Electronic Colloquium on Computational Complexity, Report No. 42 (2024)

Pebble Games and Algebraic Proof Systems Meet Again

Lisa-Marie Jaser and Jacobo Torán

Universität Ulm, Germany
{lisa-marie.jaser,jacobo.toran}@uni-ulm.de

Abstract

Analyzing refutations of the well known pebbling formulas 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 NS, MC and PC on the other side. In particular we prove:

- For any DAG G with a single sink, if there is a Monomial Calculus refutation for 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 Peb(G) having simultaneously degree s and size $2t(s-1)$. These results are analogous to those proven in [dRMNR21] for the case of reversible pebbling and Nullstellensatz. Using them we prove degree separations between NS and MC as well as strong degree-size tradeoffs for MC.
- We show that the variable space needed for the refutation of pebbling formulas in Polynomial Calculus exactly coincides with the black-white pebbling number of the corresponding graph. One direction of this result was known. We present an new elementary proof of it.
- We show that for any unsatisfiable CNF formula F, the variable space in a Resolution refutation of the formula is a lower bound for the monomial space in a PCR refutation for the extended formula $F[\oplus]$. $\mathrm{VSpace}_{\mathrm{Res}}(F \vdash) \leq \mathrm{MSpace}_{\mathrm{PCR}}(F[\oplus] \vdash)$. This implies that for any DAG G, the monomial space needed in the refutation of an XOR pebbling formulas is lower bounded by the black-white pebbling number of the corresponding graph, $\mathrm{MSpace}(\mathrm{Peb}(G)[\oplus]) \geq \mathsf{BW}(G)$. This solves affirmatively Open Problem 7.11 from [BN21].
- The last result also proves a strong separation between degree and monomial space in PCR of size $\Omega(\frac{n}{\log n})$ with the additional property that it is independent of the field characteristic. This question was posed in [FLM$^+$13].

ISSN 1433-8092

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 [Pip80, Sav98, Nor15].

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). Black pebbles 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. White pebbles (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.

Pebbling games have also become one of the most useful tools for proving results in proof complexity. The reason for this is that one can often 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 [BW01] 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. [Nor13].

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 bellow). Well known are Nullstellensatz (NS) introduced in [BIK$^+$94] and the more powerful Polynomial Calculus (PC) defined in [CEI96]. 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. A useful variation of PC defined in [ABRW02] to unify the PC with Resolution is Polynomial Calculus with Resolution, PCR.

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. We will use variable space (number of variables that are simultaneously active in a refutation) and monomial space (number of monomials kept simultaneously in memory, counted with repetitions).

In [BG15] 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 [AM13] 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 method in graph theory and descriptive complexity.

As mentioned above, connections between pebbling games and algebraic systems hve been known. Already in [BCIP02] it was proved that for any directed acyclic graph (DAG) G the corresponding pebbling formula 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 $G, \mathsf{Black}(G)$. Using pebbling results, this automatically proves a strong degree separation between NS and PC. As a more recent example, the authors in [dRMNR21] 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.

We show in this paper that besides these results, there are further parallelisms between the Reversible, Black, Black-White game hierarchy on one side, and the NS, MC and PC/PCR proof systems on the other side.

1.1 Our results

In Section 3 we prove that very similar results to those given in [dRMNR21] for NS and reversible pebbling are also true for the case of MC and black pebbling. More concretely we show in Theorem 16 that for any DAG G with a single sink, if there is a MC refutation for $\mathrm{Peb}(G)$ 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 of formulas and it is well known that input Resolution is complete for Horn formulas.

For the other direction, we show in Theorem 11 that from a black pebbling strategy for G with space s and time t it is possible to extract a MC refutation for $\mathrm{Peb}(G)$ having simultaneously degree s and size $2t(s-1)$. The small loss in the time parameter compared to the results in [dRMNR21] comes from the fact that size is measured in slight different ways in NS and MC. Using these results we are able to show degree separations between NS and MC as well as strong degree-size tradeoffs for MC in the same spirit as those in [dRMNR21].

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 in [BCIP02] it was proven 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 the connection still holds[1]. This is not a new observation, in the first paper showing space-size tradeoffs for Resolution [Ben09] where the black-white pebble game was used for the fist time in the context of proof complexity, the author proved that for any DAG G and a Resolution refutation of $\mathrm{Peb}(G)$ with variable space s, a black-white pebbling strategy for G with the same space can be extracted. This result was strengthen in [BN11]. For the concrete case of Polynomial Calculus it was shown in [BNT13] that for the variable space needed to refute $\mathrm{Peb}(G)$ is at least the black-white pebbling price of G. Again this implies tradeoff results, in this case a degree-monomial space tradeoff as well as time-space tradeoffs for PC. We give in Subsection 4.1 a new proof of the result showing that for PC variable space for pebbling formulas is lower bounded by the black-white pebbling number. Contrary to the proof in [BNT13] this proof is completely elementary and does use random restrictions or space faithful projections. We complete the result showing that it also holds in the other direction by proving that the variable space for the refutation of pebbling formulas in PC is also an upper bound for the variable space.

So far all the mentioned results deal with the pure pebbling formulas without extension variables. For studying monomial space this is not enough since it is well known that the standard pebbling formulas can be refuted in constant space. Our main results are proven when

[1]We observe that the results for MC can also be interpreted in terms of variable space.

each variable in the pebbling formulas are substituted by the XOR or two new variables, also a well known technique called XORification.

We show in that for any unsatisfiable CNF formula F, the variable space in a Resolution refutation of F is a lower bound for the monomial space in a PCR refutation for the extended formula $F[\oplus]$, in symbols $\mathrm{VSpace}_{\mathrm{Res}}(F \vdash) \leq \mathrm{MSpace}_{\mathrm{PCR}}(F[\oplus] \vdash)$ (Corollary 31). Since as mentioned above it is known that the Resolution variable space for pebbling formulas is lower bounded by the black-white pebbling number of the corresponding graph [Ben09], and the PC degree of (the XOR version) of the pebbling formulas is constant, this immediately implies for any DAG G, $\mathrm{MSpace}(\mathrm{Peb}(G)[\oplus]) \geq \mathsf{BW}(G)$ (Theorem 32). This solves affirmatively Open Problem 7.11 from [BN21]. It also proves a strong separations between degree and monomial space in PCR to be $\Omega(\frac{n}{\log n})$. The separation has the property that it is independent of the field characteristic, a question that was posed in [FLM+13]. Previously know weaker space degree separations for PCR with this property were shown in [GKT19]. Comparing degree and monomial space for PCR with width and clause space in Resolution, our separation exactly parallels that from [BN08] which is the strongest possible one for Resolution.

The bounds from Corollary 31 also improve those in Theorem 9 from [BNT13] by decreasing the Resolution variable space needed from $s \log t$ to s. As a consequence of the improvement in the parameters, also some of the size-space tradeoffs for PCR refutations of pebbling formulas reported in [BNT13] can be also be improved.

2 Preliminaries

2.1 Pebble Games

Black pebbling was first mentioned implicitly in [PH70], while black-white pebbling was introduced in [CS76]. Note, that there exist several variants of the (black-white) pebble game in the literature. For differences between these variants, we refer to [Nor15]. 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 $B_i \cap W_i = \varnothing$ 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 $\mathrm{pred}_G(v) \subseteq B_{i-1} \cup W_{i-1}$. In particular, a black pebble can always be placed on an empty source vertex s, since $\mathrm{pred}_G(s) = \varnothing$.

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 $\mathrm{pred}_G(v) \subseteq B_{i-1} \cup W_{i-1}$. 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 $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_t)$ 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 $W_i = \varnothing$ 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 $B_i = \varnothing$ for all $i \in [t]$. Observe that $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_t)$ is a black pebbling of G if and only if $\mathcal{P}' = (\mathbb{P}'_t, \ldots, \mathbb{P}'_0)$ 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 $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_t)$ is $\mathsf{time}(\mathcal{P}) := t$ and the *space* of it is $\mathsf{space}(\mathcal{P}) := \max_{i\in[t]} |B_i \cup W_i|$. The *black-white pebbling price* (also known as the *pebbling measure* or *pebbling number*) of G, which we will denote by $\mathsf{BW}(G)$, is the minimum space of any black-white pebbling of G. The *black pebbling price* of G, denoted by $\mathsf{Black}(G)$, is the minimum space of any black pebbling of G. By the observation above, the white pebbling price $\mathsf{White}(G)$ coincides with $\mathsf{Black}(G)$

Finally, we mention the reversible pebble game introduced in [Ben89]. 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. We omit the formal definition since they will not be used for the present results and refer the interested reader to [dRMNR21]. 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, $\mathrm{Var}(F)$ denotes the set of its variables.

A Horn formula in 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 [ST13]. 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 $\mathrm{pred}(v)$ the set of its direct predecessors. In particular, for a source vertex v, $\mathrm{pred}(v) = \emptyset$. The *pebbling contradiction* over G, denoted $\mathrm{Peb}(G)$, is the conjunction of the following clauses:

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

A well known method to make pebbling formulas harder to refute is to substitute some suitable Boolean function $f(x_0, \ldots, x_{d-1})$ of arity d for each variable x and expand the result into CNF ($x_0, \ldots, x_{d-1}$ are new variables). This general case is discussed in [Nor15]. We restrict ourselves to the special case of the second degree XORification in which $f(x_0, x_1) = x_0 \oplus x_1$.

Definition 4 (Substitution formulas)**.** For a positive x define the *XORification* of x to be $x[\oplus] := \{x_0 \vee x_1, \overline{x_0} \vee \overline{x_1}\}$. For a negative literal $\overline{y}$, the XORification is $\overline{y}[\oplus] := \{y_0 \vee \overline{y_1}, \overline{y_0} \vee y_1\}$. The XORification of a clause $C = a_1 \vee \cdots \vee a_k$ is the CNF formula

$$C[\oplus] := \bigwedge_{C_1\in a_1[\oplus]} \cdots \bigwedge_{C_k\in a_k[\oplus]} (C_1 \vee \cdots \vee C_k),$$

and the XORification of a CNF formula F is $F[\oplus] := \bigwedge_{C \in F} C[\oplus]$.

Remark 5 ([BN08])**.** If G has n vertices and maximal in-degree ℓ, then $\mathrm{Peb}(G)[\oplus]$ is an unsatisfiable $2(\ell+1)$-CNF formula with at most $2^{\ell+1} \cdot n$ clauses over $2n$ variables.

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 $C_1, \ldots, C_m$ is translated as set of polynomials $p(C_1), \ldots, p(C_m)$. 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. We denote by $\mathrm{mon}(p)$ the set of monomials of p and write $m \in \mathrm{mon}(p)$ or even $m \in p$ to indicate that m is a monomial of p. 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 $\bigvee_{u \in \mathrm{pred}(v)} \bar{x}_u \vee x_v$ becomes the polynomial $A_v := m_{\mathrm{pred}(v)}(1 - x_v)$, and the sink axiom $\bar{x}_z$ is transformed into the polynomial $A_{sink} := x_z$.

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

A (partial) assignment γ for a formula F is a (partial) mapping $\alpha : \mathrm{Var}(F) \longrightarrow \{0,1\}$. We will denote by $F|_\gamma$ the result of appliying the assignment to F and reducing it in the standard way. The same notation will be used when and Boolean assignment is applied to a polynomial encoding P_F. Here $P_F|_\gamma$ is the polynomial resulting after substituting the assigned variables by their values in γ and adding the terms of the resulting polynomial.

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

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

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 7. The PC proof system uses the following rules:

1. *Linear combination*
$$\frac{p \qquad q}{\alpha p + \beta q} \qquad \alpha, \beta \in \mathbb{F}.$$
2. *Multiplication*
$$\frac{p}{x_i p} \qquad i \in [n].$$

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

In order to avoid some technical problems that arise in PC and unify the strength of PC and Resolution a slight modification of PC called Polynomial Calculus with Resolution (PCR) was introduced in [ABRW02]. The polynomial equations are now in a ring $\mathbb{F}[x_1, \ldots, x_n, x'_1, \ldots, x'_n]$, i.e. for each variable x_i there is also a twin variable x' representing its negation. We have the same rules and axioms as in PC plus the axiom $x_i + x'_i - 1$ for each variable x_i. Twin variables are in principle independent from each other but the new axioms force them to take complementary values.

In a similar way as for PC, a PCR refutation of an initial unsolvable set of polynomials $\mathcal{P}$ is a sequence of polynomials $\{q_1, \ldots, q_m\}$ such that each q_i is either a polynomial in $\mathcal{P}$, a Boolean axiom or is obtained by applying one of the rules of the calculus. In this case the Boolean axioms are $x_i^2 - x_i$, $x'^2_i - x'_i$ and $1 - x_i - x'_i$.

A less known algebraic proof system between NS and PC is Monomial Calculus, MC. This system was introduced in [BG15] 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 8. The MC proof system uses the following rules:

1. *Linear combination*

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

2. *Multiplication*

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

As is the case of PC/PCR, a refutation in MC of an initial unsolvable set of polynomials $\mathcal{P}$ is a sequence of polynomials $\{q_1, \ldots, q_m\}$ 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 [BG15], 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.

In order to analyze and compare refutations we will consider several complexity measures on them.

Definition 9 (Complexity measures)**.** Let $\mathcal{C}$ be one of the mentioned systems $\mathcal{C} \in \{\text{MC}, \text{PC}, \text{PCR}\}$ Let $\pi = \{q_1, \ldots, q_m\}$ 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, $\deg_{\mathcal{C}}(\pi) = \max_{i=1,\ldots,n}(\deg(q_i))$. 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 monomials. For the space measures we need to define configurational proofs. Such a proof π in the system $\mathcal{C}$ is a sequence of configurations $\pi = C_0, \ldots C_t$ in which each C_i is a set of polynomials with $C_0 = \emptyset$ and $C_t = 1$. Each configuration represents a set of polynomials that are kept simultaneously in memory 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) or $C_{i-1} \setminus \{p\}$ (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 monomial space $\mathrm{MSpace}_{\mathcal{C}}(\pi)$ is the maximum number of monomials (counted with repetitions) appearing in any configuration in the proof. The variable space $\mathrm{VSpace}_{\mathcal{C}}(\pi)$ 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 $\mathrm{Comp}_{\mathcal{C}}(P_F \vdash)$ the minimum over all $\mathcal{C}$ refutations of P_F of $\mathrm{Comp}_{\mathcal{C}}(\pi)$.

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.

Definition 10 (Semantic derivations)**.** We refer to configurational derivations in which any line that is a logical consequence of the current derivation can be derived in one single step as semantic derivations.

3 Monomial Calculus and pebbling formulas

In [dRMNR21] 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 11. *Let G be a directed acyclic graph with a single sink z. 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 $2t(s-1)$. The variable space of this refutation coincides with its degree.*

Proof. It is convenient to consider here the equivalent notion of white pebbling. Let $\mathcal{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_t)$ be a white pebbling strategy for G with $\mathbb{P}_1 = \{z\}$ and $\mathbb{P}_t = \emptyset$ using s pebbles. We show by induction on i, that for each $\mathbb{P}_i = \{v_{i_1}, \ldots, v_{i_{k_i}}\}$ the monomial $m_i = \prod_{v \in \mathbb{P}_i} x_v$ can be derived from Peb_G in MC within size $2i(s-1)$ and degree s. This proves the result since $\mathbb{P}_{t-1} = \{v\}$ for some source vertex v and if the monomial $m_{t-1} = x_v$ can be derived in MC with the required parameters, then adding the axiom $1 - x_v$ we obtain the polynomial 1.

For the case $i = 1$, the result is clear since $\mathbb{P}_1 = \{z\}$ and x_z is an axiom. That is, for deriving $\mathbb{P}_1$ we have used one monomial. For the induction step there are two cases:

Pebble placement: if the configuration at pebbling step $i+1$ is reached after placing a white pebble on vertex v and $\mathbb{P}_i = \{u_{i_1}, \ldots, u_{i_{k_i}}\}$ with $k_i \leq s-1$ then $\mathbb{P}_{i+1} = \{v, u_{i_1}, \ldots, u_{i_{k_i}}\}$. By induction hypothesis there is a MC derivation of degree s and size $2i(s-1)$ of the monomial $m_i = \prod_{u \in \mathbb{P}_i} x_u$. By multiplying this monomial times 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 $\mathbb{P}_i = \{v, u_{i_1}, \ldots, u_{i_{k_i}}\}$ with $k_i \leq s-1$ then all predecessors $u_1, \ldots u_k$ of v are in the set $\{u_{i_1}, \ldots, u_{i_{k_i}}\}$. For the derivation of m_{i+1} we can multiply the axiom $(1 - x_v) \prod_{u \in \mathrm{pred}(v)} x_u$ by the variables in $\mathrm{Var}(m_i) \setminus (\bigcup_{u \in \mathrm{pred}(v)} x_u \cup \{x_v\})$, and add this polynomial to m_i obtaining m_{i+1}. The number of intermediate monomials added to the proof is at most $2(s-1)$.

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 12. The size bound $2t(s-1)$ 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 at time is allowed, 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 asymmetric to the NS case, in which the intermediate monomials are not counted. Defining the MC rules as those in NS would avoid the s factor in the pebbling time, as in the NS simulation of pebbling from [dRMNR21].

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. It 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 13. A MC refutation π of a contradictory set of polynomials F is called an *input refutation* if there is a sequence of monomials $M_0, \ldots, M_t$ 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 $M_0, \ldots, M_t$ the backbone of the proof.

Lemma 14. *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 was a Horn formula, each polynomial has either one or two monomials. We will represent such a polynomial $p = \alpha_m m + \alpha_{m'} m'$ by the pair (m, m'). In all these polynomials the monomial terms have some coefficients α_m and $\alpha_{m'}$ with $\alpha_m, \alpha_{m'} \in \{1, -1\}, \alpha_m = -\alpha_{m'}$ because the axiom polynomials with two monomials are polynomial encodings of Horn clauses with one negated variable. Clauses without negated variables 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 $p_1, \ldots, p_\ell$ represented by the monomials $(\emptyset, m_1), (m_1, m_2), (m_2, m_3) \ldots, (m_{\ell-1}, m)$ [2]. This is because the linear combination adds up to 1 and for this 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. We suppose that $p_1, \ldots, p_\ell$ 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 $m_\ell, \ldots, m_1$ until 1 is derived. Observe that the monomials $M_0, \ldots M_t$ are exactly those appearing in $p_1, \ldots, p_\ell$. 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 $p_1, \ldots, p_\ell$ are already in π. Besides these

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

polynomials π' contains also the ℓ new monomials in the backbone. Since the $p_1, \ldots, p_\ell$ and m belong to π and in each linear combination of two polynomials at the 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 $p_1, \ldots, p_\ell, \hat{m}$ in π from which an input monomial refutation that starts at $M_0 = \hat{m}$ and derives at some point i $M_i = m$ can be extracted. 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 $p'_1, \ldots, p'_{\ell'}$ in π represented by the monomials $(\emptyset, m'_1), (m'_1, m'_2), \ldots, (m'_r, m')$ from which an input refutation of $P_F \cup m'$ can be extracted. We can put together both input MC refutations $M_0 \ldots M_i$ and $M_{i+1}, \ldots, 1$. Again we can assume that all the monomials in the backbone are different since if $M_i = M_j$ for $i < j$, we could shorter 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 15. *Let G be a directed acyclic graph with a single sink vertex z and let π be a MC refutation of* $\mathrm{Peb}(G)$. *There is an input MC refutation π' of* $\mathrm{Peb}(G)$ *with at most the same size and degree as π.*

Theorem 16. *Let G be a directed acyclic graph with a single sink. Let π be a MC refutation of* $\mathrm{Peb}(G)$ *with degree s and size t. There is a black pebbling strategy with s pebbles and time $t + s$.*

Proof. Because of Corollary 15 we can suppose that there exits an input MC refutation with monomials $M_0, \ldots M_t$ starting with $M_1 = mx_{\mathrm{sink}}$ 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 when going from M_i to M_{i+1} variables disappear, 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 variable v $\mathrm{pred}(v)(1 - x_v)$ multiplied by some monomial m. The only variable that can disappear in M_{i+1} is x_v and in this case $M_i = \mathrm{pred}(v)x_v$. Therefore all the vertices in $\mathrm{pred}(v)$ have pebbles on them and the pebble in x_v is 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 $M_1 = mx_{\mathrm{sink}}$ and then t more pebbling steps. □

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. In [BCIP02] it was shown that pebbling formulas have constant PC degree and that for any directed acyclic graph G the formula $\mathrm{Peb}(G)$ 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 $B(G_n) = \Omega(\frac{n}{\log n})$ [PTC77], this implies a degree separation of $\Omega(\frac{n}{\log n})$ between PC and NS. From Theorem 16 follows that this is in fact a degree separation between MC and PC.

Theorem 17. *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 $\Omega(\frac{n}{\log n})$.*

Also from Theorem 11 and the equivalence between reversible pebbling price and NS degree from [dRMNR21] 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 $\lceil \log n \rceil$ [Ben89]. Translated to pebbling formulas this means:

Theorem 18. *There is an unsatisfiable family of formulas $\{F_n\}_{n=0}^{\infty}$ with $\Theta(n)$ variables each, that have MC refutations of degree 2 but require NS refutations of degree $\lceil \log n \rceil$.*

Another graph family for which such a separation is know is the class of path graphs from [CLNV15]. The separation between reversible and black pebbling for these graphs is translated into the next result.

Theorem 19. *For any function $s(n) = O(n^{1/2-\epsilon})$ for constant $0 < \epsilon < \frac{1}{2}$ there is an unsatisfiable family of 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 $\Omega(s(n) \log n)$.*

It is an open question of whether the separation between reversible and black pebbling space can be larger than a logarithmic factor in the number of nodes. The best known degree separation between NS and and MC is slightly better. It was obtained in [GP17] with very different methods. Using a classic result from descriptive complexity [Imm81], the authors show that for 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 $\log^c(\sqrt{n})$. 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 11,16 make it possible to translate space-time tradeoffs for pebbling into degree-size tradeoffs for MC. The is a slight loss of the time parameter that comes from the extra space factor in the the MC refutation from Theorem 11. 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 20. *[Sav98] There is a family of directed graphs $\{G_n\}_{n=0}^{\infty}$ having $\Theta(n^2)$ vertices each and with $\mathsf{Black}(G_n) = \Theta(n)$ for which any black pebbling strategy with $\mathsf{Black}(G_n)$ pebbles requires at least $2^{\Omega(n \log n)}$ steps while there is a pebbling strategy with $\mathsf{Black}(G_n) + 1$ pebbles and $O(n^2)$ steps.*

Corollary 21. *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 [Nor15].

Theorem 22. *There is a family of directed graphs $\{G_n\}_{n=0}^{\infty}$ having $\Theta(n)$ vertices each and with $\mathsf{Black}(G_n) = O(\log^2 n)$, with a black pebbling strategy in space $O(n/\log n)$ and time $O(n)$. There is 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 23. *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 Polynomial Calculus and pebbling formulas

4.1 PC variable space and black-white pebbling

We start this section showing for any single sink DAG G the variable space in PC for refuting $\mathrm{Peb}(G)$ exactly coincides with the black-white pebbling number for G. Since they are not important for our results, we do not consider the time bounds here. We give first the upper bound for variable space in terms of pebbling. For the case of Resolution this result was shown by [Her08].

Theorem 24. *Let G be DAG with a single sink z. If there is a black-white pebbling strategy of G with space s then there is a* PC *refutation of* Peb_G *with variable space s.*

Proof. Let $\mathcal{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_t)$ be a black-white pebbling strategy for G with $\mathbb{P}_i = (B_i, W_i)$, $\mathbb{P}_0 = (\emptyset, \emptyset)$ and $\mathbb{P}_t = (\{z\}, \emptyset)$. Assume further that $s = \max_i |\mathbb{P}_i|$. We show how to extract a PC refutation from it. For this, let $L_i = \{x_v \mid v \in B_i \cup W_i\}$ and let Peb_i be the set of polynomials in Peb_G with all variables in L_i. For each step i we define the set of polynomials $\mathcal{C}_i$. $\mathcal{C}_0 := \emptyset$ and for all $i > 0$ let $\mathcal{C}_i$ be the set of polynomials that can be PC-derived from $\mathcal{C}_{i-1} \cup \mathrm{Peb}_i$ and all variables are in L_i. It follows that $|\mathrm{VSpace}(\mathcal{C}_i)| \leq s$. We prove the following claims:

- For every pebbling configuration $\mathbb{P}_i = (B_i, W_i)$ and every vertex $v \in B_i$, there is a set $A_i^v \subseteq W_i$ such that
$$(1 - x_v) \prod_{w \in A_i^v} x_w \in \mathcal{C}_i.$$
This type of polynomial will be called a polynomial pointing to v at step i.
- Let j be the first step in which the sink z has a pebble on it. Then for any pebbling configuration $\mathbb{P}_i = (B_i, W_i)$ with $i \geq j$ there is a subset $A_i \subseteq W_i$ such that
$$\prod_{w \in A_i} x_w \in \mathcal{C}_i.$$

For the case $i = t$ we can see that $W_i = \emptyset$ and from the second part of the claim it follows that there is a PC-refutation of 1 with variable space s. Both claims will be shown by induction. For the first claim, the case for $\mathbb{P}_0$ is trivial. For each $i > 0$ there are four possible pebbling steps that could be performed. In the case that a black pebble was removed in step i nothing has to be shown because $\mathcal{C}_i \subset \mathcal{C}_{i-1}$. If a white pebble was added, the claim also follows directly because there is no change in B_i. Assume now that a black pebble was added on vertex v. If v is a source then $1 - x_v$ lies in $\mathcal{C}_i$. Else, all predecessors of v are pebbled, say $b_1, \ldots, b_l$ and $w_1, \ldots, w_m$ respectively with black and white pebbles on them. It holds

$$(1 - x_v) \prod_{j=1}^{l} x_{b_j} \prod_{k=1}^{m} x_{w_k} \in \mathcal{C}_i$$

and by induction for all predecessor b of v there is a set $A_{i-1}^b \in W_{i-1}$ such that

$$(1 - x_b) \prod_{w \in A_{i-1}^b} x_w \in \mathcal{C}_{i-1}.$$

Combining those polynomials one can derive

$$(1 - x_v) \prod_{j=1}^{l} \prod_{w \in A_{i-1}^{b_j}} \prod_{k=1}^{m} x_{w_k}.$$

This is a polynomial pointing to v at step i. The last possible pebbling step is removing a white pebble from v at step i. We have to prove that there is no vertex u for which the polynomial pointing to u in $\mathcal{C}_{i-1}$ contains the variable x_v. If v is a source vertex $1 - x_v$ belongs to $\mathcal{C}_{i-1}$ an thus all polynomials that contain x_v can be resolved to polynomials without x_v in $\mathcal{C}_i$. Assume now that v is an internal vertex, then all predecessors of v have pebbles on them, say $b_1, \ldots, b_l$ and $w_1, \ldots, w_m$ for the vertices with black and white pebbles, respectively. We now have

$$(1 - x_v) \prod_{j=1}^{l} x_{b_j} \prod_{k=1}^{m} x_{w_k} \in \mathcal{C}_{i-1}$$

and for all b_j there is a polynomial pointing to b_j in $\mathcal{C}_{i-1}$. Similarly as before we can derive a polynomial p pointing to v. Assume u is a vertex with a black pebble and there is a polynomial pointing to u in $\mathcal{C}_{i-1}$ that contains the variable x_v. Combining with p one can derive a polynomial pointing to u in $\mathcal{C}_i$.

For the second part of the claim, if z is pebbled at step j, then x_z is in $\mathcal{C}_j$. For $i > j$ we only have to consider the case that a white pebble is removed. Removing a black pebble or adding a (black or white) pebble does not change the existence of a polynomial like the one claimed. The proof for removing a white pebble v is similar as the one for the first part of the claim. We need to show that there is a subset $A_i \subseteq W_i$ such that $v \notin A_i$ and $\prod_{w \in A_i} x_w \in \mathcal{C}_i$. For this we assume $v \in A_{i-1}$. If v is a source vertex, then $1 - x_v \in \mathcal{C}_{i-1}$ and $\prod_{w \in A_i \setminus \{v\}} x_w$ can be derived. Assume now that v is an internal vertex. Similarly as in the first case we can derive a polynomial of the form $(1 - x_v) \prod_{w \in B} x_w$ for some $B \subseteq W_i$. Because $\prod_{w \in A_i \setminus \{v\}} x_w \in \mathcal{C}_{i-1}$ we get the desired polynomial and the proof is complete.

□

We show next the result in the other direction proving that the black white pebbling number of a graph G is a lower bound for the variable space needed for refuting Peb(G) in PC. The proof is similar to the one given for the case of Resolution given in [Ben09]. For this we use the concept of essential refutation from the mentioned reference, a refutation that only has polynomials that contribute towards reaching the contradiction $0 = 1$.

Definition 25. Let $\pi = \mathbb{M}_0, \ldots, \mathbb{M}_t$ be a configurational PC refutation of an unsatisfiable CNF formula F. The essential polynomials in π are defined by backwards induction:

- If the polynomial 1 appears for the first time in a configuration $\mathbb{M}_i$, then this polynomial is essential at time i.
- If p is an essential polynomial at time i and p is inferred at time i by a rule applied to polynomials p_1 and p_2, (or just to p_1 in case of a multiplication) then p_1 and p_2 are essential at time $i - 1$.
- If p is essential at time i and p belongs to $\mathbb{M}_{i-1}$ (the polynomial has been copied from the previous configuration) then p is also essential at time $i - 1$.

From a PC refutation π one can always extract an essential one π' by deleting the polynomials that are not essential, and merging together some linear combination or multiplication steps with deletion steps in π. For example if in a configuration $\mathbb{M}_i$ in π two polynomials p_1, p_2 are

combined producing the polynomial p and p_1 or p_2 (or both) are not essential at step $i+1$ in π we include in π' p and only the parent polynomials that are still essential in $\mathbb{M}_{i+1}$. (Same thing for a multiplication step). Such a step can merge together two or three steps in a standard configurational proof. We will call such a step, LC/Deletion step (or a Multiplication/Deletion step) in π'. Since a deletion in π can always happen direct after a LC or multiplication step, there are no pure deletion steps in π', only axiom download and LC/Deletion, Multiplication/Delation steps. Pure LC steps in which no deletion happen are also considered to be LC/Deletion steps (same for the multiplication steps). We will call such a proof an *essential configurational refutation*. Observe that the variable space in an essential refutation cannot be larger than that in the original sequence of configurations from which it has been extracted. We simplify even more the refutations by considering only direct ones

Definition 26. A PC refutation $\pi := \mathbb{M}_0, \ldots, \mathbb{M}_t$ is called direct if at every step in which the linear combination rule is applied to two polynomials p and q, the polynomials have some common monomial.

Lemma 27. *Let F be a contradictory set of polynomials over a field $\mathbb{F}$ and let π be a PC refutation of F. There is an direct PC refutation π' of F with at most the same degree, and variable space as π.*

Proof. Let F be a contradictory formula and $\pi = p_1, \ldots p_t$ be a PC refutation for F. We show how to extract from π a direct refutation π'. This is done by avoiding each linear combination step in the proof when the rule is applied to two polynomials p_i, p_j without common monomials. We will derive inductively for each polynomial p in the refutation a set of polynomials L_p, with the following properties:

- p is the sum of the polynomials in L_p,
- the polynomials in L_p partition the monomials in p. That is, two different polynomials in L_p are monomial disjoint, and every monomial in p belongs to some polynomial in L_p.

This would prove the result since at the end of the refutation $p_t = 1$, and L_{p_t} has to be $\{1\}$. L_p is defined inductively in the following way: If p is an axiom, then $L_p = \{p\}$. If p is obtained by multiplying x times a polynomial q, then $L_p = \{xq' \mid q' \in L_q\}$. If p is obtained by a linear combination of two polynomials $p = \alpha_i p_i + \alpha_j p_j$ in which p_i and p_j do not have any common monomials then $L_p = L'_{p_i} \cup L'_{p_j}$ where L'_{p_i} is the list of the polynomials in L_{p_i} multiplied by the coefficient α_i (same for L'_{p_j}). Finally, we show how to construct a set of polynomials L_q with the desired properties when p is the linear combination of two polynomials p_i and p_j with at least some common monomial. By hypothesis there are sets of polynomials L_{p_i} and L_{p_j} for p_i and p_j and since p is a linear combination of these two polynomials, p can be expressed as $\sum_{q \in L_{p_i} \cup L_{p_j}} \alpha_q \cdot q$, where the α's are coefficients in the field. We can consider the (bipartite) graph G_p with vertices $L_{p_i} \cup L_{p_j}$ and with the edges $E = \{(q, r) |\ q \text{ and } r \text{ have some common monomial}\}$. Observe that each monomial in the set of polynomials can contribute by at most one edge to E since at most one polynomial in L_{p_i} and at most one in L_{p_j} contain this monomial. Also, every connected component in G_p corresponds to a subset of of the polynomials that does not have any common monomial with the polynomials in other connected components of the graph. Multiplying all the polynomials times the coefficients in the linear combination for p we obtain that for every connected component c, the addition of the corresponding polynomials produces a polynomial p_c that is a sum of monomial terms of p. L_p is defined as the set of the polynomials $\{p_c \mid c \text{ is a connected component in } G_p\}$. Clearly p is the sum of the polynomials in L_p and all these polynomials are pairwise monomial disjoint. L_p contains the monomials in p exactly once. Also, the polynomials in L_p can be derived as the sum of some polynomials with

common monomials in the previous lists. This can be done by adding each time two polynomials sharing an edge (monomial) in G_p until only one polynomial for each connected component is left. Observe that all the monomials in L_p are included in p and therefore the direct proof has the same degree and variable space. □

We show next that a black-white pebbling strategy can be extracted from a PC refutation.

Theorem 28. *For every DAG G with a single sink, and for every PC configurational refutation π of* Peb(G) *with* VSpace(π) $= s$ *there is a black-white pebbling strategy for G with space s.*

Proof. Let G be a DAG with a unique sink z, and let π be a direct PC refutation of Peb(G) given by a sequence of configurations $\pi := \mathbb{M}_0, \ldots, \mathbb{M}_t$. We show how to extract a strategy for the black-white pebbling game on G with a number of pebbles bounded by the variable space in an essential refutation $\pi' := \mathbb{N}_0, \ldots, \mathbb{N}_t$ extracted from π. For a configuration $\mathbb{N}_i$, let $B(\mathbb{N}_i)$ be the set of variables x for which there is some polynomial p in $\mathbb{N}_i$ with $x \in \mathrm{Var}(p)$ that has some monomial not containing x. We define a pebbling strategy for G that keeps the following invariant:

1. At each step i only the vertices corresponding to the variables in $\mathrm{Var}(\mathbb{N}_i)$ have a pebble on them, and
2. if $x_v \in B(\mathbb{N}_i)$ there is a black pebble on v. If $x_v \in \mathrm{Var}(\mathbb{N}_i) \setminus B(\mathbb{N}_i)$ then the pebble on v can be black or white.

It should be clear that such a strategy does not use more pebbles that $\mathrm{Var}(\pi')$. We prove that there is a correct pebbling strategy satisfying these invariants. This is done by induction on the step i in the refutation. For $i = 0$ the configuration $\mathbb{N}_i$ is empty and no pebbles are being used. For the induction step, we consider several cases, corresponding to the possibilities for going from configuration $\mathbb{N}_i$ to $\mathbb{N}_{i+1}$.

Case 1: Axiom download. Let p be the axiom in Peb(G) downloaded in the configuration at step $i + 1$. This can correspond to either a source vertex, an intermediate vertex, or a target vertex. If it is the target vertex z and $x_z \notin \mathrm{Var}(\mathbb{N}_i)$ then $x_z \notin B(\mathbb{N}_{i+1})$ and z can be pebbled with a white pebble. If $x_v \in \mathrm{Var}(\mathbb{N}_i)$ then vertex z keeps the pebble from step i, which by induction is black if $x_z \in B(\mathbb{N}_i)$. If p is an axiom $\prod_{u \in \mathrm{pred}(v)} x_u(1 - x_v)$ corresponding to a vertex v in G, then one can place a pebble in each of the predecessors of v that do not have a pebble on them. This pebble is white in case the variable does not belong to $B(\mathbb{N}_{i+1})$. $x_v \in B(\mathbb{N}_{i+1})$, and v can be pebbled with a black pebble (maybe replacing a white pebble placed before) since all its predecessors have a pebble on them or v is a source vertex.

Case 2: Linear Combination/Deletion. Let p be the polynomial introduced in $\mathbb{N}_{i+1}$ in π', obtained by a linear combination of two polynomials p_1, p_2 in $\mathbb{N}_i$. Since we started from a direct refutation, p_1 and p_2 must have some common monomial m.

Case 3: Multiplication/Deletion. Let $p = x_v p'$ be the polynomial introduced at $\mathbb{N}_{i+1}$ in π', obtained by multipying variable x_v times the polynomial $p' \in \mathbb{N}_i$. The set of variables in $\mathrm{Var}(\mathbb{N}_{i+1})$ can differ from that in $\mathrm{Var}(\mathbb{N}_i)$ at most in variable x_v. But this variable belongs to all monomials in p and therefore $x_v \notin B(\mathbb{N}_i)$. Depending on whether x_v appears in $\mathbb{N}_{i+1}$ or not, an existing pebble is kept on v or a white pebble is placed on the vertex.

We show first that there cannot be any variable x_v that belongs to $B(\mathbb{N}_{i+1})$ but not to $B(\mathbb{N}_i)$. By contradiction, if this were true then x_v would belong to $\mathrm{Var}(p)$ but it is not part of some monomial $m' \in p$, and at the same time x_v is in all the monomials of p_1 and $x_v \notin \mathrm{Var}(p_2)$ (or the other way around). But we have supposed that there is some monomial m common to p_1 and p_2, so this would not be possible.

In case $\text{Var}(\mathbb{N}_{i+1}) \subset \text{Var}(\mathbb{N}_i)$ for every variable $x_v \in \text{Var}(\mathbb{N}_i) \setminus \text{Var}(\mathbb{N}_{i+1})$ it must hold that $x_v \in B(\mathbb{N}_i)$ and therefore the pebble on v must be black and can be removed. This is so because if $x_v \notin B(\mathbb{N}_i)$ then x_v must belong to each of the monomials of p_1 and p_2 and since we are supposing p is not the zero polynomial, $x_v \in \text{Var}(p)$ contradicting the fact that $x_v \notin \text{Var}(\mathbb{N}_{i+1})$. In case $\text{Var}(\mathbb{N}_i) = \text{Var}(\mathbb{N}_{i+1})$ and $B(\mathbb{N}_i) \subset B(\mathbb{N}_{i+1})$ then nothing has to be done. If a variable that was in $B(\mathbb{N}_i)$ is not in $B(\mathbb{N}_{i+1})$ its corresponding vertex keeps the black pebble that had at step i.

In all the cases we have shown that the pebbling strategy defined above follows the rules of the black-white pebbling game. Also at some point the axiom x_z has to belong to a configuration (without it the formula is satisfiable) and therefore at some point there is a pebble on vertex z. Since the last configuration in the essential proof only contains the polynomial 1, at this point there are no pebbles on G. Therefore the described strategy is a legal black white pebbling using at most $\text{Var}(\text{Peb}(G))$ pebbles.

□

4.2 Monomial space and PCR refutations of extended pebbling formulas

We prove a lower bound on monomial space of pebbling formulas analyzing the space needed for the refutation of the substitution formulas $\text{Peb}(G)[\oplus]$. This substitution is necessary since standard pebbling formulas can be refuted within constant space. We will relate monomial and variable space. For this we use the characterization of the variable space measure in terms of contradicting lists from [GTT18] as a tool.

Definition 29 (Contradicting list)**.** Let F be an unsatisfiable formula in CNF, L be a list of sets of variables $L = L_0, \ldots, L_t$, $L_i \in \text{Var}(F)$, and $\alpha = \alpha_0, \ldots, \alpha_t$ be a list of assignments for the variables in the sets, $\alpha_i : L_i \to \{0, 1\}$. We say that α is a locally consistent assignment sequence if for $0 \leq i \leq t-1$, and $x \in L_i \cap L_{i+1}$ it holds that $\alpha_i(x) = \alpha_{i+1}(x)$.

L is called a (w, t)-*contradicting list for* F if the following conditions hold:

i) $L_0 = \emptyset$ and for $1 \leq i \leq t$, L_i contains at most w variables,

ii) two consecutive lists differ in at most one variable; for $0 \leq i \leq t-1$, $|L_i \triangle L_{i+1}| \leq 1$ and

iii) any locally consistent sequence of assignments $\alpha_0, \ldots, \alpha_t$ for $L_0, \ldots, L_t$, falsifies at some point some axiom clause of F.

The concept of contradicting list characterizes variable space. In [GTT18] it is implicitly shown that a formula has a semantic Resolution refutation in variable space w and time t if and only if it has a (w, t) contradicting list. It can be noticed that the condition *ii*) in the definition can be replaced by the weaker condition that in going from L_i to L_{i+1} only new variables can be added to L_i or some variables can be removed, but not both things at the same time. Even with this weaker condition it still holds that a formula has a semantic Resolution refutation in variable space w and time t if and only if it has a (w, t) contradicting list. We will use this observation in the next result in which we show that the monomial space of a PCR refutation of an extension formula $F[\oplus]$ is upper bounded by its variable space. The same result was proven in [BN11] for the case of Resolution, with a different method.

Theorem 30. *Let F be an unsatisfiable formula in CNF and π be a configurational PCR refutation for $P_F[\oplus]$ with $\text{MSpace}(\pi) = w$ and size t. Then there exists a $(w, 2t)$-contradicting list $L_0 \ldots L_{2t}$ for F.*

Proof. Let $\pi = \mathbb{M}_0, \ldots, \mathbb{M}_r$ be the configurational PCR refutation for $P_F[\oplus]$. In a step in π a polynomial p is either added or removed from a configuration in π. In the XORirfied formula

$F[\oplus]$ each variable x in F is substituted by two new variables x_0 and x_1. Also since we are dealing with a PCR refutation, for each variable $x_a, a \in \{0,1\}$ in $P_F[\oplus]$ there is a twin variable x'_a. We will call x_0, x_1, x'_0, x'_1 the expansion variables to x and x is the projection of any of these variables.

In a first step in the proof we will construct for each configuration $\mathbb{M}_i$ in π a set of variables $L_i \subseteq \text{Var}(F)$ and define a partial assignment γ_i assigning some expansion of variables in L_i. In a second step we will show that $L_0, \ldots, L_r$ is a contradicting list for L by proving that any locally consistent sequence of assignments for this list, defines for each step i an extension of γ_i that would give value 0 to all polynomials in $\mathbb{M}_i$[3], which is a contradiction since $\mathbb{M}_r = 1$.

If we count each time a monomial is added to a configuration in π or deleted from it we it get twice the number of monomials in π (counted with repetitions) and therefore the number of steps is at most twice the size of π, since in each step π is modified by adding or deleting a whole polynomial, the number of list L_i is at most $r \leq 2t$.

L_i has at most as many variables as there are monomials in $\mathbb{M}_i$. The partial assignment $\gamma_i : \text{Var}(P_F[\oplus]) \to \{0,1\}$ assigns at each point exactly one of the expansions x_a, $a \in \{0,1\}$, of a variable $x \in L_i$ and it also automatically assigns the twin variables of x_a with the complementary value.

For some monomials $m \in \mathbb{M}_i$, we will distinguish one of its variables, denoted $d(m)$, assign $\gamma_i(d(m)) = 0$ and include the projection of this variable in L_i. The idea is that a monomial $m \in \mathbb{M}_i$ with a distinguished variable is always given value 0 by γ_i through this variable. At most one variable is distinguished in a monomial.

Given a list of variables L_i, a partial assignment γ_i as above, and a monomial m, we will say that m is covered by L_i, γ_i, if m does not have a distinguished variable but all its variables are expansions of variables in L_i. For example if $m = x_0 y_1 z'_1$ and $x, y, z \in L_i$ and $\gamma_i(x_1) = \gamma_i(y_0) = \gamma_i(z_0) = 0$ then m is covered by L_i. Concretely, $L_0 := \emptyset, \gamma_0 := \emptyset$ and for $i > 0$ if for all $j < i$ there is an extension of γ_j that satisfies $\mathbb{M}_j$ the following conditions hold for L_i and γ_i:

i) $||L_i|| \leq ||\{\text{monomials in } \mathbb{M}_i\}||$,

ii) γ_i assigns exactly one of the two expansion variables of each variable in L_i and its twin variable and

iii) every monomial remaining in $\mathbb{M}_i|_{\gamma_i}$ is covered by L_i, γ_i.

Construction of L_i and γ_i: $L_0 := \emptyset$ and we define L_i inductively. Each set L_{i+1} coincides with the previous one L_i or can be obtained by either adding one variable to L_i or deleting some. If $\mathbb{M}_{i+1}$ is an axiom download step, the axiom polynomial p can be either a complement axiom $(x_a + x'_a - 1)$ or a monomial m. For a complement axiom, if $x \in L_i$ then nothing has to be done, $L_{i+1} := L_i$ and $\gamma_{i+1} := \gamma_i$. In this case $p|_{\gamma i+1} = 0$ or all the monomials of p are covered. If $x \notin L_i$ then $L_{i+1} := L_i \cup \{x\}$ and $\gamma_{i+1} := \gamma_i \cup \{x_a = 0\}$. If the downloaded axiom is a monomial m then there are three possibilities: In case one of the variables of m is given value 0 by γ_i then this variable (any particular one if there is more than one) is defined to be the distinguished variable of m, $L_{i+1} := L_i$ and $\gamma_{i+1} := \gamma_i$. If this is not the case but all the variables in m are extensions of some variable in L_i, (m is covered) then nothing is done and $L_{i+1} := L_i, \gamma_{i+1} := \gamma_i$. Otherwise let x_a be some variable in m whose projection x is not in L_i. We set x_a to be the distinguished variable of m, $d(m) = x_a$, we add $\{x\}$ to L_{i+1} and the values $\{x_a = 0, x'_a = 1\}$ are assigned in γ_{i+1}. Observe that in all axiom download cases at least a new monomial is added to $\mathbb{M}_{i+1}$ and at most one variable is added to L_{i+1}.

[3]Since we are talking about a PCR refutation, we say that a partial assignment satisfies a monomial if some variable in it is assigned value 0, while the monomial is falsified if every variable in it receives value 1 from the assignment

If $\mathbb{M}_{i+1}$ adds the linear combination p of two polynomials $p_1, p_2 \in \mathbb{M}_i$ then since there aren't any new monomials nothing has to change in L_{i+1} or γ_{i+1} and the conditions still hold.

If $\mathbb{M}_{i+1}$ is a multiplication step of p times a variable x_a, if $p|_{\gamma_i} = 0$ then nothing has to be done. Otherwise, by induction all the monomials remaining after applying the partial assignment γ_i are covered. In case $x \in L_i$ then the monomials in $x_a p|_{\gamma_i}$ are either 0 or covered and nothing needs to be done to L_i. Otherwise we let $L_{i+1} := L_i \cup \{x\}$ and $\gamma_{i+1} := \gamma_i \cup \{x_a = 0\}$.

If $\mathbb{M}_{i+1}$ is obtained by deletion of a polynomial p we start a deletion phase by letting at the beginning of the phase $L_{i+1} := L_i$ and $\gamma_{i+1} := \gamma_i$. Then for each monomial $m \in p$ (in any order) if m is covered by L_{i+1} or it has some distinguished variable $d(m)$ and there is another monomial in $\mathbb{M}_{i+1}$ with the same distinguished variable, then there are no changes in L_{i+1} or γ_{i+1}. We have deleted one monomial, but for all variables in L_{i+1} there is a monomial in $\mathbb{M}_{i+1}$ having an expansion of this variable as distinguished variable and this assures that $||L_{i+1}|| \leq ||\mathbb{M}_{i+1}||$.

The remaining case is when a deleted monomial $m \in p$ has a distinguished variable $d(m) = x_a$ and there is no other monomial with this variable in $\mathbb{M}_{i+1}$. By the hypothesis of the construction, there is an extension of γ_i to the expansions of the variables in L_i that satisfies $\mathbb{M}_i$. This extension of γ_i assigns $x_a = 0$. Let $y_{\bar{a}}$ be the variable in $\{x_{\bar{a}}, x'_{\bar{a}}\}$ assigned 0 in the extension of γ_i satisfying $\mathbb{M}_i$. If $y_{\bar{a}}$ does not appear in a monomial in $\mathbb{M}_{i+1}$ covered by L_i, then we can delete x from L_{i+1}. If $y_{\bar{a}}$ appears in some monomial in $\mathbb{M}_{i+1}$ covered by L_{i+1}, then we consider $y_{\bar{a}}$ to be the distinguished variable of the covered monomials in which it appears, and update $\gamma_{i+1} := \gamma_{i+1} \cup \{y_{\bar{a}} = 0\} \setminus \{x_a = 0\}$. An extension of γ_{i+1} satisfies $\mathbb{M}_{i+1}$. Moreover, it does not matter what the value for x_a in this extension is, since x_a does not appear in any monomial in $\mathbb{M}_{i+1}$. Also for every variable x in L_{i+1} there is some monomial in $\mathbb{M}_{i+1}$ having an extension of x as distinguished variable.

This ends the construction of the variable lists L_i and partial assignments γ_i.

Let $j \leq r$ be the first point in the construction in which no extension of γ_j to the expansion variables of L_j satisfies $\mathbb{M}_j$. Such a j must exist since at some point $\mathbb{M}_j$ is unsatisfiable. We show that the list of variable sets $L_0, \ldots, L_j$ is a contradicting list for F. This is done by proving the following claim:

Claim: If there is a locally consistent sequence of partial assignments $\beta_0, \ldots, \beta_j$ of the variables in $L_0, \ldots, L_j$, that do not negate any axiom of F then there is a sequence of assignments $\hat{\gamma_1}, \ldots, \hat{\gamma_j}$ with the following properties for $0 \leq i \leq j$:

- $\hat{\gamma_i}$ assigns all expansion variables of L_i,
- $\hat{\gamma_i}$ is consistent with γ_i,
- $\hat{\gamma_i}$ satisfies all the polynomials in the configuration $\mathbb{M}_i$ and does not falsify any axiom of $P_F[\oplus]$.

The existence of such sequence of assignments would be a contradiction since we are supposing that no extension of γ_j satisfies $\mathbb{M}_j$. This proves that L is a (w, j) contradicting list.

To clarify things, let us recall that we are dealing with three different sequences of partial assignments in the proof: γ_i is the assignment constructed while creating the list L, β_i is the assignment of the projected variables in the list, whose existence we are supposing in order to reach a contradiction, and $\hat{\gamma_i}$ is the extension of γ_i based on β_i that would satisfy $\mathbb{M}_i$, thus creating a contradiction.

Proof of the claim. Suppose there is a locally consistent sequence of assignments $\beta_0, \ldots, \beta_j$ of $L_0, \ldots, L_j$ that do not falsify any axiom in F. We show inductively on i, $0 \leq i \leq j$ that for every variable $x \in L_i$, there is a way to translate $\beta_i(x)$ to the extension variables x_0, x_1 obtaining an assignment $\hat{\gamma_i}$ satisfying the properties above. This is done by defining $\hat{\gamma_i}$ fulfilling

the condition $\hat{\gamma}_i(x_0) \oplus \hat{\gamma}_i(x_1) = \neg\beta_i(x)$[4]. Observe that once the assignment $\beta_i(x)$ is set, there are two ways to define $\hat{\gamma}_i$ on the expansion variables of x that satisfy the condition. It also holds that if β_i does not falsify any axiom in F, then $\hat{\gamma}_i$ cannot falsify an axiom in $P_F[\oplus]$. This is because if $\hat{\gamma}_i$ would falsify a polynomial axiom A in $P_F[\oplus]$, since $A \in B[\oplus]$ for some clause axiom B from F and $\hat{\gamma}_i(A) = 1$ then for every variable $x \in B$, $\hat{\gamma}_i(x_0 \oplus x_1) = 1$. But since $\neg\beta_i(x) = \hat{\gamma}_i(x_0) \oplus \hat{\gamma}_i(x_1) = \hat{\gamma}_i(x_0 \oplus x_1)$ this means that for every variable $x \in B$, $\beta_i(x) = 0$ and β_i would falsify axiom B, which is a contradiction.

We show inductively for every step i that the claim holds. Initially $\hat{\gamma}_0$ and β_0 are the empty assignment. At each step one polynomial is added or deleted from a configuration.

Case 1: At step $i+1$ a new polynomial p is added to the configuration. We consider the different possibilities:

- If $i+1$ is an axiom download step and a new complement polynomial $p = (x_a + x'_a - 1)$ is added, then by the way the partial assignment γ_{i+1} is defined, giving always complementary values to twin variables, it must satisfies p (and therefore $\mathbb{M}_{i+1}$).
- If $i+1$ is an axiom download step and the downloaded axiom is a monomial m, again there can be several cases.
  - If m has some distinguished variable x_a with $\gamma_i(x_a) = 0$ then $L_{i+1} = L_i$, and therefore $\beta_{i+1} = \beta_i$ and $\gamma_{i+1} = \gamma_i$ By induction hypothesis $\hat{\gamma}_i(x_a) = 0$. Defining $\hat{\gamma}_{i+1} := \hat{\gamma}_i$ all properties are satisfied.
  - If m is covered by L_i, γ_i then again $L_{i+1} = L_i, \gamma_{i+1} = \gamma_i$, and $\beta_{i+1} = \beta_i$. We can define $\hat{\gamma}_{i+1} := \hat{\gamma}_i$. The induction hypothesis implies that $\hat{\gamma}_i$ satisfies $\mathbb{M}_i$ and it does not falsify any axiom in $P_F[\oplus]$.
  - The third possibility is that m has a new distinguished variable $d(m) = x_a$ and its projection x is not in L_i. In this case, x is assigned by β_{i+1} in this step. It is always possible to translate $\beta_{i+1}(x)$ to x_0 and x_1 in one of the two possible ways, so that $\hat{\gamma}_{i+1}$ satisfies x_a and therefore also m.
- If $i+1$ is a linear combination step of polynomials in $\mathbb{M}_i$ introducing a new polynomial p, then $L_{i+1} = L_i$ and defining $\hat{\gamma}_{i+1} := \hat{\gamma}_i$ the assignment satisfies p and $\mathbb{M}_{i+1}$.
- If M_{i+1} is a multiplication step of a polynomial $p \in \mathbb{M}_i$ introducing a new polynomial $x_a p$ for some variable x_a, by hypothesis $\hat{\gamma}_i$ satisfies $\mathbb{M}_i$ and therefore also p and $x_a p$. If $L_{i+1} = L_i$ then $\hat{\gamma}_{i+1} = \hat{\gamma}_i$ satisfies $x_a p$. Otherwise L_{i+1} has a new variable x_a and $\hat{\gamma}_{i+1}$ assigns value to it, but it also satisfies $\mathbb{M}_{i+1}$

Case 2: If in step $i+1$ a polynomial p is removed from the configuration, then for every deleted monomial $m \in p$ the only problem could come when a variable $x_a \in m$ is not deleted going from L_i to L_{i+1} but the assignment γ changes from assigning x_a in γ_i to assigning $x_{\bar{a}}$ in γ_{i+1} and $\gamma_{i+1}(x_a)$ might be different from $\gamma_i(x_{\bar{a}})$. We have $\beta_{i+1} = \beta_i$ and by induction $\hat{\gamma}_i$ satisfies $\mathbb{M}_i$ and therefore also $\mathbb{M}_{i+1}$ since $i+1$ is a deletion step. Also $\hat{\gamma}_i$ is consistent with γ_i. One can define $\hat{\gamma}_{i+1}(x_{\bar{a}}) = \gamma_{i+1}(x_{\bar{a}})$ and $\hat{\gamma}_{i+1}(x_a) = \gamma_{i+1}(x_{\bar{a}}) \oplus \neg\beta_i(x)$. Observe that the sequence of $\hat{\gamma}$ assignments might not be locally consistent on $\mathbb{M}$ at this point, but $\hat{\gamma}_{i+1}$ still satisfies $\mathbb{M}_{i+1}$ since as argued before, changing the value of x_a cannot falsify any monomial in $\mathbb{M}_{i+1}$. All the other values are as in $\hat{\gamma}_i$. Also since the property $\hat{\gamma}_{i+i}(x_a) \oplus \hat{\gamma}_{i+i}(x_{\bar{a}}) = \neg\beta_{i+i}(x)$ is kept, $\hat{\gamma}_{i+1}$ cannot falsify any axiom in $P_F[\oplus]$.

□

[4]We have a negation here in frot of β since we are supposing F is a CNF and P_F is its encoding as a set of polynomials.

Theorem 30 shows that for any unsatisfiable formula F, and any configurational proof π with clause space w and size t of $F[\oplus]$ there is a $(w, 2t)$-contradicting list for F. The contradicting list L we have constructed in the theorem does not necessarily fulfill the second condition of Definition 29 since when deleting variables from the list, several variables can be deleted while going form one variable list to the next one. As noticed in the observation under Definition 29, this however does not affect the property that from the contradicting list a semantic Resolution refutation with the same number of variable space and time can be obtained [GTT18]. Using this fact, the result can be restated as:

Corollary 31. *Let F be an unsatisfiable formula in CNF and π be a configurational PCR refutation for $P_F[\oplus]$ with $\mathrm{MSpace}(\pi) = w$ and size t. Then there exists a semantic Resolution refutation for F with variable space w and time $2t$.*

This improves the parameters from Theorem 9 in [BNT13] and can be used to slightly improve the time-space tradeoffs for pebbling formulas given in the reference. For pebbling formulas, using the correspondence between variable space and black-white pebbling from Subsection 4.1 it follows:

Theorem 32. *For any single sink DAG G, $\mathrm{MSpace}_{\mathrm{PCR}}(\mathrm{Peb}(G)[\oplus]) \geq \mathsf{BW}(G)$.*

This solves Open Problem 7.11 from [BN21]. It is known that for any DAG with constant in-degree, $\mathrm{Peb}(G)[\oplus]$ can be refuted in PCR within constant degree [BN11]. It is also well known that there are explicitly constructible graph families $\{G_n\}_{n=0}^{\infty}$ having $\Theta(n)$ vertices and in-degree 2 and with $\mathsf{BW}(G_n) = \Omega(\frac{n}{\log n})$ [GT78]. Since the results in this paper are independent of the field used, this also implies:

Corollary 33. *There is a family $\{F_n\}_{n=0}^{\infty}$ of formulas in 6-CNF having $\Theta(n)$ variables that have PCR refutations with constant degree and require monomial space $\Omega(\frac{n}{\log n})$ and this is independent of the characteristic of the field.*

References

[ABRW02] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002. Preliminary version in *STOC '00*.

[AM13] 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*.

[BCIP02] 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*.

[Ben89] Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM Journal on Computing*, 18(4):766–776, 1989.

[Ben09] Eli Ben-Sasson. Size-space tradeoffs for resolution. *SIAM Journal on Computing*, 38(6):2511–2525, May 2009. Preliminary version in *STOC '02*.

[BG15] 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.

[BIK+94] 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.

[BN08] Eli Ben-Sasson and Jakob Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pages 709–718, October 2008.

[BN11] Eli Ben-Sasson and Jakob Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Proceedings of the 2nd Symposium on Innovations in Computer Science (ICS '11)*, pages 401–416, January 2011.

[BN21] Sam Buss and Jakob Nordström. Proof complexity and SAT solving. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability - Second Edition*, volume 336 of *Frontiers in Artificial Intelligence and Applications*, pages 233–350. IOS Press, 2021.

[BNT13] 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.

[BW01] 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*.

[CEI96] 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.

[CLNV15] 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.

[CS76] 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*.

[dRMNR21] 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.

[FLM+13] Yuval Filmus, Massimo Lauria, Mladen Mikša, Jakob Nordström, and Marc Vinyals. Towards an understanding of polynomial calculus: New separations and lower bounds (Extended abstract). In *Proceedings of the 40th International Colloquium on Automata, Languages and Programming (ICALP '13)*, volume 7965 of *Lecture Notes in Computer Science*, pages 437–448. Springer, July 2013.

[GKT19] Nicola Galesi, Leszek Aleksander Kolodziejczyk, and Neil Thapen. Polynomial calculus space and resolution width. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019*, pages 1325–1337. IEEE Computer Society, 2019.

[GP17] 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.

[GT78] John R. Gilbert and Robert Endre Tarjan. Variations of a pebble game on graphs. Technical Report STAN-CS-78-661, Stanford University, 1978. Available at `http://infolab.stanford.edu/TR/CS-TR-78-661.html`.

[GTT18] Nicola Galesi, Navid Talebanfard, and Jacobo Torán. Cops-robber games and the resolution of Tseitin formulas. In *Proceedings of the 21th International Conference on Theory and Applications of Satisfiability Testing (SAT '18)*, volume 10929 of *Lecture Notes in Computer Science*, pages 311–326. Springer, 2018.

[Her08] Alexander Hertel. *Applications of Games to Propositional Proof Complexity*. PhD thesis, University of Toronto, May 2008. Available at `http://www.cs.utoronto.ca/~ahertel/`.

[Imm81] Neil Immerman. Number of quantifiers is better than number of tape cells. *J. Comput. Syst. Sci.*, 22(3):384–406, 1981.

[Nor13] Jakob Nordström. Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science*, 9:15:1–15:63, September 2013.

[Nor15] 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.

[PH70] 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.

[Pip80] Nicholas Pippenger. Pebbling. Technical Report RC8258, IBM Watson Research Center, 1980.

[PTC77] Wolfgang J. Paul, Robert Endre Tarjan, and James R. Celoni. Space bounds for a game on graphs. *Mathematical Systems Theory*, 10:239–251, 1977.

[Sav98] John E. Savage. *Models of computation - exploring the power of computing*. Addison-Wesley, 1998.

[ST13] Uwe Schöning and Jacobo Torán. *The Satisfiability Problem: Algorithms and Analyses*, volume 3 of *Mathematics for Applications (Mathematik für Anwendungen)*. Lehmanns Media, 2013.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il