# Short Proofs for the Determinant Identities[*]

Pavel Hrubeš[†] Iddo Tzameret[‡]

January 15, 2015

**Abstract**

We study arithmetic proof systems $\mathbb{P}_c(\mathbb{F})$ and $\mathbb{P}_f(\mathbb{F})$ operating with arithmetic circuits and arithmetic formulas, respectively, and that prove polynomial identities over a field $\mathbb{F}$. We establish a series of structural theorems about these proof systems, the main one stating that $\mathbb{P}_c(\mathbb{F})$ proofs can be balanced: if a polynomial identity of syntactic degree $d$ and depth $k$ has a $\mathbb{P}_c(\mathbb{F})$ proof of size $s$, then it also has a $\mathbb{P}_c(\mathbb{F})$ proof of size $\mathrm{poly}(s, d)$ in which every circuit has depth $O(k + \log^2 d + \log d \cdot \log s)$. As a corollary, we obtain a quasipolynomial simulation of $\mathbb{P}_c(\mathbb{F})$ by $\mathbb{P}_f(\mathbb{F})$.

Using these results we obtain the following: consider the identities

$$\det(XY) = \det(X) \cdot \det(Y) \quad \text{and} \quad \det(Z) = z_{11} \cdots z_{nn},$$

where $X, Y$ and $Z$ are $n \times n$ square matrices and $Z$ is a triangular matrix with $z_{11}, \ldots, z_{nn}$ on the diagonal (and det is the determinant polynomial). Then we can construct a polynomial-size arithmetic circuit det such that the above identities have $\mathbb{P}_c(\mathbb{F})$ proofs of polynomial-size using circuits of $O(\log^2 n)$ depth. Moreover, there exists an arithmetic formula det of size $n^{O(\log n)}$ such that the above identities have $\mathbb{P}_f(\mathbb{F})$ proofs of size $n^{O(\log n)}$.

This yields a solution to a basic open problem in propositional proof complexity, namely, whether there are polynomial-size $\mathbf{NC}^2$-Frege proofs for the determinant identities and the *hard matrix identities*, as considered, e.g. in Soltys and Cook [SC04] (cf., Beame and Pitassi [BP98]). We show that matrix identities like $AB = I \rightarrow BA = I$ (for matrices over the two element field) as well as basic properties of the determinant have polynomial-size $\mathbf{NC}^2$-Frege proofs, and quasipolynomial-size Frege proofs.

## 1 Introduction

The field of proof complexity is dominated by the question of how hard is it to prove propositional tautologies. For weak proof systems, such as resolution, many hardness results are

[*]Conference version appeared in STOC 2012.

[†]Institute of Mathematics of the Academy of Sciences of the Czech Republic, Prague. Email: `pahrubes@gmail.com`. Supported by ERC grant FEALORA 339691.

[‡]Department of Computer Science, Royal Holloway, University of London Email: `iddo.tzameret@gmail.com`.

known (cf., [Seg07] for a recent technical survey), but for strong propositional proof systems like Frege or extended Frege the question remains completely open. In this paper we continue to investigate a different but related problem: how hard is it to prove polynomial identities? For this purpose, various systems for proving polynomial identities were introduced in [HT09]. The main feature of these systems is that they manipulate arithmetic equations of the form $F = G$, where $F, G$ are arithmetic formulas over a given field. Such equations are manipulated by means of simple syntactic rules, in such a way that $F = G$ has a proof if and only if $F$ and $G$ compute the same polynomial. The central question in this framework is the following:

> What is the *length* of such proofs, namely, does every true polynomial equation have a short proof, or are there hard equations that require extremely long proofs?

In this paper, we focus on two arithmetic equational proof systems (arithmetic proofs systems, for short) for proving polynomial identities: $\mathbb{P}_f$ and $\mathbb{P}_c$. The former system was introduced in [HT09] and the latter is an extension of it. The difference between the two systems is that $\mathbb{P}_f$ operates with *arithmetic formulas*, whereas $\mathbb{P}_c$ operates with *arithmetic circuits*—this is analogous to the distinction between Frege and extended Frege proof systems (Frege and extended Frege proofs are propositional proof systems establishing propositional tautologies, essentially operating with boolean formulas and circuits, respectively).

The study of proofs of polynomial identities is motivated by at least two reasons. First, as a study of the Polynomial Identity Testing (PIT) problem. As a decision problem, polynomial identity testing can be solved by an efficient randomized algorithm [Sch80, Zip79], but no efficient deterministic algorithm is known. In fact, it is not even known whether there is a polynomial time non-deterministic algorithm or, equivalently, whether PIT is in **NP**. A proof system such as $\mathbb{P}_c$ can be interpreted as a specific non-deterministic algorithm for PIT: in order to verify that an arithmetic formula $F$ computes the zero polynomial, it is sufficient to guess a proof of $F = 0$ in $\mathbb{P}_c$. Hence, if every true equality has a polynomial-size proof then PIT is in **NP**. Conversely, $\mathbb{P}_f$ and $\mathbb{P}_c$ systems capture the common syntactic procedures used to establish equality of algebraic expressions. Thus, showing the existence of identities that require superpolynomial arithmetic proofs would imply that those syntactic procedures are not enough to solve PIT efficiently.

The second motivation comes from propositional proof complexity. The systems $\mathbb{P}_f$ and $\mathbb{P}_c$ are in fact *restricted* versions of their propositional counterparts, Frege and extended Frege, respectively (when operating over $GF(2)$). One may hope that the study of the former would help to understand the latter. Arithmetic proof systems have the advantage that they work with arithmetic circuits. The structure of arithmetic circuits is arguably better understood than the structure of their Boolean counterparts, or is at least different, suggesting different techniques and fresh perspectives.

In order to understand the strength of the systems $\mathbb{P}_f$ and $\mathbb{P}_c$, as well as their relative strength, we investigate quite a specific question, namely, how hard it is to prove basic properties of the determinant? In other words, we investigate lengths of proofs of identities such as $\det(AB) = \det(A) \cdot \det(B)$, or the cofactor expansion of the determinant. We show that such identities have polynomial-size $\mathbb{P}_c$ proofs of depth $O(\log^2 n)$ and quasipolynomial size $\mathbb{P}_f$ proofs (both results hold over any field).[1]

The determinant polynomial has a central role in both linear algebra and arithmetic circuit complexity. Therefore, an immediate motivation for our inquiry is to understand whether arithmetic proof systems are strong enough to reason efficiently about the determinant. More importantly, we take the determinant question as a pretext to present several structural properties of $\mathbb{P}_c$ and $\mathbb{P}_f$. A large part of this work is not concerned with the determinant at all, but is rather a series of general theorems showing how classical results in arithmetic circuit complexity can be translated to the setting of arithmetic proofs. We thus show how to capture efficiently the following results: (i) homogenization of arithmetic circuits (implicit in [Str73]); (ii) Strassen's technique for eliminating division gates over large enough fields (also in [Str73]); (iii) eliminating division gates over small fields—this is done by simulating large fields in small ones; and (iv) balancing arithmetic circuits (Valiant et al. [VSBR83]; see also [Hya79]). Most notably, the latter result gives a collapse of polynomial-size $\mathbb{P}_c$ proofs to polynomial-size $O(\log^2 n)$-depth $\mathbb{P}_c$ proofs (for proving identities of polynomial syntactic degrees) and a quasipolynomial simulation of $\mathbb{P}_c$ by $\mathbb{P}_f$. This is one important point where the arithmetic systems differ from Frege and extended Frege, for which no non-trivial simulation is known.

Furthermore, the proof complexity of linear algebra attracted a lot of attention in the past. This was motivated, in part, by the goal of separating the propositional proof systems Frege and extended Frege. A classical example, originally proposed by Cook and Rackoff (cf., [BP98, SC04, SU04, Sol01, Sol05]), is the so called *inversion principle* asserting that $AB = I \rightarrow BA = I$. When $A, B$ are $n \times n$ matrices over $GF(2)$, the inversion principle is a collection of propositional tautologies. Soltys and Cook [SC04, Sol01] showed that the principle has polynomial size extended Frege proofs. On the other hand, no feasible Frege proof is known, and hence the inversion principle is a candidate for separating the two proof systems. Other candidates, including several based on linear algebra, were presented by Bonet et al. [BBP95]. The inversion principle is one of the "hard matrix identities" explored in [SC04]. Inside Frege, the hard matrix identities have feasible proofs from one another, and they have short proofs from the aforementioned determinant identities. This connection between the hard matrix identities and the determinant identities serves as an evidence for the conjecture that hard matrix identities require superpolynomial Frege proofs: it seems that every Frege proof must in some sense construct the determinant, which is believed to require a superpolynomial-size formula.

A related question is whether the hard matrix identities and the determinant identities have a polynomial-size $\mathbf{NC}^2$-Frege proof—that is, a polynomial size proof using circuits of $O(\log^2 n)$-depth. $\mathbf{NC}^2$-Frege is a system which lies between Frege and extended Frege; its proofs can be simulated by polynomial-size extended Frege proofs and quasipolynomial-size Frege proofs. That such $\mathbf{NC}^2$-Frege proofs exist was conjectured in, e.g., [BBP95], based on the intuition that the determinant is $\mathbf{NC}^2$-computable, and so by the analogy between circuit classes and proofs, it is natural to assume that the determinant properties are efficiently provable in $\mathbf{NC}^2$-Frege. Again, a polynomial-size extended Frege proofs of the determinant identities have been constructed in [SC04]. Whether these identities have polynomial-size $\mathbf{NC}^2$-Frege proofs remained open. In this paper, we positively answer this

[1]The parameter $n$ is the dimension of the matrices $A, B$, and quasipolynomial size means size $n^{O(\log n)}$.

question: we show that over $GF(2)$, the hard matrix identities and the determinant identities have polynomial-size $\mathbf{NC}^2$-Frege proofs. This is a simple corollary of the results on arithmetic proof systems. Over the two element field, an $O(\log^2 n)$-depth $\mathbb{P}_c$ proof is formally also $\mathbf{NC}^2$-Frege proof[2]. Thus, if determinant identities like $\det(AB) = \det(A)\cdot\det(B)$ have polynomial-size $\mathbb{P}_c(GF(2))$ proofs with depth $O(\log^2 n)$, then the corresponding propositional tautologies have polynomial-size $\mathbf{NC}^2$-Frege proofs.

Let us remark that one can also consider propositional translations of the determinant identities (and the hard matrix identities) over different finite fields or even the rationals. There is no apparent obstacle to extending our result to other fields. We do not study these translations, simply in order not to make the paper even longer.

To understand our construction of short arithmetic proofs for the determinant identities, let us consider the following example. In [Ber84], Berkowitz constructed a quasipolynomial size arithmetic formula for the determinant. He used a clever combinatorial argument designed *specifically* for the determinant function. However, one can build such a formula in a completely oblivious way: first compute the determinant by, say, Gaussian elimination algorithm. This gives an arithmetic circuit with division gates. Second, show that any circuit with division gates computing a polynomial can be efficiently simulated by a division-free circuit [Str73], and finally, show that any arithmetic circuit of a polynomial degree can be transformed to an $O(\log^2 n)$-depth circuit computing the same polynomial, with only a polynomial increase in size [VSBR83] (or to a formula with at most a quasipolynomial increase in size [Hya79]). This paper follows a similar strategy, but in the proof-theoretic framework.

It should be stressed that in full generality, the structural theorems about $\mathbb{P}_c$ and $\mathbb{P}_f$ *cannot* be reproduced for propositional Frege and extended Frege systems. As already mentioned, no non-trivial simulation between Frege and extended Frege is known, and the other theorems are difficult to even formulate in the Boolean context. This also illustrates one final point: in order to construct a Frege proof of a tautology $T$, it may be useful to interpret $T$ as a polynomial identity and prove it in some of the—weaker but better structured—arithmetic proof systems.

### 1.1 Arithmetic proofs with circuits and formulas

Before presenting and explaining the main results of this paper (in Section 2), we need to introduce our basic arithmetic proof systems.

**Arithmetic circuits and formulas.** Let $\mathbb{F}$ be a field. *An arithmetic circuit $F$* is a finite directed acyclic graph as follows. Nodes (or gates) of in-degree zero are labeled with either a variable or a field element in $\mathbb{F}$. All the other nodes have in-degree two and they are labeled by either $+$ or $\times$. Unless stated otherwise, we assume that $F$ has exactly one node of out-degree zero, called the *output node*, and that moreover the two edges going into a gate $v$ labeled with $\times$ or $+$ are labeled with *left* and *right*. This is to determine the order of addition and multiplication[3]. An arithmetic circuit is called a *formula*, if the underlying graph is a tree. The *size* of a circuit is the number of nodes in it, and the *depth* of a circuit is the length of

[2] When $+$ and $\cdot$ modulo 2 are interpreted as Boolean connectives and $=$ is interpreted as logical equivalence.
[3] Although ultimately, addition and multiplication are commutative.

the longest directed path in it. Arithmetic circuits and formulas will be referred to simply as *circuits* and *formulas*.

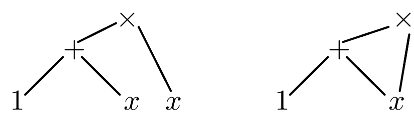
For a circuit $F$ and a node $u$ in $F$, $F_u$ denotes the subcircuit of $F$ with output node $u$. If $F, G$ are circuits then

$$F \oplus G \text{ and } F \otimes G$$

abbreviate *any* circuit $H$ whose output node is $u + v$ or $u \cdot v$, respectively, where $H_u$ is the circuit $F$ and $H_v$ the circuit $G$. Furthermore,

$$F + G \text{ and } F \cdot G$$

denote the unique circuit of the form $F' \oplus G'$ and $F' \otimes G'$, respectively, where $F'$, $G'$ are disjoint copies of $F$ and $G$. In particular, if $F$ and $G$ are formulas then so are $F + G$ and $F \cdot G$. For example, $(1 + x) \otimes x$ can be any of the following two circuits:




The first one is the formula $(1 + x) \cdot x$.

*Substitution* is understood in the following sense. Let $F = F(z)$ be a circuit and $z$ a variable. For a circuit $G$, the circuit $F(G)$ is defined as follows: let $z_1, \ldots, z_k$ be the nodes in $F$ labeled with $z$. Introduce $k$ disjoint copies $G_1, \ldots, G_k$ of $G$, and let $F(G)$ be the union of $F, G_1, \ldots, G_k$ where we replace the node $z_i$ by the output node of $G_i$. Specifically, if $F$ and $G$ are formulas then so is $F(G)$. The circuit $F(G)$ will also be written as $F(z/G)$.

**Polynomials.** A polynomial over the field $\mathbb{F}$ is a formal sum of (commuting) products of variables and elements of $\mathbb{F}$. The ring of polynomials in variables $X$ is denoted $\mathbb{F}[X]$. We emphasize that over a finite field, there is a difference between a polynomial and the function it represents. For example, over $GF(2)$, $x^2$ and $x$ are distinct polynomials whereas $x^2 = x$ holds for every $x \in GF(2)$.

A circuit $F$ computes a polynomial $\widehat{F} \in \mathbb{F}[X]$ with coefficients from $\mathbb{F}$ in the obvious manner:

(i). if $F$ consists of a single node labeled with $z$, a variable or an element of $\mathbb{F}$, we have $\widehat{F} := z$.

(ii). If $F$ is of the form $G \oplus H$ or $G \otimes H$, we let $\widehat{F} := \widehat{G} + \widehat{H}$ or $\widehat{F} := \widehat{G} \cdot \widehat{H}$, respectively.

**The system $\mathbb{P}_f(\mathbb{F})$**

We now define two proof systems for deriving polynomial identities. The systems manipulate *arithmetic equations*, that is, expressions of the form $F = G$. In the case of $\mathbb{P}_f(\mathbb{F})$, $F, G$ are formulas, and in the case of $\mathbb{P}_c(\mathbb{F})$, $F, G$ are circuits (see [HT09] for similar proof systems).

Let $\mathbb{F}$ be a field. The system $\mathbb{P}_f(\mathbb{F})$ proves equations of the form $F = G$, where $F, G$ are *formulas* over $\mathbb{F}$. The inference rules are:

| | | | |
|---|---|---|---|
| R1 | $\dfrac{F = G}{G = F}$ | R2 | $\dfrac{F = G \qquad G = H}{F = H}$ |
| R3 | $\dfrac{F_1 = G_1 \qquad F_2 = G_2}{F_1 + F_2 = G_1 + G_2}$ | R4 | $\dfrac{F_1 = G_1 \qquad F_2 = G_2}{F_1 \cdot F_2 = G_1 \cdot G_2}$. |

The axioms are equations of the following form, with $F, G, H$ formulas:

| | | | |
|---|---|---|---|
| A1 | $F = F$ | | |
| A2 | $F + G = G + F$ | A3 | $F + (G + H) = (F + G) + H$ |
| A4 | $F \cdot G = G \cdot F$, | A5 | $F \cdot (G \cdot H) = (F \cdot G) \cdot H$ |
| A6 | $F \cdot (G + H) = F \cdot G + F \cdot H$ | | |
| A7 | $F + 0 = F$ | A8 | $F \cdot 0 = 0$ |
| A9 | $F \cdot 1 = F$ | | |
| A10 | $a = b + c\,, a' = b' \cdot c'\,,$ | | if $a, b, c, a', b', c' \in \mathbb{F}$, are such that the equations hold in $\mathbb{F}$. |

The rules and axioms can be divided into two groups. The rules R1-R4 and axiom A1 determine the logical properties of equality "=", and axioms A2-A10 assert that polynomials form a commutative ring over $\mathbb{F}$.

*A proof $S$ in $\mathbb{P}_f(\mathbb{F})$* is a sequence of equations $F_1 = G_1$, $F_2 = G_2, \ldots, F_k = G_k$, with $F_i, G_i$ formulas, such that every equation is either an axiom A1-A10, or was obtained from previous equations by one of the rules R1-R4. An equation $F_i = G_i$ appearing in a proof is also called a *proof line*. We consider two measures of complexity for $S$: the *size of $S$* is the sum of the sizes of $F_i$ and $G_i$, $i \in [k]$, and $k$ is the *number of proof lines of $S$*. (Throughout the paper, $[k]$ stands for $\{1, \ldots, k\}$.)

### The system $\mathbb{P}_c(\mathbb{F})$

The system $\mathbb{P}_c(\mathbb{F})$ differs from $\mathbb{P}_f(\mathbb{F})$ in that it manipulates equations with *circuits*. $\mathbb{P}_c(\mathbb{F})$ has the same rules R1-R4 and axioms A1-A10 as $\mathbb{P}_f(\mathbb{F})$, but with $F, G, H, F_1, F_2, G_1, G_2$ *ranging over circuits*, augmented with the following two axioms:

| | | | |
|---|---|---|---|
| C1 | $F_1 \oplus F_2 = F_1 + F_2$ | C2 | $F_1 \otimes F_2 = F_1 \cdot F_2$. |

A *proof in* $\mathbb{P}_c(\mathbb{F})$ is a sequence of equations $F_1 = G_1, \ldots, F_k = G_k$, where $F_i, G_i$ are circuits, and every equation is either an axiom or was derived by one of the rules. As in $\mathbb{P}_f(\mathbb{F})$, the *size* of a proof is the sum of the sizes of all the circuits $F_i$ and $G_i$, $i \in [k]$, and $k$ is again the *number of proof lines*. The *depth* of a $\mathbb{P}_c(\mathbb{F})$ proof is the maximal depth of a circuit appearing in the proof.

The main property of the two proof systems $\mathbb{P}_c(\mathbb{F})$ and $\mathbb{P}_f(\mathbb{F})$ is that they are sound and complete with respect to polynomial identities. The systems prove an equation $F = G$ if and only if $F, G$ compute the same polynomial:

**Proposition 1.1.** *Let $\mathbb{F}$ be a field.*

*(i). For any pair $F, G$ of arithmetic formulas, $\mathbb{P}_f(\mathbb{F})$ proves $F = G$ iff $\widehat{F} = \widehat{G}$.*

*(ii). For any pair $F, G$ of arithmetic circuits, $\mathbb{P}_c(\mathbb{F})$ proves $F = G$ iff $\widehat{F} = \widehat{G}$.*

Part ((i)) was shown in [HT09], part ((ii)) is almost identical. Soundness can be easily proved by induction on the number of lines and completeness by rewriting $F$ and $G$ as a sum of monomials.

It should be noted that $\mathbb{P}_f$ and $\mathbb{P}_c$ proofs are closed under substitution. If $F_1 = G_1, \ldots, F_k = G_k$ is a $\mathbb{P}_c$ proof, $z$ a variable and $H$ a circuit then $F_1(z/H) = G_1(z/H), \ldots, F_k(z/H) = G_k(z/H)$ is also a $\mathbb{P}_c$ proof (similarly for $\mathbb{P}_f$ and a formula $H$). This means that from a general proof, one can obtain the proof of its instance.

For simplicity, we often suppress the explicit dependence on the field $\mathbb{F}$ in $\mathbb{P}_c$ and $\mathbb{P}_f$, if the relevant statement holds over any field.

**Comments on the proof systems.** The system $\mathbb{P}_c$ is an algebraic analogue of the propositional proof system *circuit Frege* (CF). Circuit Frege is polynomially equivalent to the more well-known *extended Frege* system (EF) (see [Kra95, Jeř04]). Following this analogy, one can define an *extended* $\mathbb{P}_f$ proof system, $\mathrm{E}\mathbb{P}_f$, as follows: an $\mathrm{E}\mathbb{P}_f$ proof is a $\mathbb{P}_f$ proof in which we are allowed to introduce new "extension" variables $z_1, z_2, \ldots$ via the axiom $z_i = F_i$, where we require that (i) the variable $z_i$ appears in neither $F_i$ nor in any previous proof-line; and (ii) the last equation in the proof contains none of the extension variables $z_1, z_2, \ldots$ .

The following is completely analogous to the propositional case (see [Kra95, Jeř04]):

**Proposition 1.2.**

*(i). The systems $\mathbb{P}_c$ and $\mathrm{E}\mathbb{P}_f$ polynomially simulate each other. More exactly, there is a polynomial $p$ such that for every pair of formulas $F, G$, if $F = G$ has a $\mathbb{P}_c$ proof of size $s$ then it has an $\mathrm{E}\mathbb{P}_f$ proof of size $p(s)$, and if $F = G$ has an $\mathrm{E}\mathbb{P}_f$ proof of size $s$ then it has a $\mathbb{P}_c$ proof of size $p(s)$.*

*(ii). If $F$ and $G$ are circuits of size $s$ and $F = G$ has a $\mathbb{P}_c$ proof with $k$ proof lines then $F = G$ has a $\mathbb{P}_c$ proof of size $\mathrm{poly}(s, k)$.*

The second part of this statement can be especially useful, because it is often easier to estimate the number of lines in a proof rather than its size.

**Remark 1.3.** *An alternative, polynomially equivalent, definition of $\mathbb{P}_c$ can be given as follows. For a circuit $F$, define $F^\bullet$ as the unfolding of $F$ into a* formula. *That is, $F^\bullet := F$, if $F$ is a leaf, and $(G \oplus H)^\bullet := G^\bullet + H^\bullet$, $(G \otimes H)^\bullet := G^\bullet \cdot H^\bullet$. We say that $F$ and $G$ are* similar circuits, *if $F^\bullet$ is the same formula as $G^\bullet$. Then* A1, C1, C2 *could be replaced by the following single axiom:*

A1' $\qquad F = G, \qquad$ *whenever $F$ and $G$ are similar.*

*The axiom* A1' *can be proved from* A1, C1, C2 *by a polynomial-size proof, and vice versa.*

## 1.2 List of technical notation

This paper contains quite a few definitions. Here we provide a concise list for easier navigation.

The letters $f, g, \ldots$ typically stand for polynomials or rational functions. The letters $F, G, \ldots$ usually denote arithmetic circuits. Division gates are not allowed unless otherwise stated.

| | | |
|---|---|---|
| $F_u$ | subcircuit of $F$ rooted at $u$ | Section 1.1 |
| $\oplus$, $\otimes$ $+$, $\cdot$ | circuit addition and multiplication | Section 1.1 |
| $\deg F$, $\deg u$ | syntactic degree of $F$ or $F_u$ | Section 2.2 |
| $F^{\bullet}$ | unfolding of $F$ into a formula | Remark 1.3 |
| $\widehat{F}$ | the polynomial (resp. rational function) computed by $F$ | Section 1.1 (resp. Section 2.3) |
| $F^{(k)}$ | $k$-homogeneous part of $F$ | Section 3 |
| $F^{\sharp}$ | non-redundant version of $F$ | Section 3 |
| $[F]$ | balancing of $F$ | Section 4 |
| $\mathrm{Num}(F)$, $\mathrm{Den}(F)$ | numerator, denominator | Section 6 |
| $\mathrm{pow}_k(1-z)$ | $:= 1 + z + \cdots + z^k$ | Section 5.1 |
| $\Delta_{z^k}(F)$ | $k$-th term of the Taylor expansion around $z = 0$ | Section 5.2 |
| DET | circuit with divisions computing the determinant | Section 7.1 |
| det | circuit without divisions computing the determinant | Equation (7.8) |
| $\det_c$, $\det_f$ | $[\det]$, $[\det]^{\bullet}$, respectively | Equation (8.1) |

**Notation for matrices inside proofs.** In this paper, matrices are understood as matrices whose entries are circuits and operations on matrices are operations on circuits. We illustrate this for square matrices. Let $F = \{F_{ij}\}_{i,j\in[n]}$ be an $n \times n$ matrix whose entries are circuits $F_{ij}$; and similarly $G = \{G_{ij}\}_{i,j\in[n]}$. Addition and multiplication is defined in the obvious way, namely

$$F + G = \{F_{ij} + G_{ij}\}_{i,j\in[n]}\,,\ F \cdot G = \left\{\sum\nolimits_{p=1}^{n} F_{ip} \cdot G_{pj}\right\}_{i,j\in[n]}\,,$$

where $+$ and $\cdot$ on the right-hand side is addition and multiplication on circuits. If $a$ is a single circuit, $a \cdot F$ is the matrix $\{a \cdot F_{ij}\}_{i,j\in[n]}$. An equation $F = G$ denotes the set of equations $F_{ij} = G_{ij}$, $i, j \in [n]$.

# 2 Overview of results and techniques

## 2.1 Main theorem

The determinant of a matrix can be characterized in several ways, such as the cofactor expansion, or its behavior under elementary row and column operations. The latter definition immediately allows to perform Gaussian elimination and is the one adopted in [SC04]. We choose to characterize the determinant by the following two identities. For any pair of $n \times n$ matrices $X, Y$ and any (upper or lower) triangular matrix $Z$ with $z_{11}, \ldots, z_{nn}$ on the diagonal,

$$\det(X \cdot Y) = \det(X) \cdot \det(Y), \tag{2.1}$$

$$\det(Z) = z_{11} \cdots z_{nn}. \tag{2.2}$$

That (2.1) and (2.2) indeed uniquely define the determinant follows from the fact that every square matrix is a product of triangular matrices. Moreover, other properties of the determinant, such as the cofactor expansion, easily follow from (2.1) and (2.2).

The main goal of this paper is to prove the following theorem:

**Theorem 2.1** (Main theorem)**.** *For any field $\mathbb{F}$:*

*(i). There exists a circuit* det *such that* (2.1) *and* (2.2) *have polynomial-size $\mathbb{P}_c(\mathbb{F})$ proofs. Moreover, every*[4] *circuit in the proof has depth at most $O(\log^2(n))$.*

*(ii). There exists a formula* det *such that* (2.1) *and* (2.2) *have $\mathbb{P}_f(\mathbb{F})$ proofs of size $n^{O(\log n)}$.*

**Organization of the paper.** As mentioned before, a large portion of the proof of Theorem 2.1 is not related directly to the determinant. It is rather a series of structural theorems about the systems $\mathbb{P}_f$ and $\mathbb{P}_c$. These are obtained by reproducing classical results in arithmetic circuit complexity in the setting of arithmetic proofs (for a recent survey on arithmetic circuit complexity see [SY10]). However, this is often not a straightforward task. For we must not only construct arithmetic circuits with desired properties, but also show that our proof system can efficiently prove such properties. We recommend the reader to have a glance at classical arithmetic complexity texts before moving to its proof theoretic aspect.

Sections 3 to 6 contain the structural results. The most important of these is Theorem 2.2, proved in Section 4. It shows that $\mathbb{P}_c$ proofs can be balanced, in the sense that a $\mathbb{P}_c$ proofs of size $s$ (of an equation with a polynomial syntactic degree) can be polynomially simulated by a $\mathbb{P}_c$ proof in which every circuit has depth $O(\log^2 s)$. This also implies that a $\mathbb{P}_c$ proof can be transformed to a $\mathbb{P}_f$ proof of quasipolynomial-size. A prerequisite of Theorem 2.2 is Proposition 2.5, Section 3. It asserts that in order to prove an equation of (syntactic) degree $d$, one does not need to use intermediary equations of degree greater than $d$.

The second important structural result is Theorem 2.7, proved in Section 5. We introduce the system $\mathbb{P}_c^{-1}$ which operates with circuits *with divisions*, and proves equalities between rational functions (rather than polynomials). Theorem 2.7 asserts that a $\mathbb{P}_c^{-1}$ proof, with divisions, can be simulated by a $\mathbb{P}_c$ proof, without divisions. A prerequisite of the Theorem 2.7 is Theorem 2.8 proved in in Section 6. Given a finite field $\mathbb{F}_1$ and its *extension* $\mathbb{F}_2$, we show how to polynomially simulate $\mathbb{P}_c(\mathbb{F}_2)$ proofs by $\mathbb{P}_c(\mathbb{F}_1)$ proofs.

Sections 7 to 8 deal with the determinant itself and conclude Theorem 2.1. Essentially, the determinant is first computed by a circuit *with division* gates, by a version of Gaussian elimination, and its properties (2.1) and (2.2) are proved inside the system $\mathbb{P}_c^{-1}$. The division gates are then eliminated by means of Theorem 2.7. Finally, we invoke Theorem 2.2 to balance the proofs.

In Section 9 and 2.5, we present several applications of Theorem 2.1. Theorem 2.11 asserts that the hard matrix identities have polynomial-size $\mathbf{NC}^2$-Frege proofs; Proposition 2.9 formalizes Valiant's completeness of the determinant; We also give short $\mathbb{P}_c$ proofs of the cofactor expansion and the Cayley-Hamilton theorem.

We do not know whether it is possible to prove Theorem 2.1 directly, perhaps by formalizing the elegant algorithm of Berkowitz [Ber84]. One advantage of the algorithm is that,

[4] We assume that the product $z_{11} \cdots z_{nn}$ in (2.2) is written as a formula of depth $O(\log n)$.

being division-free, it would dispense of Theorem 2.7 and allow to generalize Theorem 2.1 to an arbitrary commutative ring (as opposed to a field). We also admit that working with circuits and proofs with divisions turned out to be quite tedious. However, our construction is intended to emphasize general properties of arithmetic proof systems, and the structural theorems are in fact our main contribution.

We now describe the results in a greater detail.

## 2.2 Balancing $\mathbb{P}_c$ proofs and simulating $\mathbb{P}_c$ by $\mathbb{P}_f$

In the seminal paper [VSBR83], Valiant et al. showed that if a polynomial $f$ of degree $d$ can be computed by an arithmetic circuit of size $s$, then $f$ can be computed by a circuit of size $\mathrm{poly}(s,d)$ and depth $O(\log s \log d + \log^2 d)$. This is a strengthening of an earlier result by Hyafil [Hya79], showing that $f$ can be computed by a formula of size $(s(d+1))^{O(\log d)}$. We will show that those results can be efficiently simulated within the framework of arithmetic proofs.

Instead of the degree of a polynomial, we focus on the syntactic degree of a circuit. Let $F$ be an arithmetic circuit. *The syntactic degree* of $F$, $\deg F$, is defined as follows:

(i). If $F$ is a field element or a variable, then $\deg F = 0$ and $\deg F = 1$, respectively;

(ii). $\deg(F \oplus G) = \max(\deg F, \deg G)$, and $\deg(F \otimes G) = \deg F + \deg G$.

If $F$ is a circuit and $v$ is a node in $F$ we also write $\deg(v)$ to denote $\deg F_v$.

In accordance with [VSBR83], we will construct a map $[\cdot]$ that maps any given circuit $F$ of size $s$ and syntactic degree $d$ to a circuit $[F]$ computing the same polynomial, such that $[F]$ has size $\mathrm{poly}(s,d)$ and depth $O(\log s \log d + \log^2 d)$. We will show the following (recall that the depth of a proof is the maximum depth of a circuit in it):

**Theorem 2.2.** *Let $F, G$ be circuits of syntactic degree at most $d$.*

*(i). If $F$ is a circuit of size $s$ and depth $t$ then $F = [F]$ has a $\mathbb{P}_c$ proof of size* $\mathrm{poly}(s,d)$ *and depth $O(t + \log s \cdot \log d + \log^2 d)$.*

*(ii). If $F = G$ has a $\mathbb{P}_c$ proof of size $s$ then $[F] = [G]$ has a $\mathbb{P}_c$ proof of size* $\mathrm{poly}(s,d)$ *and depth $O(\log s \cdot \log d + \log^2 d)$.*

This readily implies:

**Corollary 2.3.** *Assume that $F, G$ are circuits of syntactic degree $\leq d$ and depth $\leq t$. If $F = G$ has a $\mathbb{P}_c$ proof of size $s$ then it has a $\mathbb{P}_c$ proof of size* $\mathrm{poly}(s,d)$ *and depth $O(t + \log s \cdot \log d + \log^2 d)$.*

We also obtain the following simulation of $\mathbb{P}_c$ by $\mathbb{P}_f$:

**Theorem 2.4.** *Assume that $F, G$ are formulas of syntactic degree $\leq d$ such that $F = G$ has a $\mathbb{P}_c$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_f$ proof of size $s^{O(\log d)}$ $\left(\leq s^{O(\log s)}\right)$.*

This simulation is polynomial if $F$ and $G$ have a constant syntactic degree. Let us emphasize that the syntactic degree of a formula of size $s$ is at most $s$, and hence the simulation is at most *quasipolynomial*.

Theorem 2.2 is arguably the most interesting (and technically most difficult) result in this paper. The map $[F]$ is constructed in essentially the same way as in [VSBR83]. While this construction is already non-trivial, we are then left with the additional challenge of proving its properties inside $\mathbb{P}_c$.

**Homogenization and degree bound in arithmetic proofs.** One ingredient of Theorems 2.2 and 2.4 is to show that using circuits of high syntactic degree cannot significantly shorten $\mathbb{P}_c$ proofs. That is, if we want to prove an equation of syntactic degree $d$, we can without loss of generality use only circuits of syntactic degree at most $d$. This result is the proof-theoretic analog of a result by Strassen, who showed how to separate arithmetic circuits into their homogeneous parts (implicit in [Str73]).

We say that a circuit $F$ is *syntactically homogeneous*, if for every sum-gate $u_1 + u_2$ in $F$ we have $\deg(u_1) = \deg(u_2)$. For a circuit $F$ and a number $k$, we introduce a circuit $F^{(k)}$ which computes the syntactically $k$-homogeneous part of $F$ (see Section 3 for the definition). The *syntactic degree of a $\mathbb{P}_c$ proof* is the maximal syntactic degree of a circuit appearing in it. We show the following:

**Proposition 2.5.** *Assume that $F = G$ has a $\mathbb{P}_c$ proof of size $s$. Then*

*(i).* $F^{(k)} = G^{(k)}$ *has a $\mathbb{P}_c$ proof of size $s \cdot \mathrm{poly}(k)$ and a syntactic degree at most $k$, for any $k$.*

*(ii). If $\deg(F), \deg(G) \leq d$ then $F = G$ has a $\mathbb{P}_c$ proof of syntactic degree at most $d$ and size $s \cdot \mathrm{poly}(d)$.*

The proof is a rather straightforward inductive argument. On the other hand, the Proposition captures a key aspect of arithmetic proofs: that the degree of equations in a proof can be bounded by the degree of the equation being proved. This has no counterpart in classical Boolean proofs.

## 2.3 Circuits and proofs with division

We denote by $\mathbb{F}(X)$ the field of formal rational functions in the variables $X$ over the field $\mathbb{F}$. It is convenient to extend the notion of a circuit so that it computes rational functions in $\mathbb{F}(X)$. This is done in the following way: *a circuit with division* $F$ is a circuit which may contain an additional type of gate with fan-in 1, called an *inverse* or a *division* gate, denoted $(\cdot)^{-1}$. Such a circuit either computes a rational function $\widehat{F} \in \mathbb{F}(X)$, or the circuit $F$ is not *well-defined* (i.e., contains division by 0). Formally, we keep the conditions (i) and (ii) from the division-free definition of $\widehat{F}$, stipulating that $G \oplus H$ or $G \otimes H$ is well-defined iff both $G$ and $H$ are. The extra condition is:

*(iii)* If $F$ is of the form $G^{-1}$ then $\widehat{F} := 1/\widehat{G}$ provided $G$ is well-defined and $\widehat{G} \neq 0$. Otherwise, $F$ is not well-defined.

One should note, for instance, that the circuit $(x^2+x)^{-1}$ over $GF(2)$ is well-defined, since $x^2+x$ is *not* the zero rational function (although it vanishes as a function over $GF(2)$).

We define the system $\mathbb{P}_c^{-1}(\mathbb{F})$, operating with equations $F = G$ where $F$ and $G$ are circuits with division. First, we extend the axioms of $\mathbb{P}_c(\mathbb{F})$ to apply to well-defined circuits with division. Second, we add the following new axiom:

$$\text{D} \qquad\qquad F \cdot F^{-1} = 1\,, \quad \text{provided that } F^{-1} \text{ is well-defined.}$$

**Remark 2.6.** *The system $\mathbb{P}_c^{-1}(\mathbb{F})$ polynomially simulates the rule*

$$\frac{F = G}{F^{-1} = G^{-1}}\,, \quad \textit{if } \widehat{F}, \widehat{G} \neq 0\,.$$

*Moreover, the identities $(F^{-1})^{-1} = F$ and $(F \cdot G)^{-1} = G^{-1} \cdot F^{-1}$ have linear size proofs in $\mathbb{P}_c^{-1}(\mathbb{F})$.*

As before, we sometimes suppress the explicit dependence on the field in $\mathbb{P}_c^{-1}(\mathbb{F})$ whenever the relevant statement is field independent.

Strassen [Str73] showed that division gates can be eliminated from arithmetic circuits computing polynomials over large enough fields, with only a polynomial increase in size. We will show the proof-theoretic analog of Strassen's result over *arbitrary* fields, namely that $\mathbb{P}_c(\mathbb{F})$ polynomially simulates $\mathbb{P}_c^{-1}(\mathbb{F})$ for any field $\mathbb{F}$, in the following sense:

**Theorem 2.7.** *Let $\mathbb{F}$ be any field and assume that $F$ and $G$ are circuits without division gates such that $\deg F, \deg G \leq d$. Suppose that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_c(\mathbb{F})$ proof of size $\mathrm{poly}(s, d)$.*

A corollary of Theorem 2.7 is that $\mathbb{P}_c$ polynomially simulates the rule

$$\frac{F \cdot G = 0}{F = 0}\,, \qquad \text{if} \quad \widehat{G} \neq 0\,,$$

provided the syntactic degree of $G$ is polynomially bounded.

Over a large enough $\mathbb{F}$, Theorem 2.7 is an adaptation of Strassen's original proof. The idea is to replace an inverse gate by a power series, truncated at a large enough degree. For example, $(1-x)^{-1}$ would be replaced by the series $1 + x + x^2 + \cdots + x^k$. This does not equal $(1-x)^{-1}$ exactly, but serves as a good approximation when dealing with polynomials of degree $\leq k$. (Note that $(1-x)(1+x+\cdots+x^k) = 1 - x^{k+1}$). A drawback of this construction is that in order to eliminate $f(x)^{-1}$, we need an $a \in \mathbb{F}$ with $f(a) \neq 0$, hence the field $\mathbb{F}$ has to be large enough.

**Simulating large fields in small fields.** To prove Theorem 2.7, we first assume that the underlying field $\mathbb{F}$ has an exponential size. Under this assumption, we cannot eliminate division gates in $GF(2)$ which is, from the Boolean proof complexity viewpoint, the most interesting field. To deal with small fields, and $GF(2)$ in particular, we have to show how to simulate large fields in small ones:

**Theorem 2.8.** *Let $p$ be a prime power and $n$ a natural number. Let $F, G$ be circuits over $GF(p)$. Assume that $F = G$ has a $\mathbb{P}_c(GF(p^n))$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_c(GF(p))$ proof of size $s \cdot \mathrm{poly}(n)$.*

The idea of the theorem is to treat the elements of $GF(p^n)$ as $n \times n$ matrices over $GF(p)$. This enables one to simulate computations and proofs over $GF(p^n)$ by those over $GF(p)$. In a nutshell, an element $a \in GF(p^n)$ is identified with an $n \times n$-matrix with entries over $GF(p)$, and a circuit $F$ over $GF(p^n)$ with an $n \times n$-matrix $\overline{F}$ of circuits over $GF(p)$. A $GF(p^n)$-proof of $F = G$ translates to a $GF(p)$-proof of the matrix equation $\overline{F} = \overline{G}$ (in fact, a list of $n^2$ equations expressing equality entry-wise). Finally, if $F, G$ are polynomials already over $GF(p)$ then $\overline{F} = I_n \cdot F$ and $\overline{G} = I_n \cdot G$ and so the equation $F = G$ is obtained by looking at the first entry in the matrix identity $\overline{F} = \overline{G}$.

### 2.4 The determinant as a rational function and as a polynomial

To prove the main theorem (Theorem 2.1) we need to construct a circuit (and a formula) which computes the determinant and which can be used efficiently inside arithmetic proofs. We first compute the determinant as a *rational function*, using a circuit with divisions denoted $\mathrm{DET}(X)$, and show that $\mathbb{P}_c^{-1}$ admits short proofs of the properties of $\mathrm{DET}(X)$. This is achieved by defining $\mathrm{DET}(X)$ in terms of the matrix inverse $X^{-1}$ and inferring properties of DET from the identities $X \cdot X^{-1} = X^{-1}X = I_n$, which are shown to have polynomial-size $\mathbb{P}_c^{-1}$ proofs. The argument is basically a Gaussian elimination.

However, we cannot yet conclude Theorem 2.1 which speaks about (division-free) $\mathbb{P}_c$ proofs (it is worth mentioning that we also cannot yet conclude the short $\mathbf{NC}^2$-Frege proofs for the determinant identities, because $\mathbb{P}_c^{-1}$ proofs do not immediately correspond to propositional Frege proofs). Theorem 2.7 cannot be directly applied because it allows to eliminate division gates in $\mathbb{P}_c^{-1}$ proofs only if the equations proved are themselves division-free. We therefore proceed to construct a division-free circuit $\det(X)$, computing the determinant as a *polynomial*. Assuming we can prove efficiently in $\mathbb{P}_c^{-1}$ that $\det(X) = \mathrm{DET}(X)$, we are done, since we can now eliminate division gates from $\mathbb{P}_c^{-1}$ proofs of division-free equations, using Theorem 2.7. To this end, we define the $\det(X)$ polynomial as the $n$th term of the Taylor expansion of $\mathrm{DET}(I_n + zX)$ at $z = 0$. This enables us to construct short proofs of $\det(X) = \mathrm{DET}(X)$ and conclude the argument.

### 2.5 Applications

Equipped with feasible proofs of the determinant identities, short proofs of several related identities follow. Cofactor expansion of the determinant and a version of the Cayley-Hamilton theorem will be given in Section 9. Another example is the formula completeness of the determinant. In [Val79], Valiant showed that every formula of size $s$ can be written as a projection of a determinant of a matrix of a linear dimension. We can conclude that this holds feasibly already in $\mathbb{P}_c$:

**Proposition 2.9.** *Let $F$ be a formula of size $s$. Then there exists a matrix $M$ of dimension $2s \times 2s$ whose entries are variables or elements of $\mathbb{F}$ such that the identity*

$$F = \det(M)$$

*has a polynomial-size $O(\log^2 s)$-depth $\mathbb{P}_c(\mathbb{F})$ proof (resp. a quasipolynomial-size $\mathbb{P}_f(\mathbb{F})$ proof), where* det *is the circuit (resp. the formula) from Theorem 2.1.*

In this paper we are mainly interested in proofs with *no* assumptions other than the axioms A1-A10. Nevertheless, we can introduce the notion of a *proof from assumptions* as follows: let $S$ be a set of equations. Then *a $\mathbb{P}_c$ proof from the assumptions $S$* is a proof that can use equations in $S$ as additional axioms (and similarly for $\mathbb{P}_f$ proofs from assumptions). Proofs from assumptions are far less well-behaved than standard arithmetic proofs. For instance, neither Theorem 2.4 nor Theorem 2.7 hold for proofs from a general set $S$ of assumptions. We now give an important example of a proof from assumptions.

Given a pair of $n \times n$ matrices $X, Y$, recall that the expressions $XY = I_n$ and $YX = I_n$, are abbreviations for the list of $n^2$ equalities between the appropriate entries. ( $I_n$ is the $n \times n$ identity matrix.)

**Proposition 2.10.** *Let $\mathbb{F}$ be any field. The equations $YX = I_n$ have polynomial-size and $O(\log^2 n)$-depth $\mathbb{P}_c(\mathbb{F})$ proofs from the equations $XY = I_n$. In the case of $\mathbb{P}_f(\mathbb{F})$, the proof has a quasipolynomial-size.*

**Determinant identities in $\mathbf{NC}^2$-Frege and Frege systems.** When considering the field $\mathbb{F}$ to be $GF(2)$, there is a close connection between our proof systems and the standard propositional proof systems. Consider the propositional proof systems Frege ($F$), extended Frege ($EF$) and circuit Frege ($CF$). For the definitions of Frege and extended Frege see [Kra95] and for the definition of circuit Frege see [Jeřo04], where it is also shown that $CF$ and $EF$ are polynomially equivalent.

For simplicity, we shall assume that $F$, $EF$ and $CF$ are all in the Boolean basis $+, \cdot, 0, 1$ (addition and multiplication modulo 2, and the two Boolean constants)[5]. Then every arithmetic circuit *is automatically also a Boolean circuit*, and an equality like $G = H$ can be interpreted as the logical equivalence $G \equiv H$, written as the boolean formula $(G + H) + 1$. Hence $\mathbb{P}_f(GF(2))$ and $\mathbb{P}_c(GF(2))$ can be considered as *fragments* of $F$ and $CF$, respectively: the finite set of (schematic) axioms and rules of $\mathbb{P}_f(GF(2))$ now serve as Frege axioms and rules, and similarly for $\mathbb{P}_c(GF(2))$. Note that $x^2 = x$ is a propositional tautology but not a polynomial identity, and hence $F$ and $CF$ are (expressively) stronger than their arithmetic counterparts. In fact, one can polynomially simulate the full $F$ or $CF$ systems by adding the following new axiom

$$G^2 = G$$

to $\mathbb{P}_f(GF(2))$ or $\mathbb{P}_c(GF(2))$, where $G$ is any formula or a circuit, respectively. To see this, it is sufficient to show that the augmented systems are complete with respect to propositional tautologies: they prove $F = 1$ whenever $F$ evaluates to 1 on every $0, 1$-input.

This means that upper bounds in $\mathbb{P}_f(GF(2))$ and $\mathbb{P}_c(GF(2))$ are in fact upper bounds in $F$ and $CF$ (and hence also in $EF$), respectively.

In the next theorem, $XY = I_n$, and similarly $YX = I_n$, denote the conjunction of $n^2$ formulas of the form $\sum_{j\in[n]} x_{i,j} \cdot y_{j,k} \equiv \delta_{ik}$, where $+, \cdot$ are addition and multiplication modulo 2, respectively, $\equiv$ is the logical equivalence, and $\delta_{ik} \in \{0, 1\}$ is given by $\delta_{ik} = 1$ iff $i = k$. We have the following:

**Theorem 2.11.**

[5]Note that by Reckhow's result, as stated in [Kra95], the particular choice of basis is immaterial. We could also have $\equiv$ as a primitive.

*(i). The properties of the determinant as in Theorem 2.1 (interpreted as Boolean tautologies over $GF(2)$) have polynomial-size circuit Frege proofs, with every circuit of depth at most $O(\log^2 n)$. In the case of Frege, the proofs have quasipolynomial-size.*

*(ii). The implication $(XY = I_n) \to (YX = I_n)$ has a polynomial-size circuit Frege proof, with every circuit of depth at most $O(\log^2 n)$, and a quasipolynomial-size Frege proof.*

*Proof.* Part (i) is a direct consequence of Theorem 2.1 and (ii) of Proposition 2.10, both using the fact that proofs in $\mathbb{P}_c(GF(2))$ and $\mathbb{P}_f(GF(2))$ can be interpreted as proofs in circuit Frege and Frege, respectively. QED

A family of polynomial-size CF proofs in which every proof-line $G$ is of depth $O(\log^2 |G|)$, is also called an $\mathbf{NC}^2$-Frege proof. Hence, Theorem 2.11 states that $\mathbf{NC}^2$-Frege has polynomial-size proofs of the propositional tautologies $(XY = I_n) \to (YX = I_n)$.

Theorem 2.11 thus settles an important open problem in proof complexity and feasible mathematics, namely, whether basic properties of the determinant like $\det(A) \cdot \det(B) = \det(AB)$ and the cofactor expansion (see Proposition 9.1), as well as the hard matrix identities, have polynomial-size proofs in a proof system which corresponds to the circuit class $\mathbf{NC}^2$.

**Remark 2.12.** *We believe that Theorem 2.11 can be extended to any finite field or the field of rationals (after encoding field elements as Boolean strings). For finite fields, this is rather straightforward. In the rational case, one would have to show that the $\mathbb{P}_c(\mathbb{Q})$ proofs constructed in Theorem 2.1 involve only constants whose Boolean representation is polynomial.*

## 3 Homogenization and bounding the degree in $\mathbb{P}_c(\mathbb{F})$ proofs

In this section we want to construct the circuits $F^{(k)}$ computing the $k$-homogeneous part of $F$ and prove Proposition 3.3. First, let us say that a circuit $F$ is *non-redundant*, if either $F$ is the constant 0, or $F$ does not contain the constant 0 at all. Any circuit $F$ can be transformed to a non-redundant circuit $F^\sharp$ as follows: successively replace all nodes of the form $u + 0$, $0 + u$ by $u$ and $u \cdot 0$, $0 \cdot u$ by 0, until no such replacement is possible.

Let $k$ be a natural number. We define $F^{(k)}$ as follows. For every node $u$ in $F$, introduce $k+1$ new nodes $u^{(0)}, \ldots, u^{(k)}$.

(i). Assume $u$ is a leaf. Then, $u^{(0)} := u$, in case $u$ is a field element, and $u^{(1)} := u$ in case $u$ is a variable, and $u^{(i)} := 0$ otherwise.

(ii). If $u = u_1 + u_2$, let $u^{(i)} := u_1^{(i)} + u_2^{(i)}$, for every $i = 0, \ldots, k$.

(iii). If $u = u_1 \cdot u_2$, let $u^{(i)} := \sum_{j=0}^{i} u_1^{(j)} \cdot u_2^{(i-j)}$.

Finally, we define $F^{(k)}$ as the circuit $G^\sharp$, where $G$ is the circuit with the output node $w^{(k)}$ and $w$ is the output node of $F$.

Note the following:

(1) $F^{(k)}$ has size $O(s(k+1)^2)$, where $s$ is the size of $F$.

(2) $F^{(k)}$ is a syntactically homogeneous non-redundant circuit. Its syntactic degree is either $k$, or $F^{(k)}$ is the constant 0.

**Notation**: We allow circuits and formulas to use only sum gates with fan-in two. An expression $\sum_{i=1}^{k} x_i$ is an abbreviation for a formula of size $O(k)$ and depth $O(\log k)$ with binary sum gates. For example, define $\sum_{i=1}^{k} x_i := \sum_{i=1}^{\lfloor k/2 \rfloor} x_i + \sum_{i=\lfloor k/2 \rfloor+1}^{k} x_i$. One can see that basic identities such as

$$\sum_{i=1}^{k} x_i = \sum_{i=1}^{m} x_i + \sum_{i=m+1}^{k} x_i\,, \quad \text{or} \quad y \cdot \sum_{i=1}^{k} x_i = \sum_{i=1}^{k} y x_i$$

have $\mathbb{P}_f$ proofs of size $O(k^2)$ and depth $O(\log k)$.

**Lemma 3.1.** *Let $F_1, F_2$ be circuits of size $\leq s$ and $k$ a natural number. The following have proofs of size $s \cdot \mathrm{poly}(k)$ and syntactic degree $\leq k$.*

*(i).* $(F_1 \oplus F_2)^{(k)} = F_1^{(k)} + F_2^{(k)}$,

*(ii).* $(F_1 \otimes F_2)^{(k)} = \sum_{i=0}^{k} F_1^{(i)} \cdot F_2^{(k-i)}$.

*Proof.* By definition, $(F_1 \oplus F_2)^{(k)}$ is either of the form $F_1^{(k)} \oplus F_2^{(k)}$, or it is the circuit $F_e^{(k)}$ and $F_{e'}^{(k)}$ is 0, $\{e, e'\} = \{1, 2\}$. In the former case, $(F_1 \oplus F_2)^{(k)} = F_1^{(k)} + F_2^{(k)}$ by axiom C1. The latter is given by $F = F + 0 = 0 + F$. This concludes (i). Part (ii) is similar. QED

**Lemma 3.2.** *If $F$ is a circuit with syntactic degree $\leq d$ and size $s$, then*

$$F = \sum_{k=0}^{d} F^{(k)}$$

*has a $\mathbb{P}_c(\mathbb{F})$ proof of syntactic degree $\leq d$ and size $s \cdot \mathrm{poly}(d)$.*

*Proof.* For every node $u$ in $F$, construct a proof of $F_u = \sum_{k=0}^{\deg(u)} F_u^{(k)}$. This is done by induction on depth of $u$. If $u$ is a leaf, this stems from the definition of $F_u^{(k)}$, and if $u = u_1 + u_2$ or $u = u_1 \cdot u_2$, it is an application of the previous lemma. QED

We now prove:

**Proposition 3.3** (Proposition 2.5 restated)**.** *Assume that $F = G$ has a $\mathbb{P}_c$ proof of size $s$. Then*

*(i).* $F^{(k)} = G^{(k)}$ *has a $\mathbb{P}_c$ proof of size $s \cdot \mathrm{poly}(k)$ and a syntactic degree at most $k$, for any $k$.*

*(ii).* *If $\deg(F), \deg(G) \leq d$ then $F = G$ has a $\mathbb{P}_c$ proof of syntactic degree at most $d$ and size $s \cdot \mathrm{poly}(d)$.*

*Proof.* Part (ii) follows from (i) by Lemma 3.2, hence it is sufficient to prove part (i). Let us first show that if $F = G$ is an axiom of $\mathbb{P}_c(\mathbb{F})$ of size $s$ then $F^{(k)} = G^{(k)}$ has a proof of size $s \cdot \mathrm{poly}(k)$ and syntactic degree $\leq k$. This is an application of Lemma 3.1. Let $c$ be the constant such that equations (i) and (ii) in Lemma 3.1 have proofs of size $O(s \cdot (k+1)^c)$.

The lemma gives a proof $(F_1 \oplus F_2)^{(k)} = (F_1 + F_2)^{(k)}$ and $(F_1 \otimes F_2)^{(k)} = (F_1 \cdot F_2)^{(k)}$, as required for the axioms C1 and C2.

Axioms A1 and A10 are immediate. For the other axioms, consider for example the axiom $F_1 \cdot (F_2 \cdot F_3) = (F_1 \cdot F_2) \cdot F_3$, where the circuits have size $\leq s$. We have to construct a proof of

$$(F_1 \cdot (F_2 \cdot F_3))^{(k)} = ((F_1 \cdot F_2) \cdot F_3)^{(k)} . \tag{3.1}$$

By part (ii) of Lemma 3.1 the equations

$$(F_1 \cdot (F_2 \cdot F_3))^{(k)} = \sum_{i=0}^{k} F_1^{(i)} \left( \sum_{j=0}^{k-i} F_2^{(j)} F_3^{(k-i-j)} \right) \tag{3.2}$$

$$((F_1 \cdot F_2) \cdot F_3)^{(k)} = \sum_{i=0}^{k} \left( \sum_{j=0}^{i} F_1^{(j)} F_2^{(i-j)} \right) \cdot F_3^{(k-i)} , \tag{3.3}$$

can be proved by proofs with size roughly $s \cdot (k+1)^c \cdot (k+1)$. In $\mathbb{P}_c(\mathbb{F})$, the right hand sides of both (3.2) and (3.3) can be written as $\sum_{i+j+l=k} F_1^{(i)} F_2^{(j)} F_3^{(l)}$, by a proof of size roughly $s(k+1)^4$. This gives the proof of (3.1) of size $s \cdot \mathrm{poly}(k)$.

Next, assume that $F = G$ is derived from the equations $F_1 = G_1, F_2 = G_2$ by means of the rules R1-R4, and we need to construct the proof of $F^{(k)} = G^{(k)}$ from the set of equations $F_1^{(i)} = G_1^{(i)}, F_2^{(i)} = G_2^{(i)}, i = 0, \ldots k$. The hardest case is the rule

$$\frac{F_1 = G_1 \qquad F_2 = G_2}{F_1 \cdot F_2 = G_1 \cdot G_2} .$$

We have to prove $(F_1 \cdot F_2)^{(k)} = (G_1 \cdot G_2)^{(k)}$. By Lemma 3.1, we have proofs of $(F_1 \cdot F_2)^{(k)} = \sum_{i=0,\ldots k} F_1^{(i)} F_2^{(k-i)}$ and $(G_1 \cdot G_2)^{(k)} = \sum_{i=0,\ldots k} G_1^{(i)} G_2^{(k-i)}$. Hence $(F_1 \cdot F_2)^{(k)} = (G_1 \cdot G_2)^{(k)}$ can be proved from the assumptions $F_1^{(i)} = G_1^{(i)}, F_2^{(i)} = G_2^{(i)}, i = 0, \ldots k$. The proof has size roughly $s \cdot (k+1)^c (k+1)$. QED

# 4 Balancing $\mathbb{P}_c$ proofs

In this section we prove Theorem 4.5 which is a proof-complexity analog of the following result:

**Theorem 4.1** (Valiant et al. [VSBR83])**.** *Let $F$ be an arithmetic circuit of size $s$ computing a polynomial $f$ of degree $d$. Then there exists an arithmetic circuit $[F]$ computing $f$ with depth $O(\log^2 d + \log s \cdot \log d)$ and size* $\mathrm{poly}(d, s)$*.*

### 4.1 Constructing balanced circuits $[F]$

We first give an outline of the construction of $[F]$, which closely follows that in [VSBR83] (we also refer the reader to [RY08] for an especially clear exposition). We emphasize that in our case, the relevant parameter is the *syntactic* degree of $F$: $[F]$ will have size $\mathrm{poly}(s,d)$ and depth $O(\log^2 d + \log s \cdot \log d)$, where $d$ is the syntactic degree of $F$.

#### 4.1.1 Outline of construction

We write $u \in F$ to mean that $u$ is a node in the circuit $F$. The following definition is important for the construction of balanced circuits: let $w, v$ be two nodes in $F$. We define the *polynomial* $\partial w F_v$ as follows:

$$\partial w F_v := \begin{cases} 0, & \text{if } w \notin F_v, \\ 1, & \text{if } w = v \text{ , and otherwise:} \\ \partial w F_{v_1} + \partial w F_{v_2}, & v = v_1 + v_2; \\ (\partial w F_{v_1}) \cdot F_{v_2}, & \text{if either } v = v_1 \cdot v_2 \text{ and } \deg(v_1) \geq \deg(v_2), \\ & \text{or } v = v_2 \cdot v_1 \text{ and } \deg(v_1) > \deg(v_2). \end{cases}$$

The idea behind this definition is the following: let $w, v$ be two nodes in $F$ such that $2\deg(w) > \deg(v)$. Then for any product node $v_1 \cdot v_2 \in F_v$, $w$ can be a node in at most one of $F_{v_1}, F_{v_2}$, namely the one of a higher syntactic degree. If we replace the node $w$ in $F_v$ by a new variable $z$, $F_v$ then computes a polynomial $g(z, x_1, \dots, x_n)$ which is linear in $z$, and $\partial w F_v$ is the usual partial derivative $\partial z g$.

It is not hard to show the following:

**Claim 4.2.** *Let $w, v$ be two nodes in a circuit $F$. Then the polynomial $\partial w F_v$ has degree at most* $\deg(v) - \deg(w)$.

In order to construct $[F]$, we can assume without loss of generality that $F$ itself is a syntactically homogenous circuit of size $s' = O(d^2 \cdot s)$. This is because a circuit of size $s$ and syntactic degree $d$ can be written as a sum of $d+1$ syntactically homogeneous circuits of size at most $s'$ and syntactic degree at most $d$. Now the construction proceeds by induction on $i = 0, \dots, \lceil \log d \rceil$. In each step $i = 0, \dots, \lceil \log d \rceil$ we construct:

(i). Circuits computing $\widehat{F}_v$, for all nodes $v$ in $F$ with $2^{i-1} < \deg(v) \leq 2^i$;

(ii). Circuits computing $\partial w F_v$, for all nodes $w, v$ in $F$ with $2^{i-1} < \deg(v) - \deg(w) \leq 2^i$ and $\deg(v) < 2\deg(w)$.

Each step adds depth $O(\log s')$, which at the end amounts to a depth $O(\log^2 d + \log d \cdot \log s)$ circuit. Furthermore, each node $v$ in $F$ adds $O(s')$ nodes in the new circuit and each pair of nodes $v, w$ in $F$ adds also $O(s')$ nodes in the new circuit. This finally amounts to a circuit of size $O(s'^3) = O(d^6 \cdot s^3)$.

#### 4.1.2 Formal definition of $[F]$

Let us now give the formal definition of $[F]$. First, for a circuit $G$ and a natural number $m$, let

$$\mathcal{B}_m(G) := \{t \in G \ : \ t = t_1 \cdot t_2, \deg(t) > m \text{ and } \deg(t_1), \deg(t_2) \leq m\}.$$

Let $F$ be an arithmetic circuit of syntactic degree $d$. If $F$ is not syntactic homogenous, let

$$[F] := [F^{(0)}] + \ldots + [F^{(d)}] .$$

Otherwise, assume that $F$ is a syntactically homogenous circuit of degree $d$. For any *node* $v \in F$ we introduce the corresponding *node* $[F_v]$ in $[F]$ (intended to compute the polynomial $\widehat{F}_v$); and for any pair of nodes $v, w \in F$ such that $2\deg(w) > \deg(v)$, we introduce the node $[\partial w F_v]$ in $[F]$ (intended to compute the polynomial $\partial w F_v$).

The construction is defined by induction on $i = 0, \ldots, \lceil \log d \rceil$, as follows:

**Part (I): definition of $[\mathbf{F_v}]$.** Let $v \in F$:

**Case 1**: Assume that $\deg(v) \le 1$. Then $F_v$ either computes a field element $a$ or a linear polynomial $\sum_i a_i x_i$. (For the sake of uniqueness, we stipulate that the $a_i$'s are non-zero). Define

$$[F_v] := a\,, \text{ or } [F_v] = \sum a_i x_i\,, \text{ respectively.}$$

**Case 2**: Assume that for some $0 \le i \le \lceil \log(d) \rceil$:

$$2^i < \deg(v) \le 2^{i+1}.$$

Put $m = 2^i$, and define

$$[F_v] := \sum_{t \in \mathcal{B}_m(F_v)} [\partial t F_v] \cdot [F_{t_1}] \cdot [F_{t_2}],$$

where $t_1, t_2$ are nodes such that $t = t_1 \cdot t_2$. (Note that here $[\partial t F_v], [F_{t_1}]$ and $[F_{t_2}]$ are *nodes*.)

**Part (II): definition of $[\partial \mathbf{w} \mathbf{F_v}]$.** Let $w, v$ be a pair of nodes in $F$ with $2\deg(w) > \deg(v)$:

**Case 1**: Assume $w$ is not a node in $F_v$. Define

$$[\partial w F_v] := 0.$$

**Case 2**: Assume that $w$ is in $F_v$ and $0 \le \deg(v) - \deg(w) \le 1$. Thus, by Claim 4.2, the polynomial $\partial w f_v$ is a linear polynomial $a_1 x_1 + \ldots + a_n x_n + b$. Define

$$[\partial w F_v] := a_1 x_1 + \ldots + a_n x_n + b.$$

**Case 3**: Assume that $w$ is in $F_v$ and that for some $0 \le i \le \lceil \log(d) \rceil$:

$$2^i < \deg(v) - \deg(w) \le 2^{i+1}.$$

Put $m = 2^i + \deg(w)$. Define:

$$[\partial w F_v] := \sum_{t \in \mathcal{B}_m(F_v)} [\partial t F_v] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}]\,,$$

where $t_1, t_2$ are nodes such that $t = t_1 \cdot t_2$ and $\deg(t_1) \geq \deg(t_2)$, or $t = t_2 \cdot t_1$ and $\deg(t_1) > \deg(t_2)$. Finally, define $[F]$ as the circuit with the output node $[F_u]$, where $u$ is the output node of $F$.

One should make sure that $[F]$ is well defined, and that it has the correct depth and size:

**Lemma 4.3.** *Let $F$ be a circuit of size $s$ and syntactic degree $d$. Then $[F]$ is a circuit computing $\widehat{F}$, $[F]$ is of size $\mathrm{poly}(s,d)$ and depth $O(\log^2 d + \log s \log d)$. Moreover, every node $[\partial w F_v]$ in $[F]$ computes the polynomial $\partial w F_v$.*

*Proof.* The proof is as in [VSBR83] (see also [RY08]). We shall give a partial sketch of the proof here, for the benefit of the reader.

First, assume that $F$ is syntactically homogeneous of degree $d$. We need to verify that $[F]$ is well-defined. That is, at stage $i = 0, \ldots, \lceil \log d \rceil$, we compute all $[F_v]$ and $[\partial_w F_u]$ for all nodes $v, u, w \in F$ such that $2^i < \deg(v) \leq 2^{i+1}$ and $2^i < \deg(v) - \deg(u) \leq 2^{i+1}$, and we want to show that the computation uses only nodes computed in previous stages.

Take, for example, Case 2 in Part (I). For any $t \in \mathcal{B}_m(F_v)$, $m < \deg(t) \leq \deg(v) \leq 2m$. This implies that $\deg(v) - \deg(t) \leq m = 2^i$ and $\deg(t) < 2\deg(v)$. Hence, we have already computed $[\partial t F_v]$. We have also already constructed $[F_{t_1}], [F_{t_2}]$, since $\deg(t_1), \deg(t_2) < m = 2^i$.

Inspecting the construction, $[F]$ has size $\mathrm{poly}(s)$ and depth $O(\log s \cdot \log d)$, given that $F$ is syntactically homogeneous of size $s$ and degree $d$. If $F$ is not syntactically homogeneous, the definition $[F] = \left[F^{(0)}\right] + \cdots + \left[F^{(d)}\right]$ gives a circuit of size $\mathrm{poly}(s,d)$ and depth $O(\log^2 d + \log s \cdot \log d)$, since every $F^{(k)}$ has size $O(s \cdot k^2)$. QED

## 4.2 Proof of the balancing lemma

We need to show that properties of $[F]$ can be proved inside the system $\mathbb{P}_c$. The key ingredient is given by the following lemma.

**Lemma 4.4** (Main simulation lemma)**.** *Let $F_1, F_2$ be circuits of syntactic degree at most $d$ and size at most $s$. Then there exist $\mathbb{P}_c$ proofs of:*

$$[F_1 \oplus F_2] = [F_1] + [F_2]\,, \tag{4.1}$$

$$[F_1 \otimes F_2] = [F_1] \cdot [F_2]\,, \tag{4.2}$$

*such that the proofs have size $\mathrm{poly}(s,d)$ and depth $O(\log d \cdot \log s + \log^2 d)$. Furthermore, $[z] = z$ has a constant-size proof whenever $z$ is a variable or a field element.*

The proof of Lemma 4.4 is deferred to the end of this section. We now use Lemma 4.4 to prove Theorems 4.5 and 4.8.

**Theorem 4.5** (Theorem 2.2 restated)**.** *Let $F, G$ be circuits of syntactic degree at most $d$.*

*(i). If $F$ is a circuit of size $s$ and depth $t$ then $F = [F]$ has a $\mathbb{P}_c$ proof of size $\mathrm{poly}(s,d)$ and depth $O(t + \log s \cdot \log d + \log^2 d)$.*

*(ii). If $F = G$ has a $\mathbb{P}_c$ proof of size $s$ then $[F] = [G]$ has a $\mathbb{P}_c$ proof of size $\mathrm{poly}(s,d)$ and depth $O(\log s \cdot \log d + \log^2 d)$.*

*Proof.* Part (i) is a straightforward induction on $t$ using Lemma 4.4. For $0 \le k \le t$, let us construct a proof $S_k$ which contains the equation $[F_v] = F_v$, for every node $v$ in $F$ such that $F_v$ has depth $\le k$.

If $k = 0$, it is sufficient to prove the equations $[z] = z$ in $S_0$, for all leaves $z$ in $F$. The proof $S_{k+1}$ is obtained by augmenting $S_k$ with the proof of $[F_v] = F_v$ for every $v$ with $F_v$ of depth $k+1$, as follows. If $F_v$ has depth $k+1$ then $v = v_1 \circ v_2$, where $F_{v_1}, F_{v_2}$ have depth $\le k$ and $\circ \in \{+, \cdot\}$. The Lemma gives $[F_v] = [F_{v_1}] \circ [F_{v_2}]$. The equations $[F_{v_i}] = F_{v_i}$, $i \in \{1,2\}$, are contained in $S_k$, which gives a proof of $[F_v] = F_{v_1} \circ F_{v_2} = F_v$.

The proof has size $\mathrm{poly}(s, d)$. The depth of the proof never exceeds the depth of $F$ and the depth of the proofs of $[F_v] = [F_{v_1}] \circ [F_{v_2}]$.

Part (ii). Assume that $F = G$ has syntactic degree $d$ and a $\mathbb{P}_c$ proof of size $s$. By Proposition 3.3, $F = G$ has a $\mathbb{P}_c$ proof of syntactic degree $d$ and size $s' = s \cdot \mathrm{poly}(d)$. So let us consider such a proof $S$. By induction on the number of lines in $S$, construct a $\mathbb{P}_c$ proof of $[F_1] = [F_2]$, where $F_1 = F_2$ is a line in $S$.

Let $m_0$ and $k_0$ be such that (4.1) and (4.2) have $\mathbb{P}_c$ proofs of size at most $m_0$ and depth $k_0$, whenever $F_1 \oplus F_2$, respectively, $F_1 \otimes F_2$ have size at most $s'$ and syntactic degree at most $d$. By Lemma 4.4, we can choose $m_0 = \mathrm{poly}(s', d)$ and $k_0 = O(\log s' \cdot \log d + \log^2 d)$.

First, show that if a line $F = H$ in $S$ is a $\mathbb{P}_c$ *axiom* then $[F] = [H]$ has a $\mathbb{P}_c$ proof of size $c_1 m_0$ and depth $c_2 k_0$, where $c_1, c_2$ are some constants independent of $s', d$. The axiom A1 is immediate and the axiom A10 follows from the fact that $[F] = \widehat{F}$, if $\deg(F) = 0$. The rest of the axioms are an application of Lemma 4.4, as follows. Axioms C1 and C2 are already the statement of Lemma 4.4. For the other axioms, take, for example,

$$F_1 \cdot (G_1 + G_2) = F_1 \cdot G_1 + F_1 \cdot G_2 \,.$$

We are supposed to give a proof of

$$[F_1 \cdot (G_1 + G_2)] = [F_1 \cdot G_1 + F_1 \cdot G_2] \,,$$

with a small size and depth. By Lemma 4.4 we have a $\mathbb{P}_c$ proof

$$[F_1 \cdot (G_1 + G_2)] = [F_1] \cdot [G_1 + G_2] = [F_1] \cdot ([G_1] + [G_2]) = [F_1] \cdot [G_1] + [F_1] \cdot [G_2] \,.$$

Lemma 4.4 gives again:

$$[F_1] \cdot [G_1] + [F_1] \cdot [G_2] = [F_1 \cdot G_1] + [F_1 \cdot G_2] = [F_1 \cdot G_1 + F_1 \cdot G_2] \,.$$

Here we applied Lemma 4.4 to circuits of size at most $s'$, and the proof of $[F_1 \cdot (G_1 + G_2)] = [F_1 \cdot G_1 + F \cdot G_2]$ has size at most, say, $100 m_0$ and depth at most $10 k_0$.

An application of rules R1, R2 translates to an application of R1, R2. For the rules R3 and R4, it is sufficient to show the following: if $S$ uses the rule

$$\frac{F_1 = F_2 \qquad G_1 = G_2}{F_1 \circ G_1 = F_2 \circ G_2}, \circ \in \{\cdot, +\},$$

then there is a proof of $[F_1 \circ G_1] = [F_2 \circ G_2]$, of size $c_1 m_0$ and depth $c_2 k_0$, from the equations $[F_1] = [G_1]$ and $[F_2] = [G_2]$. This is again an application of Lemma 4.4.

Altogether, we obtain a proof of $[F] = [G]$ of size at most $c_1 s' m_0$ and depth $c_2 k_0$. QED

**Corollary 4.6** (Corollary 2.3 restated)**.** *Assume that $F, G$ are circuits of syntactic degree $\leq d$ and depth $\leq t$. If $F = G$ has a $\mathbb{P}_c$ proof of size $s$ then it has a $\mathbb{P}_c$ proof of size* $\mathrm{poly}(s, d)$ *and depth $O(t + \log s \cdot \log d + \log^2 d)$.*

Recall the definition of the formula $F^\bullet$ from Remark 1.3. Note that if $F$ is a formula of size $s$ and $\deg F = d$ then $[F]^\bullet$ is an equivalent formula of depth $O(\log s \log d + \log^2 d) = O(\log s \log d)$ and size $s^{O(\log d)}$ (note that $d \leq s$ if $F$ is a formula).

**Lemma 4.7.** *(i). Let $F, G$ be circuits such that $F = G$ has a $\mathbb{P}_c$ proof of size $s$ and depth $k$, then $F^\bullet = G^\bullet$ has a $\mathbb{P}_f$ proof of size $O(s2^k)$.*

*(ii). If $F$ is a formula of size $s$ and* $\deg F = d$*, then $F = [F]^\bullet$ has a $\mathbb{P}_f$ proof of size $s^{O(\log d)}$.*

*Proof.* Part (i) is straightforward: every proof line $F_1 = F_2$ in a $\mathbb{P}_c$ proof translates to a proof line $F_1^\bullet = F_2^\bullet$ in a $\mathbb{P}_f$ proof. The size of $F_1^\bullet, F_2^\bullet$ grows by at most a factor of $2^k$.

Part (ii). Lemma 4.4 and part (i) show that $[F_1 + F_2]^\bullet = [F_1]^\bullet + [F_2]^\bullet$ and $[F_1 \cdot F_2]^\bullet = [F_1]^\bullet \cdot [F_2]^\bullet$ have $\mathbb{P}_f$ proofs of size $s^{O(\log d)}$, for any subformulas of $F$. The proof of $F = [F]^\bullet$ can now be easily constructed by induction on the size of $F$ (as in the proof of Theorem 4.5 part (i)). QED

**Theorem 4.8** (Theorem 2.4 restated)**.** *Assume that $F, G$ are formulas of syntactic degree at most $d$ such that $F = G$ has a $\mathbb{P}_c$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_f$ proof of size $s^{O(\log d)}$.*

*Proof.* Part (ii) of the last Lemma gives $\mathbb{P}_f$ proofs of $F = [F]^\bullet$ and $G = [G]^\bullet$ of size $s^{O(\log d)}$. By Theorem 4.5 part (ii), $[F] = [G]$ has a $\mathbb{P}_c$ proof of depth $O(\log s \log d)$ and size polynomial in $s$. By Lemma 4.7 part (i), $[F]^\bullet = [G]^\bullet$ has a $\mathbb{P}_f$ of size $s^{O(\log d)}$. QED

Part (ii) of Lemma 4.7 transforms a formula of size $s$ into a formula of depth $O(\log^2 s)$. This is hardly optimal—we know that a formula of size $s$ is equivalent to a formula of depth $O(\log s)$ (see [Brent74] or [Spi71] in the boolean case). For $\mathbb{P}_f$ proofs, one could obtain a stronger version of proof balancing:

**Remark 4.9.** *There is a map which to every formula $F$ assigns an equivalent formula $F^b$ such that $F^b$ has depth $O(\log s)$ whenever $F$ has size $s$, and such that the following hold:*

*(i). If $F$ has depth $t$ and size $s$ then $F = F^b$ has a $\mathbb{P}_f$ proof of depth $O(t)$ and size* $\mathrm{poly}(s)$*.*

*(ii). If $F = G$ has a $\mathbb{P}_f$ proof of size $s$ then $F^b = G^b$ has a $\mathbb{P}_f$ proof of size $s$ and depth $O(\log s)$.*

#### 4.2.1 Proof of Lemma 4.4

We now prove Lemma 4.4. The statement concerning $[z] = z$ is clear: if $z$ is a field element, $[z]$ and $z$ are the same circuit. If $z$ is a variable, $[z]$ is the circuit $1 \cdot z$.

We need to construct proofs of Equations (4.1) and (4.2). First, we note that it is enough to consider the syntactically homogeneous case:

**Claim.** *If Lemma 4.4 holds under the assumption that $F_1 \oplus F_2$ and $F_1 \otimes F_2$ are syntactically homogeneous, then it holds in general.*

*Proof.* First, note that for any circuit of syntactic degree $d$,

$$[F] = \left[F^{(0)}\right] + \left[F^{(1)}\right] + \cdots + \left[F^{(d)}\right]$$

has a proof of size $\mathrm{poly}(s,d)$ and depth $O(\log d \cdot \log s + \log^2 d)$: if $F$ is not syntactically homogeneous, this is by definition of $[F]$; otherwise, $F$ is syntactically homogeneous, and so $[F^{(k)}]$ is the circuit 0 whenever $k < d$. Hence it is sufficient to construct the proof of $[F] = [F^{(d)}]$, which can be done by induction on the size of $F$, applying the Lemma only to syntactically homogeneous circuits (cf. the proof of Theorem 4.5 part (i)).

Second, if for example $F_1 \oplus F_2$ is not syntactically homogenous, then by definition of $[\cdot]$, we have

$$[F_1 \oplus F_2] = \sum_{k=0}^{d} \left[(F_1 \oplus F_2)^{(k)}\right] ,$$

where $d = \deg(F_1 \oplus F_2)$. By the definition of $F^{(k)}$, $(F_1 \oplus F_2)^{(k)}$ is a syntactically homogeneous circuit which is either of the form $F_1^{(k)} \oplus F_2^{(k)}$, or it is of the form $F_e^{(k)}$, if $F_{e'}^{(k)} = 0$, $\{e, e'\} = \{1, 2\}$. In both cases we obtain a proof of $[(F_1 \oplus F_2)^{(k)}] = [F_1^{(k)}] + [F_2^{(k)}]$, of small size and depth. This gives a $\mathbb{P}_c$ proof of

$$[F_1 \oplus F_2] = \sum_{k=0}^{d} \left[(F_1 \oplus F_2)^{(k)}\right] = \sum_{k=0}^{d} \left(\left[(F_1)^{(k)}\right] + \left[(F_2)^{(k)}\right]\right) = [F_1] + [F_2] \ .$$

QED

We thus consider the syntactically homogeneous case. Let $m(s,d)$ and $r(s,d)$ be functions such that for any circuit $F$ of syntactic degree $d$ and size $s$, $[F]$ has depth at most $r(s,d)$ and size at most $m(s,d)$. By Lemma 4.3, we can choose

$$m(s,d) = \mathrm{poly}(s,d) \quad \text{and} \quad r(s,d) = O(\log^2 d + \log d \cdot \log s).$$

**Notation**: In the following, $[F_v]$ and $[\partial w F_v]$ will denote *circuits*: $[F_v]$ and $[\partial w F_v]$ are the subcircuits of $[F]$ with output nodes $[F_v]$ and $[\partial w F_v]$, respectively; the defining relations between the nodes of $[F]$ (see the definition of $[F]$ above) translate to equalities between the corresponding circuits. For example, if $v$ and $m$ are as in part (I) Case 2, of the definition of $[F]$, then, using just the axioms C1 and C2, we can prove

$$[F_v] = \sum_{t \in \mathcal{B}_m(F_v)} [\partial t F_v] \cdot [F_{t_1}] \cdot [F_{t_2}] \,. \tag{4.3}$$

Here, the left hand side is understood as the circuit $[F_v]$ in which $[\partial t F_v], [F_{t_1}], [F_{t_2}]$ appear as *subcircuits*, and so can share common nodes, while on the right hand side the circuits have *disjoint nodes*. Also, note that if $F$ has size $s$ and degree $d$, the proof of (4.3) has size $O(s^2 m(s,d))$ and has depth $O(r(s,d))$. We shall use these kind of identities in the current proof.

The following (lengthy) proposition suffices to conclude the lemma. The recurrence (4.4) below implies $\lambda(s,d) = \mathrm{poly}(s,d)$ and it is enough to take $F$ in the statement as either $F_1 \oplus F_2$ or $F_1 \otimes F_2$, and $v$ as the root of $F$.

**Proposition 4.10.** *Let $F$ be a syntactically homogenous circuit of syntactic degree $d$ and size $s$, and let $i = 0, \ldots, \lceil \log d \rceil$. There exists a function $\lambda(s,i)$ not depending on $F$ with*

$$\lambda(s,0) = O(s^4) \quad \text{and} \quad \lambda(s,i) \le O(s^4 \cdot m(s,d)) + \lambda(s,i-1), \tag{4.4}$$

*and a $\mathbb{P}_c$ proof-sequence $\Psi_i$ of size at most $\lambda(s,i)$ and depth at most $O(r(s,d))$, such that the following hold:*

***Part (I):*** *For every node $v \in F$ with*

$$\deg(v) \le 2^i, \tag{4.5}$$

*$\Psi_i$ contains the following equations:*

$$[F_v] = [F_{v_1}] + [F_{v_2}]\ , \qquad \text{in case } v = v_1 + v_2, \qquad \text{and} \tag{4.6}$$

$$[F_v] = [F_{v_1}] \cdot [F_{v_2}]\ , \qquad \text{in case } v = v_1 \cdot v_2. \tag{4.7}$$

***Part (II):*** *For every pair of nodes $w \neq v \in F$, where $w \in F_v$, and with*

$$\deg(v) - deg(w) \le 2^i \qquad \text{and} \tag{4.8}$$

$$2\deg(w) > \deg(v), \tag{4.9}$$

*$\Psi_i$ contains the following equations:*

$$[\partial w F_v] = [\partial w F_{v_1}] + [\partial w F_{v_2}], \qquad \text{in case } v = v_1 + v_2; \tag{4.10}$$

$$[\partial w F_v] = [\partial w F_{v_1}] \cdot [F_{v_2}], \qquad \text{in case } v = v_1 \cdot v_2 \text{ and } \deg(v_1) \ge \deg(v_2) \text{ or } v = v_2 \cdot v_1 \text{ and } \deg(v_1) > \deg(v_2). \tag{4.11}$$

*Proof.* We proceed to construct the sequence $\Psi_i$ by induction on $i$.

<u>Base case</u>: $i = 0$. We need to devise the proof sequence $\Psi_0$.

**Part (I): proof of (4.6) and (4.7).** Let $\deg(v) \le 2^0$. By definition, $[F_v] = \sum_{i=1}^{n} a_i x_i + b$, where $a_i$'s and $b$ are field elements. If $v = v_1 + v_2$, we have also $[F_{v_e}] = \sum_{i=1}^{n} a_i^{(e)} x_i + b^{(e)}$, for $e = 1, 2$. Hence the equation $[F_v] = [F_{v_1}] + [F_{v_2}]$ is the (true) identity:

$$\sum_{i=1}^{n} a_i x_i + b = \sum_{i=1}^{n} a_i^{(1)} x_i + b^{(1)} + \sum_{i=1}^{n} a_i^{(2)} x_i + b^{(2)}\ ,$$

which has a proof of size $O(s^2)$ and depth $O(\log s)$ (we assume without loss of generality that $n \le s$).

In case $v = v_1 \cdot v_2$, either $\deg(v_1) = 0$ or $\deg(v_2) = 0$ and the proof of $[F_v] = [F_{v_1}] \cdot [F_{v_2}]$ is similar.

**Part (II): proof of (4.10) and (4.11).** Since $\deg(v) - \deg(w) \leq 1$, we have $[\partial w F_v] = \sum_{i=1}^{n} a_i x_i + b$, for some field elements $a_i$'s and $b$.

In case $v = v_1 + v_2$, we have $\deg(v_e) - \deg(w) \leq 1$ and so $[\partial w F_{v_e}] = \sum_{i=1}^{n} a_i^{(e)} x_i + b^{(e)}$, where $e = 1, 2$. The assumption $w \neq v$ and Lemma 4.3, guarantee that $[\partial w F_v] = [\partial w F_{v_1}] + [\partial w F_{v_2}]$ is a correct identity, and we can thus proceed as the base case of Part (I) above.

In case $v = v_1 \cdot v_2$, assume without loss of generality that $\deg(v_1) \geq \deg(v_2)$. Again, we have $[\partial w F_{v_1}] = \sum_{i=1}^{n} a_i^{(1)} x_i + b^{(1)}$. From the assumptions, we have that $w \in F_{v_1}$, which implies $\deg(v_1) \geq \deg(w)$ and so $\deg(v_2) \leq 1$. Hence $[F_{v_2}] = \sum_{i=1}^{n} a_i^{(2)} x_i + b^{(2)}$. (One can note that at least one of $[\partial w F_{v_1}]$ or $[F_{v_2}]$ is constant). Thus we can prove the (correct, by virtue of the assumption $w \neq v$) identity $[\partial w F_v] = [\partial w F_{v_1}] \cdot [F_{v_2}]$ with a $\mathbb{P}_c(\mathbb{F})$ proof of size $O(s^2)$ and depth $O(\log s)$.

Overall, $\Psi_0$ will be the union of all the above proofs, so that $\Psi_0$ contains all equations (4.6), (4.7) (for all nodes $v$ satisfying (4.5)), and all equations (4.10) and (4.11) (for all nodes $v, w$ satisfying (4.8) and (4.9)). The proof sequence $\Psi_0$ has size $\lambda(s, 0) = O(s^4)$ and is and depth $O(\log s)$.

<u>*Induction step*</u>: We wish to construct the proof-sequence $\Psi_{i+1}$.

**Part (I): proof of (4.6) and (4.7).** Let $v$ be any node in $F$ such that

$$2^i < \deg(v) \leq 2^{i+1}.$$

**Case 1**: Assume that $v = v_1 + v_2$. We show how to construct the proof of $[F_v] = [F_{v_1}] + [F_{v_2}]$. Let $m = 2^i$. From the definition of $[\cdot]$ we have:

$$[F_v] = [F_{v_1+v_2}] = \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t (F_{v_1+v_2})] \,. \tag{4.12}$$

Since $\deg(v_1) = \deg(v_2) = \deg(v)$, we also have

$$[F_{v_e}] = \sum_{t \in \mathcal{B}_m(F_{v_e})} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t (F_{v_e})], \quad \text{for } e \in \{0, 1\} \,. \tag{4.13}$$

If $t \in \mathcal{B}_m(F_v)$ then $\deg(t) > m = 2^i$. Therefore, for any $t \in \mathcal{B}_m(F_v)$, since $\deg(v) \leq 2^{i+1}$, we have $\deg(v) - \deg(t) < 2^i$ and $2\deg(t) > \deg(v)$ and $t \neq v$ (since $t$ is a product gate). Thus, by induction hypothesis, the proof-sequence $\Psi_i$ contains, for any $t \in \mathcal{B}_m(F_v)$, the equations

$$[\partial t (F_{v_1+v_2})] = [\partial t F_{v_1}] + [\partial t F_{v_2}].$$

Therefore, having $\Psi_i$ as a premise, we can prove that (4.12) equals:

$$\begin{aligned} &\sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot ([\partial t F_{v_1}] + [\partial t F_{v_2}]) \\ &= \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}] + \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_2}]. \end{aligned} \tag{4.14}$$

If $t \in \mathcal{B}_m(F_v)$ and $t \notin F_{v_1}$ then $[\partial t F_{v_1}] = 0$. Similarly, if $t \in \mathcal{B}_m(F_v)$ and $t \notin F_{v_2}$ then $[\partial t F_{v_2}] = 0$. Hence we can prove

$$\sum_{t \in \mathcal{B}_m(F_v)} [\partial t F_{v_e}] = \sum_{t \in \mathcal{B}_m(F_{v_e})} [\partial t F_{v_e}], \quad \text{for } e = 1, 2. \tag{4.15}$$

Thus, using (4.13) we have that (4.14) equals:

$$\begin{aligned} \sum_{t \in \mathcal{B}_m(F_{v_1})} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}] + \sum_{t \in \mathcal{B}_m(F_{v_2})} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_2}] \\ = [F_{v_1}] + [F_{v_2}]. \end{aligned} \tag{4.16}$$

The above proof of (4.16) from $\Psi_i$ has size $O(s^2 \cdot m(s,d))$ and depth $O(r(s,d))$.

**Case 2**: Assume that $v = v_1 \cdot v_2$. We wish to prove $[F_v] = [F_{v_1}] \cdot [F_{v_2}]$. Let $m = 2^i$. We assume without loss of generality that $\deg(v_1) \geq \deg(v_2)$. By the definition of $[\cdot]$, we have:

$$[F_v] = [F_{v_1 \cdot v_2}] = \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_v].$$

If $v \in \mathcal{B}_m(F_v)$, then $\mathcal{B}_m = \{v\}$ and we have $[F_v] = [F_{v_1}] \cdot [F_{v_2}] \cdot [\partial_v F_v]$. Since $[\partial_v F_v] = 1$, this gives $[F_v] = [F_{v_1}] \cdot [F_{v_2}]$, and we are done.

Otherwise, assume $v \notin \mathcal{B}_m(F_v)$. Then $m = 2^i < \deg(v_1)$ (since, if $\deg(v_1) \leq m$, then also $\deg(v_2) \leq m$ and so by definition $v \in \mathcal{B}_m(F_v)$). Further, because $\deg(v_1) \leq 2^{i+1}$, we have

$$[F_{v_1}] = \sum_{t \in \mathcal{B}_m(F_{v_1})} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}]. \tag{4.17}$$

Since $\deg(v) \leq 2^{i+1}$ and $\deg(t) > m = 2^i$, for any $t \in \mathcal{B}_m(F_v)$, we have

$$\deg(v) - \deg(t) \leq 2^i \quad \text{and} \quad 2\deg(t) > \deg(v).$$

Since $v \neq t$, by induction hypothesis, $\Psi_i$ contains, for any $t \in \mathcal{B}_m(F_v)$, the equation:

$$[\partial t(F_{v_1 \cdot v_2})] = [\partial t F_{v_1}] \cdot [F_{v_2}]. \tag{4.18}$$

Using (4.18) for all $t \in \mathcal{B}_m(F_v)$, we can prove the following with a $\mathbb{P}_c(\mathbb{F})$ proof of size $O(s^2 \cdot m(s,d))$ and depth $O(r(s,d))$:

$$\begin{aligned} \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_v] &= \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t(F_{v_1 \cdot v_2})] \\ &= \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot ([\partial t F_{v_1}] \cdot [F_{v_2}]) \\ &= [F_{v_2}] \cdot \sum_{t \in \mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}]. \end{aligned} \tag{4.19}$$

Since $\mathcal{B}_m(F_{v_1}) \subseteq \mathcal{B}_m(F_v)$, we can conclude as in (4.15) that

$$\sum_{t\in\mathcal{B}_m(F_v)} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}] = \sum_{t\in\mathcal{B}_m(F_{v_1})} [F_{t_1}] \cdot [F_{t_2}] \cdot [\partial t F_{v_1}] \,.$$

Using (4.17), (4.19) equals $[F_{v_2}] \cdot [F_{v_1}]$. The above proof-sequence (using $\Psi_i$ as a premise) has size $O(s^2 \cdot m(s,d))$ and depth $O(r(s,d))$.

We now append $\Psi_i$ with all proof-sequences of $[F_v] = [F_{v_1}] + [F_{v_2}]$ for every $v$ from Case 1, and all proof-sequences of $[F_v] = [F_{v_1}] \cdot [F_{v_2}]$ for every $v$ from Case 2. We obtain a proof-sequence $\Psi'_{i+1}$ of size

$$\lambda(s, i+1) \leq O(s^3 \cdot m(s,d)) + \lambda(s,i),$$

and depth $O(r(s,d))$.

In Part (II), we extend $\Psi'_{i+1}$ with more proof-sequences to obtain the final $\Psi_{i+1}$.

**Part (II): proof of (4.10) and (4.11).** Let $v \neq w$ be a pair of nodes in $F$ such that $w \in F_v$ and assume that

$$2^i < \deg(v) - \deg(w) \leq 2^{i+1} \quad \text{and} \quad 2\deg(w) > \deg(v).$$

Let

$$m = 2^i + \deg(w).$$

**Case 1**: Suppose that $v = v_1 + v_2$. We need to prove

$$[\partial w F_v] = [\partial w F_{v_1}] + [\partial w F_{v_2}] \tag{4.20}$$

based on $\Psi_i$ as a premise. By construction of $[\partial w F_v]$,

$$\begin{aligned} [\partial w F_v] &= \sum_{t\in\mathcal{B}_m(F_v)} [\partial t F_v] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] \\ &= \sum_{t\in\mathcal{B}_m(F_v)} [\partial t (F_{v_1+v_2})] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}]. \end{aligned} \tag{4.21}$$

Since $\deg(v_1) = \deg(v_2) = \deg(v)$, we also have

$$[\partial w F_{v_e}] = \sum_{t\in\mathcal{B}_m(F_{v_e})} [\partial t F_{v_e}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}], \quad \text{for } e = 1, 2\,. \tag{4.22}$$

Since $m = 2^i + \deg(w)$, we have $\deg(t) > 2^i + \deg(w)$, for any $t \in \mathcal{B}_m(F_v)$. Thus, by $\deg(v) - \deg(w) \leq 2^{i+1}$, we get that for any $t \in \mathcal{B}_m(F_v)$:

$$\deg(v) - \deg(t) \leq 2^i \quad \text{and} \quad 2\deg(t) > \deg(v), \quad \text{and}$$
$$t \neq v \text{ (since } t \text{ is a product gate).}$$

Therefore, by induction hypothesis, for any $t \in \mathcal{B}_m(F_v)$, $\Psi_i$ contains the equation

$$[\partial t(F_{v_1+v_2})] = [\partial t F_{v_1}] + [\partial t F_{v_2}].$$

Thus, based on $\Psi_i$, we can prove that (4.21) equals:

$$\begin{aligned} &\sum_{t\in\mathcal{B}_m(F_v)} ([\partial t F_{v_1}] + [\partial t F_{v_2}]) \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] \\ &= \sum_{t\in\mathcal{B}_m(F_v)} [\partial t F_{v_1}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] + \sum_{t\in\mathcal{B}_m(F_v)} [\partial t F_{v_2}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}]. \end{aligned} \tag{4.23}$$

As in (4.15), using (4.22) we can derive the following from (4.23):

$$\begin{aligned} \sum_{t\in\mathcal{B}_m(F_{v_1})} [\partial t F_{v_1}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] + \sum_{t\in\mathcal{B}_m(F_{v_2})} [\partial t F_{v_2}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] \\ = [\partial w F_{v_1}] + [\partial w F_{v_2}]. \end{aligned}$$

The proof of (4.20) from $\Psi_i$ shown above has size $O(s^2 \cdot m(s,d))$ and depth $O(r(s,d))$.

**Case 2**: Suppose that $v = v_1 \cdot v_2$. We assume without loss of generality that $\deg(v_1) \geq \deg(v_2)$ and show how to prove

$$[\partial w F_v] = [\partial w F_{v_1}] \cdot [F_{v_2}]. \tag{4.24}$$

By construction of $[\partial w F_v]$:

$$\begin{aligned} [\partial w F_v] &= \sum_{t\in\mathcal{B}_m(F_v)} [\partial t F_v] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] \\ &= \sum_{t\in\mathcal{B}_m(F_v)} [\partial t (F_{v_1\cdot v_2})] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}]. \end{aligned} \tag{4.25}$$

Similar to the previous case, for any $t \in \mathcal{B}_m(F_v)$ we have

$$\deg(v) - \deg(t) < 2^i \quad \text{and} \quad 2\deg(t) > \deg(v).$$

If $v \in \mathcal{B}_m(F_v)$ then $\mathcal{B}_m(F_v) = \{v\}$ and so (4.25) is simply $[\partial v F_v] \cdot [\partial w F_{v_1}] \cdot [F_{v_2}] = [\partial w F_{v_1}] \cdot [F_{v_2}]$ as required. Otherwise, assume that $v \notin \mathcal{B}_m(F_v)$. By induction hypothesis, $\Psi_i$ contains the following equation, for any $t \in \mathcal{B}_m(F_v)$:

$$[\partial t(F_{v_1\cdot v_2})] = [\partial t F_{v_1}] \cdot [F_{v_2}].$$

Using $\Psi_i$ as a premise, we can then prove that (4.25) equals:

$$\sum_{t\in\mathcal{B}_m(F_v)} ([\partial t F_{v_1}] \cdot [F_{v_2}]) \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] = \left( \sum_{t\in\mathcal{B}_m(F_v)} [\partial t F_{v_1}] \cdot [\partial w F_{t_1}] \cdot [F_{t_2}] \right) \cdot [F_{v_2}]. \tag{4.26}$$

As in (4.15), we have $\sum_{t\in\mathcal{B}_m(F_v)}[\partial t F_{v_1}]\cdot[\partial w F_{t_1}]\cdot[F_{t_2}] = \sum_{t\in\mathcal{B}_m(F_{v_1})}[\partial t F_{v_1}]\cdot[\partial w F_{t_1}]\cdot[F_{t_2}]$. Also, since $v_1\cdot v_2 = v \notin \mathcal{B}_m(F_v)$, we have $\deg(v_1) > m = 2^i + \deg(w)$, and so

$$[\partial w F_{v_1}] = \sum_{t\in\mathcal{B}_m(F_{v_1})}[\partial t F_{v_1}]\cdot[\partial w F_{t_1}]\cdot[F_{t_2}]\,. \tag{4.27}$$

Hence by (4.27), (4.26) equals $[\partial_w F_{v_1}]\cdot[F_{v_2}]$.

The above proof of (4.24) from $\Psi_i$ has size $O(s^2\cdot m(s,d))$ and depth $O(r(s,d))$.

We now append $\Psi_i'$ from Part (I) (which also contains $\Psi_i$) with all proof-sequences of $[\partial w F_v] = [\partial w F_{v_1}] + [\partial w F_{v_2}]$ in Case 1 and all proof sequences $[\partial w F_v] = [\partial w F_{v_1}]\cdot[F_{v_2}]$ in Case 2, above. We obtain the proof-sequence $\Psi_{i+1}$ of size

$$\lambda(s, i+1) \le O(s^4\cdot m(s,d)) + \lambda(s,i),$$

and depth $O(r(s,d))$, as required. QED

This concludes the proof of Proposition 4.10, and hence of Lemma 4.4.

# 5 Proofs with division

In this section, we investigate proofs with divisions (as defined in Section 2.3), and prove Theorem 2.7. Let us first turn the reader's attention to some peculiarities of the system $\mathbb{P}_c^{-1}$:

- We must be careful not to divide by zero in $\mathbb{P}_c^{-1}$. Hence $\mathbb{P}_c^{-1}$ proofs are *not closed under substitution*. It may happen that $F(z) = G(z)$ has a $\mathbb{P}_c^{-1}$ proof $S$, $F(0) = G(0)$ is well-defined (i.e., does not contain division by zero, as in the definition in Section 2.3), but substituting $z$ by 0 throughout $S$ is not a correct $\mathbb{P}_c^{-1}$ proof (i.e., does contain a division by zero).

- Whereas $\mathbb{P}_c^{-1}$ is sound with respect to polynomial identities, it behaves erratically if one considers *proofs from assumptions*. For example, $\mathbb{P}_c^{-1}$ augmented with the axiom $x^2 - x = 0$ proves that $1 = 0$ (dividing by $x$ gives $x - 1 = 0$ and dividing by $x - 1$ gives $1 = 0$).

- Prima facie, it is not clear whether a $\mathbb{P}_c^{-1}$ proof of the equation $F = G$ can be transformed to a proof of $F = G$ that contains only the variables contained in $F$ and $G$ (we show in Proposition 5.4 that such a transformation is possible).

In the sequel, we will consider substitution instances of equations we prove in $\mathbb{P}_c^{-1}$. For instance, we will need to substitute 0 for some variables in the matrix $X$, when proving equations involving the circuit $\mathrm{DET}(X)$, and we have to guarantee that our proof remains a correct $\mathbb{P}_c^{-1}$ proof after such a substitution.

There are two *general* ways how to securely handle substitutions in $\mathbb{P}_c^{-1}$ proofs. The first one is to substitute only *algebraically independent elements*: replacing variables $z_1,\ldots,z_k$ with circuits $H_1,\ldots,H_k$ can never produce an undefined proof, if the circuits compute algebraically independent rational functions (for the definition of algebraic independence see e.g. Sec. 14.9 in [DF04]). The second way is offered in Corollary 6.5. This corollary allows to construct a new proof of $F(0) = G(0)$ from the proof of $F(z) = G(z)$. Note, however, that in Corollary 6.5 the new proof will be polynomial only if the syntactic degree of $F$ and $G$ is polynomial.

Since the determinant circuit DET has an exponential syntactic degree (see Section 7), the second approach to substitution is not suitable for the DET identities. The first approach, which substitutes algebraically independent elements, often cannot be used either, because we need to substitute variables by field elements. Therefore, in some cases we must make sure in an ad hoc manner that the specific substitutions do not make the proofs undefined. To this end, we use the following terminology.

**Notation.** Let $\overline{x} = (x_1, \ldots, x_k)$ be a list of variables and $U = (U_1, \ldots, U_k)$ a list of circuits with divisions. We say that a circuit $F(\overline{x})$ with divisions is *defined for* $\overline{x} = U$, if $F(U)$ is well-defined; likewise, we say that a $\mathbb{P}_c^{-1}$ proof $S$ is defined for $\overline{x} = U$ (or simply defined, if the context is clear), if every circuit in $S$ is defined for $\overline{x} = U$.

## 5.1 Eliminating division gates over large enough fields

We first prove Theorem 2.7 under the assumption that the underlying field $\mathbb{F}$ is large—this will be Proposition 5.3. To eliminate division gates from proofs, we follow the construction of Strassen [Str73], in which an inverse gate is replaced by a truncated power series. In order to eliminate division gates over small fields, additional work will be needed (see Section 6).

Let $F$ be a circuit with divisions. We say that $F$ is a circuit *with simple divisions*, if for every inverse gate $v^{-1}$ in $F$ the circuit $F_v$ does not contain any inverse gate. A size $s$ circuit with division $F$ can be converted to a size $O(s)$ circuit of the form $F_1 \cdot F_2^{-1}$, where $F_1, F_2$ do not contain inverse gates, as we now show.

For every node $v$ introduce two nodes $\mathrm{Den}(v)$ and $\mathrm{Num}(v)$ which will compute the numerator and denominator of the rational function computed by $v$, respectively, as follows:

(i). If $v$ is an input node of $F$, let $\mathrm{Num}(v) := v$ and $\mathrm{Den}(v) = 1$.

(ii). If $v = u^{-1}$, let $\mathrm{Num}(v) := \mathrm{Den}(u)$ and $\mathrm{Den}(v) := \mathrm{Num}(u)$.

(iii). If $v = u_1 \cdot u_2$, let $\mathrm{Num}(v) := \mathrm{Num}(v_1) \cdot \mathrm{Num}(v_2)$ and $\mathrm{Den}(v) := \mathrm{Den}(v_1) \cdot \mathrm{Den}(v_2)$.

(iv). If $v = u_1 + u_2$, let $\mathrm{Num}(v) := \mathrm{Num}(u_1) \cdot \mathrm{Den}(u_2) + \mathrm{Num}(u_2) \cdot \mathrm{Den}(u_1)$ and $\mathrm{Den}(v) := \mathrm{Den}(u_1) \cdot \mathrm{Den}(u_2)$.

Let $\mathrm{Num}(F)$ and $\mathrm{Den}(F)$ be the circuits with the output node $\mathrm{Num}(w)$ and $\mathrm{Den}(w)$, respectively, where $w$ is the output node of $F$. The following lemma will be used in Proposition 5.3:

**Lemma 5.1.** *Let $\mathbb{F}$ be any field.*

*(i). If $F$ is a size $s$ circuit with division, then*

$$F = \mathit{Num}(F) \cdot \mathit{Den}(F)^{-1}$$

*has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $O(s)$. The proof is defined whenever $F$ is defined.*

*(ii). Let $F, G$ be circuits with division. Assume that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s$. Then $Num(F) \cdot Den(F)^{-1} = Num(G) \cdot Den(G)^{-1}$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $O(s)$ such that every circuit in the proof is a circuit with* simple divisions.

*Proof.* Part (i) is proved by straightforward induction on the size of $F$ and part (ii) by induction on the number of proof lines. We omit the details. QED

Let $k$ be a fixed natural number and define $\mathrm{pow}_k(1-z)$ to be the circuit

$$\mathrm{pow}_k(1-z) := 1 + z + \cdots + z^k \,.$$

In other words, $\mathrm{pow}_k(1-z)$ is the first $k+1$ terms of the power series expansion of $1/(1-z)$ at $z = 0$.

Let $F$ be a division-free circuit and let $a := \widehat{F^{(0)}}$. Assume that $a \neq 0$, that is, the polynomial computed by $F$ has a nonzero constant term. Then $\mathrm{Inv}_k(F)$ denotes the circuit

$$\begin{aligned}\mathrm{Inv}_k(F) &:= a^{-1} \cdot \mathrm{pow}_k(a^{-1}F) \\ &= a^{-1} \cdot \Big(1 + (1 - a^{-1}F) + (1 - a^{-1}F)^2 + \cdots + (1 - a^{-1}F)^k\Big) \,.\end{aligned}$$

Note that $a^{-1}$ is a field element and hence $\mathrm{Inv}_k(F)$ is a circuit *without division*. The following lemma shows that $\mathrm{Inv}_k(F)$ can *provably* serve as the inverse polynomial of $F$ "up to the $k$-th degree".

**Lemma 5.2.** *Let $\mathbb{F}$ be any field and let $F$ be a size $s$ circuit without division such that $\widehat{F^{(0)}} \neq 0$. Then the following have $\mathbb{P}_c(\mathbb{F})$ proofs of size $s \cdot \mathrm{poly}(k)$:*

$$(F \cdot \mathrm{Inv}_k F)^{(0)} = 1 \tag{5.1}$$

$$(F \cdot \mathrm{Inv}_k F)^{(i)} = 0, \text{ for } 1 \leq i \leq k \,. \tag{5.2}$$

*Proof.* Let $z$ abbreviate the circuit $1 - a^{-1}F$, for $a := \widehat{F^{(0)}}$. Then we have $F = a(1-z)$ and by definition $\mathrm{Inv}_k(F) = a^{-1}(1 + z + z^2 + \cdots + z^k)$. By elementary rearrangement, we can prove

$$F \cdot \mathrm{Inv}_k(F) = (1-z)(1 + z + z^2 + \ldots z^k) = 1 - z^{k+1} \,.$$

By Lemma 3.1 part (i) and Proposition 3.3 part (i), $(F \cdot \mathrm{Inv}_k(F))^{(0)} = 1 - (z^{k+1})^{(0)}$ and $(F \cdot \mathrm{Inv}_k(F))^{(i)} = (z^{k+1})^{(i)}$, for $i > 0$. It is therefore sufficient to prove for every $i \leq k$, $(z^{k+1})^{(i)} = 0$. This follows by induction using Lemma 3.1 and the fact that $z^{(0)} = 0$. QED

Proposition 5.3 that follows differs from Theorem 2.7 only in the assumption on the size of $\mathbb{F}$. The dependency on the field comes from the following fact, which stems from the Schwartz-Zippel lemma [Sch80, Zip79]:

**Fact.** *Let $f_1, \ldots, f_s \in \mathbb{F}[X]$ be non-zero polynomials of degree $\leq d$, where $X = \{x_1, \ldots x_n\}$. Assume that $|\mathbb{F}| > sd$. Then there exists $b \in \mathbb{F}^n$ such that $f_i(b) \neq 0$ for every $i \in \{1, \ldots, s\}$.*

**Proposition 5.3.** *There exists a polynomial $p$ and a constant $c > 0$ such that the following holds. Let $F, G$ be circuits without division of syntactic degree at most $d$. Assume that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof with divisions of size at most $s$ and suppose that $|\mathbb{F}| \geq 2^{cs}$. Then $F = G$ has a $\mathbb{P}_c(\mathbb{F})$ proof of size $s \cdot p(d)$.*

*Proof.* Let $S$ be a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of $F = G$ of size $s$. By Lemma 5.1, we can assume that the proof contains only simple divisions. Consider the set $\mathcal{U}$ of all nodes $u^{-1}$ occurring in some circuit in $S$, and let $\mathcal{C}$ be the set of circuits with output $u$, for $u^{-1} \in \mathcal{U}$. Then $|\mathcal{C}| \leq s$ and $\deg(H) \leq 2^s$ for every $H \in \mathcal{C}$, since $H$ has size at most $s$. By the fact above, there exists a point $b \in \mathbb{F}^n$ such that $\widehat{H}(b) \neq 0$ for every $H \in \mathcal{C}$, where $n$ is the number of variables in $S$.

We assume without loss of generality that $b = 0 \in \mathbb{F}^n$ and thus the polynomials computed by the circuits in $\mathcal{C}$ all have a *nonzero constant term*. Hence, $\mathrm{Inv}_d(H)$ is defined for every $H \in \mathcal{C}$. (If $b = \langle b_1, \ldots, b_n \rangle$ is non-zero, substitute in $S$ every variable $x_i$ with $y_i - b_i$. This gives a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of $F(y_1 - b_1, \ldots, y_n - b_n) = G(y_1 - b_1, \ldots, y_n - b_n)$ with the new $b$ equal to zero. After the $\mathbb{P}_c(\mathbb{F})$ proof is obtained, substitute back $x_i + b_i$ for $y_i$). Let $S'$ be the sequence of equations obtained by replacing every circuit $(H)^{-1}$ in $S$ by $\mathrm{Inv}_d(H)$. The sequence $S'$ does not contain divisions, but is not yet a correct proof, since the translation $F \cdot \mathrm{Inv}_d(F) = 1$ of the axiom D is not a legal axiom anymore (recall that D is the axiom: $F \cdot F^{-1} = 1$, for any $F$ such that $F^{-1}$ is well-defined; see Section 2.3). However, we claim that for every equation $F_1 = F_2$ in $S'$ and every $k \leq d$, $F_1^{(k)} = G_1^{(k)}$ has a $\mathbb{P}_c$ proof of size $s \cdot p(d)$ for a suitable polynomial $p$. The proof is constructed by induction on the length of $S'$, as in Proposition 3.3. The case of the axiom D follows from Lemma 5.2: $(F \cdot \mathrm{Inv}_d(F))^{(0)} = 1 = 1^{(0)}$ and $(F \cdot \mathrm{Inv}_d(F))^{(k)} = 0 = 1^{(k)}$, if $0 < k \leq d$. Consequently, we obtain proofs of $F^{(k)} = G^{(k)}$, for every $k \leq d$. By Lemma 3.2, we have $\mathbb{P}_c(\mathbb{F})$ proofs of $F = \sum_{k \leq d} F^{(k)}$, $G = \sum_{k \leq d} G^{(k)}$. This gives $\mathbb{P}_c(\mathbb{F})$ proofs of $F = G$ with the correct size. QED

Another application of Schwartz-Zippel lemma is the following:

**Proposition 5.4.** *Let $\mathbb{F}$ be an arbitrary field and assume that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s$. Then there exists a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of $F = G$ of size $O(s^2)$ which contains only the variables appearing in $F$ or $G$.*

*Proof.* Let $S$ be a proof of $F = G$ of size $s$ which contains variables $z_1, \ldots, z_m$ not appearing in $F$ or $G$. Assume that $F$ or $G$ actually contain at least one variable $x$, otherwise the statement is clear. It is sufficient to find a substitution $z_1 = H_1, \ldots, z_m = H_m$ for which the proof $S$ is defined and $H_1, \ldots, H_m$ are circuits of size $O(s)$ in the variable $x$ only. Applying Schwartz-Zippel lemma in the field of rational functions, we can take a random substitution from the set $M = \{x^1, x^2, x^3 \ldots, x^{2^{cs}}\}$, where $c$ is a sufficiently large constant. Note that $x^k$ can be computed by a circuit of size $O(\log k)$, and so every circuit in $M$ has size $O(s)$. QED

## 5.2 Taylor series

For a later application, we need to introduce the basic notion of a power series. Let $F = F(\overline{x}, z)$ be a circuit with division. We will define $\Delta_{z^k}(F)$ as a circuit in the variables $\overline{x}$, computing the coefficient of $z^k$ in $F$, when $F$ is written as a power series at $z = 0$. This is done as follows:

**Case 1**: Assume first that no division gates in $F$ contain the variable $z$. Then we define $\Delta_{z^k}(F)$ by the following rules (the definition is similar to that of $F^{(k)}$ in Section 3, and so we will be less formal here):

(i). $\Delta_z(z) := 1$ and $\Delta_{z^k}(z) := 0$, if $k > 1$.

(ii). If $F$ does not contain $z$, then $\Delta_{z^0}(F) := F$ and $\Delta_{z^k}(F) := 0$, for $k > 0$.

(iii). $\Delta_{z^k}(F + G) = \Delta_{z^k}(F) + \Delta_{z^k}(G)$.

(iv). $\Delta_{z^k}(F \cdot G) = \sum_{i=0}^{k} \Delta_{z^i}(F) \cdot \Delta_{z^{k-i}}(G)$.

**Case 2**: Assume that some division gate in $F$ contains $z$. We let:

$$F_0 := ((\mathrm{Den}(F))(z/0))^{\sharp} ,$$

where, given a circuit $G$, $G^{\sharp}$ is the non-redundant version of $G$ (see the definition in Section 3) and $G(z/0)$ is obtained by substituting in $G$ all occurrences of $z$ by the constant 0. In case $\widehat{F_0} \neq 0$, we define:

$$\Delta_{z^k}(F) := F_0^{-1} \cdot \Delta_{z^k}\left(\mathrm{Num}(F) \cdot \mathrm{pow}_k\left(F_0^{-1} \cdot \mathrm{Den}(F)\right)\right) .$$

Here, $\mathrm{pow}_k$ (defined in Section 5.1) takes the first $k+1$ terms of the Taylor expansion of $F_0^{-1} \cdot \mathrm{Den}(F)$ around the point $z = 0$. Note that $z$ does not occur in any division gate inside $\mathrm{Num}(F) \cdot \mathrm{pow}_k\left(F_0^{-1} \cdot \mathrm{Den}(F)\right)$, and so $\Delta_{z^k}(F)$ is well-defined.

We summarize the main properties of $\Delta_{z^k}$ as follows:

**Proposition 5.5.**

*(i). If $F$ is a circuit without division of syntactic degree at most $d$ and size $s$ then $F = \sum_{i=0}^{d} \Delta_{z^i}(F) \cdot z^i$ has a $\mathbb{P}_c$ proof of size $s \cdot \mathrm{poly}(d)$.*

*(ii). If $F_0, \ldots, F_k$ are circuits with divisions not containing the variable $z$, then $\Delta_{z^j}\left(\sum_{i=0}^{k} F_i z^i\right) = F_j$ has a polynomial size $\mathbb{P}_c^{-1}$ proof, for every $j \leq k$.*

*(iii). Assume that $F, G$ are circuits with divisions such that $F = G$ has a $\mathbb{P}_c^{-1}$ proof of size $s$ that is defined for $z = 0$. Then*

$$\Delta_{z^k}(F) = \Delta_{z^k}(G)$$

*has a $\mathbb{P}_c^{-1}$ proof of size $s \cdot \mathrm{poly}(k)$.*

The proofs are almost identical to those of Proposition 3.3 and Proposition 5.3. We omit the details.

## 6 Simulating large fields in small ones

Recall the notation on matrices given in Section 1.2: matrices are understood as matrices whose entries are circuits and operations on matrices are operations on circuits.

**Lemma 6.1.** *Let $X, Y, Z$ be $n \times n$ matrices of distinct variables and $I_n$ the identity matrix. Then the following identities have polynomial-size $\mathbb{P}_c(\mathbb{F})$ proofs:*

$$\begin{array}{ll} X + Y = Y + X & X + (Y + Z) = (X + Y) + Z \\ X \cdot (Y + Z) = X \cdot Y + X \cdot Z & (Y + Z) \cdot X = Y \cdot X + Z \cdot X \\ X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z & X \cdot I_n = I_n \cdot X = X. \end{array}$$

*Similarly for non-square matrices of appropriate dimension.*

*Proof.* Each of the matrix equations is a set of $n^2$ polynomial identities of degree $\leq 3$ and circuit size $O(n^2)$. Every constant degree identity has a polynomial size proof in $\mathbb{P}_c$. QED

Let $\mathbb{F}_1 = GF(p)$ and $\mathbb{F}_2 = GF(p^n)$, where $p$ is a prime power. We will show how to simulate proofs in $\mathbb{P}_c(\mathbb{F}_2)$ by proofs in $\mathbb{P}_c(\mathbb{F}_1)$. Recall that $\mathbb{F}_2$ can be represented by $n \times n$ matrices with elements from $\mathbb{F}_1$, that is, there is an isomorphism $\theta$ between $\mathbb{F}_2$ and a subset of $GL_n(\mathbb{F}_1) \cup \{0\}$. We can also assume that $\theta(a) = aI_n$ if $a \in \mathbb{F}_1 \subseteq \mathbb{F}_2$. This allows one to treat a polynomial $f$ over $\mathbb{F}_2$ as a matrix of $n^2$ polynomials over $\mathbb{F}_1$. Similarly, we can define a translation of circuits: let $F$ be a circuit with coefficients from $\mathbb{F}_2$. Let $\overline{F}$ be an $n \times n$ matrix of circuits $\{\overline{F}_{ij}\}$, $i, j \in [n]$ with coefficients from $\mathbb{F}_1$, defined as follows: for every gate $u$ in $F$, introduce $n^2$ gates $\bar{u} = \{\bar{u}_{ij}\}_{i,j\in[n]}$, and let:

(i). If $u \in \mathbb{F}_2$ is a constant, let $\bar{u} := \theta(u)$.

(ii). If $u$ is a variable, let $\bar{u} := u \cdot I_n$.

(iii). If $u = v + w$, let $\bar{u} := \bar{v} + \bar{w}$, and if $u = v \cdot w$, let $\bar{u} := \bar{v} \cdot \bar{w}$

Then $\overline{F}$ is the matrix computed by $\bar{w}$ where $w$ is the output of $F$.

Here, $\bar{v} + \bar{w}$, $(\bar{v} \cdot \bar{w})$ and $u \cdot I_n$ are understood as the corresponding matrix operations on circuit nodes.

**Lemma 6.2.** *Let $F, G$ be circuits of size $\leq s$ with coefficients from $\mathbb{F}_2$. Then*

$$\overline{F \oplus G} = \overline{F} + \overline{G}\,, \qquad \overline{F \otimes G} = \overline{F} \cdot \overline{G}\,, \tag{6.1}$$

$$\overline{F} \cdot \overline{G} = \overline{G} \cdot \overline{F} \tag{6.2}$$

*have $\mathbb{P}_c(\mathbb{F}_1)$ proofs of size $s \cdot \mathrm{poly}(n)$*

*Proof.* Identities (6.1) follow from the definition of $\overline{F}$ by means of axioms C1, C2.

Identity (6.2) follows by induction on the circuit sizes of $F$ and $G$. We first need to construct the proof of

$$\overline{z_1} \cdot \overline{z_2} = \overline{z_2} \cdot \overline{z_1}\,,$$

where each $z_1, z_2$ is either a variable or an element of $\mathbb{F}_2$. So assume that $z_1$ is a variable. Then $\overline{z_1} = z_1 \cdot I_n$. This gives $\overline{z_1} \cdot \overline{z_2} = z_1 \cdot \overline{z_2}$. But $\overline{z_2}$ is a matrix for which each entry commutes with $z_1$, which gives a proof of $z_1 \cdot \overline{z_2} = \overline{z_2} \cdot z_1 = \overline{z_2} \cdot \overline{z_1}$. The case of $z_2$ being a variable is similar. If both $z_1, z_2 \in \mathbb{F}_2$, we are supposed to prove $\theta(z_1) \cdot \theta(z_2) = \theta(z_2) \cdot \theta(z_1)$. But this is a set of $n^2$ true equations of size $O(n)$ which contain only elements of $\mathbb{F}_1$, and hence it has a proof of size $O(n^3)$. In the inductive step, use (6.1) and Lemma 6.1 to construct proofs of $(\overline{F_1} + \overline{F_2}) \cdot \overline{G} = \overline{G} \cdot (\overline{F_1} + \overline{F_2})$ and of $(\overline{F_1} \cdot \overline{F_2}) \cdot \overline{G} = \overline{G} \cdot (\overline{F_1} \cdot \overline{F_2})$ from the proofs of $\overline{F_1} \cdot \overline{G} = \overline{G} \cdot \overline{F_1}$ and $\overline{F_2} \cdot \overline{G} = \overline{G} \cdot \overline{F_2}$. QED

We are now ready to prove Theorem 2.8:

**Theorem 6.3** (Theorem 2.8 restated)**.** *Let $p$ be a prime power and $n$ a natural number. Let $F, G$ be circuits over $GF(p)$. Assume that $F = G$ has a $\mathbb{P}_c(GF(p^n))$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_c(GF(p))$ proof of size $s \cdot \mathrm{poly}(n)$.*

*Proof.* Let $F, G$ be circuits with coefficients from $\mathbb{F}_2$ such that $F = G$ has a $\mathbb{P}_c(\mathbb{F}_2)$ proof of size $s$. We wish to show that $\overline{F} = \overline{G}$ have proofs of size $s \cdot \mathrm{poly}(n)$ in $\mathbb{P}_c(\mathbb{F}_1)$. This concludes the theorem, since if $F, G$ contain only coefficients from $\mathbb{F}_1$ then $\overline{F}_{11} = F$ and $\overline{G}_{11} = G$.

The proof is constructed by induction on the number of lines. Axioms C1, C2 follow from equations (6.1) in Lemma 6.2, and A4 from equation (6.2). A10 is a set of $n^2$ true constant equations. The rest of the axioms are application of Lemma 6.1. The rules R1, R2 are immediate, and R3, R4 are given by Lemma 6.2. QED

Now we can also prove Theorem 2.7:

**Theorem 6.4** (Theorem 2.7 restated)**.** *Let $\mathbb{F}$ be any field and assume that $F$ and $G$ are circuits without division gates such that $\deg F, \deg G \leq d$. Suppose that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s$. Then $F = G$ has a $\mathbb{P}_c(\mathbb{F})$ proof of size $\mathrm{poly}(s, d)$.*

*Proof.* Follows from Theorem 6.3 and Proposition 5.3. More precisely, let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, such that $|\mathbb{F}'| = 2^{\Omega(s)}$. Then we can consider the $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s$ of $F = G$ as a $\mathbb{P}_c^{-1}(\mathbb{F}')$ proof. Hence, by Proposition 5.3, there is also a $\mathbb{P}_c(\mathbb{F}')$ proof of $F = G$ of size $s \cdot \mathrm{poly}(d)$. By Theorem 6.3, $F = G$ has a $\mathbb{P}_c(\mathbb{F})$ proof of size $\mathrm{poly}(s, d)$. QED

For a circuit with division $F$, define its syntactic degree by

$$\deg F := \deg(\mathrm{Num}(F)) + \deg(\mathrm{Den}(F)).$$

**Corollary 6.5.** *Let $\mathbb{F}$ be any field and let $F$, $G$, $H$ be circuits with divisions. Assume that $\deg(F), \deg(G) \leq d$ and that $H$ has size $s_1$. Suppose that $F = G$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s_2$ and that $F(z/H)$, $G(z/H)$ are defined. Then $F(z/H) = G(z/H)$ has a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of size $s_1 \cdot \mathrm{poly}(s_2, d)$.*

*Proof.* We aim to construct a proof of $F = G$ of size $\mathrm{poly}(s_2, d)$ such that the proof is defined for $z = H$. We can then substitute $H$ for $z$ throughout the proof to obtain a proof of $F(z/H) = G(z/H)$ of the required size. By Lemma 5.1, we have proofs of

$$F = \mathrm{Num}(F) \cdot \mathrm{Den}(F)^{-1} \qquad G = \mathrm{Num}(G) \cdot \mathrm{Den}(G)^{-1}\,. \tag{6.3}$$

This and $F = G$ gives a $\mathbb{P}_c^{-1}(\mathbb{F})$ proof of

$$\mathrm{Num}(F) \cdot \mathrm{Den}(G) = \mathrm{Num}(G) \cdot Den(F)\,,$$

of size $O(s_2)$. The last equation does not contain division gates, and so it has a $\mathbb{P}_c(\mathbb{F})$ proof of size $\mathrm{poly}(s_2, d)$ by Theorem 6.4. This proof is defined for $z = H$ because it does not contain division gates. By Lemma 5.1, the proofs of (6.3) are defined for $z = H$ (because $F(z/H)$ and $G(z/H)$ are defined by assumption). In particular, both $\mathrm{Den}(F)(z/H)$ and $\mathrm{Den}(G)(z/H)$ are nonzero. Hence we have a proof of

$$\mathrm{Num}(F) \cdot \mathrm{Den}(F)^{-1} = \mathrm{Num}(G) \cdot \mathrm{Den}(G)^{-1}$$

which is defined for $z = H$. Using (6.3) we obtain a proof of $F = G$ of size $\mathrm{poly}(s_2, d)$ which is defined for $z = H$. QED

# 7 Computing the determinant

We are now done with the structural properties of $\mathbb{P}_c$ and $\mathbb{P}_f$ and we proceed to construct proofs of the properties of the determinant. We first compute the determinant as a rational function.

## 7.1 The determinant as a rational function

**The definition of $X^{-1}$ and $\mathrm{DET}(X)$**

Let $X = \{x_{ij}\}_{i,j\in[n]}$ be a matrix consisting of $n^2$ distinct variables. Recursively, we define an $n \times n$ matrix $X^{-1}$ whose entries are circuits with divisions, computing the inverse of $X$. We then use $X^{-1}$ to compute the determinant as a rational function. Both definitions can be seen as an algebraic formulation of Gaussian elimination.

(i). If $n = 1$, let $X^{-1} := (x_{11}^{-1})$.

(ii). If $n > 1$, partition $X$ as follows:

$$X = \begin{pmatrix} X_1 & v_1^t \\ v_2 & x_{nn} \end{pmatrix}, \tag{7.1}$$

where $X_1 = \{x_{ij}\}_{i,j\in[n-1]}$, $v_1 = (x_{1n}, \ldots, x_{(n-1)n})$ and $v_2 = (x_{n1}, \ldots, x_{n(n-1)})$. Assuming we have constructed $X_1^{-1}$, let

$$\delta(X) := x_{nn} - v_2 X_1^{-1} v_1^t\,. \tag{7.2}$$

$\delta(X)$ computes a single non-zero rational function and so $\delta(X)^{-1}$ is defined. Finally, let

$$X^{-1} := \begin{pmatrix} X_1^{-1}(I_{n-1} + \delta(X)^{-1} v_1^t v_2 X_1^{-1}) & -\delta(X)^{-1} X_1^{-1} v_1^t \\ -\delta(X)^{-1} v_2 X_1^{-1} & \delta(X)^{-1} \end{pmatrix}. \tag{7.3}$$

The circuit $\mathrm{DET}(X)$ is defined as follows:

(i). If $n = 1$, let $\mathrm{DET}(X) := x_{11}$.

(ii). If $n > 1$, partition $X$ as in (7.1) and let $\delta(X)$ be as in (7.2). Let

$$\mathrm{DET}(X) := \mathrm{DET}(X_1) \cdot \delta(X) = \mathrm{DET}(X_1) \cdot (x_{nn} - v_2 X_1^{-1} v_1^t)\,.$$

The definition in (7.3) should be understood as a circuit with $n^2$ outputs which takes $X_1^{-1}, v_1, v_2, x_{nn}$ as inputs and moreover, such that the inputs from $X_1^{-1}$ occur exactly once (so we slightly deviate from earlier notation). Altogether, we obtain polynomial size circuits for $X^{-1}$ and $\mathrm{DET}(X)$. The fact that $\mathrm{DET}(X)$ indeed computes the determinant (as a rational function) is a consequence of Proposition 7.6 below, where we show that $\mathbb{P}_c^{-1}$ can prove the two identities which characterize the determinant. That $X^{-1}$ computes the matrix inverse is proved in Proposition 7.2.

It should be emphasized that both $X^{-1}$ and $\mathrm{DET}(X)$ are circuits with division and hence *not always defined when substituting for* $X$. Let $A := \{a_{ij}\}_{i,j\in[n]}$ be an $n \times n$ matrix whose entries are circuits with division. We will say that $A$ is *invertible* if the circuit $A^{-1}$ is well-defined, that is, when we substitute the entries of $A$ into $X^{-1}$, the circuit does not use divisions by zero. Note that $A^{-1}$ may be undefined even if $A$ *has* an inverse in the original algebraic sense. For example, if

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

then both $A^{-1}$ and $\mathrm{DET}(A)$ are undefined, and so $A$ is not invertible in our sense. Moreover, note that $\mathrm{DET}(X)$ has an *exponential* syntactic degree which, in view of Corollary 6.5, further obscures the possibility of substituting in $\mathbb{P}_c^{-1}$ proofs.

On the other hand, let us state the basic cases when the determinant and matrix inverse are defined. Setting

$$A[k] := \{a_{ij}\}_{i,j\in[k]},$$

we have the following:

**Proposition 7.1.**

*(i). If $A$ is invertible (meaning the circuit $A^{-1}$ is defined) then $\mathrm{DET}(A)$ is defined.*

*(ii). If the entries of $A$ compute algebraically independent rational functions then $A$ is invertible.*

*(iii). If $A$ is a triangular matrix with $a_{11}, \dots, a_{nn}$ on the diagonal such that $a_{11}^{-1}, \dots, a_{nn}^{-1}$ are defined then $A$ is invertible.*

*(iv). The matrix $A$ is invertible if and only if $A[1], \dots, A[n-1]$ are invertible and $\delta(A)^{-1}$ is defined.*

## Properties of matrix inverse

**Proposition 7.2.** *Let $X = \{x_{ij}\}_{i,j\in[n]}$ be a matrix with $n^2$ distinct variables. Then both*

$$X \cdot X^{-1} = I_n \quad \text{and} \quad X^{-1} \cdot X = I_n$$

*have a polynomial-size $\mathbb{P}_c^{-1}$ proof. The proof is defined for $X = A$, whenever $A$ is invertible.*

We emphasize that $A$ is a matrix with circuits (with division) as entries, and that invertibility of $A$ means that the circuit $A^{-1}$ is defined.

*Proof.* Let us construct the proofs of $X \cdot X^{-1} = I_n$ and $X^{-1} \cdot X = I_n$ by induction on $n$. If $n = 1$, we have $x_{11} \cdot x_{11}^{-1} = x_{11}^{-1} \cdot x_{11} = 1$ which is a $\mathbb{P}_c^{-1}$ axiom. Otherwise let $n > 1$ and $X$ be as in (7.1). We want to construct a polynomial size proof of $X \cdot X^{-1} = I_n$ from the assumption $X_1 \cdot X_1^{-1} = I_{n-1}$. This implies that $X \cdot X^{-1} = I_n$ has a polynomial size proof.

For brevity, let $a := \delta(X)$. Using some rearrangements, and the definition of $a$, we have:

$$\begin{aligned}
X \cdot X^{-1} &= \begin{pmatrix} X_1 & v_1^t \\ v_2 & x_{nn} \end{pmatrix} \cdot \begin{pmatrix} X_1^{-1}(I_{n-1} + a^{-1}v_1^t v_2 X_1^{-1}) & -a^{-1}X_1^{-1}v_1^t \\ -a^{-1}v_2 X_1^{-1} & a^{-1} \end{pmatrix} \\
&= \begin{pmatrix} I_{n-1} + a^{-1}v_1^t v_2 X_1^{-1} - a^{-1}v_1^t v_2 X_1^{-1} & -a^{-1}v_1^t + a^{-1}v_1^t \\ v_2 X_1^{-1} + a^{-1}(v_2 X_1^{-1} v_1^t - x_{nn})v_2 X_1^{-1} & a^{-1}(-v_2 X_1^{-1} v_1^t + x_{nn}) \end{pmatrix} \\
&= \begin{pmatrix} I_{n-1} & 0 \\ v_2 X_1^{-1} - a^{-1}a v_2 X_1^{-1} & a^{-1}a \end{pmatrix} \\
&= \begin{pmatrix} I_{n-1} & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Here we use the fact that basic properties of matrix addition and multiplication have feasible proofs (see Lemma 6.1).

The proof of $X^{-1} \cdot X = I_n$ is constructed in a similar fashion (where we use the assumption $X_1^{-1}X_1 = I_{n-1}$ instead). Moreover, if $A$ is an $n \times n$ matrix such that $A^{-1}$ is defined, the proofs of $A \cdot A^{-1} = A^{-1} \cdot A = I_n$ are defined. (This is because they employ only the inverse gates appearing already in the definition of $X^{-1}$.) QED

**Corollary 7.3.** *The identity $(XY)^{-1} = Y^{-1}X^{-1}$ has a polynomial-size proof in $\mathbb{P}_c^{-1}$. The proof is defined for $X = A, Y = B$ whenever $A, B$ and $AB$ are invertible.*

Beware that invertibility (in our sense) of $A$ and $B$ does not guarantee invertibility of $AB$.

*Proof.* Let $Z := (XY)^{-1}$. Then $(Z(XY))Y^{-1}X^{-1} = Y^{-1}X^{-1}$. On the other hand, $(Z(XY))Y^{-1}X^{-1} = Z(X(YY^{-1})X^{-1}) = Z$ and so $Z = Y^{-1}X^{-1}$. QED

An application of Corollary 7.3 is the following technical observation. Let $X$ be as in (7.1) and similarly $Y = \begin{pmatrix} Y_1 & u_1^t \\ u_2 & y_{nn} \end{pmatrix}$. Comparing the entries in the bottom right corners of $(XY)^{-1}$ and $Y^{-1}X^{-1}$, we obtain that

$$\delta(Y)\delta(X) = \delta(XY)(1 + u_2 Y_1^{-1} X_1^{-1} v_1^t)\,, \tag{7.4}$$

has a polynomial size $\mathbb{P}_c^{-1}$ proof (the proof is defined for $X = A$ and $Y = B$ whenever $A$, $B$ and $AB$ are invertible).

**Properties of** DET

We now want to prove a $\mathbb{P}_c^{-1}$ analogue of Theorem 2.1, the main theorem of this article. This will be Proposition 7.6, which differs from Theorem 2.1 in that it concerns circuits with division. We first give the following two lemmas. Lemma 7.4 serves only to simplify the proof of Lemma 7.5.

**Lemma 7.4.**

*(i). Let $A, L, U$ be $n \times n$ matrices with $L$ lower triangular and $U$ upper triangular. If $A, L, U$ are invertible then so is $LAU$. Moreover,*

$$\mathrm{DET}(LAU) = \mathrm{DET}(L)\mathrm{DET}(A)\mathrm{DET}(U)$$

*has a polynomial size $\mathbb{P}_c^{-1}$ proof.*

*(ii). If $A$ is invertible, there exists an invertible lower triangular matrix $L(A)$ and an upper triangular matrix $U(A)$ such that $A = L(A) \cdot U(A)$ has a polynomial size $\mathbb{P}_c^{-1}$ proof.*

*Proof.* Part (i). It is enough to separately consider the cases $U = I_n$ and $L = I_n$. We prove the former, the latter is similar.

We want to show that $LA$ is invertible and construct the proof of $\mathrm{DET}(LA) = \mathrm{DET}(L)\mathrm{DET}(A)$. Proceed by induction on $n$. If $n = 1$, the statement is clear. If $n > 1$, write

$$L = \begin{pmatrix} L_1 & 0 \\ u & \ell_{nn} \end{pmatrix}, \; A = \begin{pmatrix} A_1 & v_1^t \\ v_2 & a_{nn} \end{pmatrix}, \; \text{and so } \; LA = \begin{pmatrix} L_1A_1 & L_1v_1^t \\ uA_1 + \ell_{nn}v_2 & \ell_{nn}a_{nn} + uv_1^t \end{pmatrix}.$$

By invertibility of $L$ and $A$, $L_1$ and $A_1$ are invertible (Proposition 7.1). By the inductive assumption, $L_1A_1$ is invertible and we have a proof of $\mathrm{DET}(L_1A_1) = \mathrm{DET}(L_1)\mathrm{DET}(A_1)$. We want to show that $LA$ is invertible and construct a proof of $\mathrm{DET}(LA) = \mathrm{DET}(L)\mathrm{DET}(A)$. We have

$$\delta(L) = \ell_{nn}\,, \; \delta(A) = a_{nn} - v_2A_1^{-1}v_1^t\,, \text{ and}$$

$$\begin{aligned}\delta(LA) &= (\ell_{nn}a_{nn} + uv_1^t) - (uA_1 + \ell_{nn}v_2)(L_1A_1)^{-1}L_1v_1^t = \\ &= (\ell_{nn}a_{nn} + uv_1^t) - (uA_1 + \ell_{nn}v_2)A_1^{-1}L_1^{-1}L_1v_1^t = \\ &= \ell_{nn}a_{nn} + uv_1^t - uv_1^t + \ell_{nn}v_2A_1^{-1}v_1^t = \ell_{nn}(a_{nn} - v_2A_1^{-1}v_1^t) = \\ &= \delta(L)\delta(A)\,.\end{aligned}$$

By invertibility of $L$ and $A$, $\delta(L)$ and $\delta(A)$ are invertible (Proposition 7.1), hence also $\delta(LA)$ is, and altogether $LA$ is invertible. Finally, we have $\mathrm{DET}(A) = \mathrm{DET}(A_1)\delta(A)$, $\mathrm{DET}(L) = \mathrm{DET}(L_1)\delta(L)$ and $\mathrm{DET}(LA) = \mathrm{DET}(L_1A_1)\delta(LA)$. We can conclude $\mathrm{DET}(LA) = \mathrm{DET}(L)\mathrm{DET}(A)$ from the assumption $\mathrm{DET}(L_1A_1) = \mathrm{DET}(L_1)\mathrm{DET}(A_1)$ and the equation $\delta(LA) = \delta(L)\delta(A)$.

In part (ii), the matrices $L(A), U(A)$, as well as the $\mathbb{P}_c^{-1}$ proof, are constructed by induction on $n$. If $n = 1$, let $L(a_{11}) = a_{11}$ and $U(a_{11}) = 1$. If $n > 1$, write $A$ as above. Assuming we have $A_1 = L(A_1)U(A_1)$, we have

$$\begin{pmatrix} A_1 & v_1^t \\ v_2 & a_{nn} \end{pmatrix} = \begin{pmatrix} L(A_1) & 0 \\ v_2U(A_1)^{-1} & a_{nn} - v_2A_1^{-1}v_1^t \end{pmatrix} \cdot \begin{pmatrix} U(A_1) & L(A_1)^{-1}v_1^t \\ 0 & 1 \end{pmatrix}.$$

QED

**Lemma 7.5.** *Let $A$ be an invertible $n \times n$ matrix and let $v_1, v_2$ be $n \times 1$ vectors such that $A + v_1^tv_2$ is invertible. Then*

$$\mathrm{DET}(A + v_1^tv_2) = \mathrm{DET}(A)(1 + v_2A^{-1}v_1^t)$$

*has a polynomial size $\mathbb{P}_c^{-1}$ proof.*

*Proof.* We first consider the special case

$$\mathrm{DET}(I_n + v_1^t v_2) = 1 + v_2 v_1^t\,, \text{if } I_n + v_1^t v_2 \text{ is invertible.} \tag{7.5}$$

The proof is constructed by induction on $n$. If $n = 1$, the identity is immediate. If $n > 1$, partition $I_n + v_1^t v_2$ as in Equation (7.1), i.e.,

$$I_n + v_1^t v_2 = \begin{pmatrix} I_{n-1} + u_1^t u_2 & c_2 u_1^t \\ c_1 u_2 & 1 + c_1 c_2 \end{pmatrix},$$

where $v_1 = (u_1, c_1)$ and $v_2 = (u_2, c_2)$. We want to construct a polynomial size proof of (7.5) from the assumption $\mathrm{DET}(I_{n-1} + u_1^t u_2) = (1 + u_2 u_1^t)$. This implies that (7.5) has a polynomial size proof.

Let $\alpha := u_2 u_1^t$. We note the following:

**Claim.** $(I_{n-1} + u_1^t u_2)^{-1} = I_{n-1} - (1+\alpha)^{-1} u_1^t u_2$ *has a polynomial size* $\mathbb{P}_c^{-1}$ *proof.*

*Proof.* It is enough to show that

$$(1+\alpha) I_{n-1} = (1+\alpha)(I_{n-1} + u_1^t u_2) - (I_{n-1} + u_1^t u_2) u_1^t u_2\,.$$

This is an elementary rearrangement using $(u_1^t u_2)(u_1^t u_2) = u_1^t(u_2 u_1^t)u_2 = \alpha u_1^t u_2$. QED

By the definition of DET, and the assumption $\mathrm{DET}(I_{n-1} + u_1^t u_2) = 1 + \alpha$, we obtain

$$\begin{aligned}
\mathrm{DET}(I_n + v_1^t v_2) =& \mathrm{DET}(I_{n-1} + u_1^t u_2) \left((1 + c_1 c_2) - c_2 u_2 (I_{n-1} + u_1^t u_2)^{-1} c_1 u_1^t\right) = \\
=& (1+\alpha) \left((1 + c_1 c_2) - c_2 u_2 (I_{n-1} - (1+\alpha)^{-1} u_1^t u_2) c_1 u_1^t\right) = \\
=& (1+\alpha)(1 + c_1 c_2) - (1+\alpha) c_1 c_2 u_2 u_1^t + c_1 c_2 u_2 u_1^t u_2 u_1^t = \\
=& (1+\alpha)(1 + c_1 c_2) - (1+\alpha) c_1 c_2 \alpha + c_1 c_2 \alpha^2 = \\
=& 1 + \alpha + c_1 c_2 = 1 + v_2 v_1^t\,.
\end{aligned}$$

This gives a polynomial size proof of (7.5).

Finally, we need to conclude $\mathrm{DET}(A + v_1^t v_2) = \mathrm{DET}(A)(1 + v_2 A^{-1} v_1^t)$ from (7.5), Let $L := L(A)$ and $U := U(A)$ be the matrices from the previous lemma. The lemma gives

$$\begin{aligned}
\mathrm{DET}(A + v_1^t v_2) =& \mathrm{DET}(LU + v_1^t v_2) = \mathrm{DET}(L)\mathrm{DET}(I_n + L^{-1} v_1^t v_2 U^{-1})\mathrm{DET}(U) = \\
=& \mathrm{DET}(LU)(1 + v_2 U^{-1} L^{-1} v_1^t) = \mathrm{DET}(A)(1 + v_2 A^{-1} v_1^t)\,.
\end{aligned}$$

QED

**Proposition 7.6.**

*(i). Let $U$ be an (upper or lower) triangular matrix with $u_1, \ldots, u_n$ on the diagonal. If $u_1^{-1}, \ldots, u_n^{-1}$ are well-defined then the following has a polynomial-size $\mathbb{P}_c^{-1}$ proof:*

$$\mathrm{DET}(U) = u_1 \cdots u_n\,.$$

*(ii). Let $X$ and $Y$ be $n \times n$ matrices, each consisting of pairwise distinct variables. Then*

$$\mathrm{DET}(X \cdot Y) = \mathrm{DET}(X) \cdot \mathrm{DET}(Y) \tag{7.6}$$

*has a polynomial-size $\mathbb{P}_c^{-1}$ proof. The proof is defined for $X = A, Y = B$ provided $A[k], B[k]$ and $A[k]B[k]$ are invertible for every $k \in [n]$.*

*Proof.* Part (i) follows from the definition of DET. We omit the details.
Part (ii) is proved by induction on $n$. If $n = 1$, it is immediate. Assume that $n > 1$. Let

$$X = \begin{pmatrix} X_1 & v_1^t \\ v_2 & x_{nn} \end{pmatrix}, \qquad Y = \begin{pmatrix} Y_1 & u_1^t \\ u_2 & y_{nn} \end{pmatrix}.$$

We want to construct a polynomial size proof of $\mathrm{DET}(XY) = \mathrm{DET}(X)\mathrm{DET}(Y)$ from the assumption $\mathrm{DET}(X_1Y_1) = \mathrm{DET}(X_1)\mathrm{DET}(Y_1)$. This implies that $\mathrm{DET}(XY) = \mathrm{DET}(X)\mathrm{DET}(Y)$ has a polynomial size proof.

By the definition of DET, we have

$$\mathrm{DET}(X) = \mathrm{DET}(X_1)\delta(X)\,, \qquad \mathrm{DET}(Y) = \mathrm{DET}(Y_1)\delta(Y) \quad \text{and}$$
$$\mathrm{DET}(XY) = \mathrm{DET}(X_1Y_1 + v_1^t u_2)\delta(XY)\,,$$

and we are supposed to prove:

$$\mathrm{DET}(X_1Y_1 + v_1^t u_2)\delta(XY) = \mathrm{DET}(X_1)\delta(X) \cdot \mathrm{DET}(Y_1)\delta(Y)\,. \tag{7.7}$$

By the previous lemma, we have $\mathrm{DET}(X_1Y_1 + v_1^t u_2) = \mathrm{DET}(X_1Y_1)(1 + u_2(X_1Y_1)^{-1}v_1^t)$. By the assumption $\mathrm{DET}(X_1Y_1) = \mathrm{DET}(X_1)\mathrm{DET}(Y_1)$, this yields

$$\mathrm{DET}(X_1Y_1 + v_1^t u_2) = \mathrm{DET}(X_1)\mathrm{DET}(Y_1)(1 + u_2 Y_1^{-1} X_1^{-1} v_1^t)\,.$$

Hence in order to prove (7.7), it is sufficient to prove

$$(1 + u_2 Y_1^{-1} X_1^{-1} v_1^t)\delta(XY) = \delta(X)\delta(Y)\,.$$

But this follows from (7.4).

On the inductive step, we have assumed invertibility of $X, Y$, $XY$, $X_1$, $Y_1$ and $X_1Y_1$, as well as invertibility of $X_1Y_1 + v_1^t u_2$. The latter follows from the invertibility of $XY$, because $(X_1Y_1 + v_1^t u_2)^{-1} = ((XY)[n-1])^{-1}$ is used in the definition of $(XY)^{-1}$. Since $X_1 = X[n-1]$, $Y_1 = Y[n-1]$, by Proposition 7.1 the proof altogether assumes invertibility of $X[k], Y[k]$ and $X[k]Y[k]$ for every $k \in [n]$. QED

Let us state explicitly the important cases when the proof of $\mathrm{DET}(AB) = \mathrm{DET}(A)\mathrm{DET}(B)$ is defined. This is so, if $A$ and $B$ are invertible and also at least one of the following conditions hold:

(i). The entries of $A, B$ compute algebraically independent rational functions;

(ii). $A$ is lower triangular or $B$ is upper triangular;

(iii). The entries of $A$ are field elements and the entries of $B$ are algebraically independent, or vice versa.

The following lemma shows that elementary Gaussian operations are well-behaved with respect to DET.

**Lemma 7.7.** *Let $X = \{x_{ij}\}_{i,j\in[n]}$ be an $n\times n$ matrix of distinct variables. Then the following have polynomial-size $\mathbb{P}_c^{-1}$ proofs:*

*(i).* $\mathrm{DET}(X) = -\mathrm{DET}(X')$, *where $X'$ is a matrix obtained from $X$ by interchanging two rows or columns.*

*(ii).* $\mathrm{DET}(X'') = u\mathrm{DET}(X)$, *where $X''$ is obtained by multiplying a row in $X$ by $u$, such that $u^{-1}$ is defined (and similarly for a column).*

*(iii).* $\mathrm{DET}(X) = \mathrm{DET}(X''')$, *where $X'''$ is obtained by adding a row to a different row in $X$ (and similarly for columns).*

*(iv).* $\mathrm{DET}(X) = x_{nn}\mathrm{DET}(X_1 - x_{nn}^{-1}v_1^t v_2)$, *where $X_1, v_1$ and $v_2$ are from the decomposition (7.1).*

*Proof.* Parts (ii) and (iii) follow from Proposition 7.6 and the fact that $X'' = AX$ and $X''' = A'X$, where $A, A'$ are suitable triangular matrices.

For part (i), we cannot directly apply Proposition 7.6. We have $X' = TX$ where $T$ is a transposition matrix, but $T$ is not invertible in our sense. However, we can write $T = A_1A_2$, where $A_1, A_2$ are invertible with $\mathrm{DET}(A_1)\mathrm{DET}(A_2) = -1$: note that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Since $X$ is a matrix of distinct variables, the following is defined:

$$\mathrm{DET}(A_1A_2X) = \mathrm{DET}(A_1)\mathrm{DET}(A_2X) = \mathrm{DET}(A_1)\mathrm{DET}(A_2)\mathrm{DET}(X)\,.$$

Part (iv) follows from Lemma 7.5: the lemma gives $\mathrm{DET}(X_1 - x_{nn}^{-1}v_1^t v_2) = \mathrm{DET}(X_1)(1 - x_{nn}^{-1}v_2X_1^{-1}v_1^t)$. This gives (iv) by elementary rearrangement and the definition of $\mathrm{DET}(X)$.

QED

### 7.2 The determinant as a polynomial

Note that we cannot yet apply Theorem 6.4 to Proposition 7.6 in order to obtain our main theorem (Theorem 2.1), because DET itself contains division gates. For our purpose it will suffice to compute the determinant by a circuit without division, denoted $\det(X)$, and construct a proof of $\det(X) = \mathrm{DET}(X)$ in $\mathbb{P}_c^{-1}$. In order to do that, we will define $\det(X)$ as the $n$th term of the Taylor expansion of $\mathrm{DET}(I + zX)$ at $z = 0$, as follows: using notation from Section 5.2, let

$$\det(X) := \Delta_{z^n}\left(\mathrm{DET}(I_n + zX)\right). \tag{7.8}$$

Let us note that:

(i). the circuit $\det(X)$ indeed computes the determinant of $X$; and (ii). the circuit $\det(X)$ is a circuit without division, of syntactic degree $n$.

This is because every variable from $X$ in the circuit $\mathrm{DET}(I_n + zX)$ occurs in a product with $z$, and thus $\Delta_{z^n}(\mathrm{DET}(I_n + zX))$ computes the $n$th homogeneous part of the determinant of $I_n + X$, which is simply the determinant of $X$. By the definition of $\Delta_{z^n}$, $\Delta_{z^n}(\mathrm{DET}(I + zX))$ contains exactly one inverse gate, namely the inverse of $\mathrm{Den}(\mathrm{DET}(I_n + zX))$ at the point $z = 0$. But $a := (\mathrm{Den}(\mathrm{DET}(I_n + zX))(z/0))^\sharp$ is a constant circuit computing a non-zero field element, and we can identify $a^{-1}$ with the field constant it computes.

**Lemma 7.8.** *Let $X$ be an $n\times n$ matrix of distinct variables. There exist circuits with divisions $P_0, \ldots, P_{n-1}$ not containing the variable $z$, such that*

$$\mathrm{DET}(zI_n + X) = z^n + P_{n-1}z^{n-1} + \cdots + P_0$$

*has a polynomial-size $\mathbb{P}_c^{-1}(\mathbb{F})$ proof. Moreover, this proof is defined for $z = 0$.*

*Proof.* Let $F$ be a circuit in which $z$ does not occur in the scope of any inverse gate. Then, we define the *$z$-degree of $F$* as the syntactic-degree of $F$ considered as a circuit computing a univariate polynomial in $z$ (so that all other variables are treated as constants).

By induction, we will construct matrices $A_1, \ldots, A_n$ with the following properties:

1. $A_1 = X + zI_n$,
2. Every $A_k$ is an $(n - k + 1) \times (n - k + 1)$ matrix of the form

$$\begin{pmatrix} z^k + f & w \\ v^t & zI_{n-k} + Q \end{pmatrix}$$

   where all the entries are circuits with divisions in which $z$ does not occur in the scope of any division gate, $v, w$ are $1 \times (n - k)$ vectors and moreover: $f$ as well as every entry of $w$ have $z$-degree less than $k$ and $v, Q$ do not contain the variable $z$.
3. The identity $\mathrm{DET}(A_k) = \mathrm{DET}(A_{k+1})$ has a polynomial-size proof.
4. The entries of $A_k$ are algebraically independent (this is to guarantee that divisions are defined).

Assume that $A_k$ is given, and let us partition it as

$$A_k = \begin{pmatrix} z^k + f_1 & w & f_2 \\ u_1^t & zI_m + Q & u_2^t \\ a_1 & v & z + a_2 \end{pmatrix}$$

where $m = (n-k-1)$ and we allow the possibility that $m = 0$. By the assumption, $f_1, w$ and $f_2$ have $z$-degree smaller than $k$, and $z$ does not occur in $u_1, u_2, Q, a_1, a_2$ and $v$. By Lemma 7.7 part (i), we can switch the first and last column to obtain a $\mathbb{P}_c^{-1}$ proof of

$$\mathrm{DET}(A_k) = -\mathrm{DET}\begin{pmatrix} f_2 & w & z^k + f_1 \\ u_2^t & zI_m + Q & u_1^t \\ z + a_2 & v & a_1 \end{pmatrix}.$$

By Lemma 7.7 part (iv), we have

$$\mathrm{DET}(A_k) = -a_1 \mathrm{DET}\begin{pmatrix} f_2 - a_1^{-1}(z^k + f_1)(z + a_2) & w - a_1^{-1}(z^k + f_1)v \\ u_2^t - a_1^{-1}u_1^t(z + a_2) & zI_m + Q - a_1^{-1}u_1^t v \end{pmatrix} =$$
$$\mathrm{DET}\begin{pmatrix} (z^k + f_1)(z + a_2) - a_1 f_2 & (z^k + f_1)v - a_1 w \\ u_2^t - a_1^{-1}u_1^t(z + a_2) & zI_m + Q - a_1^{-1}u_1^t v \end{pmatrix}.$$

We can write $(z^k + f_1)(z + a_2) = z^{k+1} + (f_1 z + a_2 z^k + f_1 a_2)$, where the $z$-degree of $(f_1 z + a_2 z^k + f_1 a_2)$, as well as of every entry of $(z^k + f_1)v - a_1 w$, is at most $k$. Hence the last matrix is of the correct form, apart from the occurrence of $zu_1^t$ in the first column. This can be remedied by multiplying by $\begin{pmatrix} 1 & 0 \\ -a_1^{-1}u_1^t & I_m \end{pmatrix}$ from the right to obtain $A_{k+1}$ of the required form.

This indicates that, given a circuit computing $A_k$, we can compute $A_{k+1}$ using polynomially many additional gates. Altogether, every $A_k$ has a polynomial size circuit. The proof of $\mathrm{DET}(A_k) = \mathrm{DET}(A_{k+1})$ has a polynomial number of lines and, as it involves polynomial size circuits, also polynomial size.

Finally, we obtain a polynomial size proof of $\mathrm{DET}(A_n) = \mathrm{DET}(A_1) = z^n + f$, where $f$ is a circuit with $z$-degree smaller than $n$ in which $z$ is not in the scope of any division gate. Writing $f$ as $\sum_{i=0}^{n-1} P_i z^i$ concludes the lemma. QED

**Proposition 7.9.**

*(i). If $U$ is a triangular matrix with $u_1, \ldots, u_n$ on the diagonal then $\det(U) = u_1 \cdots u_n$ has a polynomial size $\mathbb{P}_c^{-1}$ proof.*

*(ii). Let $X$ be an $n \times n$ matrix of distinct variables. Then*

$$\mathrm{DET}(X) = \det(X)$$

*has a polynomial-size $\mathbb{P}_c^{-1}$ proof.*

*Proof.* Part (i) follows from Proposition 7.6. For we have $\mathrm{DET}(I_n + zU) = (1 + zu_1) \cdots (1 + zu_n)$, and the proof is defined for $z = 0$. Thus, by Proposition 5.5

$$\det(U) = \Delta_{z^n}((1 + zu_1) \cdots (1 + zu_n)) = u_1 \cdots u_n$$

has a polynomial-size $\mathbb{P}_c^{-1}$ proof.

Part (ii) follows from the previous lemma, as follows. We obtain polynomial-size $\mathbb{P}_c^{-1}$ proofs of the following substitution instance:

$$\mathrm{DET}(zI_n + X^{-1}) = z^n + Q_{n-1}z^{n-1} + \cdots + Q_0, \tag{7.9}$$

where the $Q_i$'s are circuits with divisions that do not contain the variable $z$ and the proof is defined for $z = 0$.

By Proposition 7.6 we have a polynomial-size $\mathbb{P}_c^{-1}$ proof of

$$\mathrm{DET}(I_n + zX) = \mathrm{DET}(zI_n + X^{-1}) \cdot \mathrm{DET}(X)\,.$$

The proof is defined for $z = 0$ (as is witnessed by letting $X := I_n$). From equation (7.9) we get a polynomial-size proof of

$$\mathrm{DET}(I_n + zX) = z^n \mathrm{DET}(X) + z^{n-1} Q'_{n-1} + \cdots + Q'_0,$$

where $Q'_{n-1}, \ldots, Q'_0$ do not contain $z$. The proof is defined for $z = 0$ and so Proposition 5.5 gives a polynomial-size $\mathbb{P}_c^{-1}$ proof of

$$\Delta_{z^n}(\mathrm{DET}(I_n + zX)) = \Delta_{z^n}(z^n \mathrm{DET}(X) + z^{n-1} Q'_{n-1} + \cdots + Q'_0).$$

But by the definition of $\det(X)$, $\Delta_{z^n}(\mathrm{DET}(I + zX))$ is $\det(X)$ and by the definition of $\Delta_{z^n}$, $\Delta_{z^n}(z^n \mathrm{DET}(X) + z^{n-1} Q'_{n-1} + \cdots + Q'_0)$ is $\mathrm{DET}(X)$, and we are done. QED

## 8 Concluding the main theorem

Recall the definition of the circuit $\det(X)$ in Equation (7.8) and of the formula $F^\bullet$ from Remark 1.3. We define a new circuit and a formula computing the determinant, as follows

$$\det_c(X) := [\det(X)], \quad \det_f(X) := (\det_c(X))^\bullet \tag{8.1}$$

Hence, $\det_c(X)$ is a depth $O(\log^2 n)$ polynomial-size (division-free) circuit and $\det_f(X)$ is an $n^{O(\log n)}$-size division-free arithmetic formula, both computing the determinant polynomial. We can now finally prove Theorem 2.1 (main theorem), which we rephrase as follows:

**Theorem 8.1** (Theorem 2.1, rephrased). *Let $X, Y, Z$ be $n \times n$ matrices such that $X, Y$ consist of different variables and $Z$ is a triangular matrix with $z_{11}, \ldots, z_{nn}$ on the diagonal. Then:*

*(i). The identity $\det_c(XY) = \det_c(X) \cdot \det_c(Y)$ and $\det_c(Z) = z_{11} \cdots z_{nn}$ have polynomial-size $O(\log^2 n)$-depth proofs in $\mathbb{P}_c$.*

*(ii). The identity $\det_f(XY) = \det_f(X) \cdot \det_f(Y)$ and $\det_f(Z) = z_{11} \cdots z_{nn}$ have $\mathbb{P}_f$ proofs of size $n^{O(\log n)}$.*

*Proof.* Proposition 7.9 part (ii) and Proposition 7.6 imply that the equations

$$\det(XY) = \det(X) \cdot \det(Y) \qquad \text{and} \qquad \det(Z) = z_{11} \cdots z_{nn} \tag{8.2}$$

have polynomial-size $\mathbb{P}_c^{-1}$ proofs. By definition, the syntactic degree of $\det(X)$ is at most $n$. Hence, by Theorem 6.4, the identities in (8.2) have a polynomial-size $\mathbb{P}_c$ proofs. This almost concludes part (i), except for the bound on depth. By Theorem 4.5 part (i), $\det_c(X) = \det(X)$ has a polynomial size $\mathbb{P}_c$ proof (hence also $\det_c(Y) = \det(Y)$ and $\det_c(XY) = \det(XY)$ do). Equation (8.2) gives a polynomial size proof of:

$$\det_c(XY) = \det_c(X) \cdot \det_c(Y) \qquad \text{and} \qquad \det_c(Z) = z_{11} \cdots z_{nn}\,.$$

Corollary 4.6 then gives a polynomial size $\mathbb{P}_c$ proof of depth $O(\log^2 n)$.

For part (ii), the statement follows from part (i) and Lemma 4.7 part (i). Note that $(\det_c(XY))^\bullet$ and $\det_f(XY)$ is the same formula; likewise for $(\det_c(X) \cdot \det_c(Y))^\bullet$ and $\det_f(X) \cdot \det_f(Y)$. QED

We should note that in the $\mathbb{P}_c$-proof of the equation $\det(XY) = \det(X) \cdot \det(Y)$ no divisions occur and so it is defined for any substitution. In particular,

$$\det(AX) = \det(XA) = \det(A) \cdot \det(X) = a \cdot \det(X) \tag{8.3}$$

has a short $\mathbb{P}_c$ proof for any matrix $A$ of field elements whose determinant is $a \in \mathbb{F}$. Similarly, the elementary Gaussian operations stated in Lemma 7.7 carry over to polynomial-size $\mathbb{P}_c$ proofs of the corresponding properties of det.

# 9 Applications

In this section, we prove Propositions 2.9 and 2.10, as well as a $\mathbb{P}_c$-version of the Cayley-Hamilton theorem. First, we show that the cofactor expansion has short $\mathbb{P}_c$ proofs. For an $n \times n$ matrix $X$ and $i, j \in [n]$, let $X_{i,j}$ denote the $(n-1)\times(n-1)$-matrix obtained by removing the $i$th row and $j$th column from $X$. Let $\mathrm{Adj}(X)$ be the $n \times n$ matrix whose $(i, j)$-th entry is $(-1)^{i+j}\det_c(X_{j,i})$ (where $\det_c$ is the circuit from Equation (8.1)).

**Proposition 9.1** (Cofactor expansion)**.** *Let $X = \{x_{ij}\}_{i,j\in[n]}$ be an $n \times n$ matrix. Then the following identities have polynomial-size $O(\log^2 n)$-depth $\mathbb{P}_c$ proofs:*

*(i).* $\det_c(X) = \sum_{j=1}^{n}(-1)^{i+j}x_{ij}\det_c(X_{i,j})$, *for any $i \in [n]$;*

*(ii).* $X \cdot \mathrm{Adj}(X) = \mathrm{Adj}(X) \cdot X = \det_c(X) \cdot I$.

*Proof.* For part (i), we prove $\det_c(X) = \sum_{j=1}^{n}(-1)^{n+j}x_{nj}\det_c(X_{n,j})$. The general case follows after a suitable permutation of rows of $X$ (cf. equation (8.3)). It is sufficient to construct a polynomial size $\mathbb{P}_c^{-1}$ proof, for we can then eliminate the division gates by means of Theorem 6.4 and bound the depth of the proof by means of Corollary 4.6.

For $j \in [n]$, let $X_j$ be the matrix obtained by replacing $x_{ni}$ by 0 in $X$, for every $i \neq j$. We want to show that

$$\begin{aligned} \det_c(X) &= \det_c(X_1) + \cdots + \det_c(X_n) && (9.1)\\ \det_c(X_j) &= (-1)^{n+j}x_{nj}\det_c(X_{n,j})\,,\ j \in [n] && (9.2) \end{aligned}$$

have polynomial size $\mathbb{P}_c^{-1}$ proofs. This is enough to conclude (i).

Write $X = \begin{pmatrix} X_{n,n} & v_1^t \\ v_2 & x_{nn} \end{pmatrix}$. The definition of DET (Section 7.1) and the equality $\det_c =$ DET (Proposition 7.9 and Theorem 4.5 part (i)) give $\det_c(X) = \det_c(X_{n,n})(x_{nn} - v_2 X_{n,n}^{-1} v_1^t)$. This expression is linear in the last row of $X$ which gives (9.1). Setting $v_2 = 0$ gives $\det_c(X_n) = \det_c(X_{n,n})x_{n,n}$, a special case of 9.2. The general case follows by permuting the columns of $X$.

Part (ii) is an application of part (i). The $i, j$-entry of $X \cdot \mathrm{Adj}(X)$ is

$$a_{ij} = \sum_{k=1}^{n}(-1)^{i+k}x_{ik}\det_c(X_{j,k})\,.$$

Hence we already know that $a_{ij} = \det_c(X)$ whenever $i = j$ and it remains to show that $a_{ij} = 0$ if $i \neq j$. By part (i), $\sum_{k=1}^{n}(-1)^{i+k}x_{ik}\det_c(X_{j,k}) = \det_c(Y)$, where $Y$ is a matrix with two identical rows. Then $Y$ can be written as $Y = AJY$, where $J$ is a diagonal matrix with some entry on the diagonal equal to zero, and so $\det_c(Y) = \det_c(A)\det_c(J)\det_c(Y) = 0$. Finally, $X \cdot \mathrm{Adj}(X) = \det_c(X)I_n$ gives $\mathrm{Adj}(X) = \det_c(X)X^{-1}$ and hence also $\mathrm{Adj}(X) \cdot X = \det_c(X)I_n$. QED

**Proposition 9.2** (Proposition 2.10 restated)**.** *The identities $YX = I_n$ have polynomial-size and $O(\log^2 n)$-depth $\mathbb{P}_c$ proofs from the equations $XY = I_n$. In the case of $\mathbb{P}_f$, the proofs have quasipolynomial-size.*

*Proof.* Note that we are dealing with a $\mathbb{P}_c$ proof from assumptions, and hence we are not allowed to use division gates. The proof is constructed as follows. Assume $XY = I_n$. By Theorem 8.1, this gives $\det_c(X)\det_c(Y) = 1$. By Proposition 9.1, we can multiply from the left both sides of $XY = I_n$ by $\mathrm{Adj}(X)$, to obtain $\det_c(X)Y = \mathrm{Adj}(X)$. Hence,

$$\det_c(X)YX = \mathrm{Adj}(X)X = \det_c(X)I_n,$$

and so

$$\det_c(Y)\det_c(X)YX = \det_c(Y)\det_c(X)I_n,$$

which, using $\det_c(X)\det_c(Y) = 1$ gives $YX = I_n$. The $\mathbb{P}_f$ proof is identical, except that the steps involving the determinant require a quasipolynomial size. QED

We now restate and prove Proposition 2.9.

**Proposition 9.3** (Proposition 2.9 rephrased)**.** *Let $F$ be a formula of size $s$. Then there exists a matrix $M$ of dimension $2s \times 2s$ whose entries are variables or elements of $\mathbb{F}$ such that the identity $F = \det_c(M)$ has a polynomial-size $O(\log^2 s)$-depth $\mathbb{P}_c(\mathbb{F})$ proof; and $F = \det_f(M)$ has a quasipolynomial-size $\mathbb{P}_f(\mathbb{F})$ proof.*

*Proof.* The proof proceeds via a simulation of the construction in [Val79], as loosely reproduced in [HWY10]. The matrix $M$ is constructed inductively with respect to the size of the formula, as in Claim 17 of [HWY10]. It is convenient to maintain the property

$$M_{i,i+1} = 1 \qquad \text{and} \qquad M_{i,j} = 0, \text{ if } j > i + 1\,.$$

Let us call matrices of this form *nearly triangular*. If $F$ is a formula of size one, we assign it the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & \widehat{F} \end{pmatrix}.$$

Let $M_1, M_2$ be nearly triangular matrices of dimensions $s_1 \times s_1$ and $s_2 \times s_2$, respectively. In order to proceed on the inductive step, it is sufficient to show that the following equations have polynomial-size $\mathbb{P}_c$ proofs:

(i). $\det_c(M) = \det_c(M_1) \cdot \det_c(M_2)$, where

$$M = \begin{pmatrix} M_1 & E \\ 0 & M_2 \end{pmatrix},$$

and $E$ has 1 in the lower left corner and 0 otherwise.

(ii). $\det_c(M) = \det_c(M_1) + \det_c(M_2)$, with

$$M = \left( \begin{array}{cccc} 1 & v & 0 & 0 \\ 0 & M_1 & v_1 & 0 \\ M_2[1] & 0 & v_2 & M_2[2^+], \end{array} \right),$$

where $v$ is a row vector with 1 in the leftmost entry and 0 elsewhere, $v_1$ is a column vector with 1 in the bottom entry and 0 elsewhere, $v_2$ is a column vector with $(-1)^{s_2+1}$ in the bottom entry and 0 elsewhere, $M_2[1]$ is the first column of $M_2$, and $M_2[2^+]$ is the matrix $M_2$ without the first column.

Both parts are an exercise using the cofactor expansion, as stated in Proposition 9.1 (in (ii), expand along the first row). QED

### The Cayley-Hamilton theorem

Let $X = \{x_{i,j}\}_{i,j\in[n]}$ be an $n \times n$ matrix of distinct variables. For $i \in \{0, \ldots, n\}$, let $p_i$ be the circuit in variables $X$ defined by

$$p_i := \Delta_{z^i}(\det_c(zI_n - X))$$

and let $P_X(z)$ be the circuit

$$P_X(z) := \sum_{i=0}^{n} p_i z^i .$$

$P_X(z)$ computes the characteristic polynomial of the matrix $X$ and we can prove the following version of Cayley-Hamilton theorem:
**Proposition 9.4.**

$$P_X(X) = \sum_{i=0}^{n} p_i X^i = 0$$

*has a polynomial-size $\mathbb{P}_c$-proof.*

As before, if we replace the $p_i$'s by their balanced versions, we can obtain a polynomial-size $\mathbb{P}_c$-proof of depth $O(\log^2(n))$.

*Proof.* Since $\det_c(zI_n - X)$ has a syntactic degree $n$, we have a polynomial-size proof of $\det_c(zI_n - X) = P_X(z)$ by Proposition 5.5. Proposition 9.1 gives

$$\mathrm{Adj}(zI_n - X) \cdot (zI_n - X) = \det_c(zI_n - X)I_n = P_X(z)I_n .$$

Since every entry of Adj has a syntactic degree less than $n$, we can write $\mathrm{Adj}(zI_n - X) = \sum_{i=0}^{n-1} A_i z^i$, where the matrices $A_i$ do not contain $z$. Hence we also have

$$\left( \sum_{i=0}^{n-1} A_i z^i \right) \cdot (zI_n - X) = P_X(z)I_n .$$

Expanding the left-hand side and collecting terms with the same power of $z$ gives

$$-A_0X + \sum_{i=1}^{n-1}(A_{i-1} - A_iX)z^i + A_{n-1}z^n = p_X(z)I_n\,. \tag{9.3}$$

Since $P_X(z) = \sum_{i=0}^{n} p_i z^i$, where the $p_i$'s do not contain $z$, we can compare the coefficients on the left and right-hand side of (9.3) (see Proposition 5.5) to conclude

$$p_0 I_n = -A_0X\,, \qquad p_i I_n = A_{i-1} - A_iX \quad \text{if } \; i \in \{1, \dots, n-1\}\,, \qquad p_n I_n = A_{n-1}\,.$$

Hence

$$\begin{aligned}
\sum_{i=0}^{n} p_i X^i &= p_0 I_n + p_1 X + p_2 X^2 + \cdots + p_{n-1}X^{n-1} + p_n X^n \\
&= -A_0X + (A_0 - A_1X)X + (A_1 - A_2X)X^2 + \cdots + (A_{n-2} - A_{n-1}X)X^{n-1} + A_{n-1}X^n \\
&= (-A_0X + A_0X) + (-A_1X^2 - A_1X^2) + \ldots + (-A_{n-1}X^n + A_{n-1}X^n) \\
&= 0\,.
\end{aligned}$$

QED

# References


[BBP95] Maria Luisa Bonet, Samuel R. Buss, and Toniann Pitassi. Are there hard examples for Frege systems? In *Feasible mathematics, II (Ithaca, NY, 1992)*, volume 13 of *Progr. Comput. Sci. Appl. Logic*, pages 30–56. Birkhäuser Boston, Boston, MA, 1995. 1

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inf. Process. Lett.*, 18:147–150, 1984. 1, 2.1

[BP98] Paul Beame and Toniann Pitassi. Propositional proof complexity: past, present, and future. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (65):66–89, 1998. (document), 1

[Brent74] Richard P. Brent. The parallel evaluation of general arithmetic expressions. In *J. ACM*, 21(2): 201–206, 1974. 4.2

[DF04] David S. Dummit and Richard M. Foote. Abstract Algebra. 3rd Ed. John Wiley and Sons, 2004. 5

[HT09] Pavel Hrubeš and Iddo Tzameret. The proof complexity of polynomial identities. In *Proceedings of the 24th IEEE Conference on Computational Complexity (CCC)*, pages 41–51, 2009. 1, 1.1, 1.1

[HWY10] Pavel Hrubeš, Avi Wigderson, and Amir Yehudayoff. Relationless completeness and separations. In *Proceedings of the 25th IEEE Conference on Computational Complexity*, pages 280–290, 2010. 9

[Hya79] Laurent Hyafil. On the parallel evaluation of multivariate polynomials. *SIAM J. Comput.*, 8(2):120–123, 1979. 1, 2.2

[Jeř04] Emil Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Ann. Pure Appl. Logic*, 129(1-3):1–37, 2004. 1.1, 2.5

[Kra95] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. 1.1, 2.5, 5

[RY08] Ran Raz and Amir Yehudayoff. Balancing syntactically multilinear arithmetic circuits. *Computational Complexity*, 17:515–535, 2008. 4.1, 4.1.2

[SC04] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. *Ann. Pure Appl. Logic*, 130(1-3):277–323, 2004. (document), 1, 2.1

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. 1, 5.1

[Seg07] Nathan Segerlind. The complexity of propositional proofs. *Bull. Symbolic Logic*, 13(4):417–481, 2007. 1

[Sol01] Michael Soltys. *The complexity of derivations of matrix identities*. PhD thesis, University of Toronto, Toronto, Canada, 2001. 1

[Sol05] Michael Soltys. Feasible proofs of matrix properties with Csanky's algorithm. In *19th International Workshop on Computer Science Logic*, pages 493–508, 2005. 1

[Spi71] Philip M. Spira On time-hardware complexity tradeoffs for Boolean functions. In *Hawaii Symp.on Syst.Sc.*, pages 525–527, 1971. 4.2

[Str73] Volker Strassen. Vermeidung von divisionen. *J. Reine Angew. Math.*, 264:182–202, 1973. (in German). 1, 2.2, 2.3, 5.1

[SU04] Michael Soltys and Alasdair Urquhart. Matrix identities and the pigeonhole principle. *Arch. Math. Logic*, 43(3):351–357, 2004. 1

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. 2.1

[Val79] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on the Theory of Computing*, pages 249–261. ACM, 1979. 2.5, 9

[VSBR83] Leslie G. Valiant, Sven Skyum, S. Berkowitz, and Charles Rackoff. Fast parallel computation of polynomials using few processors. *SIAM J. Comput.*, 12(4):641–644, 1983. 1, 2.2, 2.2, 2.2, 4.1, 4.1, 4.1.2

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, pages 216–226. Springer-Verlag, 1979. 1, 5.1