Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 1 (2020)

Nullstellensatz Size-Degree Trade-offs from Reversible Pebbling*

Susanna F. de Rezende
Mathematical Institute of the
Czech Academy of Sciences

Jakob Nordström
University of Copenhagen and
KTH Royal Institute of Technology

Or Meir
University of Haifa

Robert Robere
DIMACS and
Institute for Advanced Study

January 7, 2020

Abstract

We establish an exactly tight relation between reversible pebblings of graphs and Nullstellensatz refutations of pebbling formulas, showing that a graph G can be reversibly pebbled in time t and space s if and only if there is a Nullstellensatz refutation of the pebbling formula over G in size $t+1$ and degree s (independently of the field in which the Nullstellensatz refutation is made). We use this correspondence to prove a number of strong size-degree trade-offs for Nullstellensatz, which to the best of our knowledge are the first such results for this proof system.

1 Introduction

In this work, we obtain strong trade-offs in proof complexity by making a connection to pebble games played on graphs. In this introductory section we start with a brief overview of these two areas and then explain how our results follow from connecting the two.

1.1 Proof Complexity

Proof complexity is the study of efficiently verifiable certificates for mathematical statements. More concretely, statements of interest claim to provide correct answers to questions like:

- Given a CNF formula, does it have a satisfying assignment or not?
- Given a set of polynomials over some finite field, do they have a common root?

There is a clear asymmetry here in that it seems obvious what an easily verifiable certificate for positive answers to the above questions should be, while it is not so easy to see what a concise certificate for a negative answer could look like. The focus of proof complexity is therefore on the latter scenario.

In this paper we study the algebraic proof system system *Nullstellensatz* introduced by Beame et al. [BIK+94]. A *Nullstellensatz refutation* of a set of polynomials $\mathcal{P} = \{p_i \mid i \in [m]\}$ with coefficients in a field $\mathbb{F}$ is an expression

$$\sum_{i=1}^{m} r_i \cdot p_i + \sum_{j=1}^{n} s_j \cdot (x_j^2 - x_j) = 1 \tag{1.1}$$

(where r_i, s_j are also polynomials), showing that 1 lies in the polynomial ideal in the ring $\mathbb{F}[x_1, \ldots, x_n]$ generated by $\mathcal{P} \cup \{x_j^2 - x_j \mid j \in [n]\}$. By (a slight extension of) Hilbert's Nullstellensatz, such a refutation exists if and only if there is no common $\{0,1\}$-valued root for the set of polynomials $\mathcal{P}$.

*A preliminary version of this work appeared in CCC 2019.

ISSN 1433-8092

Nullstellensatz can also be viewed as a proof system for certifying the unsatisfiability of CNF formulas. If we translate a clause like, e.g., $C = x \vee y \vee \overline{z}$ to the polynomial $p(C) = (1-x)(1-y)z = z - yz - xz + xyz$, then an assignment to the variables in a CNF formula $F = \bigwedge_{i=1}^{m} C_i$ (where we think of 1 as true and 0 as false) is satisfying precisely if all the polynomials $\{p(C_i) \mid i \in [m]\}$ vanish.

The *size* of a Nullstellensatz refutation (1.1) is the total number of monomials in all the polynomials $r_i \cdot p_i$ and $s_j \cdot (x_j^2 - x_j)$ expanded out as linear combinations of monomials. Another, more well-studied, complexity measure for Nullstellensatz is *degree*, which is defined as $\max\{\deg(r_i \cdot p_i), \deg(s_j \cdot (x_j^2 - x_j))\}$.

In order to prove a lower bound d on the Nullstellensatz degree of refuting a set of polynomials $\mathcal{P}$, one can construct a d-*design*, which is a map D from degree-d polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ to $\mathbb{F}$ such that

1. D is linear, i.e., $D(\alpha p + \beta q) = \alpha D(p) + \beta D(q)$ for $\alpha, \beta \in \mathbb{F}$;

2. $D(1) = 1$;

3. $D(rp) = 0$ for all $p \in \mathcal{P}$ and $r \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\deg(rp) \leq d$;

4. $D(x^2 s) = D(xs)$ for all $s \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\deg(s) \leq d - 2$.

Designs provide a characterization of Nullstellensatz degree in that there is a d-design for $\mathcal{P}$ if and only if there is no Nullstellensatz refutation of $\mathcal{P}$ in degree d [Bus98]. Another possible approach to prove degree lower bounds is by computationally efficient versions of Craig's interpolation theorem. It was shown in [PS98] that constant-degree Nullstellensatz refutations yield polynomial-size monotone span programs, and that this is also tight: every span program is a unique interpolant for some set of polynomials refutable by Nullstellensatz. This connection has not been used to obtain Nullstellensatz degree lower bounds, however, due to the difficulty of proving span program lower bounds.

Lower bounds on Nullstellensatz degree have been proven for sets of polynomials encoding combinatorial principles such as the pigeonhole principle [BCE+98], induction principle [BP98], housesitting principle [CEI96, Bus98], matching [BIK+97], and pebbling [BCIP02]. It seems fair to say that research in algebraic proof complexity soon moved on to stronger systems such as *polynomial calculus* [CEI96, ABRW02], where the proof that 1 lies in the ideal generated by $\mathcal{P} \cup \{x_j^2 - x_j \mid j \in [n]\}$ can be constructed dynamically by a step-by-step derivation. However, the Nullstellensatz proof system has been the focus of renewed interest in a recent line of works [RPRC16, PR17, PR18, dRMN+19] showing that Nullstellensatz lower bounds can be lifted to stronger lower bounds for more powerful computational models using composition with gadgets. The size complexity measure for Nullstellensatz has also received attention in recent papers such as [Ber18, AO19].

In this work, we are interested in understanding the relation between size and degree in Nullstellensatz. In this context it is relevant to compare and contrast Nullstellensatz with polynomial calculus as well as with the well-known *resolution* proof system [Bla37], which operates directly on the clauses of a CNF formula and repeatedly derives resolvent clauses $C \vee D$ from clauses of the form $C \vee x$ and $D \vee \overline{x}$ until contradiction, in the form of the empty clause without any literals, is reached. For resolution, size is measured by counting the number of clauses, and *width*, measured as the number of literals in a largest clause in a refutation, plays an analogous role to degree for Nullstellensatz and polynomial calculus.

By way of background, it is not hard to show that for all three proof systems upper bounds on degree/width imply upper bounds on size, in the sense that if a CNF formula over n variables can be refuted in degree/width d, then such a refutation can be carried out in size $n^{O(d)}$. Furthermore, this upper bound has been proven to be tight up to constant factors in the exponent for resolution and polynomial calculus [ALN16], and it follows from [LLMO09] that this also holds for Nullstellensatz. In the other direction, it has been shown for resolution and polynomial calculus that strong enough lower bounds on degree/width imply lower bounds on size [IPS99, BW01]. This is known to be false for Nullstellensatz, and the pebbling formulas discussed in more detail later in this paper provide a counter-example [BCIP02].

The size lower bounds in terms of degree/width in [IPS99, BW01] can be established by transforming refutations in small size to refutations in small degree/width. This procedure blows up the size of the refutations exponentially, however. It is natural to ask whether such a blow-up is necessary or whether it is just an artifact of the proof. More generally, given that a formula has proofs in small size and small degree/width, it is an interesting question whether both measures can be optimized simultaneously, or whether there has to be a trade-off between the two.

For resolution this question was finally answered in [Tha16], which established that there are indeed strong trade-offs between size and width making the size blow-up in [BW01] unavoidable. For polynomial calculus, the analogous question remains open.

In this paper, we show that there are strong trade-offs between size and degree for Nullstellensatz. We do so by establishing a tight relation between Nullstellensatz refutations of pebbling formulas and reversible pebblings of the graphs underlying such formulas. In order to discuss this connection in more detail, we first need to describe what reversible pebblings are. This brings us to our next topic.

1.2 Pebble Games

In the *pebble game* first studied by Paterson and Hewitt [PH70], one places pebbles on the vertices of a directed acyclic graph (DAG) G according to the following rules:

- If all (immediate) predecessors of an empty vertex v contain pebbles, a pebble may be placed on v.
- A pebble may be removed from any vertex at any time.

The game starts and ends with the graph being empty, and a pebble should be placed on the (unique) sink of G at some point. The complexity measures to minimize are the total number of pebbles on G at any given time (the *pebbling space*) and the number of moves (the *pebbling time*).

The pebble game has been used to study flowcharts and recursive schemata [PH70], register allocation [Set75], time and space as Turing-machine resources [Coo74, HPV77], and algorithmic time-space trade-offs [Cha73, SS77, SS79, SS83, Tom78]. In the last two decades, pebble games have seen a revival in the context of proof complexity (see, e.g., [Nor13]), and pebbling has also turned out to be useful for applications in cryptography [DNW05, AS15]. An excellent overview of pebbling up to ca. 1980 is given in [Pip80] and some more recent developments are covered in the upcoming survey [Nor20].

Bennett [Ben89] introduced the *reversible pebble game* as part of a broader program [Ben73] aimed at eliminating or reducing energy dissipation during computation. Reversible pebbling has also been of interest in the context of quantum computing. For example, it was noted in [MSR+19] that reversible pebble games can be used to capture the problem of “uncomputing” intermediate values in quantum algorithms.

The reversible pebble game adds the requirement that the whole pebbling performed in reverse order should also be a correct pebbling, which means that the rules for pebble placement and removal become symmetric as follows:

- If all predecessors of an empty vertex v contain pebbles, a pebble may be placed on v.
- If all predecessors of a pebbled vertex v contain pebbles, the pebble on v may be removed.

Reversible pebblings have been studied in [LV96, Krá04, KSS18] and have been used to prove time-space trade-offs in reversible simulation of irreversible computation in [LTV98, LMT00, Wil00, BTV01]. In a different context, Potechin [Pot10] implicitly used reversible pebbling to obtain lower bounds in monotone space complexity, with the connection made explicit in later works [CP14, FPRC13]. The paper [CLNV15] (to which this overview is indebted) studied the relative power of standard and reversible pebblings with respect to space, and also established PSPACE-hardness results for estimating the minimum space required to pebble graphs (reversibly or not).

1.3 Our Contributions

In this paper, we obtain an exactly tight correspondence between on the one hand reversible pebblings of DAGs and on the other hand Nullstellensatz refutations of pebbling formulas over these DAGs. We show that for any DAG G it holds that G can be reversibly pebbled in time t and space s if and only if there is a Nullstellensatz refutation of the pebbling formula over G in size $t+1$ and degree s. This correspondence holds regardless of the field in which the Nullstellensatz refutation is operating, and so, in particular, it follows that pebbling formulas have exactly the same complexity for Nullstellensatz regardless of the ambient field.

We then revisit the time-space trade-off literature for the standard pebble game, focusing on the papers [CS80, CS82, LT82]. The results in these papers do not immediately transfer to the reversible pebble game, and we are not fully able to match the tightness of the results for standard pebbling, but we nevertheless obtain strong time-space trade-off results for the reversible pebble game.

This allows us to derive Nullstellensatz size-degree trade-offs from reversible pebbling time-space trade-offs as follows. Suppose that we have a DAG G such that:

1. G can be reversibly pebbled in time $t_1 \ll t_2$.
2. G can be reversibly pebbled in space $s_1 \ll s_2$.
3. There is no reversible pebbling of G that simultaneously achieves time t_1 and space s_1.

Then for Nullstellensatz refutations of the pebbling formula Peb_G over G (which will be formally defined shortly) we can deduce that:

1. Nullstellensatz can refute Peb_G in size $t_1+1 \ll t_2+1$.
2. Nullstellensatz can also refute Peb_G in degree $s_1 \ll s_2$.
3. There is no Nullstellensatz refutation of Peb_G that simultaneously achieves size t_1+1 and degree s_1.

We prove four such trade-off results, which can be found in Section 4. The following theorem is one example of such a result (specifically, it is a simplified version of Theorem 4.1).

Theorem 1.1. *There is a family of* 3*-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\Theta(n)$ *such that:*

1. *There is a Nullstellensatz refutation of* F_n *in degree* $s_1 = \mathrm{O}\big(\sqrt[6]{n}\log n\big)$.
2. *There is a Nullstellensatz refutation of* F_n *of near-linear size and degree* $s_2 = \mathrm{O}\big(\sqrt[3]{n}\log n\big)$.
3. *Any Nullstellensatz refutation of* F_n *in degree at most* $\sqrt[3]{n}$ *must have exponential size.*

It should be noted that this is not the first time proof complexity trade-off results have been obtained from pebble games. Pebbling formulas were used in [Ben09, BN11] to obtain size-space trade-offs for resolution, and later in [BNT13] also for polynomial calculus. However, the current reductions between pebbling and Nullstellensatz are much stronger in that they go in both directions and are exact even up to additive constants.

With regard to Nullstellensatz, it was shown in [BCIP02] that Nullstellensatz degree is lower-bounded by standard pebbling price. This was strengthened in [dRMN+19], which used the connection between designs and Nullstellensatz degree discussed above to establish that the degree needed to refute a pebbling formula exactly coincides with the reversible pebbling price of the corresponding DAG (which is always at least the standard pebbling price, but can be much larger). Our reduction significantly improves on [dRMN+19] by constructing a more direct reduction, inspired by [GKRS18], that can simultaneously capture both time and space.

1.4 Outline of This Paper

After having discussed the necessary preliminaries in Section 2, we present the reductions between Nullstellensatz and reversible pebblings in Section 3. In Section 4, we prove time-space trade-offs for reversible pebblings in order to obtain size-degree trade-offs for Nullstellensatz. Section 5 contains some concluding remarks with suggestions for future directions of research.

2 Preliminaries

All logarithms in this paper are base 2 unless otherwise specified. For a positive integer n we write $[n]$ to denote the set of integers $\{1, 2, \ldots, n\}$.

A *literal* a over a Boolean variable x is either the variable x itself or its negation $\overline{x}$ (a *positive* or *negative* literal, respectively). A *clause* $C = a_1 \vee \cdots \vee a_k$ is a disjunction of literals. A k-*clause* is a clause that contains at most k literals. A formula F in *conjunctive normal form (CNF)* is a conjunction of clauses $F = C_1 \wedge \cdots \wedge C_m$. A k-*CNF formula* is a CNF formula consisting of k-clauses. We think of clauses and CNF formulas as sets, so that the order of elements is irrelevant and there are no repetitions. A truth value assignment ρ to the variables of a CNF formula F is satisfying if every clause in F contains a literal that is true under ρ.

2.1 Nullstellensatz

Let $\mathbb{F}$ be any field and let $\vec{x} = \{x_1, \ldots, x_n\}$ be a set of variables. We identify a set of polynomials $\mathcal{P} = \{p_i(\vec{x}) \mid i \in [m]\}$ in the ring $\mathbb{F}[\vec{x}]$ with the statement that all $p_i(\vec{x})$ have a common $\{0,1\}$-valued root. A *Nullstellensatz refutation* of this claim is a syntactic equality

$$\sum_{i=1}^{m} r_i(\vec{x}) \cdot p_i(\vec{x}) + \sum_{j=1}^{n} s_j(\vec{x}) \cdot (x_j^2 - x_j) = 1 \ , \tag{2.1}$$

where r_i, s_j are also polynomials in $\mathbb{F}[\vec{x}]$. We sometimes refer to the polynomials $p_i(\vec{x})$ as axioms and $(x_j^2 - x_j)$ as Boolean axioms.

As discussed in the introduction, Nullstellensatz can be used as a proof system for CNF formulas by translating a clause $C = \bigvee_{x \in P} x \vee \bigvee_{y \in N} \overline{y}$ to the polynomial $p(C) = \prod_{x \in P}(1 - x) \cdot \prod_{y \in N} y$ and viewing Nullstellensatz refutations of $\{p(C_i) \mid i \in [m]\}$ as refutations of the CNF formula $F = \bigwedge_{i=1}^{m} C_i$.

The *degree* of a Nullstellensatz refutation (1.1) is $\max\{\deg(r_i(\vec{x}) \cdot p_i(\vec{x})), \deg(s_j(\vec{x}) \cdot (x_j^2 - x_j))\}$. We define the *size* of a refutation (2.1) to be the total number of monomials encountered when all products of polynomials are expanded out as linear combinations of monomials. To be more precise, let $mSize(p)$ denote the number of monomials in a polynomial p written as a linear combination of monomials. Then the size of a Nullstellensatz refutation on the form (1.1) is

$$\sum_{i=1}^{m} mSize\big(r_i(\vec{x})\big) \cdot mSize\big(p_i(\vec{x})\big) + \sum_{j=1}^{n} 2 \cdot mSize\big(s_j(\vec{x})\big) \ . \tag{2.2}$$

This is consistent with how size is defined for the "dynamic version" of Nullstellensatz known as polynomial calculus [CEI96, ABRW02], and also with the general size definitions for so-called algebraic and semialgebraic proof systems in [ALN16, Ber18, AO19].

We remark that this is not the only possible way of measuring size, however. It can be noted that the definition (2.2) is quite wasteful in that it forces us to represent the proof in a very inefficient way. Other papers in the semialgebraic proof complexity literature, such as [GHP02, KI06, DMR09], instead define size in terms of the polynomials in isolation, more along the lines of

$$\sum_{i=1}^{m} \Big(mSize\big(r_i(\vec{x})\big) + mSize\big(p_i(\vec{x})\big)\Big) + \sum_{j=1}^{n} \Big(mSize\big(s_j(\vec{x})\big) + 2\Big) \ , \tag{2.3}$$

or as the bit size or "any reasonable size" of the representation of all polynomials $r_i(\vec{x}), p_i(\vec{x})$, and $s_j(\vec{x})$.

In the end, the difference is not too important since the two measures (2.2) and (2.3) are at most a square apart, and for size we typically want to distinguish between polynomial and superpolynomial. In addition, and more importantly, in this paper we will only deal with k-CNF formulas with $k = \mathrm{O}(1)$, and in this setting the two definitions are the same up to a constant factor 2^k. Therefore, we will stick with (2.2), which matches best how size is measured in the closely related proof systems resolution and polynomial calculus, and which gives the cleanest statements of our results.[1]

When proving lower bounds for algebraic proof systems it is often convenient to consider a *multilinear* setting where refutations are presented in the ring $\mathbb{F}[\vec{x}]/\{x_j^2 - x_j \mid j \in [n]\}$. Since the Boolean axioms $x_j^2 - x_j$ are no longer needed, the refutation (2.1) can be written simply as

$$\sum_{i=1}^{m} r_i(\vec{x}) \cdot p_i(\vec{x}) = 1 \quad , \tag{2.4}$$

where we assume that all results of multiplications are implicitly multilinearized. It is clear that any refutation on the form (2.1) remains valid after multilinearization, and so the size and degree measures can only decrease in a multilinear setting. In this paper, we prove our lower bound in our reduction in the multilinear setting and the upper bound in the non-multilinear setting, making the tightly matching results even stronger.

2.2 Reversible Pebbling and Pebbling Formulas

Throughout this paper $G = (V, E)$ denotes a directed acyclic graph (DAG) of constant fan-in with vertices $V(G) = V$ and edges $E(G) = E$. For an edge $(u, v) \in E$ we say that u is a *predecessor* of v and v a *successor* of u. We write $\mathit{pred}_G(v)$ to denote the sets of all predecessors of v, and drop the subscript when the DAG is clear from context. Vertices with no predecessors/successors are called *sources*/*sinks*. Unless stated otherwise we will assume that all DAGs under consideration have a unique sink z.

A *pebble configuration* on a DAG $G = (V, E)$ is a subset of vertices $\mathbb{P} \subseteq V$. A *reversible pebbling strategy* for a DAG G with sink z, or a *reversible pebbling* of G for short, is a sequence of pebble configurations $\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_t)$ such that $\mathbb{P}_0 = \mathbb{P}_t = \emptyset$, $z \in \bigcup_{0 \le t \le t} \mathbb{P}_t$, and such that each configuration can be obtained from the previous one by one of the following rules:

1. $\mathbb{P}_{i+1} = \mathbb{P}_i \cup \{v\}$ for $v \notin \mathbb{P}_i$ such that $\mathit{pred}_G(v) \subseteq \mathbb{P}_i$ (a *pebble placement* on v).
2. $\mathbb{P}_{i+1} = \mathbb{P}_i \setminus \{v\}$ for $v \in \mathbb{P}_i$ such that $\mathit{pred}_G(v) \subseteq \mathbb{P}_i$ (a *pebble removal* from v).

The *time* of a pebbling $\mathcal{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_t)$ is $\mathsf{time}(\mathcal{P}) = t$ and the *space* is $\mathsf{space}(\mathcal{P}) = \max_{0 \le t \le t}\{|\mathbb{P}_t|\}$.

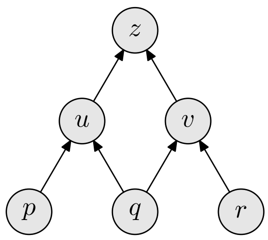
We could also say that a reversible pebbling $\mathcal{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_t)$ should be such that $\mathbb{P}_0 = \emptyset$ and $z \in \mathbb{P}_t$, and define the time of such a pebbling to be $2t$. This is so since once we have reached a configuration containing z we can simply run the pebbling backwards (because of reversibility) until we reach the empty configuration again, and without loss of generality all time- and space-optimal reversible pebblings can be turned into such pebblings. For simplicity, we will often take this viewpoint in what follows.

For technical reasons it is sometimes important to distinguish between *visiting pebblings*, for which $z \in \mathbb{P}_t$, and *persistent pebblings*, which meet the more stringent requirement that $z \in \mathbb{P}_t = \{z\}$. (It can be noted that for the more relaxed standard pebble game discussed in the introductory section any pebbling can be assumed to be persistent without loss of generality.)

Pebble games can be encoded in CNF by so-called *pebbling formulas* [BW01], or *pebbling contradictions*. Given a DAG $G = (V, E)$ with a single sink z, we associate a variable x_v with every vertex v and add clauses encoding that

- the source vertices are all true;
- if all immediate predecessors are true, then truth propagates to the successor;
- but the sink is false.

[1] We refer the reader to Section 2.4 in [AH18] for a more detailed discussion of the definition of proof size in algebraic and semialgebraic proof systems.



(a) Pyramid of height 2.

$$
\begin{aligned}
& x_p \\
\wedge\ & x_q \\
\wedge\ & x_r \\
\wedge\ & (\overline{x}_p \vee \overline{x}_q \vee x_u) \\
\wedge\ & (\overline{x}_q \vee \overline{x}_r \vee x_v) \\
\wedge\ & (\overline{x}_u \vee \overline{x}_v \vee x_z) \\
\wedge\ & \overline{x}_z
\end{aligned}
$$

(b) Pebbling formula in CNF.

$$
\begin{aligned}
& x_p - 1 \\
& x_q - 1 \\
& x_r - 1 \\
& x_p x_q (1 - x_u) \\
& x_q x_r (1 - x_v) \\
& x_u x_v (1 - x_z) \\
& x_z
\end{aligned}
$$

(c) Polynomial translation.

Figure 1: Example pebbling contradiction for the pyramid graph of height 2.

In short, the pebbling formula over G consists of the clauses $x_v \vee \bigvee_{u \in pred(v)} \neg x_u$ for all $v \in V$ (note that if v is a source $pred(v) = \emptyset$), and the clause $\neg x_z$.

We encode this formula by a set of polynomials in the standard way. Given a set $U \subseteq V$, we denote by x_U the monomial $\prod_{u \in U} x_u$ (in particular, $x_\emptyset = 1$). For every vertex $v \in V$, we have the polynomial

$$A_v := (1 - x_v) \cdot x_{\mathrm{pred}(v)} \quad , \tag{2.5}$$

and for the sink z we also have the polynomial

$$A_{\mathrm{sink}} := x_z \quad . \tag{2.6}$$

See Figure 1 for an illustration, including how the CNF formula is translated to a set of polynomials.

3 Reversible Pebblings and Nullstellensatz Refutations

In this section, we prove the correspondence between the reversible pebbling game on a graph G and Nullstellensatz refutation of the pebbling contradiction of G. Specifically, we prove the following result.

Theorem 3.1. *Let G be a directed acyclic graph with a single sink, let ϕ be the corresponding pebbling contradiction, and let $\mathbb{F}$ be a field. Then, there is a reversible pebbling strategy for G with time at most t and space at most s if and only if there is a Nullstellensatz refutation for ϕ over $\mathbb{F}$ of size at most $t + 1$ and degree at most s. Moreover, the same holds for multilinear Nullstellensatz refutations.*

We prove each of the directions of Theorem 3.1 separately in Sections 3.1 and 3.2 below.

3.1 From Pebbling to Refutation

We start by proving the "only if" direction of Theorem 3.1. Let

$$\mathbb{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_t) \tag{3.1}$$

be an optimal reversible pebbling strategy for G. Let $\mathbb{P}_{t'}$ be the first configuration in which there is a pebble on the sink z. Without loss of generality, we may assume that $t = 2 \cdot t'$: if the last $t - t'$ steps were more efficient than the first t' steps, we could have obtained a more efficient strategy by replacing the first t' steps with the (reverse of) the last $t - t'$ steps, and vice versa.

We use $\mathbb{P}$ to construct a Nullstellensatz refutation over $\mathbb{F}$ for the pebbling contradiction ϕ. To this end, we will first construct for each step $i \in [t']$ of $\mathbb{P}$ a Nullstellensatz derivation of the polynomial $x_{\mathbb{P}_{i-1}} - x_{\mathbb{P}_i}$. The sum of all these polynomials is a telescoping sum, and is therefore equal to

$$x_{\mathbb{P}_0} - x_{\mathbb{P}_{t'}} = 1 - x_{\mathbb{P}_{t'}} \quad . \tag{3.2}$$

We will then transform this sum into a Nullstellensatz refutation by adding the polynomial

$$x_{\mathbb{P}_{t'}} = A_{\mathrm{sink}} \cdot x_{\mathbb{P}_{t'} - \{z\}} \quad . \tag{3.3}$$

We turn to constructing the aforementioned derivations. To this end, for every $i \in [t']$, let $v_i \in V$ denote the vertex which was pebbled or unpebbled during the i-th step, i.e., during the transition from $\mathbb{P}_{i-1}$ to $\mathbb{P}_i$. Then, we know that in both configurations $\mathbb{P}_{i-1}$ and $\mathbb{P}_i$ the predecessors of v_i have pebbles on them, i.e., $\mathrm{pred}(v) \subseteq \mathbb{P}_{i-1}, \mathbb{P}_i$. Let us denote by $R_i = \mathbb{P}_i - \{v_i\} - \mathrm{pred}(v_i)$ the set of other vertices that have pebbles during the i-th step. Finally, let p_i be a number that equals to 1 if v_i was pebbled during the i-th step, and equals to -1 if v_i was unpebbled. Now, observe that

$$x_{\mathbb{P}_{i-1}} - x_{\mathbb{P}_i} = p_i \cdot x_{\mathbb{P}_{i-1}}(1 - x_{v_i}) = p_i \cdot x_{R_i} A_{v_i} \quad , \tag{3.4}$$

where the last step follows since the predecessors of v_i are necessarily in $\mathbb{P}_{i-1}$. Therefore, our final refutation for ϕ is

$$\begin{aligned} \sum_{i=1}^{t'} A_{v_i} \cdot p_i \cdot x_{R_i} + A_{\text{sink}} \cdot x_{\mathbb{P}_{t'} - \{z\}} &= x_{\mathbb{P}_{t'}} + \sum_{i=1}^{t'} x_{\mathbb{P}_{i-1}} - x_{\mathbb{P}_i} \\ &= x_{\mathbb{P}_{t'}} + (x_{\mathbb{P}_0} - x_{\mathbb{P}_{t'}}) \\ &= x_{\mathbb{P}_{t'}} + (1 - x_{\mathbb{P}_{t'}}) = 1 \quad . \end{aligned} \tag{3.5}$$

Note, in fact, it is a multilinear Nullstellensatz refutation, since it contains only multilinear monomials and does not use the Boolean axioms. It remains to analyze its degree and size.

For the degree, observe that every monomial in the proof is of the form $x_{\mathbb{P}_i}$, and the degree of each such monomial is exactly the number of pebbles used in the corresponding configuration. It follows that the maximal degree is exactly the space of the pebbling strategy $\mathbb{P}$.

Let us turn to considering the size. Observe that for each of the configurations $\mathbb{P}_1, \ldots, \mathbb{P}_{t'}$, the refutation contains exactly two monomials: for all $i \in [t' - 1]$, one monomial for $\mathbb{P}_i$ is generated in the i-th step, and another in the $(i + 1)$-th step, and for the configuration $\mathbb{P}_{t'}$ the second monomial is generated when we add $A_{\text{sink}} \cdot x_{\mathbb{P}_{t'} - \{z\}}$. In addition, the refutation contains exactly one monomial for the configuration $\mathbb{P}_0$, which is generated in the first step. Hence, the total number of monomials generated in the refutation is exactly $2 \cdot t' + 1 = t + 1$, as required.

3.2 From Refutation to Pebbling

We turn to prove the "if" direction of Theorem 3.1. We note that it suffices to prove it for multilinear Nullstellensatz refutations, since every standard Nullstellensatz refutation implies the existence of a multilinear one with at most the same size and degree. Let

$$\sum_{v \in V} A_v \cdot Q_v + A_{\text{sink}} \cdot Q_{\text{sink}} = 1 \tag{3.6}$$

be a multilinear Nullstellensatz refutation of ϕ over $\mathbb{F}$ of degree s. We use this refutation to construct a reversible pebbling strategy $\mathbb{P}$ for G.

To this end, we construct a "configuration graph" $\mathbb{C}$, whose vertices consist of all possible configurations of at most s pebbles on G (i.e., the vertices will be all subsets of V of size at most s). The edges of $\mathbb{C}$ will be determined by the polynomials Q_v of the refutation, and every edge $\{U_1, U_2\}$ in $\mathbb{C}$ will constitute a legal move in the reversible pebbling game (i.e., it will be legal to move from U_1 to U_2 and vice versa). We will show that $\mathbb{C}$ contains a path from the empty configuration $\emptyset$ to a configuration U_z that contains the sink z, and our pebbling strategy will be generated by walking on this path from $\emptyset$ to U_z and back.

The edges of the configuration graph $\mathbb{C}$ are defined as follows: Let $v \in V$ be a vertex of G, and let q be a monomial of Q_v that *does not contain* x_v. Let $W \subseteq V$ be the set of vertices such that $q = x_W$ (such a set W exists since the refutation is multilinear). Then, we put an edge e_q in $\mathbb{C}$ that connects $W \cup \mathrm{pred}(v)$ and $W \cup \mathrm{pred}(v) \cup \{v\}$ (we allow parallel edges). It is easy to see that the edge e_q connects configurations of size at most s, and that it indeed constitutes a legal move in the reversible pebbling game. We note that $\mathbb{C}$ is a bipartite graph: to see it, note that every edge e_q connects a configuration of an odd size to a configuration of an even size.

For the sake of the analysis, we assign the edge e_q a weight in $\mathbb{F}$ that is equal to coefficient of q in Q_v. We define *the weight of a configuration* U to be the sum of the weights of all the edges that touch U (where the addition is done in the field $\mathbb{F}$). We use the following technical claim, which we prove at the end of this section.

Claim 3.2. Let $U \subseteq V$ be a configuration in $\mathbb{C}$ that does not contain the sink z. If U is empty, then its weight is 1. Otherwise, its weight is 0.

We now show how to construct the required pebbling strategy $\mathbb{P}$ for G. To this end, we first prove that there is a path in $\mathbb{C}$ from the empty configuration to a configuration that contains the sink z. Suppose for the sake of contradiction that this is not the case, and let $\mathbb{H}$ be the connected component of $\mathbb{C}$ that contains the empty configuration. Our assumption says that none of the configurations in $\mathbb{H}$ contains z.

The connected component $\mathbb{H}$ is bipartite since $\mathbb{C}$ is bipartite. Without loss of generality, assume that the empty configuration is in the left-hand side of $\mathbb{H}$. Clearly, the sum of the weights of the configurations on the left-hand side should be equal to the corresponding sum on the right-hand side, since they are both equal to the sum of the weights of the edges in $\mathbb{H}$. However, the sum of the weights of the configurations on the right-hand side is 0 (since all these weights are 0 by Claim 3.2), while the sum of the weights of the left-hand side is 1 (again, by Claim 3.2). We reached a contradiction, and therefore $\mathbb{H}$ must contain some configuration U_z that contains the sink z.

Next, let $\emptyset = \mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_{t'} = U_z$ be a path from the empty configuration to U_z. Our reversible pebbling strategy for G is

$$\mathbb{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_{t'-1}, \mathbb{P}_{t'}, \mathbb{P}_{t'-1}, \ldots, \mathbb{P}_0) \quad . \tag{3.7}$$

This is a legal pebbling strategy since, as noted above, every edge of $\mathbb{C}$ constitutes a legal move of the reversible pebbling game. The strategy $\mathbb{P}$ uses space s, since all the configurations in $\mathbb{C}$ contain at most s pebbles by definition. The time of $\mathbb{P}$ is $t = 2 \cdot t'$. It therefore remains to show that the size of the Nullstellensatz refutation from Equation 3.6 is at least $t + 1$.

To this end, note that every edge e_q in the path corresponds to some monomial q in some polynomial Q_v. When the monomial q is multiplied by the axiom A_v, it generates two monomials in the proof: the monomial $q \cdot x_{\text{pred}(v)}$ and the monomial $q \cdot x_{\text{pred}(v)} \cdot x_v$. Hence, the Nullstellensatz refutation contains at least $2 \cdot t'$ monomials that correspond to edges from the path. In addition, the product $A_{\text{sink}} \cdot Q_{\text{sink}}$ must contains at least one monomial, since the refutation must use the sink axiom A_{sink} (because ϕ without this axiom is not a contradiction). It follows that the refutation contains at least $2 \cdot t' + 1 = t + 1$ monomials, as required. We conclude this section by proving Claim 3.2.

Proof of Claim 3.2. We start by introducing some terminology. First, observe that a monomial m may be generated multiple times in the refutation of Equation 3.6, and we refer to each time it is generated as an *occurrence* of m. We say that an occurrence of m is *generated by a monomial* q_v *of* Q_v if it is generated by the product $A_v \cdot q_v$. Throughout the proof, we identify a configuration U with the monomial x_U.

We first prove the claim for the non-empty case. Let $U \subseteq V$ be a non-empty configuration. We would like to prove the weight of U is 0. Recall that the weight of U is the sum of the coefficients of the occurrences of U that are generated by monomials q_v *that do not contain the corresponding vertex* v. Observe that Equation 3.6 implies that the sum of the coefficients of *all* the occurrences of U is 0: the coefficient of U on the right-hand side is 0, and it must be equal to the coefficient of U on the left-hand side, which is the sum of the coefficients of all the occurrences.

To complete the proof, we argue that every monomial q_v that does contain the vertex v contributes 0 to that sum. Let q_v be a monomial of Q_v that contains the vertex v and generates an occurrence of U. Let α be the coefficient of q. Then, it must hold that

$$\begin{aligned} A_v \cdot q_v &= x_{\text{pred}(v)} \cdot q_v - x_v \cdot x_{\text{pred}(v)} \cdot q_v \\ &= x_{\text{pred}(v)} \cdot q_v - x_{\text{pred}(v)} \cdot q_v \\ &= \alpha \cdot x_U - \alpha \cdot x_U \quad , \end{aligned} \tag{3.8}$$

where the second equality holds since we q_v contains v and we are working with a multilinear refutation, and the third equality holds since we assumed that q_v generates an occurrence of U. It follows that q_v generates two occurrences of U, one with coefficient α and one with coefficient $-\alpha$, and therefore it contributes 0 to the sum of the coefficients of all the occurrences of U.

We have shown that the sum of the coefficients of all the occurrences of U is 0, and that the occurrences generated by monomials q_v that contain v contribute 0 to this sum, and therefore the sum of coefficients of occurrences that are generated by monomials q_v that do not contain v must be 0, as required. In the case that U is the empty configuration, the proof is identical, except that the sum of the coefficients of all occurrences is 1, since the coefficient of $\emptyset$ is 1 on the right hand side of Equation 3.6. □

4 Nullstellensatz Trade-offs from Reversible Pebbling

In this section we prove Nullstellensatz refutation size-degree trade-offs for different degree regimes. Let us first recall what is known with regards to degree and size. In what follows, a Nullstellensatz refutation of a CNF formula F refers to a Nullstellensatz refutation of the translation of F to polynomials. As mentioned in the introduction, if a CNF formula over n variables can be refuted in degree d then it can be refuted in simultaneous degree d and size $n^{\mathrm{O}(d)}$. However, for Nullstellensatz it is not the case that strong enough degree lower bounds imply size lower bounds.

A natural question is whether for any given function $d_1(n)$ there is a family of CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that

1. F_n has a Nullstellensatz refutation $d_1(n)$;
2. F_n has a Nullstellensatz refutation of (close to) linear size and degree $d_2(n) \gg d_1(n)$;
3. Any Nullstellensatz refutation of F_n in degree only slightly below $d_2(n)$ must have size nearly $n^{d_1(n)}$.

We present explicit constructions of formulas providing such trade-offs in several different parameter regimes. We first show that there are formulas that require exponential size in Nullstellensatz if the degree is bounded by some polynomial function, but if we allow slightly larger degree there is a nearly linear size proof.

Theorem 4.1. *There is a family of explicitly constructible unsatisfiable* 3*-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\Theta(n)$ *such that:*

1. *There is a Nullstellensatz refutation of* F_n *in degree* $d_1 = \mathrm{O}\big(\sqrt[6]{n}\log n\big)$.
2. *For any constant* $\epsilon > 0$*, there is a Nullstellensatz refutation of* F_n *of size* $\mathrm{O}(n^{1+\epsilon})$ *and degree* $d_2 = \mathrm{O}\big(d_1 \cdot \sqrt[6]{n}\big) = \mathrm{O}\big(\sqrt[3]{n}\log n\big)$.
3. *There exists a constant* $K > 0$ *such that any Nullstellensatz refutation of* F_n *in degree at most* $d = Kd_2/\log n = \mathrm{O}\big(\sqrt[3]{n}\big)$ *must have size* $\big(\sqrt[6]{n}\big)!$.

We also analyse a family of formulas that can be refuted in close to logarithmic degree and show that even if we allow up to a certain polynomial degree, the Nullstellensatz size required is superpolynomial.

Theorem 4.2. *Let* $\delta > 0$ *be an arbitrarily small positive constant and let* $g(n)$ *be any arbitrarily slowly growing monotone function* $\omega(1) = g(n) \leq n^{1/4}$. *Then there is a family of explicitly constructible unsatisfiable* 3*-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\Theta(n)$ *such that:*

1. *There is a Nullstellensatz refutation of* F_n *in degree* $d_1 = g(n)\log(n)$.
2. *For any constant* $\epsilon > 0$*, there is a Nullstellensatz refutation of* F_n *of size* $\mathrm{O}(n^{1+\epsilon})$ *and degree*

$$d_2 = \mathrm{O}\big(d_1 \cdot n^{1/2}/g(n)^2\big) = \mathrm{O}\big(n^{1/2}\log n/g(n)\big).$$

3. *Any Nullstellensatz refutation of F_n in degree at most*
$$d = \mathrm{O}\big(d_2/n^{\delta} \log n\big) = \mathrm{O}\big(n^{1/2-\delta}/g(n)\big)$$
must have size superpolynomial in n.

Still in the small-degree regime, we present a very robust trade-off in the sense that superpolynomial size lower bound holds for degree from $\log^2(n)$ to $n/\log(n)$.

Theorem 4.3. *There is a family of explicitly constructible unsatisfiable 3-CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that:*

1. *There is a Nullstellensatz refutation of F_n in degree $d_1 = \mathrm{O}(\log^2 n)$.*
2. *For any constant $\delta > 0$, there is a Nullstellensatz refutation of F_n of size $\mathrm{O}(n)$ and degree*
$$d_2 = \mathrm{O}(d_1 \cdot n/\log^{3-\delta} n) = \mathrm{O}(n/\log^{1-\delta} n).$$
3. *There exists a constant $K > 0$ such that any Nullstellensatz refutation of F_n in degree at most $d = Kd_2/\log^{\delta} n = O(n/\log n)$ must have size $n^{\Omega(\log\log n)}$.*

Finally, we study a family of formulas that have Nullstellensatz refutation of quadratic size and that present a smooth size-degree trade-off.

Theorem 4.4. *There is a family of explicitly constructible unsatisfiable 3-CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that any Nullstellensatz refutation of F_n that optimizes size given degree constraint $d = n^{\Theta(1)}$ (and less than n) has size $\Theta\big(n^2/d\big)$.*

We prove these results by obtaining the analogous time-space trade-offs for reversible pebbling and then applying the tight correspondence between size and degree in Nullstellensatz and time and space in reversible pebbling.

4.1 Reversible Pebbling Time-Space Trade-offs

Our strategy for proving reversible pebbling trade-offs will be to analyse standard pebbling trade-offs. Clearly lower bounds from standard pebbling transfer to reversible pebbling; the next theorem shows how, in a limited sense, we can also transfer *upper bounds*. It is based on a reversible simulation of irreversible computation proposed by [Ben89] and analysed precisely in [LS90].

Theorem 4.5 ([Ben89, LS90]). *Let G be an arbitrary DAG and suppose G can be pebbled (in the standard way) using s pebbles in time $t \geq 2s$. Then for any $\epsilon > 0$, G can be reversibly pebbled in time $t^{1+\epsilon}/s^{\epsilon}$ using $\epsilon(2^{1/\epsilon} - 1)\, s \log(t/s)$ pebbles.*

We also use the following general proposition, which allows upper bounding the reversible pebbling price of a graph by using its depth and maximum in-degree.

Proposition 4.6. *Any DAG with maximum indegree ℓ and depth d has a persistent reversible pebbling strategy in space at most $d\ell + 1$.*

Proof. We will use the fact that if a graph has a persistent reversible strategy in space s then it has a visiting reversible strategy in space s.

The proof is by induction on the depth. For $d = 0$ we can clearly persistently reversibly pebble the graph with 1 pebble. For $d \geq 1$, we persistently reversibly pebble all but one of the (that is, at most $\ell - 1$) immediate predecessors of the sink one at a time. By the induction hypothesis, this can be done with at most $\ell - 2 + (d-1)\ell + 1 = d\ell - 1$ pebbles. At this point there are at most $\ell - 1$ predecessors of the sink which are pebbled and no other pebbles on the graph. Let v be the only non-pebbled predecessor of the sink. We do a visiting reversible pebbling of v until a pebble is placed on v. We now pebble the sink and then reverse the visiting pebbling of v until the subtree rooted at v has no pebbles on it. By the induction hypothesis, this can be done with at most $\ell + (d-1)\ell + 1 = d\ell + 1$ pebbles. All that is left to do is to to remove the $\ell - 1$ pebbles which are on predecessors of the sink. Again by the induction hypothesis, this can be done with $\ell + (d-1)\ell + 1$ pebbles. ∎

4.2 Carlson-Savage Graphs

The first family of graphs for which we present reversible pebbling trade-offs consists of the so-called Carlson-Savage graphs, which are illustrated in Figure 2 and are defined as follows.

Definition 4.7 (Carlson-Savage graph [CS80, CS82, Nor12]). The two-parameter graph family $\Gamma(c,r)$, for $c,r \in \mathbb{N}^+$, is defined by induction over r. The base case $\Gamma(c,1)$ is a DAG consisting of two sources s_1, s_2 and c sinks $\gamma_1,\ldots,\gamma_c$ with directed edges (s_i,γ_j), for $i=1,2$ and $j=1,\ldots,c$, i.e., edges from both sources to all sinks. The graph $\Gamma(c,r+1)$ has c sinks and is built from the following components:

- c disjoint copies $\Pi_r^{(1)},\ldots,\Pi_r^{(c)}$ of a pyramid graph of height r.
- one copy of $\Gamma(c,r)$.
- c disjoint and identical line graphs called *spines*, where each spine is composed of r *sections*, and every section contains $2c$ vertices.

The above components are connected as follows: In every section of every spine, each of the first c vertices has an incoming edge from the sink of one of the first c pyramids, and each of the last c vertices has an incoming edge from one of the sinks of $\Gamma(c,r)$ (where different vertices in the same section are connected to different sinks).

Note that $\Gamma(c,r)$ has multiple sinks. We define a (reversible) pebbling of a multi-sink graph to be a (reversible) pebbling that places pebbles on each sink at some point (the pebbles do not need to be present in the last configuration). Let $\Gamma'(c,r)$ be the single-sink subgraph of $\Gamma(c,r)$ consisting of all vertices that reach the first sink of $\Gamma(c,r)$. Since all sinks are symmetric, pebbling $\Gamma'(c,r)$ and pebbling $\Gamma(c,r)$ are almost equivalent.

Proposition 4.8. *Any (reversible) pebbling $\mathcal{P}$ of $\Gamma(c,r)$ induces a (reversible) pebbling $\mathcal{P}'$ of $\Gamma'(c,r)$ in at most the same space and the same time. From any (reversible) pebbling $\mathcal{P}'$ of $\Gamma'(c,r)$ we can obtain (reversible) pebbling $\mathcal{P}$ of $\Gamma(c,r)$ by (reversibly) pebbling each sink of $\Gamma(c,r)$ one at a time, that is, simulating $\mathcal{P}'$ c times, once for each sink. Note that $\mathsf{space}(\mathcal{P}) = \mathsf{space}(\mathcal{P}')$ and $\mathsf{time}(\mathcal{P}) = c \cdot \mathsf{time}(\mathcal{P}')$.*

Carlson and Savage proved the following properties of this graph.

Lemma 4.9 ([CS82]). *The graphs $\Gamma(c,r)$ are of size $\Theta\big(cr^3 + c^2r^2\big)$, have in-degree 2, and have standard pebbling price $r+2$.*

Theorem 4.10 ([CS82]). *Suppose that $\mathcal{P}$ is a standard pebbling of $\Gamma(c,r)$ in space less than $(r+2)+s$ for $0 < s \leq c-3$. Then*

$$\mathsf{time}(\mathcal{P}) \geq \left(\frac{c-s}{s+1}\right)^r \cdot r! \enspace .$$

This lower bound holds for space up to $c+r-1$. By allowing only a constant factor more pebbles it is possible to pebble the graph (in the standard way) in linear time.

Lemma 4.11 ([Nor12]). *The graphs $\Gamma(c,r)$ have standard pebbling strategies in simultaneous space $\mathrm{O}(c+r)$ and time linear in the size of the graphs.*

The standard pebbling price upper bound does not carry over to reversible pebbling because the line graph requires more pebbles in reversible pebbling than in standard pebbling. However, we can adapt the standard pebbling strategy to reversible pebbling using the following fact on the line graph.

Proposition 4.12 ([LV96]). *The visiting reversible pebbling price of the line graph on n vertices is $\lceil \log(n+1) \rceil$ and the persistent reversible pebbling price is $\lfloor \log(n-1) \rfloor + 2$.*

Using this result, we get the following upper bound (which is slightly stronger then what we would get by applying Theorem 4.5).

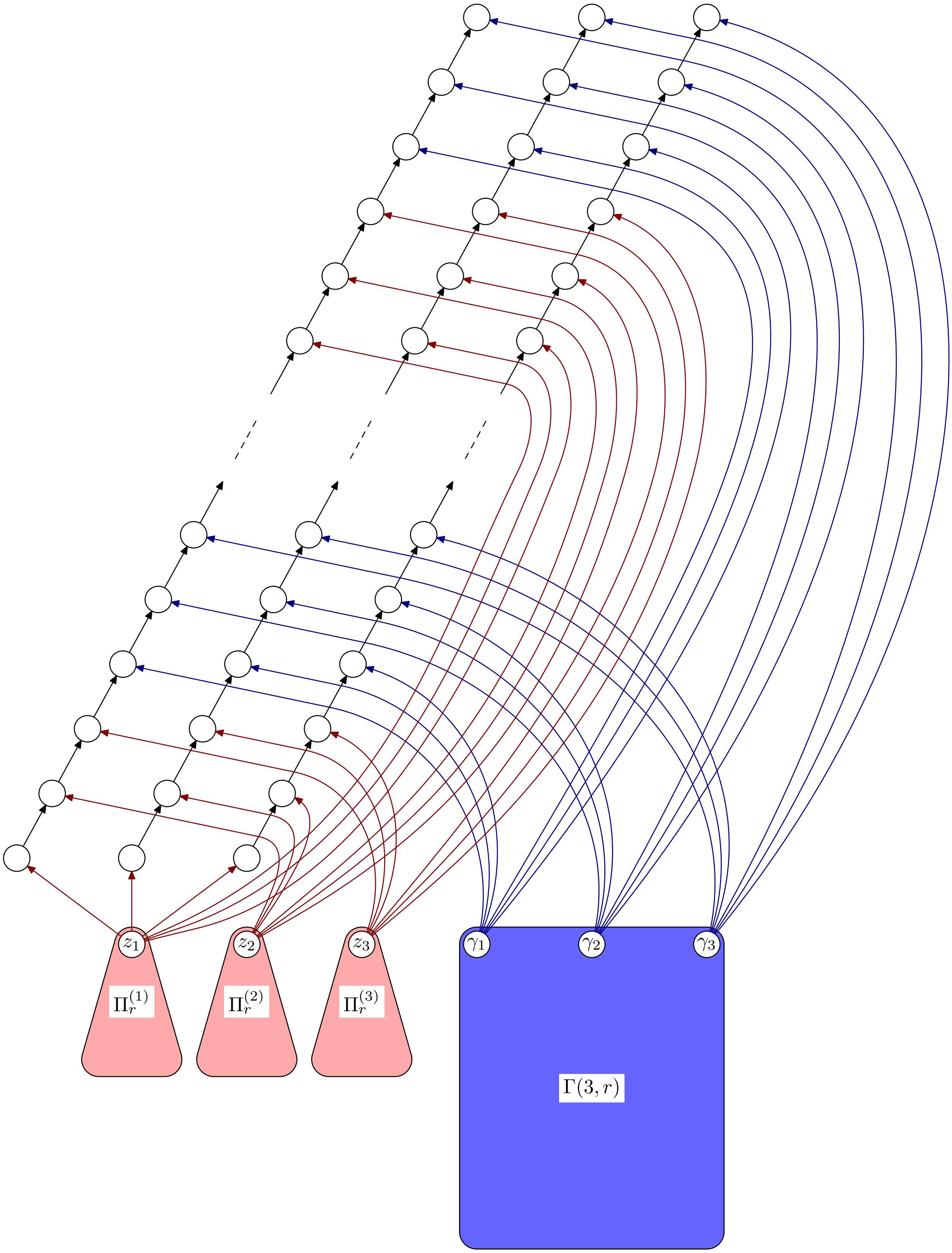


Figure 2: Inductive definition of Carlson-Savage graph $\Gamma(3, r + 1)$ with 3 spines and sinks.

Lemma 4.13. *The graphs $\Gamma(c, r)$ have reversible pebbling price at most $r(\log(cr) + 3)$.*

Proof. The proof is by induction on r. Clearly, $\Gamma(c, 1)$ can be reversibly pebbled with 3 pebbles. In order to pebble any sink of $\Gamma(c, r)$, we can reversibly pebble the corresponding spine with the space-efficient strategy for reversibly pebbling a line graph (as per Proposition 4.12) and every time we need to place or remove a pebble on a given vertex of the spine, we reversibly pebble the subgraph that reaches this vertex. By Proposition 4.6, pyramids of depth $r - 1$ can be reversibly pebbled with $2(r - 1) + 1$ pebbles. Therefore, by induction on r we get that the reversible pebbling price of $\Gamma(c, r)$ is at most $\max\{(r - 1)(\log(cr) + 3), 2(r - 1) + 1\} + \log(2cr) + 2 \leq (r - 1)(\log(cr) + 3) + \log(cr) + 3$. □

In order to obtain nearly linear time reversible pebbling, we apply Theorem 4.5 to Lemma 4.11.

Lemma 4.14. *For any $\epsilon > 0$, the graphs $\Gamma(c, r)$ have reversible pebbling strategies in simultaneous space $\mathrm{O}(\epsilon 2^{1/\epsilon}(c + r)\log(cr))$ and time $\mathrm{O}(n^{1+\epsilon})$ (where n denotes the number of vertices).*

We can now choose different values for the parameters c and r and obtain graphs with trade-offs in different space regimes. The first family of graphs we consider are those that exhibit exponential time lower-bounds.

Theorem 4.15. *There are explicitly constructible families of single-sink DAGs $\{G_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ and maximum in-degree 2 such that:*

1. *The graph G_n has reversible pebbling price $s_1 = \mathrm{O}\big(\sqrt[6]{n}\log n\big)$.*
2. *For any constant $\epsilon > 0$, there is a reversible pebbling of G_n in time $\mathrm{O}(n^{1+\epsilon})$ and space*

$$s_2 = \mathrm{O}\big(s_1 \cdot \sqrt[6]{n}\big) = \mathrm{O}\big(\sqrt[3]{n}\log n\big) \ .$$

3. *There is a constant $K > 0$ such that any standard pebbling of G_n in space at most*

$$s = \frac{Ks_2}{\log n} = \mathrm{O}\big(\sqrt[3]{n}\big)$$

must take time at least $\big(\sqrt[6]{n}\big)!$.

Proof. Let G_n be the single-sink subgraph of $\Gamma(c(n), r(n))$ consisting of all vertices that reach the first sink, for $c(n) = \sqrt[3]{n}$ and $r(n) = \sqrt[6]{n}$.

By Lemma 4.9, G_n has $\Theta(n)$ vertices and by Proposition 4.8, items 1–3 follow from Lemma 4.13, Lemma 4.14 and Theorem 4.10, respectively. □

Given Theorem 3.1 which proves the tight correspondence between reversible pebbling and Nullstellensatz refutations, Theorem 4.1 follow from Theorem 4.15.

It is also interesting to consider families of graphs that can be reversibly pebbled in very small space, close to the logarithmic lower bound on the number of pebbles required to reversibly pebble a single-sink DAG. In this small-space regime, we cannot expect exponential time lower bounds, but we can still obtain superpolynomial ones.

Theorem 4.16. *Let $\delta > 0$ be an arbitrarily small positive constant and let $g(n)$ be any arbitrarily slowly growing monotone function $\omega(1) = g(n) \leq n^{1/4}$. Then there is a family of explicitly constructible single-sink DAGs $\{G_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ and maximum in-degree 2 such that:*

1. *The graph G_n has reversible pebbling price $s_1 \leq g(n)\log(n)$.*
2. *For any constant $\epsilon > 0$, there is a reversible pebbling of G_n in time $\mathrm{O}(n^{1+\epsilon})$ and space*

$$s_2 = \mathrm{O}\big(s_1 \cdot n^{1/2}/g(n)^2\big) = \mathrm{O}\big(n^{1/2}\log n/g(n)\big) \ .$$

3. *Any standard pebbling of G_n in space at most*

$$s = \mathrm{O}\big(s_2/n^{\delta}\log n\big) = \mathrm{O}\big(n^{1/2-\delta}/g(n)\big)$$

requires time superpolynomial in n.

Proof. The proof is analogous to that of Theorem 4.16 with parameters $r(n) = g(n)$ and $c(n) = n^{1/2}/g(n)$. ☐

By applying Theorem 3.1 to the above result we obtain Theorem 4.2.

Remark 4.17. We note that in the second items of both the foregoing theorems, we could have reduced the time of the reversible pebbling to $\mathrm{O}(n^{1+\mathrm{o}(1)})$ by applying Theorem 4.5 with $\epsilon = \mathrm{O}\left(\frac{1}{\log\log n}\right)$. This would have come at a cost of an extra logarithmic factor in the corresponding space bounds.

4.3 Stacks of Superconcentrators

Lengauer and Tarjan [LT82] studied robust superpolynomial trade-offs for standard pebbling and showed that there are graphs that have standard pebbling price $\mathrm{O}(\log^2 n)$, but that any standard pebbling in space up to $Kn/\log n$, for some constant K, requires superpolynomial time. For reversible pebbling we get almost the same result for the same family of graphs.

Theorem 4.18. *There are explicitly constructible families of single-sink DAGs $\{G_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ and maximum in-degree 2 such that:*

1. *The graph G_n has reversible pebbling price $s_1 = \mathrm{O}(\log^2 n)$.*

2. *For any constant $\delta > 0$, there is a reversible pebbling of G_n in time $\mathrm{O}(n)$ and space*

$$s_2 = \mathrm{O}(s_1 \cdot n/\log^{3-\delta} n) = \mathrm{O}(n/\log^{1-\delta} n) \ .$$

3. *There exists a constant $K > 0$ such that any standard pebbling $\mathcal{P}_n$ of G_n using at most pebbles $s = \frac{Ks_2}{\log^{\delta} n} = O(n/\log n)$ requires time $n^{\Omega(\log\log n)}$.*

Note that, together with Theorem 3.1, this implies Theorem 4.3. Now in order to prove this theorem we must first introduce the family of graphs we will consider.

Definition 4.19 (Superconcentrator [Val75]). A directed acyclic graph G is an m-superconcentrator if it has m sources $S = \{s_1, \ldots, s_m\}$, m sinks $Z = \{z_1, \ldots, z_m\}$, and for any subsets S' and Z' of sources and sinks of size $|S'| = |Z'| = \ell$ it holds that there are ℓ vertex-disjoint paths between S' and Z' in G.

Pippenger [Pip77] proved that there are superconcentrators of linear size and logarithmic depth, and Gabber and Galil [GG81] gave the first explicit construction. For concreteness, we will consider the explicit construction by Alon and Capalbo [AC03] which has better parameters.

Theorem 4.20 ([AC03]). *For all integers $k \geq 6$, there are explicitly constructible m-superconcentrators for $m = \mathrm{O}(2^k)$ with $\mathrm{O}(m)$ edges, depth $\mathrm{O}(\log m)$, and maximum indegree $\mathrm{O}(1)$.*

It is easy to see that we can modify these superconcentrators so that the maximum indegree is 2 by substituting each vertex with indegree $\delta > 2$ by a binary tree with δ leafs. Note that this only increase the size and the depth by constant factors.

Corollary 4.21. *There are m-superconcentrators with $\mathrm{O}(m)$ vertices, maximum indegree 2 and depth $\mathrm{O}(\log m)$.*

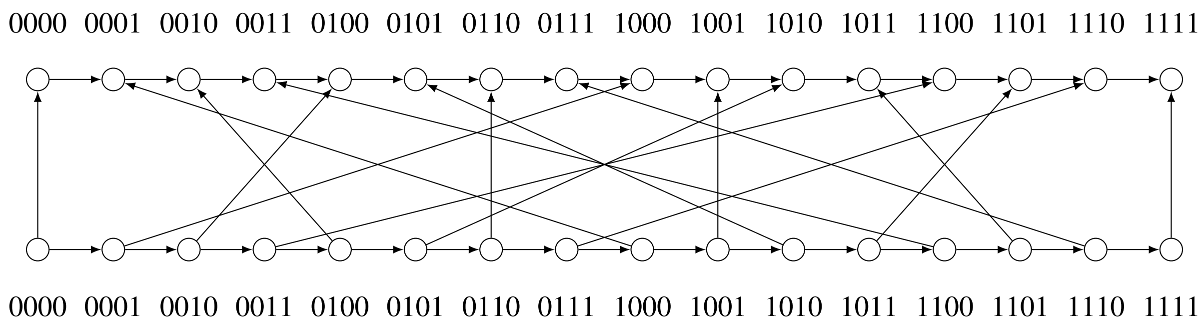


Figure 3: A bit-reversal permutation graph.

Given an m-superconcentrator G_m, we define a stack of r superconcentrators G_m to be r disjoint copies of G_m where each sink of the ith copy is connected to a different source of the $i+1$st copy for $i \in [r-1]$. Since we want single-sink DAGs, we add a binary tree with m leafs and depth $\lceil \log m \rceil$, and connect each sink of the rth copy of G_m to a different leaf of the tree. Lengauer and Tarjan [LT82] proved the following theorem for stacks of superconcentrators.

Theorem 4.22 ([LT82]). *Let $\Phi(m, r)$ denote a stack of r (explicitly constructible) linear-size m-superconcentrator with bounded indegree and depth $\log m$. Then the following holds:*

1. *The standard pebbling price of $\Phi(m, r)$ is $\mathrm{O}(r \log m)$.*
2. *There is a linear-time standard pebbling strategy $\mathcal{P}$ for $\Phi(m, r)$ with $\mathsf{space}(\mathcal{P}) = \mathrm{O}(m)$.*
3. *If $\mathcal{P}$ is a standard pebbling strategy for $\Phi(m, r)$ in space $s \leq m/20$, then $\mathsf{time}(\mathcal{P}) \geq m \cdot \left(\frac{rm}{64s}\right)^r$.*

With this result in hand we can now proceed to prove Theorem 4.18.

Proof of Theorem 4.18. Let G_n be a stack of $\log n$ linear-size $(n/\log n)$-superconcentrators as per Corollary 4.21. Note that G_n has $\Theta(n)$ vertices, indegree 2 and depth $\mathrm{O}(\log^2 n)$. By Proposition 4.6 we have that G_n can be reversibly pebbled with $\mathrm{O}(\log^2 n)$ pebbles (proving item 1).

By item 2 in Theorem 4.22 and by choosing $\epsilon = 1/(\delta \log\log n)$ in Theorem 4.5 we conclude that G_n can be reversibly pebbled in simultaneous time $\mathrm{O}\big(n2^{1/\delta}\big)$ and space $\mathrm{O}\big(n/(\delta \log^{1-\delta} n)\big)$, from which item 2 follows. Finally, item 3 in the theorem follows from item 3 in Theorem 4.22. ☐

4.4 Permutation Graphs

Another family of graphs that has been studied in the context of standard pebbling trade-offs is that of permutation graphs.

Definition 4.23. Given a permutation $\sigma \in \mathfrak{S}([n])$, the *permutation graph* $G(\sigma)$ consists of two lines $(x_1, \ldots, x_n)$ (the *bottom line*) and $(y_1, \ldots, y_n)$ (*top line*) which are connected as follows: for every $1 \leq i \leq n$, there is an edge from x_i to $y_{\sigma(i)}$.

Lengauer and Tarjan [LT82] proved that permutation graphs present the following smooth trade-off when instantiated with the permutation that reverses the binary representation of the index i (see Figure 3 for an illustration).

Theorem 4.24 ([LT82]). *Let G be a bit-reversal permutation graph on $2n$ vertices. For any $3 \leq s \leq n$, there is a standard pebbling in space s and time $\mathrm{O}\big(n^2/s\big)$. Moreover, any standard pebbling $\mathcal{P}$ in space s satisfies $\mathsf{time}(\mathcal{P}) = \Omega\big(n^2/s\big)$.*

We show that these graphs also present a smooth reversible pebbling trade-off and, in particular, for $s = n^{\Theta(1)}$ and $s \leq n$, any reversible pebbling $\mathcal{P}$ in space s satisfies $\mathsf{time}(\mathcal{P}_n) = \Omega\big(n^2/s\big)$ and there are matching upper bounds. To this end, we use the following proposition.

Proposition 4.25. *For every natural number k, the line graph over n vertices can be reversibly pebbled using $2k \cdot n^{1/k}$ pebbles in time $2^k \cdot n$.*

Proof. Observe that the line graph over n can be pebbled (in the standard way) using 2 pebbles in time $2n$. The proposition follows now by applying Theorem 4.5 with $\epsilon = k/\log(n)$. □

Using Proposition 4.25, we obtain the following result.

Theorem 4.26. *Let G_n be a bit-reversal permutation graph on $2n$ vertices. Then G_n satisfies the following properties:*

1. *The reversible pebbling price of G_n is at most $2\log n + 2$.*
2. *If s satisfies $4\log n \leq s \leq 2n$ and k is such that $s = 4kn^{1/k}$, then there is a reversible strategy in simultaneous space s and time $\mathrm{O}\big(k2^{2k} \cdot n^2/s\big)$.*
3. *Any standard pebbling $\mathcal{P}_n$ of G_n satisfies $\mathsf{time}(\mathcal{P}_n) = \Omega\big(n^2/\mathsf{space}(\mathcal{P}_n)\big)$.*

Proof. The upper bounds (item 1 and item 2) hold for any permutation graph.

For item 1, we can simulate a reversible pebbling of the top line that uses space at most $\log n + 1$ (as per Proposition 4.12), and every time we need a pebble on a vertex v of the bottom line in order to place or remove a pebble on the top line, we reversibly pebble the bottom line until v is pebbled (can be done with $\log n + 1$ pebbles), make the move on the top line, and then unpebble the bottom line.

To obtain item 2, we consider a two stage strategy. In the first phase, we place $n^{1/k}$ pebbles spaced equally apart on the bottom line. We refer to these pebbles as *fixed* pebbles, since they will remain on the graph until the sink is pebbled. In the second phase, we simulate a reversible pebbling on the top line with $2kn^{1/k}$ pebbles and every time we need a pebble on a vertex v on the bottom line to make a move on the top line, we reversibly pebble v (with $2(k-1)n^{1/k}$ pebbles) from the nearest fixed pebble, make the move on the top line, and then unpebble the segment on the bottom line.

All that is left to show is that this can be done within the space budget of $4kn^{1/k}$ in time $\mathrm{O}(2^{2k} \cdot n^2/s)$. For the first phase, we reversibly pebble $n^{1/k}$ segments of length $m = n^{1-1/k}$. By Proposition 4.25, each of the segments can be reversibly pebbled using $2(k-1)n^{1/k} = 2(k-1)m^{k-1}$ pebbles in time $2^{k-1}n^{1-1/k}$. Since every segment must be pebbled and then unpebbled, the total time for the first phase is $2 \cdot 2^{k-1}n^{1-1/k} \cdot n^{1/k} = 2^k n$, and the total number of pebbles used is less than $2kn^{1/k}$: $n^{1/k}$ for the fixed pebbles and $2(k-1)n^{1/k}$ for pebbling each segment.

We turn to analyze the second phase. By Proposition 4.25, the top line can be reversibly pebbled in simultaneous space $2kn^{1/k}$ and time $2^k n$. For each move in the top line, we need to pebble and unpebble a segment of length at most $n^{1-1/k}$. As argued before, this can be done in simultaneous space $2(k-1)n^{1/k}$ and time $2 \cdot 2^{k-1}n^{1-1/k}$. Therefore, at any point in the pebbling strategy there are at most $2kn^{1/k}$ pebbles on the bottom line and at most $2kn^{1/k}$ pebbles on the top line, and the total time of the pebbling is at most $2^k n + 2^{2k}n^{2-1/k} \leq 4k2^{2k}n^2/s$.

Finally, item 3 follows from the standard pebbling lower bound in Theorem 4.24. □

From Theorem 4.26 we obtain the following corollary that, together with Theorem 3.1, implies Theorem 4.4.

Corollary 4.27. *Any reversible pebbling strategy $\mathcal{P}_n$ for G_n that optimizes time given space constraint $n^{\Theta(1)}$ (and less than n) exhibits a trade-off $\mathsf{time}(\mathcal{P}_n) = \Theta\big(n^2/\mathsf{space}(\mathcal{P}_n)\big)$.*

5 Concluding Remarks

In this paper we prove that size and degree of Nullstellensatz refutations in any field of pebbling formulas are exactly captured by time and space of the reversible pebble game on the underlying graph. This allows us to prove a number of strong size-degree trade-offs for Nullstellensatz. To the best of our understanding no such results have been known previously.

The most obvious, and also most interesting, open question is whether there are also size-degree trade-offs for the stronger polynomial calculus proof system. Such trade-offs cannot be exhibited by the pebbling formulas considered in this work, since such formulas have small-size low-degree polynomial calculus refutations, but the formulas exhibiting size-width trade-offs for resolution [Tha16] appear to be natural candidates.[2]

Another interesting question is whether the tight relation between Nullstellensatz and reversible pebbling could make it possible to prove even sharper trade-offs for size versus degree in Nullstellensatz, where just a small constant drop in the degree would lead to an exponential blow-up in size. Such results for pebbling time versus space are known for the standard pebble game, e.g., in [GLT80]. It is conceivable that a similar idea could be applied to the reversible pebbling reductions in [CLNV15], but it is not obvious whether just adding a small amount of space makes it possible to carry out the reversible pebbling time-efficiently enough.

Finally, it can be noted that our results crucially depend on that we are in a setting with variables only for positive literals. For polynomial calculus it is quite common to consider the stronger setting with "twin variables" for negated literals (as in the generalization of polynomial calculus in [CEI96] to *polynomial calculus resolution* in [ABRW02]). It would be nice to generalize our size-degree trade-offs for Nullstellensatz to this setting, but it seems that some additional ideas are needed to make this work.

Acknowledgements

We are grateful for many interesting discussions about matters pebbling-related (and not-so-pebbling-related) with Arkadev Chattopadhyay, Toniann Pitassi, and Marc Vinyals.

This work was mostly carried out while the authors were visiting the Simons Institute for the Theory of Computing in association with the DIMACS/Simons Collaboration on Lower Bounds in Computational Complexity, which is conducted with support from the National Science Foundation.

Or Meir was supported by the Israel Science Foundation (grant No. 1445/16). Robert Robere was supported by NSERC, and also conducted part of this work at DIMACS with support from the National Science Foundation under grant number CCF-1445755. Susanna F. de Rezende and Jakob Nordström were supported by the *Knut and Alice Wallenberg* grant KAW 2016.0066 *Approximation and Proof Complexity*. Jakob Nordström was also supported by the Swedish Research Council grants 621-2012-5645 and 2016-00782.

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*.

[AC03] Noga Alon and Michael Capalbo. Smaller explicit superconcentrators. *Internet Mathematics*, 1(2):151–163, 2003.

[AH18] Albert Atserias and Tuomas Hakoniemi. Size-degree trade-offs for sums-of-squares and Positivstellensatz proofs. Technical Report 1811.01351, arXiv.org, November 2018.

[ALN16] Albert Atserias, Massimo Lauria, and Jakob Nordström. Narrow proofs may be maximally long. *ACM Transactions on Computational Logic*, 17(3):19:1–19:30, May 2016. Preliminary version in *CCC '14*.

[AO19] Albert Atserias and Joanna Ochremiak. Proof complexity meets algebra. *ACM Transactions on Computational Logic*, 20:1:1–1:46, February 2019. Preliminary version in *ICALP '17*.

[2] Such a result was very recently reported in [LNSS20].

[AS15] Joël Alwen and Vladimir Serbinenko. High parallel complexity graphs and memory-hard functions. In *Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC '15)*, pages 595–603, June 2015.

[BCE+98] Paul Beame, Stephen A. Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. The relative complexity of NP search problems. *Journal of Computer and System Sciences*, 57(1):3–19, August 1998. Preliminary version in *STOC '95*.

[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*.

[Ben73] Charles H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17(6):525–532, November 1973.

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

[Ber18] Christoph Berkholz. The relation between polynomial calculus, Sherali-Adams, and sum-of-squares proofs. In *Proceedings of the 35th Symposium on Theoretical Aspects of Computer Science (STACS '18)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:14, February 2018.

[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, November 1994.

[BIK+97] Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiri Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1997.

[Bla37] Archie Blake. *Canonical Expressions in Boolean Algebra*. PhD thesis, University of Chicago, 1937.

[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.

[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.

[BP98] Samuel R. Buss and Toniann Pitassi. Good degree bounds on Nullstellensatz refutations of the induction principle. *Journal of Computer and System Sciences*, 2(57):162–171, October 1998. Preliminary version in *CCC '96*.

[BTV01] Harry Buhrman, John Tromp, and Paul Vitányi. Time and space bounds for reversible simulation. *Journal of physics A: Mathematical and general*, 34:6821–6830, 2001. Preliminary version in *ICALP '01*.

[Bus98] Samuel R. Buss. Lower bounds on Nullstellensatz proofs via designs. In *Proof Complexity and Feasible Arithmetics*, volume 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 59–71. American Mathematical Society, 1998. Available at http://www.math.ucsd.edu/~sbuss/ResearchWeb/designs/.

[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.

[Cha73] Ashok K. Chandra. Efficient compilation of linear recursive programs. In *Proceedings of the 14th Annual Symposium on Switching and Automata Theory (SWAT '73)*, pages 16–25, 1973.

[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, October 2015.

[Coo74] Stephen A. Cook. An observation on time-storage trade off. *Journal of Computer and System Sciences*, 9(3):308–316, 1974. Preliminary version in *STOC '73*.

[CP14] Siu Man Chan and Aaron Potechin. Tight bounds for monotone switching networks via Fourier analysis. *Theory of Computing*, 10:389–419, October 2014. Preliminary version in *STOC '12*.

[CS80] David A. Carlson and John E. Savage. Graph pebbling with many free pebbles can be difficult. In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC '80)*, pages 326–332, 1980.

[CS82] David A. Carlson and John E. Savage. Extreme time-space tradeoffs for graphs with small space requirements. *Information Processing Letters*, 14(5):223–227, 1982.

[DMR09] Stefan S. Dantchev, Barnaby Martin, and Martin Rhodes. Tight rank lower bounds for the Sherali–Adams proof system. *Theoretical Computer Science*, 410(21–23):2054–2063, May 2009.

[DNW05] Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In *Proceedings of the 25th Annual International Cryptology Conference (CRYPTO '05)*, volume 3621 of *Lecture Notes in Computer Science*, pages 37–54. Springer, August 2005.

[dRMN+19] 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. Technical Report TR19-186, Electronic Colloquium on Computational Complexity (ECCC), 2019.

[FPRC13] Yuval Filmus, Toniann Pitassi, Robert Robere, and Stephen A Cook. Average case lower bounds for monotone switching networks. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS '13)*, pages 598–607, November 2013.

[GG81] Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. *Journal of Computer and System Sciences*, 22(3):407–420, 1981.

[GHP02] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Exponential lower bound for static semi-algebraic proofs. In *Proceedings of the 29th International Colloquium on Automata, Languages and Programming (ICALP '02)*, volume 2380 of *Lecture Notes in Computer Science*, pages 257–268. Springer, July 2002.

[GKRS18] Mika Göös, Pritish Kamath, Robert Robere, and Dmitry Sokolov. Adventures in monotone complexity and TFNP. Technical Report TR18-163, Electronic Colloquium on Computational Complexity (ECCC), September 2018.

[GLT80] John R. Gilbert, Thomas Lengauer, and Robert Endre Tarjan. The pebbling problem is complete in polynomial space. *SIAM Journal on Computing*, 9(3):513–524, August 1980. Preliminary version in *STOC '79*.

[HPV77] John Hopcroft, Wolfgang Paul, and Leslie Valiant. On time versus space. *Journal of the ACM*, 24(2):332–337, April 1977. Preliminary version in *FOCS '75*.

[IPS99] 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.

[KI06] Arist Kojevnikov and Dmitry Itsykson. Lower bounds of static Lovász–Schrijver calculus proofs for Tseitin tautologies. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP '06)*, volume 4051 of *Lecture Notes in Computer Science*, pages 323–334. Springer, July 2006.

[Krá04] Richard Královič. Time and space complexity of reversible pebbling. *RAIRO – Theoretical Informatics and Applications*, 38(02):137–161, April 2004.

[KSS18] Balagopal Komarath, Jayalal Sarma, and Saurabh Sawlani. Pebbling meets coloring: Reversible pebble game on trees. *Journal of Computer and System Sciences*, 91:33–41, 2018.

[LLMO09] Jesús A. De Loera, Jon Lee, Susan Margulies, and Shmuel Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert's Nullstellensatz. *Combinatorics, Probability and Computing*, 18(4):551–582, July 2009.

[LMT00] Klaus-Jörn Lange, Pierre McKenzie, and Alain Tapp. Reversible space equals deterministic space. *Journal of Computer and System Sciences*, 60(2):354–367, April 2000.

[LNSS20] Guillaume Lagarde, Jakob Nordström, Dmitry Sokolov, and Joseph Swernofsky. Trade-offs between size and degree in polynomial calculus. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference (ITCS '20)*, January 2020. To appear.

[LS90] Robert Y. Levin and Alan T. Sherman. A note on Bennett's time-space tradeoff for reversible computation. *SIAM Journal on Computing*, 19:673–677, 08 1990.

[LT82] Thomas Lengauer and Robert Endre Tarjan. Asymptotically tight bounds on time-space trade-offs in a pebble game. *Journal of the ACM*, 29(4):1087–1130, October 1982. Preliminary version in *STOC '79*.

[LTV98] Ming Li, John Tromp, and Paul Vitányi. Reversible simulation of irreversible computation. *Physica D: Nonlinear Phenomena*, 120(1–2):168–176, September 1998.

[LV96] Ming Li and Paul Vitányi. Reversibility and adiabatic computation: Trading time and space for energy. *Proceedings of the Royal Society of London, Series A*, 452(1947):769–789, April 1996.

[MSR+19] Giulia Meuli, Mathias Soeken, Martin Roetteler, Nikolaj Bjørner, and Giovanni De Micheli. Reversible pebbling game for quantum memory management. *CoRR*, abs/1904.02121, 2019.

[Nor12] Jakob Nordström. On the relative strength of pebbling and resolution. *ACM Transactions on Computational Logic*, 13(2):16:1–16:43, April 2012. Preliminary version in *CCC '10*.

[Nor13] Jakob Nordström. Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science*, 9(3):15:1–15:63, September 2013.

[Nor20] Jakob Nordström. New wine into old wineskins: A survey of some pebbling classics with supplemental results. Manuscript in preparation. To appear in *Foundations and Trends in Theoretical Computer Science*. Current draft version available at http://www.csc.kth.se/~jakobn/research/, 2020.

[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.

[Pip77] Nicholas Pippenger. Superconcentrators. *SIAM Journal on Computing*, 6(2):298–304, June 1977.

[Pip80] Nicholas Pippenger. Pebbling. Technical Report RC8258, IBM Watson Research Center, 1980. in Proceedings of the 5th IBM Symposium on Mathematical Foundations of Computer Science, Japan.

[Pot10] Aaron Potechin. Bounds on monotone switching networks for directed connectivity. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS '10)*, pages 553–562, October 2010.

[PR17] Toniann Pitassi and Robert Robere. Strongly exponential lower bounds for monotone computation. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing (STOC '17)*, pages 1246–1255, June 2017.

[PR18] Toniann Pitassi and Robert Robere. Lifting Nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th Annual ACM Symposium on Theory of Computing (STOC '18)*, pages 1207–1219, June 2018.

[PS98] Pavel Pudlák and Jirí Sgall. Algebraic models of computation and interpolation for algebraic proof systems. In *Proof Complexity and Feasible Arithmetics*, volume 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 279–296. American Mathematical Society, 1998. Available at http://users.math.cas.cz/~pudlak/span.pdf.

[RPRC16] Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook. Exponential lower bounds for monotone span programs. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS '16)*, pages 406–415, October 2016.

[Set75] Ravi Sethi. Complete register allocation problems. *SIAM Journal on Computing*, 4(3):226–248, September 1975.

[SS77] Sowmitri Swamy and John E. Savage. Space-time trade-offs on the FFT-algorithm. Technical Report CS-31, Brown University, 1977.

[SS79] John E. Savage and Sowmitri Swamy. Space-time tradeoffs for oblivious interger multiplications. In *Proceedings of the 6th International Colloquium on Automata, Languages and Programming (ICALP '79)*, pages 498–504, 1979.

[SS83] Sowmitri Swamy and John E. Savage. Space-time tradeoffs for linear recursion. *Mathematical Systems Theory*, 16(1):9–27, 1983.

[Tha16] Neil Thapen. A trade-off between length and width in resolution. *Theory of Computing*, 12(5):1–14, August 2016.

[Tom78] Martin Tompa. Time-space tradeoffs for computing functions, using connectivity properties of their circuits. In *Proceedings of the 10th annual ACM symposium on Theory of computing (STOC '78)*, pages 196–204, 1978.

[Val75] Leslie G. Valiant. On non-linear lower bounds in computational complexity. In *Proceedings of the 7th annual ACM symposium on Theory of computing (STOC '75)*, pages 45–53, 1975.

[Wil00] Ryan Williams. Space-efficient reversible simulations. Technical report, Cornell University, 2000. Available at http://web.stanford.edu/~rrwill/spacesim9_22.pdf.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il