

Pebble Games and Algebraic Proof Systems

Lisa-Marie Jaser  

Institut für Theoretische Informatik, Universität Ulm, Germany

Jacobo Torán   

Institut für Theoretische Informatik, Universität Ulm, Germany

Abstract

Analyzing refutations of the well known pebbling formulas $\text{Peb}(G)$ we prove some new strong connections between pebble games and algebraic proof system, showing that there is a parallelism between the reversible, black and black-white pebbling games on one side, and the three algebraic proof systems Nullstellensatz, Monomial Calculus and Polynomial Calculus on the other side. In particular we prove that for any DAG G with a single sink, if there is a Monomial Calculus refutation for $\text{Peb}(G)$ having simultaneously degree s and size t then there is a black pebbling strategy on G with space s and time $t + s$. Also if there is a black pebbling strategy for G with space s and time t it is possible to extract from it a MC refutation for $\text{Peb}(G)$ having simultaneously degree s and size ts . These results are analogous to those proven in [14] for the case of reversible pebbling and Nullstellensatz. Using them we prove degree separations between NS, MC and PC, as well as strong degree-size tradeoffs for MC.

We also notice that for any directed acyclic graph G the space needed in a pebbling strategy on G , for the three versions of the game, reversible, black and black-white, exactly matches the variable space complexity of a refutation of the corresponding pebbling formula $\text{Peb}(G)$ in each of the algebraic proof systems NS, MC and PC. Using known pebbling bounds on graphs, this connection implies separations between the corresponding variable space measures.

2012 ACM Subject Classification Theory of computation \rightarrow Proof complexity; Theory of computation \rightarrow Complexity theory and logic; Mathematics of computing \rightarrow Graph theory

Keywords and phrases Proof Complexity, Algebraic Proof Systems, Pebble Games

Digital Object Identifier 10.4230/LIPIcs.MFCS.2024.64

1 Introduction

The use of pebble games in complexity theory goes back many decades. They offer a very clean tool to analyze certain complexity measures, mainly space and time, in an isolated way on a graph, which can then be translated to specific computational models. Very good overviews of these results can be found in [26, 28, 23].

We consider several versions of the game, defined formally in the preliminaries. Intuitively, the goal of these games is to measure the minimum number of pebbles needed by a single player in order to place a pebble on the sink of a directed acyclic graph (DAG) following certain rules (this is called the pebbling price). A black pebble can only be placed on a vertex if it is a source or if all its direct predecessors already have a pebble on them, but these pebbles can be removed at any time. A white pebble (modelling non-determinism) can be placed on any vertex at any time but can only be removed if all its direct predecessors contain a pebble. In the reversible pebble game, pebbles can only be placed or removed from a vertex if all the direct predecessors of the vertex contain a pebble. These three games define a short hierarchy being reversible pebbling weaker than black pebbling and this in turn weaker than the black-white pebble game.

In proof complexity one tries to understand the resources needed for a proof of a mathematical statement in a formalized system. Pebbling games have also become one of the most useful tools for proving results in this area. The reason for this is that one can often



© Lisa-Marie Jaser and Jacobo Torán;

licensed under Creative Commons License CC-BY 4.0

49th International Symposium on Mathematical Foundations of Computer Science (MFCS 2024).

Editors: Rastislav Kráľovič and Antonín Kučera; Article No. 64; pp. 64:1–64:14

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

translate a certain measure for the pebbling game, mainly number of pebbles or pebbling time, into a suitable complexity measure for a concrete proof system. Very often the bounds for this measure in a graph translate accurately to bounds in the different proof systems for a certain kind of contradictory formulas mimicking the game, called pebbling formulas. These formulas were introduced in [6] and have been extremely useful for proving separations, upper and lower bounds as well as tradeoff results in basically all studied proof systems. See e.g. [22].

In the present paper we will concentrate on algebraic proof system. In these systems formulas are encoded as sets of polynomials over a field and the question of whether a formula is unsatisfiable is translated to the question of whether the polynomials have a common root. Powerful algebraic tools like the Gröbner Basis Algorithm can be used for this purpose. Several algebraic proof systems have been introduced in the literature (defined formally below). Well known are Nullstellensatz (NS) introduced in [3] and the more powerful Polynomial Calculus (PC) defined in [11]. The first one is usually considered as a static system in which a “one-shot” proof has to be produced, while in PC there are certain derivation rules like in a more standard proof system.

The best studied complexity measures for refutations in these systems are the degree (maximum degree of a polynomial) and size (number of monomials counted with repetitions). For studying the connections with the pebble games it is very useful to consider also space measures and the configurational refutations associated with space. We will use the variable space measure (number of variables that are simultaneously active in a refutation).

In [8] the Monomial Calculus system (MC) was identified. This system is defined by limiting the multiplication rule in PC to monomials and its power lies between NS and PC. Building on results from [2] for the Sherali-Adams proof system, the authors proved that for any pair of non-isomorphic graphs, the MC degree for the refutation of the corresponding isomorphism formulas exactly corresponds to the Weisfeiler-Leman bound for separating the graphs, a very important tool in graph theory and descriptive complexity. This equivalence (as well as the relations to pebbling shown here) motivates the study of Monomial Calculus as a natural proof system between NC and PC.

As mentioned above, connections between pebbling games and algebraic systems have been known. Already in [9] it was proved that for any directed acyclic graph (DAG) G the corresponding pebbling formula $\text{Peb}(G)$ can be refuted with constant degree in PC but in NS it requires degree $\Omega(s)$, where s is the black pebbling price of G , $\text{Black}(G)$. Using pebbling results, this automatically proves a strong degree separation between NS and PC. As a more recent example, the authors in [14] proved a very tight connection between NS and the reversible pebbling game. They showed that space and time in the game played on a DAG exactly correspond to the degree and size measures in a NS refutation of the corresponding pebbling formula. From this connection strong degree-size tradeoffs for NS follow. This result also improves degree separation from [9] since it is known that there are graphs for which the reversible pebbling price is a logarithmic factor larger than the black pebbling price.

We show in this paper that besides these results, there are further parallelisms between the reversible, black and black-white game hierarchy on one side, and the NS, MC and PC proof systems on the other side.

1.1 Our Results

In Section 3 we prove that very similar results to those given in [14] for NS and reversible pebbling are also true for the case of MC and black pebbling. More concretely we show in Theorem 13 that for any DAG G with a single sink, if there is a MC refutation for $\text{Peb}(G)$

having simultaneously degree s and size t then there is a black pebbling strategy on G with space s and time $t + s$. This is done by proving that any Horn formula has a very especial kind of MC refutation, which we call input monomial refutation since it is the same concept as an input refutation in Resolution. Horn formulas constitute an important class with applications in many areas like program verification or logic programming. It is well known that input Resolution is complete for Horn formulas.

For the other direction, we show in Theorem 8 that from a black pebbling strategy for G with space s and time t it is possible to extract a MC refutation for $\text{Peb}(G)$ having simultaneously degree s and size ts . The small loss in the time parameter compared to the results in [14] comes from the fact that size complexity is measured in slightly different ways in NS and MC. Using these results we are able to show degree separations between NS and MC as well as the first strong degree separations between MC and PC. We also use the simultaneous relation with time and space in the black pebbling game to obtain strong degree-size tradeoffs for MC in the same spirit as those in [14]. The results also show that strong degree lower bounds for MC refutations do not imply exponential size lower bounds as it happens in the PC proof system [19].

The degrees of the refutation for pebbling formulas in NS and MS correspond exactly to the space in reversible and black games respectively. It would be very nice if the same could be said about PC degree and space in the black-white game. Unfortunately this is not the case since as mentioned above, it was proven in [9] that for any DAG the corresponding pebbling formula can be refuted within constant PC degree. We notice however that if instead of the degree we consider the complexity measure of variable space, then the connection still holds. We notice that for any single sink DAG G the variable space complexity of refuting $\text{Peb}(G)$ in each of the algebraic proof systems NS, MC and PC is exactly the space needed in a strategy for pebbling G in each of the three versions Reversible, Black and Black-White of the pebble game. These results allow us to apply known separations between the pebbling space needed in the different versions of the game, in order to obtain separations in the variable space measure between the different proof systems.

2 Preliminaries

2.1 Pebble Games

Black pebbling was first mentioned implicitly in [24], while black-white pebbling was introduced in [12]. Note, that there exist several variants of the (black-white) pebble game in the literature. For differences between these variants, we refer to [23]. For the following definitions, let $G = (V, E)$ be a DAG with a unique sink vertex z .

► **Definition 1** (Black and black-white pebble games). *The black-white pebble game on G is the following one-player game: At any time i of the game, there is a pebble configuration $\mathbb{P}_i := (B_i, W_i)$, where $B_i \cap W_i = \emptyset$ and $B_i \subseteq V$ is the set of black pebbles and $W_i \subseteq V$ is the set of white pebbles, respectively. A pebble configuration $\mathbb{P}_{i-1} = (B_{i-1}, W_{i-1})$ can be changed to $\mathbb{P}_i = (B_i, W_i)$ by applying exactly one of the following rules:*

Black pebble placement on v : *If all direct predecessors of an empty vertex v have pebbles on them, a black pebble may be placed on v . More formally, letting $B_i = B_{i-1} \cup \{v\}$ and $W_i = W_{i-1}$ is allowed if $v \notin B_{i-1} \cup W_{i-1}$ and $\text{pred}_G(v) \subseteq B_{i-1} \cup W_{i-1}$. In particular, a black pebble can always be placed on an empty source vertex s , since $\text{pred}_G(s) = \emptyset$.*

Black pebble removal from v : *A black pebble may be removed from any vertex at any time. Formally, if $v \in B_{i-1}$, then we can set $B_i = B_{i-1} \setminus \{v\}$ and $W_i = W_{i-1}$.*

White pebble placement on v : A white pebble may be placed on any empty vertex at any time. Formally, if $v \notin B_{i-1} \cup W_{i-1}$, then we can set $B_i = B_{i-1}$ and $W_i = W_{i-1} \cup \{v\}$.

White pebble removal from v : If all direct predecessors of a white-pebbled vertex v have pebbles on them, the white pebble on v may be removed. Formally, letting $B_i = B_{i-1}$ and $W_i = W_{i-1} \setminus \{v\}$ is allowed if $v \in W_{i-1}$ and $\text{pred}_G(v) \subseteq B_{i-1} \cup W_{i-1}$. In particular, a white pebble can always be removed from a source vertex.

A black-white pebbling of G is a sequence of pebble configurations $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_t)$ such that $\mathbb{P}_0 = \mathbb{P}_t = (\emptyset, \emptyset)$, for some $i \leq t$, $z \in B_i \cup W_i$, and for all $i \in [t]$ it holds that \mathbb{P}_i can be obtained from \mathbb{P}_{i-1} by applying exactly one of the above-stated rules.

A black pebbling is a pebbling where $W_i = \emptyset$ for all $i \in [t]$. Observe that w.l.o.g. we can always assume that $B_{t-1} = \{z\}$. For convenience we will also use the dual notion of white pebbling game. A white (only) pebbling is a pebbling where $B_i = \emptyset$ for all $i \in [t]$. Notice that $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_t)$ is a black pebbling of G if and only if $\mathcal{P}' = (\mathbb{P}'_t, \dots, \mathbb{P}'_0)$ is a white pebbling of G , where each configuration \mathbb{P}'_i contains the same set of pebbled vertices as in \mathbb{P}_i , but with white pebbles instead of black pebbles. In a white pebbling we can always suppose that $W_1 = \{z\}$.

► **Definition 2** (Pebbling time, space, and price). The time of a pebbling $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_t)$ is $\text{time}(\mathcal{P}) := t$ and the space of it is $\text{space}(\mathcal{P}) := \max_{i \in [t]} |B_i \cup W_i|$. The black-white pebbling price (also known as the pebbling measure or pebbling number) of G , which we will denote by $\text{BW}(G)$, is the minimum space of any black-white pebbling of G . The black pebbling price of G , denoted by $\text{Black}(G)$, is the minimum space of any black pebbling of G . By the observation above, the white pebbling price $\text{White}(G)$ coincides with $\text{Black}(G)$.

Finally, we mention the reversible pebble game introduced in [7]. In the reversible pebble game, the moves performed in reverse order should also constitute a legal black pebbling, which means that the rules for pebble placements and removals have to become symmetric. This implies that reversible pebbling is a restricted version of black pebbling. The notions of reversible pebbling time, space, and price are defined as in the other pebbling variants.

2.2 Formulas and Polynomials

We will only consider propositional formulas in conjunctive normal form (CNF). Such a formula is a conjunction of clauses and a clause is a disjunction of literals. A literal is a variable or its negation. For a formula F , $\text{Var}(F)$ denotes the set of its variables.

A Horn formula is a special type of CNF formula in which each clause has at most one positive literal. For a more detailed treatment of formulas as well as the well known Resolution proof system we refer the interested reader to some of the introductory texts in the area like [29]. We will basically only deal with pebbling formulas. These provide the connection between pebbling games and proof complexity.

► **Definition 3** (Pebbling formulas). Let $G = (V, E)$ be a DAG with a set of sources $S \subseteq V$ and a unique sink z . We identify every vertex $v \in V$ with a Boolean variable x_v . For a vertex $v \in V$ we denote by $\text{pred}(v)$ the set of its direct predecessors. In particular, for a source vertex v , $\text{pred}(v) = \emptyset$. The pebbling contradiction over G , denoted $\text{Peb}(G)$, is the conjunction of the following clauses:

- for all vertices v , the clause $\bigvee_{u \in \text{pred}(v)} \bar{x}_u \vee x_v$, (pebbling axioms)
- for the unique sink z , the unit clause \bar{x}_z . (sink axiom)

Observe that every clause in a pebbling formulas has at most one positive literal. These formulas are therefore Horn formulas.

A way to prove that a CNF formula is unsatisfiable is by translating it into a set of polynomials over a field \mathbb{F} and then show that these polynomials do not have any common $\{0, 1\}$ -valued root. A clause $C = \bigvee_{x \in P} x \vee \bigvee_{y \in N} \bar{y}$ can be encoded as the polynomial $p(C) = \prod_{x \in P} (1 - x) \prod_{y \in N} y$. A set of clauses C_1, \dots, C_m is translated as set of polynomials $p(C_1), \dots, p(C_m)$. Adding the polynomials $x_i^2 - x_i$ (as axioms) for each variable x_i , there is no common $\{0, 1\}$ -valued root for all these polynomials if and only if the original set of clauses is unsatisfiable. The intuition here is to identify false with 1 and true with 0. A monomial is falsified by a Boolean assignment if all its variables get value 1, while it is satisfied if one of its variables gets value 0. In this context we will consider a monomial m as a set of variables and a polynomial p as a linear combination of monomials. A monomial with its coefficient in \mathbb{F} is called a monomial term.

When encoding the pebbling formulas as polynomials, for a set $U \subseteq V$, we denote by m_U the monomial $\prod_{u \in U} x_u$. For $U = \emptyset$, $m_U = 1$. For every vertex $v \in V$ the axiom $\bigvee_{u \in \text{pred}(v)} \bar{x}_u \vee x_v$ becomes the polynomial $A_v := m_{\text{pred}(v)}(1 - x_v)$, and the sink axiom \bar{x}_z is transformed into the polynomial $A_{\text{sink}} := x_z$. Observe that every polynomial in the encoding of a pebbling formula has one or two monomials.

To avoid confusion we will denote the polynomial encoding of a CNF formula F by P_F .

2.3 Algebraic Proof Systems

Several proof systems that work with polynomials have been defined in the literature. The simplest one is *Nullstellensatz*, NS.

► **Definition 4.** A *Nullstellensatz refutation* of the set of polynomials p_1, \dots, p_m in $\mathbb{F}[x_1, \dots, x_n]$ consists of a set of polynomials $g_1, \dots, g_m, h_1, \dots, h_n$ such that

$$\sum_{j=1, \dots, m} p_j g_j + \sum_{i=1, \dots, n} h_i (x_i^2 - x_i) = 1.$$

As a consequence of Hilbert's Nullstellensatz, the NS proof systems is sound and complete for the set of encodings of unsatisfiable CNF formulas.

A stronger more dynamic algebraic refutational calculus also dealing with polynomials is the Polynomial Calculus (PC). As in the case of Nullstellensatz, PC is intended to prove the unsolvability of a set of polynomial equations.

► **Definition 5.** The PC proof system uses the following rules:

1. Linear combination

$$\frac{p \quad q}{\alpha p + \beta q} \quad \alpha, \beta \in \mathbb{F}.$$

2. Multiplication

$$\frac{p}{x_i p} \quad i \in [n].$$

A refutation in PC of an initial unsolvable set of polynomials \mathcal{P} is a sequence of polynomials $\{q_1, \dots, q_m\}$ such that each q_i is either a polynomial in \mathcal{P} , a Boolean axiom $x_i^2 - x_i$ or it is obtained by previous polynomials in the sequence applying one of the rules of the calculus.

A less known algebraic proof system between NS and PC is Monomial Calculus, MC. This system was introduced in [8] identifying exactly the complexity of refuting graph isomorphism formulas. This proof system is defined like PC but the multiplication rule is only allowed to be applied to a monomial, or to a monomial times an axiom.

► **Definition 6.** *The MC proof system uses the following rules:*

1. Linear combination

$$\frac{p \quad q}{\alpha p + \beta q} \quad \alpha, \beta \in \mathbb{F}.$$

2. Multiplication

$$\frac{p}{x_i p} \quad i \in [n], \quad p \text{ is a monomial or the product of a monomial and an axiom.}$$

As is the case of PC, a refutation in MC of an initial unsolvable set of polynomials \mathcal{P} is a sequence of polynomials $\{q_1, \dots, q_m\}$ where each one of them is either in \mathcal{P} , an axiom or is obtained by applying one of the rules of the calculus.

As pointed out in [8], an equivalent definition of the Nullstellensatz system, but a dynamic one, would be to restrict the multiplication rule in the above definition even more, and only allow to apply it to polynomials that are a monomial multiplied by an axiom. In this way, the difference in the definition of the three systems NS, MC and PC is just a variation on how the multiplication rule can be applied. This alternative view of the definition also allows to consider configurational proofs in the NS system. In order to analyze and compare refutations we will consider several complexity measures on them.

► **Definition 7 (Complexity measures).** *Let \mathcal{C} be one of the mentioned systems $\mathcal{C} \in \{\text{NS}, \text{MC}, \text{PC}\}$. Let $\pi = \{q_1, \dots, q_m\}$ be a \mathcal{C} refutation. The degree of a polynomial q_i , $\deg(q_i)$ is the maximum degree of its monomials and the degree of π , $\deg_{\mathcal{C}}(\pi) = \max_{i=1, \dots, m}(\deg(q_i))$. The size of π , denoted by $\text{Size}_{\mathcal{C}}(\pi)$ is the total number of monomials in π (counted with repetitions), when all polynomials p_i are fully expanded as linear combinations of monomials¹.*

For the space measures we need to define configurational proofs. Such a proof π in the system \mathcal{C} is a sequence of configurations $\pi = C_0, \dots, C_t$ in which each C_i is a set of polynomials with $C_0 = \emptyset$ and $C_t = 1$. Each configuration C_i represents a set of polynomials that are kept simultaneously in memory at time i in the refutation, and for each $i, 0 < i \leq t$, C_i is either

- $C_{i-1} \cup \{p\}$ for some axiom p (axiom download),
- $C_{i-1} \setminus \{p\}$ (erasure) or
- $C_{i-1} \cup \{p\}$ for some p inferred by the rules of \mathcal{C} by some rule of the system (inference).

The variable space of the proof π , $\text{VSpace}_{\mathcal{C}}(\pi)$ is defined as the maximum number of different variables appearing in any configuration of the proof.

For any of the defined complexity measures Comp and proof systems \mathcal{C} , and for every unsatisfiable set of polynomials P_F we denote by $\text{Comp}_{\mathcal{C}}(P_F \vdash)$ the minimum over all \mathcal{C} refutations of P_F of $\text{Comp}_{\mathcal{C}}(\pi)$.

It is often convenient to consider a multilinear setting in which the multiplications in the mentioned algebraic systems are implicitly multilinearized. Clearly the degree and size measures can only decrease in this setting.

¹ Usually the size in the NS proof system is defined in a different way, for simplicity we keep this unifying definition although in some of the referenced results the size of NS refutations corresponds to the size definition given in the reference.

3 Monomial Calculus and pebbling formulas

In [14] it was shown that for any DAG G with a single sink, the reversible pebbling space and time of G , exactly coincides with the degree and the size of a NS refutation of Peb_G . We show that a very similar relation holds for the case of black pebbling and Monomial Calculus.

► **Theorem 8.** *Let G be a directed acyclic graph with a single sink z . If there is a black pebbling strategy of G with time t and space s then there is a MC refutation of Peb_G with degree s and size ts . The variable space of this refutation coincides with its degree.*

Proof. It is convenient to consider here the equivalent notion of white pebbling. Let $\mathcal{P} = (\mathbb{P}_0, \dots, \mathbb{P}_t)$ be a white pebbling strategy for G with $\mathbb{P}_1 = \{z\}$ and $\mathbb{P}_t = \emptyset$ using s pebbles. We show that for each pebbling configuration \mathbb{P}_i , $i \in [t]$, $\mathbb{P}_i = \{v_{i_1}, \dots, v_{i_{k_i}}\}$ the monomial $m_i = \prod_{v \in \mathbb{P}_i} x_v$ can be derived from Peb_G and m_{i-1} in degree s and size 1 if \mathbb{P}_i adds a pebble, or size $2s - 1$ if \mathbb{P}_i removes a pebble. This proves the result since in the t steps of the pebbling strategy half of the steps add a pebble and the other half of the steps remove a pebble (each added pebble has to be removed). The total number of steps is therefore $\frac{t}{2} + \frac{t}{2}(2s - 1) = ts$.

Pebble placement. If the configuration at pebbling step $i + 1$ is reached after placing a white pebble on vertex v and $\mathbb{P}_i = \{u_{i_1}, \dots, u_{i_{k_i}}\}$ with $k_i \leq s - 1$ then $\mathbb{P}_{i+1} = \{v, u_{i_1}, \dots, u_{i_{k_i}}\}$. Multiplying the monomial $m_i = \prod_{u \in \mathbb{P}_i} x_u$ by the variable x_v we obtain m_{i+1} . We have just added one more monomial of degree at most s to the proof.

Pebble removal. If the configuration at pebbling step $i + 1$ is reached after removing a white pebble from vertex v and $\mathbb{P}_i = \{v, u_{i_1}, \dots, u_{i_{k_i}}\}$ with $k_i \leq s - 1$ then all predecessors of v are in the set $\{u_{i_1}, \dots, u_{i_{k_i}}\}$. For the derivation of m_{i+1} we can multiply the axiom $(1 - x_v) \prod_{u \in \text{pred}(v)} x_u$ by the variables in $\text{Var}(m_i) \setminus (\bigcup_{u \in \text{pred}(v)} x_u \cup \{x_v\})$, and add this polynomial to m_i obtaining m_{i+1} . Since there are at most $s - 1$ variables in $\text{Var}(m_i) \setminus (\bigcup_{u \in \text{pred}(v)} x_u \cup \{x_v\})$, the number of intermediate monomials added to the proof (counting also monomial m_{i+1}) is at most $2(s - 1) + 1 = 2s - 1$.

Observe that in all the steps in the refutation, at most two different monomials are active and the number of different variables in these monomials coincides with the largest of their degrees. This shows that the variable space of the MC refutation is also bounded by s . ◀

► **Observation 9.** *The size bound ts in the above proof comes from the way the MC rules are defined. As is the case of PC, in the multiplication rule only one variable at a time is multiplied, even when multiplying the axiom polynomials. When an axiom is multiplied by a monomial with several variables, all the intermediate polynomials contribute to the size of the MC refutation. This is different from the usual way to measure the size in the NS case, where intermediate monomials are not counted. If we would define the MC rules as those in NS, that is, if a whole monomial could be multiplied by an axiom in one step, the size of the MC proof would avoid the s factor in the monomial size and obtain size $2t$ instead.*

In order to prove a result in the other direction we consider a very restricted kind of refutation in MC, similar to what is known as an input refutation in Resolution. In this kind of refutation in every Resolution step one of the parent clauses must be an axiom. Input Resolution is not complete, but it is complete for Horn formulas. We will show that the same is true for MC input refutations.

► **Definition 10.** *A MC refutation π of a contradictory set of polynomials F is called an input refutation if there is a sequence of monomials M_0, \dots, M_t such that M_0 is the product of a monomial and an axiom, $M_t = 1$ and for each i M_i is obtained by multiplying M_{i-1}*

times a variable, or by the linear combination rule from M_{i-1} and a monomial multiplied by an axiom polynomial. We will call the sequence of monomials M_0, \dots, M_t the backbone of the proof.

► **Lemma 11.** *Let F be an unsatisfiable Horn formula and let P_F be the encoding of F as a set of polynomials. Let π be any MC refutation of P_F . There is an input MC refutation π' of P_F with at most the same size and degree as π .*

Proof. Let d and t be the degree and size of π . We can suppose that π is multilinear. We prove the result by induction on k , the number of times the multiplication rule is applied to a monomial derived in π . In the base case $k = 0$, π is just a NS refutation of P_F . This means that there is a linear combination of a set of polynomials S that adds up to 1. Each of these polynomials has the form of a polynomial axiom multiplied by a monomial and since F is a Horn formula, each polynomial in S has either one or two monomials. We will represent such a polynomial $p = \alpha_m m + \alpha_{m'} m'$ by the pair of monomials (m, m') . In all these polynomials the monomial terms have some coefficients α_m and $\alpha_{m'}$. Clauses without positive literals are encoded as single monomials. Some polynomial in S has a single monomial otherwise the whole set S would have a common root by setting all variables to 1. Moreover, there has to be a sequence of polynomials p_1, \dots, p_ℓ represented by the monomials $(\emptyset, m_1), (m_1, m_2), (m_2, m_3) \dots, (m_{\ell-1}, m)$ ². This is because the linear combination adds up to 1 and for this to happen, there has to be a polynomial (\emptyset, m_1) in the linear combination since otherwise all monomials would have variables. Also the monomial m_1 in (\emptyset, m_1) has to be cancelled and there has to be some other polynomial of the form (m_1, m_2) and so on. It must also hold that some polynomial in the sequence must have the form $(m_{\ell-1}, m)$ that can cancel with one of the polynomials with a single monomial m in S . We suppose that p_1, \dots, p_ℓ is a minimal sequence with these properties. Now we can define the input monomial refutation π starting at $M_0 = m$ and applying then ℓ linear combinations with axioms multiplied by monomials and deriving all the monomials m_ℓ, \dots, m_1 until 1 is derived. Observe that the monomials M_0, \dots, M_t are exactly those appearing in p_1, \dots, p_ℓ . By the minimality of the sequence we also know that the monomials in the backbone are all different.

All the monomials in π' belong also to π , therefore the degree of the new refutation is not larger than that in π . In fact all the polynomials in p_1, \dots, p_ℓ are already in π . Besides these polynomials π' contains also the ℓ new monomials in the backbone. Since the p_1, \dots, p_ℓ and m belong to π and in each linear combination of two polynomials at most one monomial vanishes, there are at least ℓ intermediate polynomials in π until 1 is reached. This means that the size of π' is bounded by t .

For the case $k > 0$ let m' be the first monomial in the proof that is the result of a multiplication from a derived monomial m and a variable x , $m' = xm$ in π . The same argument as above shows that there is a sequence of polynomials $p_1, \dots, p_\ell, \hat{m}$ in π from which we can extract an input monomial refutation that starts at $M_0 = \hat{m}$ and derives at some point $M_i = m$. In the next step the multiplication rule is applied to obtain $M_{i+1} = m'$. Observe that the set of polynomials $m' \cup P_F$ still has the Horn property and that there is sub-proof of π that refutes this set to the monomial 1 applying the multiplication rule at most $k - 1$ times. By induction hypothesis we know that there is a sequence of polynomials p'_1, \dots, p'_ℓ in π represented by the monomials $(\emptyset, m'_1), (m'_1, m'_2), \dots, (m'_\ell, m')$ from which an input refutation of $P_F \cup m'$ can be extracted. We can put together both input MC refutations $M_0 \dots M_i$ and $M_{i+1}, \dots, 1$. Again we can assume that all the monomials in the backbone

² Since we are representing monomials by their set of variables, the monomial 1 is represented by \emptyset

are different since if $M_i = M_j$ for $i < j$, we could shorten π' by connecting M_i with M_{j+1} . By the same argument as in the base case the size and degree of the input MC refutation cannot be larger than that of π . ◀

Since pebbling formulas are Horn formulas we immediately obtain:

► **Corollary 12.** *Let G be a directed acyclic graph with a single sink vertex z and let π be a MC refutation of $\text{Peb}(G)$. There is an input MC refutation π' of $\text{Peb}(G)$ with at most the same size and degree as π .*

We consider next a result in the other direction.

► **Theorem 13.** *Let G be a directed acyclic graph with a single sink. Let π be a MC refutation of $\text{Peb}(G)$ with degree s and size t . There is a black pebbling strategy with s pebbles and time $t + s$.*

Proof. Because of Corollary 12 we can suppose that there exists an input MC refutation with monomials M_0, \dots, M_t starting with $M_1 = mx_{\text{sink}}$ for some monomial m and with $M_t = 1$. We describe a strategy for a white pebbling of G following π . At each step i only the vertices corresponding to variables in M_i have a pebble on them. In a multiplication step a new pebble is added, which is always possible in a white pebbling strategy. We only have to show that in case variables disappear when going from M_i to M_{i+1} , this is a correct pebbling move. But in this case, the step from i to $i + 1$ is a linear combination of M_i with the axiom for some vertex v , $m_{\text{pred}(v)}(1 - x_v)$ multiplied by some monomial m . The only variable that can disappear in M_{i+1} is x_v and in this case $M_i = m_{\text{pred}(v)}x_v$. Therefore all the vertices in $\text{pred}(v)$ have pebbles on them and the pebble in x_v can be removed. At the end of the refutation, when the 1 monomial is reached there are no pebbles left on G . The number of pebbles present at any moment is the number of variables in any of the monomials and this is the degree of π . The number of pebbling steps needed is at most d steps to place a pebble in each variable of $M_1 = mx_{\text{sink}}$ and then t more pebbling steps. ◀

► **Observation 14.** *For the case of Polynomial Calculus it is known that strong degree lower bounds imply size lower bounds. If a set of unsatisfiable polynomials P_F with n variables and constant degree requires PC refutations of degree s , then any PC refutation of P_F requires size at least $2^{\Omega(\frac{d^2}{n})}$ [19]. The previous results show that this does not hold for Monomial Calculus. This follows from the fact that there are graph families $\{G_n\}_{n=0}^{\infty}$ with n vertices and constant in-degree that require black pebbling space $\Omega(\frac{n}{\log n})$ [25]. Theorem 13 implies that the pebbling formulas for this graph family needs degree $\Omega(\frac{n}{\log n})$. On the other hand, for every single-sink DAG with n vertices there is a trivial black pebbling strategy using space n and pebbling time $2n$. By Theorem 8 this implies that the pebbling formulas corresponding to the graphs in $\{G_n\}_{n=0}^{\infty}$ have MC refutations of quadratic size in n . This is a family of formulas with MC refutation degree $\Omega(\frac{n}{\log n})$ but having quadratic size refutations, a very different situation from the PC case.*

3.1 Degree separations

The given relationships between MC and the black pebbling game allow for the immediate translation of pebbling results to Monomial Calculus. We start with some degree separations between MC and PC. The original motivation for introducing MC was the close connection between the degree complexity of the refutation of the graph isomorphism formulas in this proof system, and the Weisfeiler-Leman hierarchy [8]. Formulas corresponding to non-isomorphic graphs pairs that can only be distinguished using a large level of the WL algorithm,

require a MC refutation with large degree. It was proven later in [1, 15], that the degree of a PC refutation of the isomorphism formulas cannot be much smaller than in the MC case, in fact the degrees of a MC and a PC refutation can only be a constant factor apart. We improve this separation and obtain an almost optimal degree separations by considering the pebbling formulas. In [9] it was shown that pebbling formulas have constant PC degree and that for any directed acyclic graph G with black pebbling price $B(G)$, the formula $\text{Peb}(G)$ requires NS refutations with degree $\Omega(B(G))$. Since it is known that there are graph families $\{G_n\}_{n=0}^\infty$ with $\Theta(n)$ vertices and $B(G_n) = \Omega(\frac{n}{\log n})$ [25], this implies a degree separation of $\Omega(\frac{n}{\log n})$ between PC and NS. From Theorem 13 follows that this is in fact a degree separation between MC and PC.

► **Theorem 15.** *There is an unsatisfiable family of formulas $\{F_n\}_{n=0}^\infty$ with $\Theta(n)$ variables each, that have PC refutations of constant degree but require MC refutations of degree $\Omega(\frac{n}{\log n})$.*

For the case of NS, from Theorem 8 and the equivalence between reversible pebbling price and NS degree from [13], [14], follows that a separation between reversible and black pebbling price for a graph family implies a degree separation between NS and MC for the corresponding pebbling formulas. For example it is known that a directed path graphs with n vertices can be black pebbled with 2 pebbles but requires reversible pebbling number $\lceil \log n \rceil$ [7]. Translated to pebbling formulas this means:

► **Theorem 16.** *There is a family of unsatisfiable formulas $\{F_n\}_{n=0}^\infty$ with $\Theta(n)$ variables each, that have MC refutations of degree 2 but require NS refutations of degree $\lceil \log n \rceil$.*

There are other graph families for which a separation between the black and reversible pebbling prices by a logarithmic factor in the number of vertices is known, [10],[30]. The separations in pebbling for these graphs is translated into the next result.

► **Theorem 17.** *For any function $s(n) = O(n^{1/2-\epsilon})$ for constant $0 < \epsilon < \frac{1}{2}$ there is a family of unsatisfiable formulas $\{F_n\}_{n=0}^\infty$ with $\Theta(n)$ variables each, that have MC refutations of degree $O(s(n))$ but require NS refutations of degree $\Omega(s(n) \log n)$.*

The question of whether the separation between reversible and black pebbling space can be larger than a logarithmic factor in the number of nodes is open. The best known degree separation between NS and MC is slightly better. This was obtained in [16] with very different methods. Using a classic result from descriptive complexity [18], the authors show that for every constant $c \geq 1$ there are families of formulas F_n with $O(n)$ variables that have a degree 3 MC refutation but require NS degree at least $\log^c(n)$. It is also open whether this degree separation between NS and MC is optimal.

3.2 Size-degree tradeoffs for MC

The close connections between black pebbling space and monomial calculus expressed in Theorems 8,13 make it possible to translate space-time tradeoffs for pebbling into degree-size tradeoffs for MC. There is a slight loss of the time parameter that comes from the extra space factor in the the MC refutation from Theorem 8. We present two such results as examples. The first one is an extreme tradeoff result that shows how decreasing the degree by one can make the size increase exponentially.

► **Theorem 18** ([28]). *There is a family of directed graphs $\{G_n\}_{n=0}^\infty$ having $\Theta(n^2)$ vertices each and with $\text{Black}(G_n) = \Theta(n)$ for which any black pebbling strategy with $\text{Black}(G_n)$ pebbles requires at least $2^{\Omega(n \log n)}$ steps while there is a pebbling strategy with $\text{Black}(G_n) + 1$ pebbles and $O(n^2)$ steps.*

► **Corollary 19.** *There is a family of unsatisfiable formulas $\{F_n\}_{n=0}^{\infty}$ with F_n having $O(n^2)$ variables and $d_n \in O(n)$ such that F_n has a MC refutation of degree d_n but any MC refutation with this degree requires size $2^{\Omega(n \log n)}$. On the other side there is a MC refutation of F_n with degree $d_n + 1$ and size $O(n^3)$.*

As a second example we present a robust time-space result from [23].

► **Theorem 20.** *There is a family of directed graphs $\{G_n\}_{n=0}^{\infty}$ having $\Theta(n)$ vertices each and with $\text{Black}(G_n) = O(\log^2 n)$, with a black pebbling strategy in space $O(n/\log n)$ and time $O(n)$. There is also a constant $c > 0$ for which any pebbling strategy using less than $cn/\log n$ pebbles requires at least $n^{\Omega(\log \log n)}$ steps.*

► **Corollary 21.** *There is a family of unsatisfiable formulas $\{F_n\}_{n=0}^{\infty}$ with F_n having $O(n)$ variables, and a constant $c > 0$ such that F_n has a MC refutation of degree $O(n/\log n)$ and size $O(n^2/\log n)$ but for which any MC refutation with degree smaller than $cn/\log n$ requires size at least $n^{\Omega(\log \log n)}$.*

4 Pebble Games and Variable Space

The equality between degree and pebbling price for the cases of Monomial Calculus and black pebbling from the previous section, as well as for Nullstellensatz and reversible pebbling from [14] cannot be extended to the case of Polynomial Calculus and black-white pebbling price since as already mentioned, it was proven in [9] that for any DAG G , $\deg_{\text{PC}}(\text{Peb}(G)) = O(1)$. We show in this section that the correspondence between the three pebbling variations and the proof systems holds if we consider the variables space measure instead.

It can be seen in the proof of Theorem 8, that not only the minimum degree of a monomial calculus refutation of $\text{Peb}(G)$, but also the minimum variable space is bounded by the black pebbling price of G . The same can be observed in the proof of Theorem 3.1 in [14] for the case of Nullstellensatz and reversible pebbling. Considering the trivial fact that variable space measure is always greater or equal that the degree needed for the refutation of a formula in all three proof systems NS, MC and PC, and considering Theorems 13 as well as Theorem 3.4 in [14] this implies:

► **Observation 22.** *For every DAG G with a single sink, $\text{VSpace}_{\text{NS}}(\text{Peb}(G) \vdash) = \text{Rev}(G)$ and $\text{VSpace}_{\text{MC}}(\text{Peb}(G) \vdash) = \text{Black}(G)$.*

For the case of black-white pebbling it is known that for the Resolution proof system, the variable space needed in a refutation of $\text{Peb}(G)$ equals $\text{BW}(G)$. The inclusion from left to right is from [5] while the other inclusion appeared in [17]. This results can be extended to other proof systems using the following result:

► **Lemma 23** ([4], [27]). *Let S be a proof system that can simulate Resolution step by step without including new variables. For every unsatisfiable formula F , $\text{VSpace}_S(F \vdash) = \text{VSpace}_{\text{Res}}(F \vdash)$.*

This implies:

► **Observation 24.** *For every DAG G with a single sink, $\text{VSpace}_{\text{PC}}(\text{Peb}(G) \vdash) = \text{BW}(G)$.*

Which together with Observation 22 shows the equivalence between variable space in the proof systems and the pebbling price in the three variations of the game.

4.1 Variable Space Separations

These observations allow us to use pebbling results to obtain separation in the variable space complexity in the algebraic proof systems. The reason why these results do not contradict Lemma 23, is that MC (or NS) cannot simulate Resolution step by step since the intermediate polynomials are not necessarily monomials.

For the variable space separations between NS and MC on pebbling formulas, the same degree separations given in Subsection 3.1 hold, since as we have seen, for this kind of formulas the variable space and the degree coincide in both proof systems. For the case of MC versus PC, it is known that for any DAG G , the separation between the black and the black-white pebbling prices can be at most quadratic [21]. This limits the variable space gap between MC and PC that can be obtained using pebbling formulas. In [31] a family of graphs is given that shows an asymptotic separation between the black-white and black pebbling prices. Translating this to our context we obtain:

► **Theorem 25.** *There is a family of unsatisfiable formulas $\{F_n\}_{n=0}^\infty$ with polynomially many variables (in n) such that $\text{VSpace}_{\text{PC}}(F_n \vdash) = O(n)$ and $\text{VSpace}_{\text{MC}}(F_n \vdash) = \Omega(\frac{n \log n}{\log \log n})$.*

An optimal quadratic separation between the black-white and black pebbling price was given in [20] but for a family of graphs having exponentially many vertices respect to their pebbling price. This implies:

► **Theorem 26.** *There is a family of unsatisfiable formulas $\{F_n\}_{n=0}^\infty$ with $\exp(\Theta(n \log n))$ many variables such that $\text{VSpace}_{\text{PC}}(F_n \vdash) = O(n)$ and $\text{VSpace}_{\text{MC}}(F_n \vdash) = \Omega(n^2)$.*

5 Conclusions and Open Questions

We have proven a strong connection between the black pebble game and the Monomial Calculus proof system by showing that the degree and size bounds required simultaneously in a MC refutation of the pebbling formula for a DAG G closely correspond to the number of pebbles and the time in a pebbling strategy for G . This improves the known relations between the complexities of pebble games and algebraic proof systems and implies strong degree-size tradeoffs for the MC system as well as degree separations between NS, MC and PC.

We have also shown that the variable space measure for the refutation of pebbling formulas in the three systems PC, MC and NS exactly corresponds to the number of pebbles in the black, black-white and reversible games. From this equivalence we obtain variable space separations between the proof systems.

It is open whether these separations are optimal or can be improved using other techniques. Finding out what is the optimal degree separation between the NS and MC proof systems is another interesting open question.

References

- 1 Albert Atserias and Joanna Fijalkow. Definable ellipsoid method, sums-of-squares proofs, and the graph isomorphism problem. *SIAM J. Comput.*, 52(5):1193–1229, 2023. doi:10.1137/20m1338435.
- 2 Albert Atserias and Elitza N. Maneva. Sherali–Adams relaxations and indistinguishability in counting logics. *SIAM Journal on Computing*, 42(1):112–137, January 2013. Preliminary version in *ITCS '12*. doi:10.1137/120867834.

- 3 Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS '94)*, pages 794–806, 1994. doi:10.1109/SFCS.1994.365714.
- 4 Chris Beck, Jakob Nordström, and Bangsheng Tang. Some trade-off results for polynomial calculus. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 813–822, May 2013. doi:10.1145/2488608.2488711.
- 5 Eli Ben-Sasson. Size space tradeoffs for resolution. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC '02)*, pages 457–464, May 2002. doi:10.1145/509907.509975.
- 6 Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – Resolution made simple. *Journal of the ACM*, 48(2):149–169, March 2001. Preliminary version in *STOC '99*. doi:10.1145/375827.375835.
- 7 Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM Journal on Computing*, 18(4):766–776, 1989. doi:10.1137/0218053.
- 8 Christoph Berkholz and Martin Grohe. Limitations of algebraic approaches to graph isomorphism testing. In *ICALP 2015*, volume 9134 of *Lecture Notes in Computer Science*, pages 155–166. Springer, 2015. doi:10.1007/978-3-662-47672-7_13.
- 9 Joshua Buresh-Oppenheim, Matthew Clegg, Russell Impagliazzo, and Toniann Pitassi. Homogenization and the polynomial calculus. *Computational Complexity*, 11(3-4):91–108, 2002. Preliminary version in *ICALP '00*. doi:10.1007/s00037-002-0171-6.
- 10 Siu Man Chan, Massimo Lauria, Jakob Nordström, and Marc Vinyals. Hardness of approximation in PSPACE and separation results for pebble games (Extended abstract). In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS '15)*, pages 466–485, 2015. doi:10.1109/FOCS.2015.36.
- 11 Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 174–183, May 1996. doi:10.1145/237814.237860.
- 12 Stephen A. Cook and Ravi Sethi. Storage requirements for deterministic polynomial time recognizable languages. *Journal of Computer and System Sciences*, 13(1):25–37, 1976. Preliminary version in *STOC '74*. doi:10.1016/S0022-0000(76)80048-7.
- 13 Susanna F. de Rezende, Or Meir, Jakob Nordström, Toniann Pitassi, Robert Robere, and Marc Vinyals. Lifting with simple gadgets and applications to circuit and proof complexity. *CoRR*, abs/2001.02144, 2020. doi:10.48550/arXiv.2001.02144.
- 14 Susanna F. de Rezende, Or Meir, Jakob Nordström, and Robert Robere. Nullstellensatz size-degree trade-offs from reversible pebbling. *Comput. Complex.*, 30(1):4, 2021. doi:10.1007/s00037-020-00201-y.
- 15 Erich Grädel, Martin Grohe, Benedikt Pago, and Wied Pakusa. A finite-model-theoretic view on propositional proof complexity. *Log. Methods Comput. Sci.*, 15(1), 2019. doi:10.23638/LMCS-15(1:4)2019.
- 16 Martin Grohe and Wied Pakusa. Descriptive complexity of linear equation systems and applications to propositional proof complexity. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017*, pages 1–12. IEEE Computer Society, 2017. doi:10.1109/LICS.2017.8005081.
- 17 Alexander Hertel. *Applications of Games to Propositional Proof Complexity*. PhD thesis, University of Toronto, May 2008. Available at <http://www.cs.utoronto.ca/~ahertel/>. URL: <http://hdl.handle.net/1807/16735>.
- 18 Neil Immerman. Number of quantifiers is better than number of tape cells. *J. Comput. Syst. Sci.*, 22(3):384–406, 1981. doi:10.1016/0022-0000(81)90039-8.
- 19 Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. doi:10.1007/s000370050024.

- 20 Balasubramanian Kalyanasundaram and George Schnitger. On the power of white pebbles. *Combinatorica*, 11(2):157–171, June 1991. Preliminary version in *STOC '88*. doi:10.1007/BF01206359.
- 21 Friedhelm Meyer auf der Heide. A comparison of two variations of a pebble game on graphs. *Theoretical Computer Science*, 13(3):315–322, 1981. doi:10.1016/S0304-3975(81)80004-7.
- 22 Jakob Nordström. Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science*, 9:15:1–15:63, September 2013. doi:10.2168/LMCS-9(3:15)2013.
- 23 Jakob Nordström. New wine into old wineskins: A survey of some pebbling classics with supplemental results. Manuscript in preparation. Current draft version available at <http://www.csc.kth.se/~jakobn/research/PebblingSurveyTMP.pdf>, 2015.
- 24 Michael S. Paterson and Carl E. Hewitt. Comparative schematology. In *Record of the Project MAC Conference on Concurrent Systems and Parallel Computation*, pages 119–127, 1970. doi:10.1145/1344551.1344563.
- 25 Wolfgang J. Paul, Robert Endre Tarjan, and James R. Celoni. Space bounds for a game on graphs. *Mathematical Systems Theory*, 10:239–251, 1977. doi:10.1007/BF01683275.
- 26 Nicholas Pippenger. Pebbling. Technical Report RC8258, IBM Watson Research Center, 1980.
- 27 Alexander A. Razborov. On space and depth in resolution. *Computational Complexity*, 27(3):511–559, 2018. doi:10.1007/s00037-017-0163-1.
- 28 John E. Savage. *Models of computation - exploring the power of computing*. Addison-Wesley, 1998.
- 29 Uwe Schöning and Jacobo Torán. *The Satisfiability Problem: Algorithms and Analyses*, volume 3 of *Mathematics for Applications (Mathematik für Anwendungen)*. Lehmanns Media, 2013.
- 30 Jacobo Torán and Florian Wörz. Reversible pebble games and the relation between tree-like and general resolution space. *Comput. Complex.*, 30(1):7, 2021. doi:10.1007/s00037-021-00206-1.
- 31 Robert E. Wilber. White pebbles help. *Journal of Computer and System Sciences*, 36(2):108–124, 1988. Preliminary version in *STOC '85*. doi:10.1016/0022-0000(88)90023-2.