Limitations of Algebraic Approaches to Graph Isomorphism Testing

Christoph Berkholz(✉) and Martin Grohe

RWTH Aachen University, Aachen, Germany
{berkholz,grohe}@informatik.rwth-aachen.de

Abstract. We investigate the power of graph isomorphism algorithms based on algebraic reasoning techniques like Gröbner basis computation. The idea of these algorithms is to encode two graphs into a system of equations that are satisfiable if and only if if the graphs are isomorphic, and then to (try to) decide satisfiability of the system using, for example, the Gröbner basis algorithm. In some cases this can be done in polynomial time, in particular, if the equations admit a bounded degree refutation in an algebraic proof systems such as Nullstellensatz or polynomial calculus. We prove linear lower bounds on the polynomial calculus degree over all fields of characteristic $\neq 2$ and also linear lower bounds for the degree of Positivstellensatz calculus derivations.

We compare this approach to recently studied linear and semidefinite programming approaches to isomorphism testing, which are known to be related to the combinatorial Weisfeiler-Lehman algorithm. We exactly characterise the power of the Weisfeiler-Lehman algorithm in terms of an algebraic proof system that lies between degree-k Nullstellensatz and degree-k polynomial calculus.

1 Introduction

The graph isomorphism problem (GI) is notorious for its unresolved complexity status. While there are good reasons to believe that GI is not NP-complete, it is wide open whether it is in polynomial time.

Complementing recent research on linear and semidefinite programming approaches to GI [1,7,10,13,14], we investigate the power of GI-algorithms based on algebraic reasoning techniques like Gröbner basis computation. The idea of all these approaches is to encode isomorphisms between two graphs as solutions to a system of equations and possibly inequalities and then try to solve this system or relaxations of it. Most previous work is based on the following encoding: let G, H be graphs with adjacency matrices A, B, respectively. Note that G and H are isomorphic if and only if there is a permutation matrix X such that $AX = XB$. If we view the entries x_{vw} of the matrix X as variables, we obtain a system of linear equations. We introduce equations forcing all row- and column

RWTH Aachen University—The first author is currently at KTH Stockholm, supported by a fellowship within the Postdoc-Program of the German Academic Exchange Service (DAAD).

M.M. Halldórsson et al. (Eds.): ICALP 2015, Part I, LNCS 9134, pp. 155–166, 2015.
DOI: 10.1007/978-3-662-47672-7_13

sums of X to be 1 and add the inequalities $x_{vw} \geq 0$. It follows that the integer solutions to this system are 0/1-solutions that correspond to isomorphisms between G and H. Of course this does not help to solve GI, because we cannot find integer solutions to a system of linear inequalities in polynomial time. The first question to ask is what happens if we drop the integrality constraints. Almost thirty years ago, Tinhofer [17] proved that the system has a rational (or, equivalently, real) solution if and only if the so-called colour refinement algorithm does not distinguish the two graphs. *Colour refinement* is a simple combinatorial algorithm that iteratively colours the vertices of a graph according to their "iterated degree sequences", and, to distinguish two graphs, tries to detect a difference in their colour patterns. For every k, there is a natural generalisation of the colour refinement algorithm that colours k-tuples of vertices instead of single vertices; this generalisation is known as the *k-dimensional Weisfeiler-Lehman algorithm (k-WL)*. Atserias and Maneva [1] and independently Malkin [13] proved that the Weisfeiler-Lehman algorithm is closely tied to the *Sherali-Adams* hierarchy [16] of increasingly tighter LP-relaxations of the integer linear program for GI described above: the distinguishing power of k-WL is between that of the $(k-1)$st and kth level of the Sherali-Adams hierarchy. Otto and the second author of this paper [10] gave a precise correspondence between k-WL and the nonnegative solutions to a system of linear equations between the $(k-1)$st and kth level of the Sherali-Adams hierarchy. Already in 1992, Cai, Fürer, and Immerman [5] had proved that for every k there are non-isomorphic graphs G_k, H_k (called *CFI-graphs* in the following) of size $O(k)$ that are not distinguished by k-WL, and combined with the results of Atserias-Maneva and Malkin, this implies that no sublinear level of the Sherali-Adams hierarchy suffices to decide isomorphism. O'Donnell, Wright, Wu, and Zhou [14] (also see [7]) studied the Lasserre hierarchy [12] of semi-definite relaxations of the integer linear program for GI. They proved that the same CFI-graphs cannot even be distinguished by sublinear levels of the Lasserre hierarchy.

However, there is a different way of relaxing the integer linear program to obtain a system that can be solved in polynomial time: we can drop the nonnegativity constraints, which are the only inequalities in the system. Then we end up with a system of linear equalities, and we can ask whether it is solvable over some finite field or over the integers. As this can be decided in polynomial time, it gives us a new polynomial time algorithm for graph isomorphism: we solve the system of equations associated with the given graphs. If there is no solution, then the graphs are nonisomorphic. (We say that the system of equations *distinguishes* the graphs.) If there is a solution, though, we do not know if the graphs are isomorphic or not. Hence the algorithm is "sound", but not necessarily "complete". Actually, it is not obvious that the algorithm is not complete. If we interpret the linear equations over $\mathbb{F}_2$ or over the integers, the system does distinguish the CFI-graphs (which is not very surprising because these graphs encode systems of linear equations over $\mathbb{F}_2$). Thus the lower bound techniques applied in all previous results do not apply here. However, we construct nonisomorphic graphs that cannot be distinguished by this system (see Theorem 6.4).

In the same way, we can drop the nonnegativity constraints from the levels of the Sherali-Adams hierarchy and then study solvability over finite fields or over the integers, which gives us increasingly stronger systems. Even more powerful algorithms can be obtained by applying algebraic techniques based on Gröbner basis computations. Proof complexity gives us a good framework for proving lower bounds for such algorithms. There are algebraic proof systems such as the polynomial calculus [6] and the weaker Nullstellensatz system [2] that characterise the power of these algorithms. The degree of refutations in the algebraic systems roughly corresponds to the levels of the Sherali-Adams and Lasserre hierarchies for linear and semi-definite programming, and to the dimension of the Weisfeiler-Lehman algorithm. We identify a fragment of the polynomial calculus, called the monomial polynomial calculus, such that degree-k refutations in this system precisely characterise distinguishability by k-WL (see Theorem 4.4).

As our main lower bounds, we prove that for every field $\mathbb{F}$ of characteristic $\neq 2$, there is a family of nonisomorphic graphs G_k, H_k of size $O(k)$ that cannot be distinguished by the polynomial calculus in degree k. Furthermore, we prove that there is a family of nonisomorphic graphs G_k, H_k of size $O(k)$ that cannot be distinguished by the Positivstellensatz calculus in degree k. The Positivstellensatz calculus [9] is an extension of the polynomial calculus over the reals and subsumes semi-definite programming hierarchies. Thus, our results slightly generalise the results of O'Donnell et al. [14] on the Lasserre hierarchy (described above). Technically, our contribution is a low-degree reduction from systems of equations describing so-called Tseitin tautologies to the systems for graph isomorphism. Then we apply known lower bounds [3,9] for Tseitin tautologies.

2 Algebraic Proof Systems

Polynomial calculus (PC) is a proof system to prove that a given system of (multivariate) polynomial equations P over a field $\mathbb{F}$ has no 0/1-solution. We always normalise polynomial equations to the form $p = 0$ and just write p to denote the equation $p = 0$. The derivation rules are the following (for polynomial equations $p \in \mathsf{P}$, polynomials f, g, variables x and field elements a, b):

$$\frac{}{p}, \quad \frac{}{x^2 - x}, \quad \frac{f}{xf}, \quad \frac{g \quad f}{ag + bf}.$$

The *axioms* of the systems are all $p \in \mathsf{P}$ and $x^2 - x$ for all variables x. A PC *refutation* of P is a derivation of 1. The polynomial calculus is sound and complete, that is, P has a PC refutation if and only if it is unsatisfiable. The *degree* of a PC derivation is the maximal degree of all polynomials in the derivation. Originally, Clegg et. al. [6] introduced the polynomial calculus to model Gröbner basis computation. Moreover, using the Gröbner basis algorithm, it can be decided in time $n^{O(d)}$ whether a given system of polynomial equations has a PC refutation of degree d (see [6]).

We introduce the following restricted variant of the polynomial calculus. A *monomial-PC* derivation is a PC-derivation where we require that the polynomial f in the multiplication rule $\frac{f}{xf}$ is either a monomial or the product of a monomial and an axiom.

If we restrict the application of the multiplication rule even further and require f to be the product of a monomial and an axiom, we obtain the Nullstellensatz proof system [2]. This proof system is usually stated in the following static form. A *Nullstellensatz* refutation of a system P of polynomial equations consists of polynomials f_p, for $p \in \mathsf{P}$, and g_x, for all variables x, such that

$$\sum_{p \in \mathsf{P}} f_p p + \sum_{x} g_x(x^2 - x) = 1.$$

The degree of a Nullstellensatz refutation is the maximum degree of all polynomials $f_p p$.

2.1 Low-Degree Reductions

To compare the power of the polynomial calculus for different systems of polynomial equations, we use *low degree reductions* [4]. Let P and R be two sets of polynomials in the variables $\mathcal{X}$ and $\mathcal{Y}$, respectively. A *degree-*(d_1, d_2) *reduction* from P to R consist of the following:

– for each variable $y \in \mathcal{Y}$ a polynomial $f_y(x_1, \dots, x_k)$ of degree at most d_1 in variables $x_1, \dots, x_k \in \mathcal{X}$;
– for each polynomial $r(y_1, \dots, y_\ell) \in \mathsf{R}$ a degree-d_2 PC derivation of

$$r\big(f_{y_1}(x_{11}, \dots, x_{1k_1}), \dots, f_{y_\ell}(x_{\ell 1}, \dots, x_{\ell k_\ell})\big)$$

from P.
– for each variable $y \in \mathcal{Y}$ a degree-d_2 PC derivation of

$$f_y(x_1, \dots, x_k)^2 - f_y(x_1, \dots, x_k)$$

from P.

Lemma 2.1 ([4]). *If there is a degree-*(d_1, d_2) *reduction from* P *to* R *and* R *has a polynomial calculus refutation of degree* k*, then* P *has a polynomial calculus refutation of degree* $\max(d_2, kd_1)$*.*

2.2 Linearisation

For a system of polynomial equations P over variables x_i let P^r be the set of all polynomial equations of degree at most r obtained by multiplying a polynomial in P by a monomial over the variables x_i. Furthermore, for a system of polynomial equations P let $\mathrm{MLIN}(\mathsf{P})$ be the the multi-linearisation of P obtained by replacing every monomial $x_{i_1} \cdots x_{i_\ell}$ by a variable $X_{\{i_1,\dots,i_\ell\}}$. Observe that if P has a 0/1-solution α, then so does $\mathrm{MLIN}(\mathsf{P})$ as we can set $\alpha(X_{\{i_1,\dots,i_\ell\}}) := \alpha(x_{i_1}) \cdots \alpha(x_{i_\ell})$. The converse however does not hold since a solution α for $\mathrm{MLIN}(\mathsf{P})$ does not have to satisfy $\alpha(X_{\{ab\}}) = \alpha(X_{\{a\}})\alpha(X_{\{b\}})$. The next lemma states a well-known connection between Nullstellensatz and Linear Algebra.

Lemma 2.2 [**3**]**.** *Let* P *be a system of polynomial equations. The following statements are equivalent.*

– P *has a degree* r *Nullstellensatz refutation.*
– *The system of linear equations* $\mathrm{MLIN}(\mathsf{P}^r)$ *has no solution.*

This characterisation of Nullstellensatz proofs in terms of a linear system of equations (also called *design* [3]) is a useful tool for proving lower bounds on the Nullstellensatz degree. Unfortunately, a similar characterisation for bounded degree PC is not in sight. However, for the newly introduced system monomial-PC, which lies between Nullstellensatz and PC, we have a similar criterion for the non-existence of refutations. The proof is deferred to the appendix.

Lemma 2.3. *If* $\mathrm{MLIN}(\mathsf{P}^d)$ *has a solution* α *that additionally satisfies*

$$\alpha(X_\pi) = 0 \Longrightarrow \alpha(X_\rho) = 0, \text{ for all } \pi \subseteq \rho,$$

then P *has no degree* d *monomial-PC derivation.*

2.3 Linear and Semidefinite-Programming Approaches

In the previous section we have seen that degree-d Nullstellensatz corresponds to solving a system of *linear equations* of size $n^{O(d)}$, which can be done in time $n^{O(d)}$. Over the reals, this approach can be strengthened by considering hierarchies of relaxations for linear and semi-definite programming.

In this setting one additionally adds linear inequalities, typically $0 \leq x \leq 1$. In the same way as for the Nullstellensatz, one lifts this problem to higher dimensions, by multiplying the inequalities and equations with all possible monomials of bounded degree. Afterwards, one linearises this system as above to obtain a system of *linear inequalities* of size $n^{O(d)}$, which can also be solved in polynomial time using linear programming techniques. This lift-and-project technique is called Sherali-Adams relaxation of level d [16].

Another even stronger relaxation is based on semidefinite programming techniques. This technique has different names: Positivstellensatz, Sum-of-Squares (SOS), or Lasserre Hierarchy. Here we take the view point as a proof system, which was introduced by Grigoriev and Vorobjov [9] and directly extends the Nullstellensatz over the reals. A degree-d *Positivstellensatz* refutation of a system P of polynomial equations consists of polynomials f_p, for $p \in \mathsf{P}$, and g_x, for all variables x, and in addition polynomials h_i such that

$$\sum_{p \in \mathsf{P}} f_p p + \sum_x g_x(x^2 - x) = 1 + \sum_i h_i^2.$$

The degree of a Positivstellensatz refutation is the maximum degree of all polynomials $f_p p$ and h_i^2. It is important to note that Positivstellensatz refutations can be found in time $n^{O(d)}$ using semi-definite programming. This has been independently observed by Parrilo [15] in the context of algebraic geometry and by Lasserre [12] in the context of linear optimisation.

Grigoriev and Vorobjov [9] also introduced a proof system called Positivstellensatz calculus, which extends polynomial calculus in the same way as Positivstellensatz extends Nullstellensatz. A *Positivstellensatz calculus* refutation of a system of polynomials P is a polynomial calculus derivation over the reals of $1+\sum_i h_i^2$. Again, the degree of such a refutation is the maximum degree of every polynomial in the derivation.

3 Equations for Graph Isomorphism

We find it convenient to encode isomorphism using different equations than those from the system $AX = XB$ described in the introduction. However, the equations $AX = XB$ can easily be derived in our system, and thus lower bounds for our system imply lower bounds for the $AX = XB$-system.

Throughout this section, we fix graphs G and H, possibly with coloured vertices and/or edges. Isomorphisms between coloured graphs are required to preserve the colours. We assume that either $|V(G)| \geq 2$ or $|V(H)| \geq 2$. We shall define a system $\mathsf{P}_{\text{iso}}(G,H)$ of polynomial equations that has a solution if and only if G and H are isomorphic. The equations are defined over variables $x_{vw}, v \in V(G), w \in V(H)$. A solution to the system is intended to describe an isomorphism ι from G to H, where $x_{vw} \mapsto 1$ if $\iota(v) = w$ and $x_{vw} \mapsto 0$ otherwise. The system $\mathsf{P}_{\text{iso}}(G,H)$ consists of the following linear and quadratic equations:

$$\sum_{v\in V(G)} x_{vw} - 1 = 0 \qquad \text{for all } w \in V(H) \tag{3.1}$$

$$\sum_{w\in V(H)} x_{vw} - 1 = 0 \qquad \text{for all } v \in V(G) \tag{3.2}$$

$$x_{vw}x_{v'w'} = 0 \qquad \text{for all } v,v' \in V(G), w,w' \in V(H) \text{ such that } \{(v,w),(v',w')\} \text{ is not a local isomorphism.} \tag{3.3}$$

A *local isomorphism* from G to H is an injective mapping π with domain in $V(G)$ and range in $V(H)$ (often viewed as a subset of $V(G) \times V(H)$) that preserves adjacencies, that is $vw \in E(G) \iff \pi(v)\pi(w) \in E(H)$. If G and H are coloured graphs, local isomorphisms are also required to preserve colours.

To enforce 0/1-assignments we add the following set Q of quadratic equalities

$$x_{vw}^2 - x_{vw} = 0 \qquad \text{for all } v \in V(G), w \in V(H). \tag{3.4}$$

We treat these equations separately because they are axioms of the polynomial calculus anyway. Observe that the equations (3.1) and (3.2) in combination with (3.4) make sure that every solution to the system describes a bijective mapping from $V(G)$ to $V(H)$. The equations (3.3) make sure that this bijection is an isomorphism. Thus, for every field $\mathbb{F}$, the system $\mathsf{P}_{\text{iso}}(G,H) \cup \mathsf{Q}$ has a solution over $\mathbb{F}$ if and only G and H are isomorphic.

4 Weisfeiler-Lehman Is Located Between Nullstellensatz and Polynomial Calculus

To relate the Weisfeiler-Lehman algorithm to our proof systems, we use the following combinatorial game. The *bijective k-pebble game* [11] on graphs G and H is played by two players called *Spoiler* and *Duplicator*. Positions of the game are sets $\pi \subseteq V(G) \times V(H)$ of size $|\pi| \leq k$. The game starts in an initial position π_0. If $|V(G)| \neq |V(H)|$ or if π_0 is not a local isomorphism, then Spoiler wins the game immediately, that is, after 0 rounds, Otherwise, the game is played in a sequence of *rounds*. Suppose the position after the ith round is π_i. In the $(i+1)$st round, Spoiler chooses a subset $\pi \subseteq \pi_i$ of size $|\pi| < k$. Then Duplicator chooses a bijection $f : V(G) \to V(H)$. Then Spoiler chooses a vertex $v \in V(G)$, and the new position is $\pi_{i+1} := \pi \cup \{(v, f(v))\}$. If π_{i+1} is not a local isomorphism, then Spoiler wins the play after $(i+1)$ rounds. Otherwise, the game continues with the $(i+2)$nd round. Duplicator wins the play if it lasts forever, that is, if Spoiler does not win after finitely many rounds. *Winning strategies* for either player in the game are defined in the natural way.

Lemma 4.1 ([5,11]). *k-WL distinguishes G and H if and only if Spoiler has a winning strategy for the bijective k-pebble game on G, H with initial position $\emptyset$.*

Observe that each game position $\pi = \{(v_1, w_1), \dots, (v_\ell, w_\ell)\}$ of size ℓ corresponds to a multilinear monomial $\boldsymbol{x}_\pi = x_{v_1 w_1} \dots x_{v_\ell w_\ell}$ of degree ℓ; for the empty position we let $\boldsymbol{x}_\emptyset := 1$.

Lemma 4.2. *Let $\mathbb{F}$ be a field of characteristic 0. If Spoiler has a winning strategy for the r-round bijective k-pebble game on G, H with initial position π_0, then there is a degree k monomial-PC derivation of $\boldsymbol{x}_{\pi_0}$ from $\mathsf{P}_{\text{iso}}(G, H)$ over $\mathbb{F}$.*

Proof. The proof is by induction over r. For the base case $r = 0$, suppose that Spoiler wins after round 0. If $|V(G)| \neq |V(H)|$, the system $\mathsf{P}_{\text{iso}}(G, H)$ has the following degree-1 Nullstellensatz refutation:

$$\sum\nolimits_{v \in V(G)} \tfrac{1}{a} \Big(\sum\nolimits_{w \in V(H)} x_{vw} - 1 \Big) + \sum\nolimits_{w \in V(H)} -\tfrac{1}{a} \Big(\sum\nolimits_{v \in V(G)} x_{vw} - 1 \Big) = 1,$$

where $a = |V(G) - V(H)|$. It yields a degree-1 monomial PC refutation of $\mathsf{P}_{\text{iso}}(G, H)$ and thus a derivation of $\boldsymbol{x}_{\pi_0}$ of degree $|\pi_0| \leq k$. Otherwise, π_0 is not a local isomorphism. Then there is a 2-element subset $\pi := \{(v, w), (v', w')\} \subseteq \pi_0$ that is not a local isomorphism. Multiplying the axiom $x_{vw} x_{v'w'} = \boldsymbol{x}_\pi$ with the monomial $\boldsymbol{x}_{\pi_0 \setminus \pi}$, we obtain a monomial-PC derivation of $\boldsymbol{x}_{\pi_0}$ of degree $|\pi_0| \leq k$.

For the inductive step, suppose that Spoiler has a winning strategy for the $(r+1)$-round game starting in position π_0. Let $\pi \subseteq \pi_0$ with $|\pi| < k$ be the set chosen by Spoiler in the first round of the game. We can derive $\boldsymbol{x}_{\pi_0}$ from $\boldsymbol{x}_\pi$ by multiplying with the monomial $\boldsymbol{x}_{\pi_0 \setminus \pi}$. Hence it suffices to show that we can derive $\boldsymbol{x}_\pi$ in degree k.

Consider the bipartite graph B on $V(G) \uplus V(H)$ which has an edge vw for all $v \in V(G), w \in V(H)$ such that Spoiler *cannot* win from position $\pi \cup \{(v, w)\}$

in at most r rounds. As from position π, Spoiler wins in $r+1$ rounds, there is no bijection $f : V(G) \to V(H)$ such that $(v, f(v)) \in E(B)$ for all $v \in V(G)$. By Hall's Theorem, it follows that there is a set $S \subseteq V(G)$ such that $|N^B(S)| < |S|$. Let S be a maximal set with this property and let $T := N^B(S)$.

We claim that $N^B(T) = S$. To see this, suppose for contradiction that there is a vertex $v \in N^B(T) \setminus S$. By the maximality of S, we have $N^B(v) \not\subseteq T$. Let $w \in N^B(v) \setminus T$. Moreover, let $w' \in N^B(v) \cap T$ (exists because $v \in N^B(T)$) and $v' \in N^B(w') \cap S$ (exists because $T = N^B(S)$). Then by the definition of B, Duplicator has a winning strategy for the r-round bijective k-pebble game with initial positions $\pi \cup \{(v', w')\}$, $\pi \cup \{(v, w')\}$, and $\pi \cup \{(v, w)\}$, which implies that she also has a winning strategy for the game with initial position $\pi \cup \{(v', w)\}$. Here we use the fact that the relation "duplicator has a winning strategy for the r-round bijective k-pebble game" defines an equivalence relation on the initial positions. Thus $(v', w) \in E(B)$, which contradicts $w \notin N^B(S)$. This proves the claim.

By the induction hypothesis and the claim we know that $(\star)$ $\boldsymbol{x}_\pi x_{vw}$ has a degree-k monomial PC derivation if $v \in S, w \notin T$ or $v \notin S, w \in T$. Furthermore, we can derive

$$\sum_{v \in S} \boldsymbol{x}_\pi \left(\sum_{w \in V(H)} x_{vw} - 1 \right) - \sum_{w \in T} \boldsymbol{x}_\pi \left(\sum_{v \in V(G)} x_{vw} - 1 \right) \tag{4.1}$$

by multiplying the axioms (3.1), (3.2) with $\boldsymbol{x}_\pi$ and building a linear combination. By subtracting and adding monomials from $(\star)$, this polynomial simplifies to $(|T| - |S|)\boldsymbol{x}_\pi$. After dividing by the coefficient $|T| - |S| \neq 0$, we get $\boldsymbol{x}_\pi$. We can divide by $|T| - |S|$ because the characteristic of the field $\mathbb{F}$ is 0. $\square$

The following lemma is, at least implicitly, from [10]. As the formal framework is different there, we nevertheless give the proof in the appendix.

Lemma 4.3. *Let $\mathbb{F}$ be a field of characteristic 0 and $k \geq 2$. If Duplicator has a winning strategy for the bijective k-pebble game on G, H then there is a solution α of $\mathrm{MLIN}(\mathsf{P}_{\mathrm{iso}}(G,H)^k)$ over $\mathbb{F}$ that additionally satisfies $\alpha(X_\pi) = 0 \Longrightarrow \alpha(X_\rho) = 0$ for all $\pi \subseteq \rho$.*

Theorem 4.4. *Let $\mathbb{F}$ be a field of characteristic 0. Then the following statements are equivalent for two graphs G and H.*

(1) The graphs are distinguishable by k-WL.
(2) There is a degree-k monomial-PC refutation of $\mathsf{P}_{\mathrm{iso}}(G,H)$ over $\mathbb{F}$.

Proof. Follows immediately from lemmas 2.3, 4.2 and 4.3. $\square$

We do not now the exact relation between Nullstellensatz and monomial-PC for the graph isomorphism polynomials. In particular, we do not know whether degree-k Nullstellensatz is as strong as the k-dimensional Weisfeiler-Lehman algorithm and leave this as open question. In the other direction, we remark that, at least for degree 2, full polynomial calculus is strictly stronger than degree-2 monomial-PC and hence the Colour Refinement Algorithm. However, we believe that the gap is not large. Our intuition is supported by Theorem 6.2, which implies that low-degree PC is not able to distinguish Cai-Fürer-Immerman graphs. Thus, polynomial calculus has similar limitations as the Weisfeiler-Lehman algorithm [5], Resolution [18], the Sherali-Adams hierarchy [1,10] and the Positivstellensatz [14].

5 Groups CSPs and Tseitin Polynomials

5.1 From Group CSPs to Graph Isomorphism

We start by defining a class of constraint satisfaction problems (CSPs) where the constraints are co-sets of certain groups. Throughout this section, we let Γ be a finite group. Recall that a *CSP-instance* has the form $(\mathcal{X}, D, \mathcal{C})$, where $\mathcal{X}$ is a finite set of *variables*, D is a finite set called the *domain* and $\mathcal{C}$ a finite set of *constraints* of the form $(\bar{x}, R)$, where $\bar{x} \in \mathcal{X}^k$ and $R \subseteq D^k$, for some $k \geq 1$. A *solution* to such an instance is an assignment $\alpha : X \to D$ such that $\alpha(\bar{x}) \in R$ for all constraints $(\bar{x}, R) \in \mathcal{C}$. An instance of a Γ*-CSP* has domain Γ and constraints of the form $\big(\bar{x}, \Delta\gamma\big)$, where $\Delta \leq \Gamma^k$ is a subgroup of a k-fold direct product Γ^k of Γ and $\gamma \in \Gamma^k$, so that $\Delta\gamma$ is a right coset of Δ. We specify instances as sets $\mathcal{C}$ of constraints; the variables are given implicitly. With each constraint $C = \big((x_1, \ldots, x_k), \Delta\gamma\big)$, we associate the *homogeneous* constraint $\widetilde{C} = \big((x_1, \ldots, x_k), \Delta\big)$. For an instance $\mathcal{C}$, we let $\widetilde{\mathcal{C}} = \{\widetilde{C} \mid C \in \mathcal{C}\}$.

Next, we reduce Γ-CSP to GI. Let $\mathcal{C}$ be a Γ-CSP in the variable set $\mathcal{X}$. We construct a coloured graph $G(\mathcal{C})$ as follows.

- For every variable $x \in \mathcal{X}$ we take vertices $\gamma^{(x)}$ for all $\gamma \in \Gamma$. We colour all these vertices with a fresh colour $L^{(x)}$.
- For every constraint $C = ((x_1, \ldots, x_k), \Delta\gamma) \in \mathcal{C}$ we add vertices $\beta^{(C)}$ for all $\beta \in \Delta\gamma$. We colour all these vertices with a fresh colour $L^{(C)}$. If $\beta = (\beta_1, \ldots, \beta_k)$, we add an edge $\{\beta^{(C)}, \beta_i^{(x_i)}\}$ for all $i \in [k]$. We colour this edge with colour $M^{(i)}$.

We let $\widetilde{G}(\mathcal{C})$ be the graph $G(\widetilde{\mathcal{C}})$ where for all constraints $C \in \mathcal{C}$ we identify the two colours $L^{(C)}$ and $L^{(\widetilde{C})}$.

Lemma 5.1. *A Γ-CSP instance $\mathcal{C}$ is satisfiable if and only if the graphs $G(\mathcal{C})$ and $\widetilde{G}(\mathcal{C})$ are isomorphic.*

Example 1 (The Tseitin Tautologies and the CFI-construction). For every graph H and set $T \subseteq V(H)$ we define the following $\mathbb{Z}_2$-CSP $\mathcal{TS} = \mathcal{TS}(H, T)$.

- For every edge $e \in E(H)$ we have a variable z_e.
- For every vertex $v \in V(H)$ we define a constraint C_v. Suppose that v is incident with the edges $e_1, \ldots, e_k$ (in an arbitrary order), and let $z_i := z_{e_i}$.

Let $\Delta := \{(i_1, \dots, i_k) \in \mathbb{Z}_2^k \mid \sum_{i=1}^k i_j = 0\} \leq \mathbb{Z}_2^k$. We will also use the coset $\Delta + (1, 0, \dots, 0) = \{(i_1, \dots, i_k) \in \mathbb{Z}_2^n \mid \sum_{i=1}^k i_j = 1\}$ If $v \notin T$, we let $C_v := \big(z_1, \dots, z_k, \Delta\big)$, and if $v \in T$ we let $C_v := \big(z_1, \dots, z_k, \Delta + (1, 0, \dots, 0)\big)$.

Observe that $\mathcal{TS}$ is a set of Boolean constraints, all of them linear equations over the field $\mathbb{F}_2$; they are known as the *Tseitin tautologies* associated with H and T. We think of assigning a "charge" 1 to every vertex in T and charge 0 to all remaining vertices. Now we are looking for a set $F \subseteq E(H)$ of edges such that for every vertex v, the number of edges in F incident with v is congruent to the charge of v modulo 2. A simple double counting argument shows that $\mathcal{TS}$ is unsatisfiable if $|T|$ is odd. (The sum of degrees in the graph $(V(H), F)$ is even and, by construction, equal to the sum $|T|$ of the charges, which is odd.)

It turns out that the graphs $G(\mathcal{TS})$ and $\widetilde{G}(\mathcal{TS})$ are precisely the *CFI-graphs* defined from H with all vertices in T "twisted". These graphs have been introduced by Cai, Fürer, and Immerman [5] to prove lower bounds for the Weisfeiler-Lehman algorithm and have found various other applications in finite model theory since then.

5.2 Low-Degree Reduction From Tseitin to Isomorphism

For every graph H and set $T \subseteq V(H)$, we let $\mathsf{P}_{\mathrm{Ts}}(H, T)$ be the following system of polynomial equations:

$$z_e^2 - 1 = 0 \quad \text{for all } e \in E(H), \tag{5.1}$$

$$1 + z_{e_1} z_{e_2} \cdots z_{e_k} = 0 \quad \text{for all } v \in T \text{ with incident edges } e_1, \dots, e_k, \tag{5.2}$$

$$1 - z_{e_1} z_{e_2} \cdots z_{e_k} = 0 \quad \text{for all } v \in V(H) \setminus T \text{ with incident edges } e_1, \dots, e_k. \tag{5.3}$$

Observe that for every field $\mathbb{F}$ of characteristic $\neq 2$ there is a one-to-one correspondence between solutions to the system $\mathsf{P}_{\mathrm{Ts}}(H, T)$ over $\mathbb{F}$ and solutions for the CSP-instance $\mathcal{TS}(H, T)$ (see Example 1) via the "Fourier" correspondence $1 \mapsto 0, -1 \mapsto 1$.

Lemma 5.3. *Let $\mathbb{F}$ be a field of characteristic $\neq 2$. Let $k \geq 2$ be even and H a k-regular graph, and let $T \subseteq V(H)$. Let $G := G(\mathcal{TS}(H, T))$ and $\widetilde{G} := \widetilde{G}(\mathcal{TS}(H, T))$.*

Then there is a degree-$(k, 2k)$ reduction from $\mathsf{P}_{\mathrm{Ts}}(H, T)$ to $\mathsf{P}_{\mathrm{iso}}(G, H)$.

6 Lower Bounds

We obtain our lower bounds combining the low-degree reduction of the previous section with known lower bounds for Tseitin polynomials due to Buss et al. [4] for polynomial calculus and Grigoriev [8] for the Positivstellensatz calculus.

Theorem 6.1 ([4,8]). *For every $n \in \mathbb{N}$ there is a 6-regular graph H_n of size $O(n)$ such that $\mathsf{P}_{\mathrm{Ts}}(H_n, V(H_n))$ is unsatisfiable, but:*

(1) there is no degree-n polynomial calculus refutation of $\mathsf{P}_{\mathrm{Ts}}(H_n, V(H_n))$ *over any field* $\mathbb{F}$ *of characteristic* $\neq 2$*;*
(2) there is no degree-n Positivstellensatz calculus refutation of $\mathsf{P}_{\mathrm{Ts}}(H_n, V(H_n))$ *over the reals.*

Now our main lower bound theorem reads as follows.

Theorem 6.2. *For every* $n \in \mathbb{N}$ *there are non-isomorphic graphs* G_n, $\widetilde{G}_n$ *of size* $O(n)$, *such that*

(1) there is no degree-n polynomial calculus refutation of $\mathsf{P}_{\mathrm{iso}}(G_n, \widetilde{G}_n)$ *over any field* $\mathbb{F}$ *of characteristic* $\neq 2$*;*
(2) there is no degree-n Positivstellensatz calculus refutation of $\mathsf{P}_{\mathrm{iso}}(G_n, \widetilde{G}_n)$ *over the reals.*

Proof. This follows from Lemmas 2.1 and 5.3 and Theorem 6.1. □

It follows that over finite fields, polynomial calculus has similar shortcomings than over fields of characteristic 0. However, a remarkable exception is $\mathbb{F}_2$, where we are not able to prove linear lower bounds on the degree. Here the approach to reduce from Tseitin fails, as the Tseitin Tautologies are satisfiable over $\mathbb{F}_2$. As a matter of fact, the next theorem shows that CFI-graphs can be distinguished with Nullstellensatz of degree 2 over $\mathbb{F}_2$.

Theorem 6.3. *Let* H *be a graph* $T \subseteq V(H)$ *such that* $|T|$ *is odd. Then there is a degree-2 Nullstellensatz refutation over* $\mathbb{F}_2$ *of* $\mathsf{P}_{\mathrm{iso}}(G, \widetilde{G})$, *where* $G = G(\mathcal{TS}(H,T))$ *and* $\widetilde{G} = \widetilde{G}(\mathcal{TS}(H,T))$.

Thus, to prove lower bounds for algebraic proof systems over $\mathbb{F}_2$ we need new techniques. Our final theorem, which even derives lower bound over $\mathbb{Z}$, is a first step.

Theorem 6.4. *There are non-isomorphic graphs* G, H *such that the system of linear Diophantine equations* $\mathrm{MLIN}(\mathsf{P}_{\mathrm{iso}}(G,H)^2)$ *has a solution over* $\mathbb{Z}$.

Corollary 6.5. *There are non-isomorphic graphs* G, H *such that* $\mathsf{P}_{\mathrm{iso}}(G,H)$ *has no degree-2 Nullstellensatz refutation over* $\mathbb{F}_q$ *for any prime* q.

7 Concluding Remarks

Employing results and techniques from propositional proof complexity, we prove strong lower bounds for algebraic algorithms for graph isomorphism testing, which show that these algorithm are not much stronger than known algorithms such as the Weisfeiler-Lehman algorithm.

Our results hold over all fields except—surprisingly—fields of characteristic 2. For fields of characteristic 2, and also for the ring of integers, we only have very weak lower bounds. It remains an challenging open problem to improve these.

Acknowledgments. We thank Anuj Dawar and Erkal Selman for many inspiring discussions in the initial phase of this project.

References

1. Atserias, A., Maneva, E.: Sherali-Adams relaxations and indistinguishability in counting logics. SIAM J. Comput. **42**(1), 112–137 (2013)
2. Beame, P., Impagliazzo, R., Krajicek, J., Pitassi, T., Pudlak, P.: Lower bounds on Hilbert's nullstellensatz and propositional proofs. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 794–806 (1994)
3. Buss, S.: Lower bounds on nullstellensatz proofs via designs. In: Proof Complexity and Feasible Arithmetics, pp. 59–71. American Mathematical Society (1998)
4. Buss, S., Grigoriev, D., Impagliazzo, R., Pitassi, T.: Linear gaps between degrees for the polynomial calculus modulo distinct primes. Journal of Computer and System Sciences **62**(2), 267–289 (2001)
5. Cai, J., Fürer, M., Immerman, N.: An optimal lower bound on the number of variables for graph identification. Combinatorica **12**, 389–410 (1992)
6. Clegg, M., Edmonds, J., Impagliazzo, R.: Using the Groebner basis algorithm to find proofs of unsatisfiability. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 174–183 (1996)
7. Codenotti, P., Schoenbeck, G., Snook, A.: Graph isomorphism and the Lasserre hierarchy (2014). CoRR arXiv:1107.0632v2
8. Grigoriev, D.: Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. Theoretical Computer Science **259**(1–2), 613–622 (2001)
9. Grigoriev, D., Vorobjov, N.: Complexity of null- and positivstellensatz proofs. Annals of Pure and Applied Logic **113**(1–3), 153–160 (2001)
10. Grohe, M., Otto, M.: Pebble games and linear equations. In: Cégielski, P., Durand, A. (eds.) Proceedings of the 26th International Workshop on Computer Science Logic. Leibniz International Proceedings in Informatics (LIPIcs), vol. 16, pp. 289–304 (2011)
11. Hella, L.: Logical hierarchies in PTIME. Information and Computation **129**, 1–19 (1996)
12. Lasserre, J.B.: Global optimization with polynomials and the problem of moments. SIAM Journal on Optimization **11**(3), 796–817 (2001)
13. Malkin, P.: Sherali-Adams relaxations of graph isomorphism polytopes. Discrete Optimization **12**, 73–97 (2014)
14. O'Donnell, R., Wright, J., Wu, C., Zhou, Y.: Hardness of robust graph isomorphism, Lasserre gaps, and asymmetry of random graphs. In: Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 1659–1677 (2014)
15. Parrilo, P.: Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization. Ph.D. thesis, California Institute of Technology (2000)
16. Sherali, H.D., Adams, W.P.: A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. SIAM Journal on Discrete Mathematics **3**(3), 411–430 (1990)
17. Tinhofer, G.: Graph isomorphism and theorems of Birkhoff type. Computing **36**, 285–300 (1986)
18. Torán, J.: On the resolution complexity of graph non-isomorphism. In: Järvisalo, M., Van Gelder, A. (eds.) SAT 2013. LNCS, vol. 7962, pp. 52–66. Springer, Heidelberg (2013)