathbf{r}) \rangle \equiv B(x_0, x_1)\left[1 - A\left(p(x_0, \mathbf{r}), p(x_1, \mathbf{r})\right)\right] \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}. \tag{24}$$

Since it is possible to efficiently compute the reduced polynomial

$$B(x_0, x_1)\left[1 - A\left(p(x_0, \mathbf{r}), p(x_1, \mathbf{r})\right)\right] \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}, \tag{25}$$

it follows that it must be NP-hard to determine whether or not some arbitrary multivariate polynomial $f(\mathbf{x}, \mathbf{r}) \in \mathbb{C}[\mathbf{x}, \mathbf{r}]$ admits an expansion of the form

$$f(\mathbf{x}, \mathbf{r}) = \langle (\mathbf{r} - \mathbf{P}_\gamma \mathbf{w}), \mathbf{g}(\mathbf{x}, \mathbf{r}) \rangle \tag{26}$$

for some permutation $\gamma \in S_n$ and a vector $\mathbf{g}(\mathbf{x}, \mathbf{r}) \in (\mathbb{C}[\mathbf{x}, \mathbf{r}])^n$.

Let $\mathrm{Aut} f$ denote the automorphism group of $f \in \mathbb{C}[\mathbf{x}, \mathbf{r}]$, defined by

$$\mathrm{Aut}\ f\ := \{\sigma \in S_n, \text{ s.t.} \quad f(\mathbf{x}, \mathbf{r}) - f(\mathbf{x}, \mathbf{P}_\sigma \mathbf{r}) = 0\}, \tag{27}$$

and hence $\mathrm{Aut} f$ denotes the stabilizer subgroup of S_n which fixes f, under permutation of the entries of the symbolic vector $\mathbf{r}$.

Theorem (Combinatorial resolvent) : The reduced polynomial

$$f(\mathbf{x}, \mathbf{r})\ := \left[1 - A\left(p(x_0, \mathbf{r}), p(x_1, \mathbf{r})\right)\right] B(x_0, x_1) \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}, \tag{28}$$

admits an expansion of the form

$$\langle (\mathbf{r} - \mathbf{P}_\gamma \mathbf{w}), \mathbf{g}(\mathbf{x}, \mathbf{r}) \rangle \equiv \left[1 - A\left(p(x_0, \mathbf{r}), p(x_1, \mathbf{r})\right)\right] B(x_0, x_1) \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}. \tag{29}$$

for some permutation $\gamma \in S_n$ and a vector $\mathbf{g}(\mathbf{x}, \mathbf{r}) \in (\mathbb{C}[\mathbf{x}, \mathbf{r}])^n$, if and only if

$$0 \equiv \prod_{\sigma \in S_n / \mathrm{Aut}_f} f(\mathbf{x}, \mathbf{P}_\sigma \mathbf{r}) \mod \left\{ \begin{array}{c} \mathbf{r} - \mathbf{w} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\} \tag{30}$$

Proof : The proof of the theorem is an immediate consequence of Euclidean division. We have

$$\forall\, \sigma^{-1} \in S_n,\ f(\mathbf{x}, \mathbf{r}) = \kappa_{\sigma^{-1}}(\mathbf{x}) + \langle (\mathbf{r} - \mathbf{P}_{\sigma^{-1}} \mathbf{w}), \mathbf{g}_{\sigma^{-1}}(\mathbf{x}, \mathbf{r}) \rangle \tag{31}$$

$$\Rightarrow f\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right) = \kappa_{\sigma^{-1}}\left(\mathbf{x}\right) + \left\langle \mathbf{P}_{\sigma^{-1}}\left(\mathbf{r}-\mathbf{w}\right),\, \mathbf{g}_{\sigma^{-1}}\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right)\right\rangle \tag{32}$$

$$\Rightarrow f\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right) = \kappa_{\sigma^{-1}}\left(\mathbf{x}\right) + \left\langle \left(\mathbf{r}-\mathbf{w}\right),\, \mathbf{P}_{\sigma}\mathbf{g}_{\sigma^{-1}}\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right)\right\rangle \tag{33}$$

and hence

$$\prod_{\sigma\in S_n} f\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right) \equiv \prod_{\sigma\in S_n} \kappa_{\sigma^{-1}}\left(\mathbf{x}\right) \mod \left\{ \begin{array}{c} \mathbf{r}-\mathbf{w} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}$$

furthermore we note that

$$\prod_{\sigma\in S_n} f\left(\mathbf{x},\, \mathbf{P}_{\sigma^{-1}}\mathbf{r}\right) \equiv \left(\prod_{\sigma\in S_n/\mathrm{Aut}_f} f\left(\mathbf{x},\, \mathbf{P}_{\sigma}\mathbf{r}\right) \right)^{|\mathrm{Aut}_f|} \tag{34}$$

from which it immediately follows that

$$\prod_{\sigma\in S_n/\mathrm{Aut}_f} f\left(\mathbf{x},\, \mathbf{P}_{\sigma}\mathbf{r}\right) \equiv 0 \mod \left\{ \begin{array}{c} \mathbf{r}-\mathbf{w} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\} \Leftrightarrow \exists\, \sigma\in S_n \text{ s.t. } \kappa_{\sigma}\left(\mathbf{x}\right) \equiv 0. \,\square \tag{35}$$

We refer to the polynomial $\prod_{\sigma\in S_n/\mathrm{Aut}_f} f\left(\mathbf{x},\, \mathbf{P}_{\sigma}\mathbf{r}\right)$ as the combinatrial resolvent because of the close resemblance with the Galois resolvent. The reader is refered to [G] for further discussion on Galois theory approaches to graph isomorphism problems.

4.2 Subgraph isomorphism dual Nullstellensatz construction

In order to mimic the Alon and Tarsi polynomial constructions discussed in [AT] for determining the existence of solutions to a subgraph isomorphism instance, one would seek instead a polynomial construction which will be identically zero if H is not sub-isomorphic to G, and the polynomial construction would admit a non vanishing term otherwise. For the purpose of the construction let us consider the adjacency polynomials associated with the graphs

$$A\left(x_0,\, x_1\right) = n^{-2} \sum_{0\le k_0,\, k_1<n} \left\langle \mathbf{w}^{\star^{-k_0}},\, \mathbf{w}^{\star^{-k_1}} \right\rangle_{\mathbf{A}} \left(x_0\right)^{k_0} \left(x_1\right)^{k_1},$$

$$B\left(x_0,\, x_1\right) = n^{-2} \sum_{0\le k_0,\, k_1<n} \left\langle \mathbf{w}^{\star^{-k_0}},\, \mathbf{w}^{\star^{-k_1}} \right\rangle_{\mathbf{B}} \left(x_0\right)^{k_0} \left(x_1\right)^{k_1},$$

deduced as usual from the adjacency matrices $\mathbf{A},\, \mathbf{B} \in \{0,1\}^{n\times n}$. Furthermore consider the set $\mathfrak{G}_{\mathbf{B}}$ which denote the set of adjacency matrices of non isomorphic graphs which do not contain H as a subgraph. Formally we write

$$\mathfrak{G}_{\mathbf{B}} := \left\{ \mathbf{C}\in\{0,\,1\}^{n\times n},\ \text{s.t.} \begin{array}{c} \forall \sigma\in S_n\ \left(\mathbf{1}_{n\times n} - \mathbf{P}_{\sigma}^{T}\mathbf{C}\mathbf{P}_{\sigma}\right) \star \mathbf{B} \neq \mathbf{0}_{n\times n} \\ \forall \sigma\in S_n \text{ and } \left(\mathbf{C}_0,\mathbf{C}_1\right) \in \left(\mathfrak{G}_B \backslash \{\mathbf{C}_1\}\right) \times \left(\mathfrak{G}_B, \backslash\, \{\mathbf{C}_0\}\right),\ \left(\mathbf{P}_{\sigma}^{T}\mathbf{C}_0\mathbf{P}_{\sigma}\right) \neq \mathbf{C}_1 \end{array} \right\} \tag{36}$$

finally let $\mathfrak{P}_{\mathbf{B}}$ denote the corresponding set of adjacency polynomials defined as

$$\mathfrak{P}_{\mathbf{B}} := \left\{ n^{-2} \sum_{0\le k_0,\, k_1<n} \left\langle \mathbf{w}^{\star^{-k_0}},\, \mathbf{w}^{\star^{-k_1}} \right\rangle_{\mathbf{C}} \left(x_0\right)^{k_0} \left(x_1\right)^{k_1},\ \text{s.t. } \mathbf{C}\in\mathfrak{G}_{\mathbf{B}} \right\}. \tag{37}$$

The corresponding Alon and Tarsi polynomial construction for determining the existence of solution to subgraph Isomorphism instances is expressed by

$$f_B\left(A,\, \mathbf{x},\, \mathbf{r}\right) = \prod_{0\le i<j<n} \left\langle \left(\mathbf{e}_i - \mathbf{e}_j\right),\, \mathbf{r}\right\rangle \times$$

$$\prod_{C(x_0,x_1)\in\mathfrak{P}_{\mathbf{B}}} \left[\left[1 - A\left(x_0,x_1\right)\right] C\left(p\left(x_0,\mathbf{r}\right), p\left(x_1,\mathbf{r}\right)\right)\right] \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}. \tag{38}$$

It follows by construction that if $f_B(A,\,\mathbf{x},\,\mathbf{r})$ is identically zero then this fact constitutes a certificate of non-existence of solutions to the subisomorphism instance. Incidentally, we think of the construction as dual to the initial polynomial encoding of subgraph isomorphism problem described in the previous section. Similarly, the dual polynomial construction for graph Isomorphism instances is expressed by

$$g_B(A,\,\mathbf{x},\,\mathbf{r}) = \prod_{0\leq i<j<n} \langle (\mathbf{e}_i - \mathbf{e}_j),\,\mathbf{r}\rangle \times$$

$$\prod_{C(x_0,x_1)\in\mathfrak{P}_{\mathbf{B}}} [[1-A(x_0,x_1)]\,C(p(x_0,\mathbf{r}),p(x_1,\mathbf{r})) + [1-C(p(x_0,\mathbf{r}),p(x_1,\mathbf{r}))]\,A(x_0,x_1)] \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{w}^{\star^0} \\ \mathbf{x}^{\star^n} - \mathbf{1}_{2\times 1} \end{array} \right\}. \tag{39}$$

Acknowledgments

This material is based upon work supported by the National Science Foundation under agreements Princeton University Prime Award No. CCF-0832797 and Sub-contract No. 00001583. The author would like to thank the IAS for providing excellent working conditions. The author is also grateful to Vladimir Retakh, Ahmed Elgammal, Avi Wigderson, Noga Alon for insightful comments while preparing this manuscript.

References

[A] N. Alon, Combinatorial Nullstellensatz, Comb. Prob. Comput. 8 , 7-29, (1999).

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

[AKS] M. Agrawal, N. Kayal and N. Saxena, PRIMES is in P, Ann. Math. v. 160, 781–793, (2004)

[B] Bruno Buchberger. An algorithmic criterion for the solvability of a system of algebraic equations. Aequationes Mathematicae 4, 374–383, (1970).

[CLO] D. A. Cox J. B. L.D. O'Shea. Ideals, Varieties, and Algorithms Third Edition, Springer, (2007).

[G] D. Grigoriev "Two reductions of graph isomorphism to problems for polynomials" p.56-61 (English translation in J.Soviet Math., vol.20, 1982, p.2296-2298)

[H] P. C. Heinig, Proof of the combinatorial nullstellensatz over integral domains in the spirit of Kouba, Electron. J. Combin. 17 (2010).

[K] E. Kranakis: Invited Talk: Symmetry and Computability in Anonymous Networks. SIROCCO 1-16, (1996).

[Ko] J. Kollár, "Sharp Effective Nullstellensatz", J. of AMS. 1 (4): 963–975 (1988).

[Kou] O. Kouba, A Duality Based Proof of the Combinatorial Nullstellensatz, Elect. J. of Combinatorics, V. 16, (2009).

[La] M. Lasoń, A generalization of Combinatorial Nullstellensatz, Electron. J. Combin. 17 (2010).

[LHMO] J. A. Loera, C. J. Hillar, P. N. Malkin, M. Omar, Recognizing Graph Theoretic Properties with Polynomial Ideals, Elect. J. of Combinatorics, V. 17, (2010).

[LMM] J. A. De Loera, J. Lee, P. N. Malkin, and S. Margulies. Hilbert's nullstellensatz and an algorithm for proving combinatorial infeasibility. In Proceedings of the twenty-first international symposium on Symbolic and algebraic computation (ISSAC 2008). ACM, New York, NY, USA, 197-206. (2008).

[LMO] J. A. Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and hilbert's nullstellensatz. Comb. Probab. Comput. 18, 4 , 551-582 (2009).

[Lo] L. Lovász. Stable sets and polynomials. Discrete Mathematics, 124:137–153, (1994).

[M] S. Margulies, Computer Algebra, Combinatorics, and Complexity: Hilbert's Nullstellensatz and NP-Complete Problems. Ph.D. Dissertation. University of California at Davis, Davis, CA, USA. AAI3336295. (2008)

[Mi] M. Michalek, A short proof of Combinatorial Nullstellensatz, Amer. Math. Monthly 117 , 821–823, (2010).

[RW] R. Ramamurthi, D. B. West, Hypergraph extension of the Alon–Tarsi list coloring theorem, Combinatorica 25 , 355-366 (2005).

[S] U. Schauz, Algebraically solvable problems: describing polynomials as equivalent to explicit solutions. Electron. J. Combin. 15 , no. 1, Research Paper 10 (2008).

[SSK] S. Ben-Israel, Eli Ben-Sasson, David R. Karger: Breaking local symmetries can dramatically reduce the length of propositional refutations. Electronic Colloquium on Computational Complexity (ECCC) 17: 68 (2010)