

# Average-Case Separation in Proof Complexity: Short Propositional Refutations for Random 3CNF Formulas

Sebastian Müller\*

Iddo Tzameret<sup>†</sup>

## Abstract

Separating different propositional proof systems—that is, demonstrating that one proof system cannot efficiently simulate another proof system—is one of the main goals of proof complexity. Nevertheless, all known separation results between non-abstract proof systems are for *specific* families of hard tautologies: for what we know, in the *average case* all (non-abstract) propositional proof systems are no stronger than resolution. In this paper we show that this is not the case by demonstrating polynomial-size propositional refutations whose lines are  $TC^0$  formulas (i.e.,  $TC^0$ -Frege proofs) for random 3CNF formulas with  $n$  variables and  $\Omega(n^{1.4})$  clauses. By known lower bounds on resolution refutations, this implies an exponential separation of  $TC^0$ -Frege from resolution in the average case.

The idea is based on demonstrating efficient propositional correctness proofs of the random 3CNF unsatisfiability witnesses given by Feige, Kim and Ofek [17]. Since the soundness of these witnesses is verified using spectral techniques, we develop an appropriate way to reason about eigenvectors in propositional systems. To carry out the full argument we work inside weak formal systems of arithmetic, use a general translation scheme to propositional proofs and then show how to turn these proofs into random 3CNF refutations.

---

\*Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic. Email: [muller@karlin.mff.cuni.cz](mailto:muller@karlin.mff.cuni.cz). Supported by the Marie Curie Initial Training Network in Mathematical Logic - MALOA - From MAThematical LOGic to Applications, PITN-GA-2009-238381

<sup>†</sup>Institute for Theoretical Computer Science, the Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084, China. Email: [tzameret@tsinghua.edu.cn](mailto:tzameret@tsinghua.edu.cn). Supported by the National Natural Science Foundation of China Grant and the National Basic Research Program of China Grant; Part of this work was done while the author was a research fellow at the Mathematical Institute of the Academy of Science, Prague, Czech Republic, supported by The Eduard Čech Center for Algebra and Geometry and The John Templeton Foundation.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Background in proof complexity . . . . .	3
1.2	Our result . . . . .	5
1.3	The structure of the argument . . . . .	6
1.4	Organization of the paper . . . . .	8
<b>2</b>	<b>Preliminaries</b>	<b>8</b>
2.1	Miscellaneous linear algebra notations . . . . .	8
2.2	Propositional proofs and $TC^0$ -Frege systems . . . . .	9
<b>3</b>	<b>Theories of bounded arithmetic</b>	<b>11</b>
3.1	The theory $V^0$ . . . . .	12
3.1.1	Extending $V^0$ with new function and relation symbols . . . . .	14
3.1.2	Basic formalizations in $V^0$ . . . . .	16
3.2	The theory $VTC^0$ . . . . .	19
3.2.1	Extending $VTC^0$ with new function and relation symbols . . . . .	20
3.2.2	Summation in $VTC^0$ . . . . .	21
3.2.3	Counting in $VTC^0$ . . . . .	22
3.2.4	Manipulating big sums in $VTC^0$ . . . . .	26
3.2.5	The relation between $VTC^0$ and $TC^0$ -Frege . . . . .	28
<b>4</b>	<b>Feige-Kim-Ofek witnesses and the main formula</b>	<b>30</b>
<b>5</b>	<b>Proof of the main formula</b>	<b>33</b>
5.1	Formulas satisfied as 3XOR . . . . .	37
5.2	Bounding the number of NAE satisfying assignments . . . . .	40
<b>6</b>	<b>The spectral bound</b>	<b>42</b>
6.1	Notations . . . . .	43
6.2	Rational approximations of real numbers, vectors and matrices . . . . .	43
6.3	The predicate EIGVALBOUND . . . . .	43
6.4	Certifying the matrix identity . . . . .	46
<b>7</b>	<b>Wrapping up the proof: <math>TC^0</math>-Frege refutations of random 3CNFs</b>	<b>50</b>
7.1	Converting the main formula into a $\forall\Sigma_0^B$ formula . . . . .	51
7.2	Propositional proofs . . . . .	52

## 1 Introduction

This paper deals with the average complexity of propositional proofs. Our major aim is to demonstrate that already standard propositional proof systems, well within the hierarchy of Frege proofs, can do much better than resolution, not only for *specific* families of hard instances, but rather for *almost all* unsatisfiable 3CNF formulas (for sufficiently large clause-to-variable ratio). Specifically, we will show that most 3CNF formulas with  $n$  variables and at least  $cn^{1.4}$  clauses, for a sufficiently

large constant  $c$ , have polynomial-size in  $n$  propositional refutations whose proof-lines are constant depth circuits with threshold gates (namely,  $TC^0$ -Frege proofs). This is in contrast to resolution (that can be viewed as depth-1 Frege) for which it is known that most 3CNF formulas with at most  $n^{1.5-\epsilon}$  clauses (for  $0 < \epsilon < \frac{1}{2}$ ) do not admit sub-exponential refutations [8]. This result establishes essentially the first average-case separation between non-abstract propositional proof systems, and places a stream of recent results on efficient probabilistic refutation algorithms, culminating in the work of Feige et al. [17], within the framework of propositional proof complexity.

## 1.1 Background in proof complexity

Propositional proof complexity is the systematic study of the efficiency of proof systems establishing propositional tautologies (or dually, refute unsatisfiable formulas). One can view a propositional proof system *abstractly* as a deterministic polynomial-time algorithm  $A$  that receives a string  $\pi$  (“the proof”) and a propositional formula  $\Phi$  such that there exists a  $\pi$  with  $A(\pi, \Phi) = 1$  iff  $\Phi$  is a tautology. Such an  $A$  is called an *abstract proof system*. Nevertheless, most research in proof complexity is dedicated to more concrete or structured models, in which proofs are sequences of lines, and each line is derived from previous lines by “local” and sound rules.

Perhaps the most studied family of propositional proof systems are those coming from propositional logic, under the name Frege systems, and their fragments (and extensions). In this setting, proofs are written as sequences of Boolean formulas (proof-lines) where each line is either an axiom or was derived from previous lines by means of simple sound derivation rules. The *complexity* of a proof is just the number of symbols it contains, that is, the total size of formulas in it. And different proof systems are compared via the concept of *polynomial simulation*: a proof system  $P$  polynomially-simulates another proof system  $Q$  if there is a polynomial  $p$  such that for every propositional tautology  $\tau$ , if the minimal  $Q$ -proof of  $\tau$  is of size  $s$  then the minimal  $P$ -proof of  $\tau$  is of size at most  $p(s)$ . The definition of Frege systems is sufficiently robust, in the sense that different formalizations can polynomially-simulate each other [29].

It is common to consider fragments (or extensions) of Frege proofs induced by restricting the proof-lines to contain presumably weaker (or stronger) circuit classes than Boolean formulas. The stratification of Frege proofs is thus analogous to that of Boolean circuit classes: Frege proofs consist of Boolean formulas (i.e.,  $NC^1$ ) as proof-lines,  $TC^0$ -Frege (also known as Threshold Logic) consists of  $TC^0$  proof-lines, Bounded Depth Frege has  $AC^0$  proof-lines, depth- $d$  Frege has circuits of depth- $d$  proof-lines, etc. In this framework, the resolution system can be viewed as *depth-1 Frege*. Similarly, one usually considers extensions of Frege system such as  $NC^i$ -Frege, for  $i > 1$ , and  $P$ /**poly**-Frege (known as Extended Frege). Restrictions (and extensions) of Frege proofs form a hierarchy with respect to polynomial-simulations, though it is open whether the hierarchy is proper.

It thus constitutes one of the main goals of proof complexity to understand the above hierarchy of Frege proofs, and most importantly to separate different propositional proof systems—that is, to show that one proof system does not polynomially simulate another proof system. These questions also relate in certain sense to the hierarchy of Boolean circuits (from  $AC^0$ , through,  $AC^0[p]$ ,  $TC^0$ ,  $NC^1$ , and so forth; see [12]). Many separations between propositional proof systems (not just in the Frege hierarchy) are known. For this kind of results it is enough to demonstrate a *single* family of tautologies requiring super-polynomial proof-size in one system, while having polynomial-size proofs in the other system. In the case of Frege proofs there are already known separations between certain fragments of it (e.g., separation of depth- $d$  Frege from depth  $d+1$  Frege was shown

by Krajíček [25]). It is also known that  $TC^0$ -Frege is strictly stronger than resolution, since, e.g., the former admits polynomial-size proofs of the propositional pigeonhole principle, while the latter does not (see [23] for the resolution lower bound and [13] for the corresponding  $TC^0$ -Frege upper bound).

**Average case proof complexity.** Much like in algorithmic research, it is important to know the average-case complexity of propositional proof systems, and not just their worst-case behavior. To this end one usually considers the model of random 3CNFs, where  $m$  clauses with three literals each, out of all possible  $2^3 \cdot \binom{n}{3}$  clauses with  $n$  variables, are chosen independently, with repetitions. When  $m$  is greater than  $cn$  for some sufficiently large  $c$  (say,  $c = 5$ ), it is known that with high probability a random 3CNF is unsatisfiable. (As  $m$  gets larger the task of refuting the 3CNF becomes easier since we have more constraints to use.) In average-case analysis of proofs we investigate whether such unsatisfiable random 3CNFs also have short (polynomial-size) refutations in a given proof system. The importance of average-case analysis of proof systems is that it gives us a better understanding of the complexity of a system than merely the worst-case analysis. If we separate two proof systems in the average case—i.e., show that for almost all 3CNF one proof system admit polynomial-size refutations, while the other system does not—we establish a stronger separation.

Until today only weak proof systems like resolution and  $\text{Res}(k)$  (for  $k \leq \sqrt{\log n / \log \log n}$ ; the latter system can be viewed as Frege operating with disjunctions of fan-in at most  $k$ ) and polynomial calculus (and an extension of it) were analyzed in the average case; for these systems exponential lower bounds are known for random 3CNFs (with varying number of clauses) [11, 5, 8, 4, 30, 1, 7, 2, 20]. For random 3CNFs with  $n$  variables and  $n^{1.5-\epsilon}$  ( $0 < \epsilon < \frac{1}{2}$ ) clauses it is known that there are no sub-exponential size resolution refutations [8]. For many proof systems, like cutting planes (CP) and bounded depth Frege ( $\mathbf{AC}^0$ -Frege), it is a major open problem to prove average case lower bounds (even for number of clauses near the threshold of unsatisfiability, e.g., random 3CNFs with  $n$  variables and  $5n$  clauses). The results mentioned above only concerned lower bounds. On the other hand, to the best of our knowledge, the only known non-trivial polynomial-size *upper bound* on random  $k$ CNFs refutations in any non-abstract propositional proof system is for resolution. This is a result of Beame et al. [5], and it applies for fairly large number of clauses (specifically,  $\Omega(n^{k-1} / \log n)$ ). This implies that no (non-abstract) average-case separations were known till now.

**Efficient probabilistic refutation algorithms.** A different kind of results on refuting random  $k$ CNFs were investigated in Goerdt and Krivelevich [21] and subsequent works by Goerdt and Lanka [22], Friedman, Goerdt and Krivelevich [19], Feige and Ofek [18] and Feige [16]. Here, one studies efficient probabilistic refutation *algorithms* for  $k$ CNFs. Specifically, an *efficient probabilistic refutation algorithm* receives a  $k$ CNF (above the unsatisfiability threshold) and outputs either “unsatisfiable” or “don’t know”; if the algorithm answers “unsatisfiable” then the  $k$ CNF is required to be indeed unsatisfiable; also, the algorithm should output “unsatisfiable” with high probability (which by definition, is also the correct answer). Such refutation algorithms can be viewed as *abstract* proof systems (according to the definition in Subsection 1.1) having short proofs on the average-case:  $A(\Phi)$  is a deterministic polytime machine whose input is only  $k$ CNFs (we can think of the proposed proof  $\pi$  input as being always the empty string). On input  $\Phi$  the machine  $A$  runs the refutation algorithm and answers 1 iff the refutation algorithm answers “unsatisfiable”; otherwise,  $A$  can decide, e.g. by brute-force search, whether  $\Phi$  is unsatisfiable or not. (In a similar manner, if the original efficient refutation algorithm is *non-deterministic* then we also get an abstract proof

system for  $k$ CNFs; now the proof  $\pi$  that  $A$  receives is the description of an accepting run of the refutation algorithm.)

Goerdt and Krivelevich [21] initiated the use of *spectral methods* to devise efficient probabilistic algorithms for refuting  $k$ CNFs. The idea is that a  $k$ CNF with  $n$  variables can be associated with a graph on  $n$  vertices (or directly with a certain matrix). It is possible to show that certain properties of the associated graph witness the unsatisfiability of the original  $k$ CNF. One then uses a spectral method to give evidence for the desired graph property, and hence to witness the unsatisfiability of the original  $k$ CNF. Now, if we consider a random  $k$ CNF then the associated graph essentially becomes random too, and so one may show that the appropriate property witnessing the unsatisfiability of the  $k$ CNF occurs with high probability in the graph. The refutation algorithms devised in this way work for 3CNFs with at least  $\Omega(n^{1.5})$  clauses [18].

Continuing this line of research, Feige, Kim and Ofek [17] considered efficient *non-deterministic* refutation algorithms (in other words, efficient *witnesses* for unsatisfiability of 3CNFs). They established the *currently best*—with respect to the number of clauses—efficient refutation procedure (alas non-deterministic): they showed that with probability converging to 1 a random 3CNF with  $n$  variables and at least  $cn^{1.4}$  clauses has a polynomial-size witness, for sufficiently big constant  $c$ .

The result in the current paper shows that all the above probabilistic refutation algorithms, viewed as abstract proof systems, *are not stronger in the average case than  $TC^0$ -Frege*. The short  $TC^0$ -Frege refutations will be based on the witnesses from [17], and so the refutations hold for the same clause-to-variable ratio as in that paper.

## 1.2 Our result

The main result of this paper is an average case polynomial-size upper bound on proofs operating with constant-depth threshold circuits (known as Threshold Logic or  $TC^0$ -Frege; see Definition 2.4). Since Frege and Extended Frege proof systems polynomially simulate  $TC^0$ -Frege proofs, the upper bound holds for these proof systems as well. (The actual formulation of  $TC^0$ -Frege is not important since different formulations, given in [10, 26, 9, 28, 13], polynomially simulate each other.)

**Theorem 1** *With probability  $1 - o(1)$  a random 3CNF formula with  $n$  variables and  $cn^{1.4}$  clauses (for a sufficiently large constant  $c$ ) has polynomial-size  $TC^0$ -Frege refutations.*

Beame, Karp, Pitassi, and Saks [5] and Ben-Sasson and Wigderson [8] showed that with probability  $1 - o(1)$  resolution does not admit sub-exponential refutations for random 3CNF formulas when the number of clauses is at most  $n^{1.5-\epsilon}$ , for any constant  $0 < \epsilon < 1/2$ .<sup>1</sup> Therefore, Theorem 1 shows that  $TC^0$ -Frege has an exponential speed-up over resolution for random 3CNFs with at least  $cn^{1.4}$  clauses (when the number of clauses does not exceed  $n^{1.5-\epsilon}$ , for  $0 < \epsilon < 1/2$ ).

We now explain the significance and motivations behind our work. It is well known that most contemporary SAT-solvers are based on the resolution proof system. Formally, this means that these SAT-solvers use a backtracking algorithm that branch on a single variable and construct in effect a resolution refutation (in case the CNF instance considered is unsatisfiable). (The original

---

<sup>1</sup>Beame *et al.* [5] showed such a lower bound for  $n^{5/4-\epsilon}$  number of clauses (for any constant  $0 < \epsilon < 1/4$ ). Ben-Sasson and Wigderson [8] introduced the size-width tradeoff that enabled them to prove an exponential lower bound for random 3CNF formulas with  $n^{1.5-\epsilon}$  number of clauses (for any constant  $0 < \epsilon < 1/2$ ), but the actual proof for this specific clause-number appears in [6].

backtracking algorithm DPLL constructs a *tree-like* resolution refutation [15, 14].) It was known since [11] that resolution is weak in the average case, but prior to the current work there was no evidence that searching for (or constructing) refutations in a stronger propositional proof system can potentially lead to better average case performance (some researchers have expressed the belief that in the average case even Extended Frege do not outperform resolution). Although there is little hope to devise polytime algorithms for constructing minimal  $TC^0$ -Frege proofs or even resolution refutations (this stems from the conditional non-automatizability results for  $TC^0$ -Frege and resolution, proved in [9] and [3], respectively), practical experience shows that current resolution based SAT-solvers are quite powerful. Therefore, our average case upper bound theoretically justifies an attempt to extend SAT-solvers beyond resolution.

Our result also advances our understanding of the relative strength of propositional proof systems: proving non-trivial upper bounds clearly rules out corresponding lower bounds attempts. We conjecture that average case upper bounds similar to Theorem 1 could be achieved even for systems weaker than  $TC^0$ -Frege on the expense of at most a quasipolynomial increase in the size of proofs. This might help in understanding the limits of known techniques used to prove random 3CNFs lower bounds on resolution and  $Res(k)$  refutations.

The main result also contributes to our understanding of probabilistic refutation algorithms: we give an explicit logical characterization of the Feige et al. [17] witnesses. This further places a stream of results on probabilistic refutation algorithms using spectral methods, starting from Goerdt and Krivelevich [21], in the propositional proof complexity setting. This is a non-trivial job, especially because of the need to propositionally simulate spectral arguments.

### 1.3 The structure of the argument

Here we outline informally (and in some places in a simplified manner) the structure of the proof of the main theorem. We need to construct certain  $TC^0$ -Frege proofs. However, to construct such propositional proofs directly is technically too cumbersome, and so we opt to construct it indirectly, by using a first-order characterization of  $TC^0$ -Frege. For this purpose we use the first-order (two-sorted) theory, denoted  $VTC^0$ , introduced in [28] (we follow tightly [13]). Roughly speaking, when restricted to proving only statements of a certain form (formally,  $\Sigma_0^B$  formulas), the theory  $VTC^0$  characterizes (uniform) polynomial-size  $TC^0$ -Frege proofs. The construction of polynomial-size  $TC^0$ -Frege refutations for random 3CNF formulas, will consist of the following steps:

**I.** Formalize the following statement as a first-order formula:

$$\forall \text{ assignment } A \left( \text{if } \mathbf{C} \text{ is a 3CNF and } w \text{ is its FKO unsatisfiability witness} \longrightarrow \right. \\ \left. \text{exists a clause } C_i \text{ in } \mathbf{C} \text{ such that } C_i(A) = 0 \right), \quad (1)$$

where an *FKO witness* is a suitable formalization of the unsatisfiability witness defined by Feige, Kim and Ofek [17]. The corresponding predicate is called *the FKO predicate*.

**II.** Prove formula (1) in the theory  $VTC^0$ .

**III.** Translate the proof in Step II into a family of propositional  $TC^0$ -Frege proofs (of the family of propositional translations of (1)). By Theorem 3.25 (proved in [13]), this will be a polynomial-size propositional proof (in the size of  $\mathbf{C}$ ). The translation of (1) will consist of a family of



propositional formulas of the form:

$$\begin{aligned} \llbracket \text{if } \mathbf{C} \text{ is a 3CNF and } w \text{ is its FKO unsatisfiability witness} \rrbracket &\longrightarrow \\ \llbracket \text{exists a clause } C_i \text{ in } \mathbf{C} \text{ such that } C_i(A) = 0 \rrbracket, & \quad (2) \end{aligned}$$

where  $\llbracket \cdot \rrbracket$  denotes the mapping from first-order formulas to families of propositional formulas. By the nature of the propositional translation (second-sort) variables in the original first-order formula translate into a collection of propositional variables. Thus, (2) will consist of propositional variables derived from the variables in (1).

**IV.** For the next step we first note the following two facts:

- (i) Assume that  $\underline{\mathbf{C}}$  is a random 3CNF with  $n$  variables and  $cn^{1.4}$  clauses (for a sufficiently large constant  $c$ ). Then by [17] with high probability there exists an FKO unsatisfiability witness  $\underline{w}$  for  $\underline{\mathbf{C}}$ . These  $\underline{w}$  and  $\underline{\mathbf{C}}$  can be encoded as *finite sets of numbers* as required by the predicates for 3CNF and for the FKO witness formalized in (1), respectively. Let us identify  $\underline{w}$  and  $\underline{\mathbf{C}}$  with their encodings. Then, assuming (1) was formalized correctly, assigning  $\underline{w}$  and  $\underline{\mathbf{C}}$  to (1) satisfies the *premise* of the implication in (1).
- (ii) Now, by the definition of the translation from first-order formulas to propositional formulas, if an object  $\alpha$  satisfies the predicate  $P(X)$  (i.e.,  $P(\alpha)$  is true in the standard model), then there is a propositional assignment of 0, 1 values that satisfies the propositional translation of  $P(X)$ . Thus, by Item (i) above, there exists an 0, 1 assignment  $\zeta$  that satisfies the premise of (2) (i.e., the propositional translation of the premise of the implication in (1)).

Therefore, in this step we show that after assigning  $\zeta$  to the conclusion of (2) (i.e., to the propositional translation of the conclusion in (1)) one obtains precisely  $\neg \underline{\mathbf{C}}$  (formally, a renaming of  $\neg \underline{\mathbf{C}}$ , where  $\neg \underline{\mathbf{C}}$  is the 3DNF obtained by negating  $\underline{\mathbf{C}}$  and using the deMorgan rules).

**V.** Take the propositional proof obtained in **(III)**, and apply the assignment  $\zeta$  to it. The proof then becomes a polynomial-size  $\mathbf{TC}^0$ -Frege proof of a formula  $\phi \rightarrow \neg \underline{\mathbf{C}}$ , where  $\phi$  is a propositional sentence (without variables) logically equivalent to TRUE (because  $\zeta$  satisfies it, by **(IV)**). From this, one can easily obtain a polynomial-size  $\mathbf{TC}^0$ -Frege refutation of  $\underline{\mathbf{C}}$  (or equivalently, a proof of  $\neg \underline{\mathbf{C}}$ ).

The bulk of our work lies in **(I)** and especially in **(II)**. We need to formalize the necessary properties used in proving the correctness of the FKO witnesses and show that the correctness argument can be carried out in the weak theory. There are two main obstacles in this process. The first obstacle is that the correctness (soundness) of the witness is originally proved using spectral methods, which assumes that eigenvalues and eigenvectors are over the *reals*; whereas the reals are not defined in our weak theory. The second obstacle is that one needs to prove the correctness of the witness, and in particular the part related to the spectral method, *constructively* (formally in our case, inside  $\mathbf{VTC}^0$ ). Specifically, linear algebra is not known to be (computationally) in  $\mathbf{TC}^0$ , and (proof-complexity-wise) it is conjectured that  $\mathbf{TC}^0$ -Frege do not admit short proofs of the statements of linear algebra (more specifically still, short proofs relating to inverse matrices and the determinant properties; see [31] on this).

The first obstacle is solved by using rational approximations of sufficient accuracy (polynomially small errors), and showing how to carry out the proof in the theory with such approximations. The second obstacle is solved basically by constructing the argument (the main formula; see above) in a way that exploits non-determinism (i.e., in a way that enables supplying additional witnesses for the properties needed to prove the correctness of the original witness; e.g, all eigenvectors and all eigenvalues of the appropriate matrices in the original witness). In other words, we do not have to construct certain objects but can provide them, given the possibility to certify the property we need. Formally, this means that we put additional witnesses in the FKO predicate occurring in the main formula in **(I)** above.

## 1.4 Organization of the paper

The remainder of the paper is organized as follows. Section 2 contains general preliminary definitions and notations, including propositional proof systems and the  $\mathbf{TC}^0$ -Frege proof system. Section 3 contains a long exposition of the basic logical setting we use, that is, the relevant theories of (two-sorted) bounded arithmetic ( $\mathbf{V}^0$  and  $\mathbf{VTC}^0$ , from [13]), and a detailed explanation of how to formalize certain proofs in these theories. This includes defining certain syntactic objects in the theories as well as counting and doing computations in the theory. Readers who already know the basics of bounded arithmetic can skip Section 3, and look only at specific parts or definitions, when needed. Section 4 provides the formalization of the main formula we prove in the theory. This formula expresses the correctness of the Feige et al. witnesses for unsatisfiability [17]. Section 5 contains the proof of the main formula, excluding the lemma establishing the spectral inequality which is deferred to a section of its own. Section 6 provides the full proof in the theory of the spectral inequality. Section 7 finally puts everything together, and shows how to obtain short propositional refutations from the proof in the theory of the main formula.

## 2 Preliminaries

We write  $[n]$  for  $\{1, \dots, n\}$ . We denote by  $\top, \perp$  the truth values *true* and *false*, respectively.

**Definition 2.1 (3CNF)** *A literal is a propositional variable  $x_i$  or its negation  $\neg x_i$ . A 3-clause is a disjunction of three literals. A 3CNF is a conjunction of 3-clauses.*

**Definition 2.2 (Random 3CNF)** *A random 3CNF is generated by choosing independently, with repetitions,  $m$  clauses with three literals each, out of all possible  $2^3 \cdot \binom{n}{3}$  clauses with  $n$  variables  $x_1, \dots, x_n$ .*

We say that a property holds *with high probability* when it holds with probability  $1 - o(1)$ .

### 2.1 Miscellaneous linear algebra notations

We denote by  $\mathbb{R}^k$  and  $\mathbb{Q}^k$  the  $k$ -dimensional real and rational vector spaces in the canonical basis  $e_1, \dots, e_k$ . The vectors in these spaces are given as sequences  $a = (a_1 \dots a_k)$ . In this context for some  $k$ -dimensional vector space  $V$  and two vectors  $a, b \in V$  by  $\langle a, b \rangle$  we denote the *inner product* of  $a$  and  $b$  which is defined by  $\langle a, b \rangle := \sum_{i=1}^k a_i \cdot b_i$ . Two vectors  $a, b$  are *orthogonal* if  $\langle a, b \rangle = 0$ . The (*Euclidean*) *norm* of a vector  $a$  is denoted by  $\|a\|$  and is defined as  $\sqrt{\sum_{i=1}^k a_i^2}$ . A vector  $a$  is



called *normal* if  $\|a\| = 1$ . A set of vectors is called *orthonormal* if they are pairwise orthogonal and normal. A function  $f : V \rightarrow W$  is *linear* if for all  $v, w \in V$ ,  $f(c_1v + c_2w) = c_1f(v) + c_2f(w)$ . Every linear function  $f : V \rightarrow W$  can be represented by a matrix  $A_f = (a_{i,j})_{i \leq \dim(W), j \leq \dim(V)}$ . Observe that the representation depends not only on  $f$  but also on the bases of  $V$  and  $W$ . A matrix  $A = (a_{i,j})$  is symmetric if  $a_{i,j} = a_{j,i}$  for all  $i, j$ . If for some matrix  $A$  and vector  $v$  it holds that  $Av = \lambda v$  we call  $v$  an *eigenvector* and  $\lambda$  an *eigenvalue* of  $A$ .

**Fact 1 (cf. [24])** *The eigenvectors of any real symmetric matrix  $A : V \rightarrow V$  are an orthogonal basis of  $V$ , and the eigenvalues of  $A$  are all reals numbers.*

## 2.2 Propositional proofs and $TC^0$ -Frege systems

In this section we define the notion of  $TC^0$  formulas. Then we define the propositional proof system  $TC^0$ -Frege as a sequent calculus operating with  $TC^0$  formulas and prove basic properties of it. We will follow the exposition from [13]. The system we give is only one of many possibilities to define such proof systems (see e.g. [9] for a polynomially-equivalent definition).

The class of  $TC^0$  formulas consists basically of unbounded fan-in constant depth formulas with  $\wedge, \vee, \neg$  and threshold gates. Formally, we define:

**Definition 2.3 ( $TC^0$  formula)** *A  $TC^0$  formula is built from*

- (i) *propositional constants  $\perp$  and  $\top$ ,*
- (ii) *propositional variables  $p_i$  for  $i \in \mathbb{N}$ ,*
- (iii) *connectives  $\neg$  and  $\text{Th}_i$ , for  $i \in \mathbb{N}$ .*

*Items (i) and (ii) constitute the atomic formulas.  $TC^0$  formulas are defined inductively from atomic formulas via the connectives:*

- (a) *if  $A$  is a formula, then so is  $\neg A$  and*
- (b) *for  $n > 1$  and  $i \in \mathbb{N}$ , if  $A_1, \dots, A_n$  are formulas, then so is  $\text{Th}_i A_1 \dots A_n$ .*

*The depth of a formula is the maximal nesting of connectives in it and the size of the formula is the total number of connectives in it.*

For the sake of readability we will also use parentheses in our formulas, though they are not necessary. The semantics of the *Threshold Connectives*  $\text{Th}_i$  are as follows.  $\text{Th}_i(A_1, \dots, A_n)$  is true if and only if at least  $i$  of the  $A_k$  are true. Therefore we will abbreviate  $\text{Th}_i(A_1, \dots, A_i)$  as  $\bigwedge_{k \leq i} A_k$  and  $\text{Th}_1(A_1, \dots, A_i)$  as  $\bigvee_{k \leq i} A_k$ . Moreover we let  $\text{Th}_0(A_1, \dots, A_n) = \top$  and  $\text{Th}_i(A_1, \dots, A_n) = \perp$ , for  $i > n$ .

The following is the sequent calculus  $TC^0$ -Frege.

**Definition 2.4 ( $TC^0$ -Frege)** *A  $TC^0$ -Frege proof system is a sequent calculus with the axioms*

$$A \rightarrow A, \quad \perp \rightarrow, \quad \rightarrow \top,$$

*where  $A$  is any  $TC^0$  formula, and the following derivation rules:*

**Weaken-left:** *From the sequent  $\Gamma \rightarrow \Delta$  we may infer the sequent  $\Gamma, A \rightarrow \Delta$ .*

**Weaken-right:** *From the sequent  $\Gamma \rightarrow \Delta$  we may infer the sequent  $\Gamma \rightarrow A, \Delta$ .*

**Exchange-left:** From the sequent  $\Gamma_1, A_1, A_2, \Gamma_2 \longrightarrow \Delta$  we may infer the sequent  $\Gamma_1, A_2, A_1, \Gamma_2 \longrightarrow \Delta$ .

**Exchange-right:** From the sequent  $\Gamma \longrightarrow \Delta_1, A_1, A_2, \Delta_2$  we may infer the sequent  $\Gamma \longrightarrow \Delta_1, A_2, A_1, \Delta_2$ .

**Contract-left:** From the sequent  $\Gamma, A, A \longrightarrow \Delta$  we may infer the sequent  $\Gamma, A \longrightarrow \Delta$ .

**Contract-right:** From the sequent  $\Gamma \longrightarrow A, A, \Delta$  we may infer the sequent  $\Gamma \longrightarrow A, \Delta$ .

**$\neg$ -left:** From the sequent  $\Gamma \longrightarrow A, \Delta$  we may infer the sequent  $\Gamma, \neg A \longrightarrow \Delta$ .

**$\neg$ -right:** From the sequent  $\Gamma, A \longrightarrow \Delta$  we may infer the sequent  $\Gamma \longrightarrow \neg A, \Delta$ .

**All-left:** From the sequent  $A_1, \dots, A_n, \Gamma \longrightarrow \Delta$  we may infer the sequent  $\text{Th}_n A_1 \dots A_n, \Gamma \longrightarrow \Delta$ .

**All-right:** From the sequents  $\Gamma \longrightarrow A_1, \Delta \dots \Gamma \longrightarrow A_n, \Delta$  we may infer the sequent  $\Gamma \longrightarrow \text{Th}_n A_1 \dots A_n, \Delta$ .

**One-left:** From the sequents  $A_1, \Gamma \longrightarrow \Delta \dots A_1, \Gamma \longrightarrow \Delta$  we may infer the sequent  $\text{Th}_1 A_1 \dots A_n, \Gamma \longrightarrow \Delta$ .

**One-right:** From the sequent  $\Gamma \longrightarrow A_1, \dots, A_n, \Delta$  we may infer the sequent  $\Gamma \longrightarrow \text{Th}_1 A_1 \dots A_n, \Delta$ .

**$\text{Th}_i$ -left:** From the sequents  $\text{Th}_i A_2 \dots A_n, \Gamma \longrightarrow \Delta$  and  $\text{Th}_{i-1} A_2 \dots A_n, A_1, \Gamma \longrightarrow \Delta$  we may infer the sequent  $\text{Th}_i A_1 \dots A_n, \Gamma \longrightarrow \Delta$ .

**$\text{Th}_i$ -right:** From the sequents  $\Gamma \longrightarrow \text{Th}_i A_2 \dots A_n, A_1, \Delta$  and  $\Gamma \longrightarrow \text{Th}_{i-1} A_2 \dots A_n, \Delta$  we may infer the sequent  $\Gamma \longrightarrow \text{Th}_i A_1 \dots A_n, \Delta$ .

**Cut:** From the sequents  $\Gamma \longrightarrow A, \Delta$  and  $\Gamma, A \longrightarrow \Delta$  we may infer the sequent  $\Gamma \longrightarrow \Delta$ ,

for arbitrary  $\mathbf{TC}^0$  formulas  $A_i$  and sets  $\Gamma, \Delta$  of  $\mathbf{TC}^0$  formulas. The intended meaning of  $\Gamma \longrightarrow \Delta$  is that the conjunction of the formulas in  $\Gamma$  implies the disjunction of the formulas in  $\Delta$ . formula. A  $\mathbf{TC}^0$ -Frege proof of a formula  $\varphi$  is a sequence of sequents  $\pi = (S_1, \dots, S_k)$  such that  $S_k \longrightarrow \varphi$  and every sequent in it is either an axiom or was derived from previous lines by a derivation rule. The size of the proof  $\pi$  is the total size of all formulas in its sequents. The depth of the proof  $\pi$  is the maximal depth of a formula in its sequents. A  $\mathbf{TC}^0$ -Frege proof of a family of formulas  $\{\varphi_i : i \in \mathbb{N}\}$  is a family of sequences  $\{(S_1^i, \dots, S_{k_i}^i) : i \in \mathbb{N}\}$ , where each  $S_j^i$  is a  $\mathbf{TC}^0$  formula that can be derived from some  $S_k^i$  for  $k < j$  using the above rules, such that  $S_{k_i}^i \longrightarrow \varphi_i$ , and there is a common constant  $c$  bounding the depth of every formula in all the sequences.

**Proposition 2.5** *The proof system  $\mathbf{TC}^0$ -Frege is sound and complete. That is, every formula  $A$  proven in the above way is a tautology and every tautology can be derived by proofs in the above sense.*

**Definition 2.6 (Polynomial simulation; separation)** *Let  $P, Q$  be two propositional proof systems that establish Boolean tautologies (or refute unsatisfiable Boolean formulas, or refute unsatisfiable CNF formulas). We say that  $P$  polynomially simulates  $Q$  if there is a polynomial  $p$  such that for every propositional tautology  $\tau$ , if the minimal  $Q$ -proof of  $\tau$  is of size  $s$  then the minimal  $P$ -proof of  $\tau$  is of size at most  $p(s)$ . If  $P$  does not polynomially simulate  $Q$  or vice versa we say that  $P$  is separated from  $Q$ .*

For a possibly partial  $\{0, 1\}$  assignment  $\vec{a}$  to the propositional variables, we write  $\varphi[\vec{a}]$  to denote the formula  $\varphi$  in which propositional variables are substituted by their values in  $\vec{a}$ . For a proof  $\pi = (\varphi_1, \dots, \varphi_\ell)$  we write  $\pi[\vec{a}]$  to denote  $\pi = (\varphi_1[\vec{a}], \dots, \varphi_\ell[\vec{a}])$ . The system  $\mathbf{TC}^0$ -Frege can efficiently evaluate assignments to some of the variables of formulas in the following sense.

**Claim 2.7** Let  $\varphi(\vec{p}, \vec{q})$  be a propositional formula in variables  $p_1 \dots p_{m_1}$  and  $q_1 \dots q_{m_2}$  and let  $\vec{a} \in \{0, 1\}^{m_1}$ . If  $\mathbf{TC}^0$ -Frege proves  $\varphi(\vec{p}, \vec{q})$  with a proof  $\pi_\varphi$  of length  $n$ , then it also proves  $\varphi(\vec{a}, \vec{q})$  in a proof  $\pi_{\varphi[\vec{a}]}$  of length  $n$ . Additionally, for any formula  $\varphi(\vec{p})$  in variables  $p_1 \dots p_{m_1}$  and an assignment  $\vec{a} \in \{0, 1\}^{m_1}$ ,  $\mathbf{TC}^0$ -Frege has polynomial size proofs of either  $\varphi[\vec{a}]$  or  $\neg\varphi[\vec{a}]$ .

*Proof sketch:* Consider with  $\pi_\varphi$  and substitute each occurrence of  $p_i$  by  $a_i$ . The resulting proof remains correct and proves  $\varphi(\vec{a}, \vec{q})$ , because every  $\mathbf{TC}^0$ -Frege rule application is still correct after the assignment.

The second claim is proved by induction over the complexity of  $\varphi$ . If  $\varphi[\vec{a}]$  is true we can construct a proof by proving the (substitution instances of the) atomic formulas and then proceeding using the appropriate rules of the calculus by the way the formula is built up.

If  $\varphi[\vec{a}]$  is false, then we proceed in the same way as above with  $\neg\varphi[\vec{a}]$  instead of  $\varphi[\vec{a}]$ . ■ Claim

### 3 Theories of bounded arithmetic

In this section we give some of the necessary background from logic. Specifically, we present the theory  $\mathbf{V}^0$  and its extension  $\mathbf{VTC}^0$ , as developed by Cook and Nguyen [13] (see also [32]). These are weak systems of arithmetic, namely, fragments of Peano Arithmetic. The theories are (first-order) two-sorted theories, having a first sort for natural numbers and a second sort for finite sets of numbers (representing bit-strings via their characteristic function). The theory  $\mathbf{V}^0$  corresponds (in a manner made precise) to bounded depth Frege, and  $\mathbf{VTC}^0$  corresponds to  $\mathbf{TC}^0$ -Frege (see Section 3.2.5). The complexity classes  $\mathbf{AC}^0$ ,  $\mathbf{TC}^0$ , and their corresponding function classes  $\mathbf{FAC}^0$  and  $\mathbf{FTC}^0$  are also defined using the two-sorted universe (specifically, the first-ordered sort [numbers] are given to the machines in unary representation and the second-sort as binary strings).

**Definition 3.1 (Language of two-sorted arithmetic  $\mathcal{L}_A^2$ )** The language of two-sorted arithmetic, denoted  $\mathcal{L}_A^2$ , consists of the following relation, function and constant symbols:

$$\{+, \cdot, \leq, 0, 1, |, =_1, =_2, \in\}.$$

We describe the intended meaning of the symbols by considering the standard model  $\mathbb{N}_2$  of two-sorted Peano Arithmetic. It consists of a first-sort universe  $U_1 = \mathbb{N}$  and a second-sort universe  $U_2$  of all finite subsets of  $\mathbb{N}$ . The constants 0 and 1 are interpreted in  $\mathbb{N}_2$  as the appropriate natural numbers zero and one, respectively. The functions  $+$  and  $\cdot$  are the usual addition and multiplication on the universe of natural numbers, respectively. The relation  $\leq$  is the appropriate “less or equal than” relation on the first-sort universe. The function  $|\cdot|$  maps a finite set of numbers to its largest element plus one. The relation  $=_1$  is interpreted as equality between numbers,  $=_2$  is interpreted as equality between finite sets of numbers. The relation  $n \in N$  holds for a number  $n$  and a finite set of numbers  $N$  if and only if  $n$  is an element of  $N$ .

We denote the first-sort (number) variables by lower-case letters  $x, y, z, \dots$ , and the second-sort (string) variables by capital letters  $X, Y, Z, \dots$ . We build formulas in the usual way, using two sorts of quantifiers: number quantifiers and string quantifiers. A number quantifier is said to be *bounded* if it is of the form  $\exists x(x \leq t \wedge \dots)$  or  $\forall x(x \leq t \rightarrow \dots)$ , respectively, for some number term  $t$  that does not contain  $x$ . We abbreviate  $\exists x(x \leq t \wedge \dots)$  and  $\forall x(x \leq t \rightarrow \dots)$  by  $\exists x \leq t$  and  $\forall x \leq t$ , respectively. A string quantifier is said to be *bounded* if it is of the form

$\exists X(|X| \leq t \wedge \dots)$  or  $\forall X(|X| \leq t \rightarrow \dots)$  for some number term  $t$  that does not contain  $X$ . We abbreviate  $\exists X(|X| \leq t \wedge \dots)$  and  $\forall X(|X| \leq t \rightarrow \dots)$  by  $\exists X \leq t$  and  $\forall X \leq t$ , respectively. A formula is in  $\Sigma_0^B$  or  $\Pi_0^B$  if it uses no string quantifiers and all number quantifiers are bounded. A formula is in  $\Sigma_{i+1}^B$  or  $\Pi_{i+1}^B$  if it is of the form  $\exists X_1 \leq t_1 \dots \exists X_m \leq t_m \psi$  or  $\forall X_1 \leq t_1 \dots \forall X_m \leq t_m \psi$ , where  $\psi \in \Pi_i^B$  and  $\psi \in \Sigma_i^B$ , respectively, and  $t_i$  does not contain  $X_i$ , for all  $i = 1, \dots, m$ . We write  $\forall \Sigma_0^B$  to denote the universal closure of  $\Sigma_0^B$ . (i.e., the class of  $\Sigma_0^B$ -formulas that possibly have (not necessarily bounded) universal quantifiers in their front). We usually abbreviate  $t \in T$ , for a number term  $t$  and a string term  $T$ , as  $T(t)$ .

For a language  $\mathcal{L} \supseteq \mathcal{L}_A^2$  we write  $\Sigma_0^B(\mathcal{L})$  to denote  $\Sigma_0^B$  formulas in the language  $\mathcal{L}$ .

As mentioned before a finite set of natural numbers  $N$  represents a finite string  $S_N = S_N^0 \dots S_N^{|N|-1}$  such that  $S_N^i = 1$  if and only if  $i \in N$ . We will abuse notation and identify  $N$  and  $S_N$ .

In the context of a proof in the theory, we write  $n^c$  to mean the term  $\underbrace{n \cdot \dots \cdot n}_c$ .

**The (first-order) two-sorted proof system  $\mathbf{LK}^2$ .** For proving statements in the two-sorted theories we need to specify a proof system to work with (this should not be confused with the propositional proof system we use). We shall work with a standard (two sorted) sequent calculus  $\mathbf{LK}^2$  as defined in [13], section IV.4. This sequent calculus includes the standard logical rules of the sequent calculus for first-order logic  $\mathbf{LK}$  augmented with four rules for introducing second-sort quantifiers. We also have the standard equality axioms (for first- and second-sorts) for the underlying language  $\mathcal{L}_A^2$  (and when we extend the language, we assume we also add the equality axioms for the additional function and relation symbols). It is not essential to know precisely the system  $\mathbf{LK}^2$  since we shall not be completely formal when proving statements in the two-sorted theories.

### 3.1 The theory $\mathbf{V}^0$

The base theory we shall work with is  $\mathbf{V}^0$  and it consists of the following axioms:

<b>Basic 1.</b> $x + 1 \neq 0$	<b>Basic 2.</b> $x + 1 = y + 1 \rightarrow x = y$
<b>Basic 3.</b> $x + 0 = x$	<b>Basic 4.</b> $x + (y + 1) = (x + y) + 1$
<b>Basic 5.</b> $x \cdot 0 = 0$	<b>Basic 6.</b> $x \cdot (y + 1) = (x \cdot y) + x$
<b>Basic 7.</b> $(x \leq y \wedge y \leq x) \rightarrow x = y$	<b>Basic 8.</b> $x \leq x + y$
<b>Basic 9.</b> $0 \leq x$	<b>Basic 10.</b> $x \leq y \vee y \leq x$
<b>Basic 11.</b> $x \leq y \leftrightarrow x < y + 1$	<b>Basic 12.</b> $x \neq 0 \rightarrow \exists y \leq x(y + 1 = x)$
<b>L1.</b> $X(y) \rightarrow y <  X $	<b>L2.</b> $y + 1 =  X  \rightarrow X(y)$
<b>SE.</b> $( X  =  Y  \wedge \forall i \leq  X  (X(i) \leftrightarrow Y(i))) \rightarrow X = Y$	
<b><math>\Sigma_0^B</math>-COMP.</b> $\exists X \leq y \forall z < y (X(z) \leftrightarrow \varphi(z))$ , for all $\varphi \in \Sigma_0^B$ where $X$ does not occur free in $\varphi$ .	

Here, the Axioms **Basic 1** through **Basic 12** are the usual axioms used to define Peano Arithmetic without induction ( $\text{PA}^-$ ), which settle the basic properties of addition, multiplication, ordering, and of the constants 0 and 1. The Axiom **L1** says that the length of a string coding a finite set is an upper bound to the size of its elements. **L2** says that  $|X|$  gives the largest element of  $X$  plus 1. **SE** is the extensionality axiom for strings which states that two strings are equal if they code the same sets. Finally,  $\Sigma_0^B$ -**COMP** is the comprehension axiom scheme for  $\Sigma_0^B$  formulas (it is an axiom for each such formula) and implies the existence of all sets which contain exactly the elements that fulfill any given  $\Sigma_0^B$  property.

When speaking about theories we will always assume that the theories are two-sorted theories.

**Proposition 3.2 (Corollary V.1.8. [13])** *The theory  $\mathbf{V}^0$  proves the (number) induction axiom scheme for  $\Sigma_0^B$  formulas  $\Phi$ :*

$$(\Phi(0) \wedge \forall x (\Phi(x) \rightarrow \Phi(x + 1))) \rightarrow \forall z \Phi(z).$$

In the above induction axiom,  $x$  is a number variable and  $\Phi$  can have free variables of both sorts.

The following is a basic notion needed to extend our language we new function symbols (we write  $\exists!y\Phi$  to denote  $\exists x(\Phi(x) \wedge \forall y(\Phi(y/x) \rightarrow x = y))$ , where  $y$  is a new variable not appearing in  $\Phi$ ):

**Definition 3.3 (Two-sorted definability)** *Let  $\mathcal{T}$  be a theory over the language  $\mathcal{L} \supseteq \mathcal{L}_A^2$  and let  $\Phi$  be a set of formulas in the language  $\mathcal{L}$ . A number function  $f$  is  $\Phi$ -definable in a theory  $\mathcal{T}$  iff there is a formula  $\varphi(\vec{x}, y, \vec{X})$  in  $\Phi$  such that  $\mathcal{T}$  proves*

$$\forall \vec{x} \forall \vec{X} \exists! y \varphi(\vec{x}, y, \vec{X})$$

and it holds that<sup>2</sup>

$$y = f(\vec{x}, \vec{X}) \leftrightarrow \varphi(\vec{x}, y, \vec{X}). \quad (3)$$

A string function  $F$  is  $\Phi$ -definable in a theory  $\mathcal{T}$  iff there is a formula  $\varphi(\vec{x}, \vec{X}, Y)$  in  $\Phi$  such that  $\mathcal{T}$  proves

$$\forall \vec{x} \forall \vec{X} \exists! Y \varphi(\vec{x}, \vec{X}, Y)$$

and it holds that

$$Y = F(\vec{x}, \vec{X}) \leftrightarrow \varphi(\vec{x}, \vec{X}, Y). \quad (4)$$

Finally, a relation  $R(\vec{x}, \vec{X})$  is  $\Phi$ -definable in a theory  $\mathcal{T}$  iff there is a formula  $\varphi(\vec{x}, \vec{X}, Y)$  in  $\Phi$  such that it holds that

$$R(\vec{x}, \vec{X}) \leftrightarrow \varphi(\vec{x}, \vec{X}). \quad (5)$$

The formulas (3), (4), and (6) are the defining axioms for  $f$ ,  $F$ , and  $R$ , respectively.

**Definition 3.4 (Conservative extension of a theory)** *Let  $\mathcal{T}$  be a theory in the language  $\mathcal{L}$ . We say that a theory  $\mathcal{T}' \supseteq \mathcal{T}$  in the language  $\mathcal{L}' \supseteq \mathcal{L}$  is conservative over  $\mathcal{T}$  if every  $\mathcal{L}$  formula provable in  $\mathcal{T}'$  is also provable in  $\mathcal{T}$ .*

---

<sup>2</sup>Meaning it holds in the standard two-sorted model  $\mathbb{N}_2$ .

We can expand the language  $\mathcal{L}$  and a theory  $\mathcal{T}$  over the language  $\mathcal{L}$  by adding symbols for arbitrary functions  $f$  (or relations  $R$ ) to  $\mathcal{L}$  and their defining axioms  $A_f$  (or  $A_R$ ) to the theory  $\mathcal{T}$ . If the appropriate functions are definable in  $\mathcal{T}$  (according to Definition 3.3) then the theory  $\mathcal{T} + A_f$  ( $+A_R$ ) is conservative over  $\mathcal{T}$ . This enables one to add new function and relation symbols to the language while proving statement inside a theory; as long as these function and relation symbols are definable in the theory, every statement in the original language proved in the extended theory (with the additional defining-axioms for the functions and relations) is provable in the original theory over the original language. *However*, extending the language and the theory in such a way *does not guarantee* that one can use the new function symbols in the comprehension (and induction) axiom schemes. In other words, using the comprehension (and induction) axioms over the expanded language might not result in a conservative extension. Therefore, definability will not be enough for our purposes. We will show precisely in the sequel (Sections 3.1.2 and 3.2) how to make sure that a function is both definable in the theories we work with and also can be used in the corresponding comprehension and induction axiom schemes (while preserving conservativity).

When expanding the language with new function symbols we can assume that in *bounded formulas* the bounding terms possibly use function symbols from the the expanded language<sup>3</sup>.

### 3.1.1 Extending $\mathbf{V}^0$ with new function and relation symbols

Here we describe a process (presented in Section V.4. in [13]) by which we can extend the language  $\mathcal{L}_A^2$  of  $\mathbf{V}^0$  by new function symbols, obtaining a conservative extension of  $\mathbf{V}^0$  that can also prove the comprehension and induction axiom schemes in the extended language.

First note that every relation or function symbol has an intended or standard interpretation over the standard model  $\mathbb{N}_2$  (for instance, the standard interpretation of the binary function “+” is that of the addition of two natural numbers). If not explicitly defined otherwise, we will always assume that a defining axiom of a symbol in the language defines a symbol in a way that its interpretation in  $\mathbb{N}_2$  is the standard one. Note also that we shall use the same symbol  $F(\vec{x}, \vec{X})$  to denote a function and the function *symbol* in the (extended) language in the theory.

**Definition 3.5 (Relation representable in a language)** *Let  $\Phi$  be a set of formulas in a language  $\mathcal{L}$  extending  $\mathcal{L}_A^2$ . We say a relation  $R(\vec{x}, \vec{X})$  is representable by a formula from  $\Phi$  iff there is a formula  $\varphi(\vec{x}, \vec{X}, Y)$  in  $\Phi$  such that in the standard two-sorted model  $\mathbb{N}_2$  (and when all relation and function symbols in  $\mathcal{L}$  get their intended interpretation), it holds that:*

$$R(\vec{x}, \vec{X}) \leftrightarrow \varphi(\vec{x}, \vec{X}). \quad (6)$$

We say that a number function  $f(\vec{x}, \vec{X})$  is *polynomially-bounded* if  $f(\vec{x}, \vec{X}) \leq \text{poly}(\vec{x}, \vec{X})$ . We say that a string function  $F(\vec{x}, \vec{X})$  is *polynomially-bounded* if  $|F(\vec{x}, \vec{X})| \leq \text{poly}(\vec{x}, \vec{X})$ .

**Definition 3.6 (Bit-definition)** *Let  $F(\vec{x}, \vec{X})$  be a polynomially-bounded string function. We define the bit-graph of  $F$  to be the relation  $R(i, \vec{x}, \vec{X})$ , where  $i$  is a number variable, such that*

$$F(\vec{x}, \vec{X})(i) \leftrightarrow i < t(\vec{x}, \vec{X}) \wedge R(i, \vec{x}, \vec{X}),$$

for some number term  $t(\vec{x}, \vec{X})$ .

---

<sup>3</sup>Because any definable function in a bounded theory can be bounded by a term in the original language  $\mathcal{L}_A^2$  (cf. [13]).



**Definition 3.7** ( $\Sigma_0^B$ -definability from a language; Definition V.4.1.2. in [13]) *We say that a number function  $f$  is  $\Sigma_0^B$ -definable from a language  $\mathcal{L} \supseteq \mathcal{L}_A^2$ , if  $f$  is polynomially-bounded and its graph is represented by a  $\Sigma_0^B(\mathcal{L})$  formula  $\varphi$ . We call the formula  $\varphi$  the defining axiom of  $f$ . We say that a string function  $F$  is  $\Sigma_0^B$ -definable from a language  $\mathcal{L} \supseteq \mathcal{L}_A^2$ , if  $F$  is polynomially-bounded and its bit-graph is representable by a  $\Sigma_0^B(\mathcal{L})$  formula  $\varphi$ . We call the formula  $\varphi$  the defining axiom of  $F$  or the bit-defining axiom of  $F$ .*

**Note:** We used the term *defining axiom of a function  $f$*  in both the case where  $f$  is defined from a language (Definition 3.7) and in case  $f$  is definable in the theory (Definition 3.3). We will show in the sequel that for our purposes these two notions coincide: when we define a function from a language the function will be definable also in the relevant theory, and so the defining axiom of  $f$  from the language will be the defining axiom of  $f$  in the theory (when the theory is possibly extended conservatively to include new function symbols).

Also, note that if the graph of a function  $F$  is representable by a  $\Sigma_0^B(\mathcal{L})$  formula then clearly also the bit-graph of  $F$  is representable by a  $\Sigma_0^B(\mathcal{L})$  formula. Therefore, *it suffices to show a  $\Sigma_0^B(\mathcal{L})$  formula representing the graph of a function  $F$  to establish that  $F$  is  $\Sigma_0^B$ -definable from  $\mathcal{L}$ .*

**Definition 3.8 (AC<sup>0</sup>-reduction)** *A number function  $f$  is AC<sup>0</sup>-reducible to  $\mathcal{L} \supseteq \mathcal{L}_A^2$  iff there is a possibly empty sequence of functions  $F_1, \dots, F_k$  such that  $F_i$  is  $\Sigma_0^B$ -definable from  $\mathcal{L} \cup \{F_1, \dots, F_{i-1}\}$ , for any  $i = 1, \dots, k$ , and  $f$  is  $\Sigma_0^B$ -definable from  $\mathcal{L} \cup \{F_1, \dots, F_k\}$ .*

We now describe the standard process enabling one to extend a theory  $\mathcal{T} \supseteq \mathbf{V}^0$  over the language  $\mathcal{L}_A^2$  with new function symbols obtaining a conservative extension of  $\mathcal{T}$  such that the new function symbols can also be used in comprehension and induction axiom schemes in the theory (see Section V.4. in [13] for the proofs):

- (i) If the number function  $f$  is  $\Sigma_0^B$ -definable from  $\mathcal{L}_A^2$ , then  $\mathcal{T}$  over the language  $\mathcal{L}_A^2 \cup \{f\}$ , augmented with the defining axiom of  $f$ , is a conservative extension of  $\mathcal{T}$  and we can also prove the comprehension and induction axioms for  $\Sigma_0^B(f)$  formulas.
- (ii) If the string function  $F$  is  $\Sigma_0^B$ -definable from  $\mathcal{L}_A^2$ , then  $\mathcal{T}$  over the language  $\mathcal{L}_A^2 \cup \{F\}$ , augmented with the bit-defining axiom of  $F$ , is a conservative extension of  $\mathcal{T}$  and we can also prove the comprehension and induction axioms for  $\Sigma_0^B(F)$  formulas.
- (iii) We can now iterate the above process of extending the language  $\mathcal{L}_A^2(f)$  (or equivalently,  $\mathcal{L}_A^2(F)$ ) to conservatively add more functions  $f_2, f_3, \dots$  to the language, which can also be used in comprehension and induction axioms.

By the aforementioned and by Definition 3.8, we can extend the language of a theory with a new function symbol  $f$ , *whenever  $f$  is AC<sup>0</sup>-reducible to  $\mathcal{L}_A^2$* . This results in an extended theory (in an extended language) which is conservative, and can prove the comprehension and induction axioms for formulas in the extended language. In the sequel, when defining a new function in  $\mathbf{V}^0$  we may simply say that it is  $\Sigma_0^B$ -definable (or bit-definable) in  $\mathbf{V}^0$  and give its  $\Sigma_0^B$ -defining (bit-defining, respectively) axiom (that can possibly use also previously  $\Sigma_0^B$ -defined (or bit defined) function symbols).

Extending the language of  $\mathbf{V}^0$  with new *relation* symbols is simple: every relation  $R(\vec{x}, \vec{X})$  which is representable by a  $\Sigma_0^B(\mathcal{L})$  formula, where  $\mathcal{L}$  is an extension of the language with new

function symbols obtained as shown above, can be added itself to the language. This results in a conservative extension of  $\mathbf{V}^0$  that also proves the  $\Sigma_0^B$  induction and comprehension axioms in the extended language.

**Definition 3.9 (FAC<sup>0</sup>)** *A string (number) function is in FAC<sup>0</sup> if it is polynomially-bounded and its bit-graph (graph, respectively) is definable by a  $\Sigma_0^B$  formula in the language  $\mathcal{L}_A^2$ .*

### 3.1.2 Basic formalizations in $\mathbf{V}^0$

In this section we show how to formalize basic notions in the theory  $\mathbf{V}^0$ .

**Characteristic function of a relation.** For a given predicate  $R$  we denote by  $\chi_R$  the *characteristic function* of  $R$ . If  $R$  is  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$  then  $\chi_R$  is  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$ , using the following defining axiom:

$$y = \chi_R(\vec{x}, \vec{X}) \leftrightarrow \left( R(\vec{x}, \vec{X}) \rightarrow y = 1 \wedge \neg R(\vec{x}, \vec{X}) \rightarrow y = 0 \right).$$

**Natural number sequences of constant length.** For two numbers  $x, y$  let  $\langle x, y \rangle := (x + y)(x + y + 1) + 2y$  be the *pairing function*, and let  $left(z), right(z)$  be the (easily  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$ ) projection functions of the first and second element in the pair  $z$ , respectively. It should be clear from the context when we mean  $\langle a, b \rangle$  as an inner product of two vectors and when we mean it as the pairing function. We also  $\Sigma_0^B$ -define inductively  $\langle v_1, \dots, v_k \rangle := \langle \langle v_1, \dots, v_{k-1} \rangle, v_k \rangle$ , for any constant  $k$ . Then  $\mathbf{V}^0$  proves the injectivity of the pairing function and lets us handle such pairs in a standard way.

**Notation:** Given a number  $x$ , coding a sequence of natural numbers of length  $k$ , we write  $\langle x \rangle_i^k$ , for  $i = 1, \dots, k$ , to denote the number in the  $i$ th position in  $x$ . This is a  $\Sigma_0^B$ -definable function in  $\mathbf{V}^0$  (defined via  $left(x), right(x)$  functions).

**Rational numbers.** Given the natural numbers, we can define the integers in  $\mathbf{V}^0$  by identifying an integer number with a pair  $\langle a, b \rangle$ , such that  $a$  is its “positive” part and  $b$  is its “negative” part. We can define addition, product and subtraction of integers. All with  $\Sigma_0^B$  definitions.

Having the integer numbers, we define the rational numbers as follows: for two integer numbers  $a, b$ , the rational number  $a/b$ , is defined by the pair  $\langle a, b \rangle$ . We can define addition, subtraction and multiplication of rational numbers in  $\mathbf{V}^0$  by  $\Sigma_0^B$  definitions. (See for example in [27]). However, we shall take a simpler path in this paper: ***throughout this paper, all rational numbers used inside the theories have the same denominator  $n^{2c}$ , for some fixed constant  $c$ .*** This enables us to represent every rational number with a pair of integer numbers, such that each has a value polynomial in  $n$ . Addition and multiplication of two rational numbers is also  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$ . This also makes it more convenient to sum a non-constant number of rational numbers in  $\mathbf{VTC}^0$  (see Proposition 3.16). To keep the invariant that all denominators are  $n^{2c}$ , we then make sure that all the rational numbers resulting from computation in the proof in the theory are indeed integer products of  $1/n^{2c}$ . This will hold since by inspection of the computations made in the theory it will be clear that:

1. all initial rational numbers will be integer products of  $1/n^c$ ;

2. all arithmetic operations done on rational numbers are one of the following:

- (a) addition of two rational numbers (this preserves the denominator);
- (b) if we multiply two rational numbers  $x, y$  then  $x = \frac{n^c \cdot a}{n^{2c}}$  and  $y = \frac{n^c \cdot b}{n^{2c}}$  for some two integers  $a, b$ , and so  $x \cdot y = \frac{ab}{n^{2c}}$  will have  $n^{2c}$  as a denominator.

**Convention:** For the sake of readability we sometimes treat integer numbers in the theory  $m$  as their corresponding rational number  $m/1$ , thus enabling one to compute with both types. (This is simple to achieve formally. E.g., one can define a function  $numones'(X)$  that outputs the corresponding rational number of  $numones(X)$ .)

**Absolute numbers.** We can  $\Sigma_0^B$ -define in  $\mathbf{V}^0$  the absolute value function for integer numbers  $abs_{\mathbb{Z}}(\cdot)$  from the language  $\mathcal{L}_A^2$  as follows (the function  $\max$  is easily  $\Sigma_0^B$ -definable):

$$y = abs_{\mathbb{Z}}(x) \leftrightarrow y = \langle \max(\text{left}(x) - \text{right}(x), \text{right}(x) - \text{left}(x)), 0 \rangle.$$

We  $\Sigma_0^B$ -define the absolute value function for rational numbers  $abs_{\mathbb{Q}}(\cdot)$  in  $\mathbf{V}^0$  as follows:

$$y = abs_{\mathbb{Q}}(x) \leftrightarrow y = \langle abs_{\mathbb{Z}}(\text{left}(x)), \langle n^{2c}, 0 \rangle \rangle.$$

For simplicity, we shall suppress the subscript  $\mathbb{Z}, \mathbb{Q}$  in  $abs_{\mathbb{Z}}, abs_{\mathbb{Q}}$ ; the choice of function can be determined from the context.

**Number (natural, integers and rational) sequences of polynomial length.** If we wish to talk about sequences of numbers (whether natural, integers or rationals) where the lengths of the sequences are non-constant, we have to use string variables. Using the number tupling function we can encode sequences as sets of numbers (recall that a string is identified with the finite set of numbers encoding it). Essentially, a sequence is encoded as a string  $Z$  such that the  $x$ th number in the sequence is  $y$  if the number  $\langle x, y \rangle$  is in  $Z$ . Formally we have the following  $\Sigma_0^B$ -defining formula for the function  $seq(x, Z)$ :

$$\begin{aligned} y = seq(x, Z) \leftrightarrow & (y < |Z| \wedge Z(\langle x, y \rangle) \wedge \forall z < y \neg Z(\langle x, z \rangle)) \\ & \vee (\forall z < |Z| \neg Z(\langle x, z \rangle) \wedge y = |Z|). \end{aligned} \tag{7}$$

Formula (7) states that the  $x$ th element in the sequence coded by  $Z$  is  $y$  iff  $\langle x, y \rangle$  is in  $Z$  and no other number smaller than  $y$  also ‘‘occupies the  $x$ th position in the sequence’’, and that if no number occupies position  $x$  then the function returns the length of the string variable  $Z$ . We write  $Z[x]$  to abbreviate  $seq(x, Z)$ .

According to the definition of the function  $seq(x, Z)$  above, there might be more than one string  $Z$  that encodes the same sequence of numbers. However, we sometimes need to determine a *unique* string encoding a sequence. To this end we use a  $\Sigma_0^B$  formula, denoted  $SEQ(y, Z)$ , which asserts that  $Z$  is the lexicographically smallest string that encodes a sequence of  $y + 1$  numbers (i.e., no string with smaller binary code encodes the same sequence). Specifically, the formula states that if  $w = \langle i, j \rangle$  is in  $Z$  then  $j$  is indeed the  $i$ th element in the sequence coded by  $Z$ , and for all  $y \geq j$  the pair  $\langle i, y \rangle$  is not contained in  $Z$ :

$$SEQ(y, Z) \equiv \forall w < |Z| (Z(w) \leftrightarrow \exists i \leq y \exists j < |Z| (w = \langle i, j \rangle \wedge j = Z[i])). \quad (8)$$

Note that elements of sequences  $Z$  coded by strings are referred to as  $Z[i]$ , while elements of sequences  $x$  coded by a number are referred to as  $\langle x \rangle_i^k$  (for  $k$  the length of the sequence  $x$ ). We define the number function  $length(Z)$  to be the length of the sequence  $Z$ , as follows:

$$\ell = length(Z) \leftrightarrow SEQ(\ell, Z) \wedge \exists w < |Z| \exists j < |Z| (Z(w) \wedge w = \langle \ell - 1, j \rangle).$$

The defining axiom of  $length(Z)$  states that  $Z$  encodes a sequence and is the lexicographically smallest string that encodes this sequence and that the largest position in the sequence which is occupied is  $\ell - 1$  (by definition there will be no pair  $\langle a, b \rangle \in Z$  with  $a > \ell - 1$ ).

**Array of strings.** We want to encode a sequence of strings as an array. We use the relation  $RowArray(x, Z)$  to denote the  $x$ th string in  $Z$  as follows (we follow the treatment in [13], Definition V.4.26, page 114).

**Definition 3.10 (Array of strings)** *The function  $RowArray(x, Z)$ , denoted  $Z^{[x]}$ , is  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$  using the following bit-definition.<sup>4</sup>*

$$RowArray(x, Z)(i) \leftrightarrow (i < |Z| \wedge Z(\langle x, i \rangle)).$$

We will abuse notation and write  $length(Z)$  for the length of the array  $Z$  (i.e., numbers of strings in  $Z$ ) even when  $Z$  is a  $RowArray$  (and not a sequence according to the predicate  $SEQ$ ).

### Functions for constructing sequences.

**Definition 3.11 ( $Sequence_f(y, \vec{x}, \vec{X})$ )** *Let  $f(z, \vec{x}, \vec{X})$  be a  $\Sigma_0^B$ -definable number function in  $\mathbf{V}^0$  (or a  $\Sigma_1^B$ -definable number function in  $\mathbf{VTC}^0$  [see section 3.2 below]), then  $Sequence_f(y, \vec{x}, \vec{X})$  is the string function  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$  (or  $\Sigma_1^B$ -definable in  $\mathbf{VTC}^0$ , respectively) that returns the number sequence whose  $j$ th position is  $f(j, \vec{x}, \vec{X})$ , for  $j = 0, \dots, y$ .*

In other words,  $Sequence_f(y, \vec{x}, \vec{X})$  returns the graph of the function  $f(z, \vec{x}, \vec{X})$  up to  $y$  (that is, the sequence  $\langle f(0, \vec{x}, \vec{X}), \dots, f(y, \vec{x}, \vec{X}) \rangle$ ). The following is the  $\Sigma_0^B$ -definition of the  $Sequence_f(y, \vec{x}, \vec{X})$ :

$$Y = Sequence_f(y, \vec{x}, \vec{X}) \leftrightarrow SEQ(y, Y) \wedge \forall z \leq y (Y[z] = f(z, \vec{x}, \vec{X})).$$

**Sequences of numbers with higher-dimensions.** For a constant  $k$ , let  $S$  be a  $k$ -dimensional sequence of rational numbers. We encode a sequence  $S$  as a string variable  $Z$  such that the  $\langle i_1, \dots, i_k \rangle$ th element in  $S$  is extracted by the function  $seq$  (defined above). Specifically, we have  $S[\langle i_1, \dots, i_k \rangle] = y$  iff  $\langle \langle i_1, \dots, i_k \rangle, y \rangle \in Z$  and there is no  $z < y$  for which  $\langle \langle i_1, \dots, i_k \rangle, z \rangle \in Z$ . Accordingly, we write  $Z[\langle i_1, \dots, i_k \rangle]$  to abbreviate  $seq(\langle i_1, \dots, i_k \rangle, Z)$ .

<sup>4</sup>We use the name “RowArray” (instead of the name “Row” used in [13]).

**Matrices.** Given a rational  $n \times n$  matrix  $M$ , we define it as a two-dimensional sequence in the manner defined above; and refer to the number at row  $1 \leq i \leq n$  and column  $1 \leq j \leq n$  of  $M$  as  $M[i, j]$ . We can define the *string* function that extracts the  $x$ th row of  $M$ , and the  $x$ th column of  $M$ , respectively, with  $\Sigma_0^B$  formulas as follows. First define  $f(M, i, x) := M[i, x]$ ,  $g(M, i, x) := M[x, i]$ , for any  $i = 0, 1, \dots, n$  (for  $i = 0$ , the value of  $M[i, x]$  and  $M[x, i]$  does not matter; but this value is still defined by definition of the function *seq*). Then use Definition 3.11 to define:

$$\begin{aligned} \text{Row}(i, M) &:= \text{Sequence}_f(i, n) \\ \text{Column}(i, M) &:= \text{Sequence}_g(i, n). \end{aligned}$$

### 3.2 The theory $VTC^0$

It is known that  $\mathbf{V}^0$  is incapable of proving basic counting statements. Specifically, it is known that the function that sums a sequence of numbers (of non-constant length) is not provably total, namely, is not  $\Sigma_1^B$ -definable in  $\mathbf{V}^0$ . Therefore, if a proof involves such computations we might not be able to perform it in  $\mathbf{V}^0$ . The theory  $VTC^0$  extends  $\mathbf{V}^0$ , and is meant to allow reasoning that involves counting, and specifically to sum a non-constant sequence of numbers. The theory  $VTC^0$  was introduced in [28]; we refer the reader to Section IX.3.2 [13] for a full treatment of this theory. The  $\Sigma_0^B$  theorems of  $VTC^0$  correspond to polynomial-size  $TC^0$ -Frege propositional proofs, which will enable us to prove the main result of this paper.

**Definition 3.12 (NUMONES)** Let  $\delta_{\text{NUM}}(y, X, Z)$  be the following  $\Sigma_0^B$  formula:

$$\begin{aligned} \delta_{\text{NUM}}(y, X, Z) &:= \text{SEQ}(y, Z) \wedge Z[0] = 0 \wedge \forall u < y ((X(u) \rightarrow Z[u+1] = Z[u] + 1) \\ &\quad \wedge (\neg X(u) \rightarrow Z[u+1] = Z[u])). \end{aligned} \tag{9}$$

Define NUMONES to be the following  $\Sigma_1^B$  formula:

$$\text{NUMONES} := \exists Z \leq 1 + \langle y, y \rangle \delta_{\text{NUM}}(y, X, Z). \tag{10}$$

Informally one can think of the sequence  $Z(X)$ , which existence is guaranteed by NUMONES, as a sequence counting the number of ones in a string  $X$ , that is, the  $u$ th entry in  $Z(X)$  is the number of ones appearing in the string  $X$  up to the  $u$ th position.

**Definition 3.13 ( $VTC^0$ )** The theory  $VTC^0$  is the theory containing all axioms of  $\mathbf{V}^0$  and the axiom NUMONES.

Using NUMONES we can define the function  $\text{numones}(y, X)$  that, given  $y$  and  $X$ , returns the  $y$ th entry of  $Z(X)$  via the following  $\Sigma_1^B$ -defining axiom

$$\text{numones}(y, X) = z \leftrightarrow \exists Z \leq 1 + \langle |X|, |X| \rangle (\delta_{\text{NUM}}(|X|, X, Z) \wedge Z[y] = z). \tag{11}$$

We shall use the following abbreviation:

$$\text{numones}(X) := \text{numones}(|X| - 1, X).$$

Next we show how to obtain the functions we will use in the theory  $VTC^0$  (these will include the function  $\text{numones}$ ).

### 3.2.1 Extending $VTC^0$ with new function and relation symbols

Similar to the case of  $V^0$ , we would like to extend the language  $\mathcal{L}_A^2$  of  $VTC^0$  with new function and relation symbols, to obtain a conservative extension. Moreover, we require that the new function and relation symbols could be used in induction and comprehension axioms (while preserving conservativity). We can do this, using results from Sections I.X.3.2 and I.X.3.3 in [13], as follows.

**Definition 3.14 (Number summation)** *For any number function  $f(z, \vec{x}, \vec{X})$  define the number function  $\text{sum}_f(y, \vec{x}, \vec{X})$  by<sup>5</sup>*

$$\text{sum}_f(y, \vec{x}, \vec{X}) = \sum_{i=0}^y f(i, \vec{x}, \vec{X}).$$

Recall that by Definition 3.7, a string (number) function  $F$  is  $\Sigma_0^B$ -definable from  $\mathcal{L} \supseteq \mathcal{L}_A^2$  iff there is a  $\Sigma_0^B$  formula over the language  $\mathcal{L}$  that bit-defines (defines, respectively) the function  $F$  (when all the functions and relation symbols in  $\mathcal{L}$  get their intended interpretation).

We can use the following facts to extend the language of  $VTC^0$  with new function symbols (proved in Section IX.3.2 in [13]): if  $f$  is a (number or string) function in  $\mathbf{FTC}^0$  (see below), then there is a  $\Sigma_1^B$  formula  $\varphi$  that represents its graph, and the theory  $VTC^0$  extended with the defining axiom for  $f$  (using  $\varphi$ , as in Definition 3.7) over the language  $\mathcal{L} = \mathcal{L}_A^2 \cup \{f\}$  is a conservative extension of  $VTC^0$ . And by Theorem IX.3.7 in Section IX.3.2 [13],  $VTC^0$  can prove the induction and comprehension axioms for any  $\Sigma_0^B(\mathcal{L})$  formula.

Thus, to extend  $VTC^0$  with new *function* symbols, by the above it suffices to show how to obtain  $\mathbf{FTC}^0$  functions. For this we use the following equivalent characterizations of  $\mathbf{FTC}^0$  (see Sections IX.3.2 and IX.3.3 in [13]):

**Proposition 3.15 (Theorem IX.3.12, Proposition IX.3.1 in [13])** *The following statements are equivalent:*

1. *The function  $f$  is  $\Sigma_1^B$ -definable in  $VTC^0$ , and is applicable inside comprehension and induction axiom schemes.*
2. *The function  $f$  is in  $\mathbf{FTC}^0$ .*
3. *The function  $f$  is obtained from  $\mathbf{FAC}^0$  by number summation and  $\mathbf{AC}^0$ -reductions.*
4. *There exist a natural  $k$  and functions  $f_1, \dots, f_k = f$  such that for every  $i = 1, \dots, k$ , the function  $f_i$  is either definable by a  $\Sigma_0^B$  formula in the language  $\mathcal{L}_A^2 \cup \{f_1, \dots, f_{i-1}\}$  or there exists  $h \in \mathcal{L}_A^2 \cup \{f_1, \dots, f_{i-1}\}$  such that  $f_i = \text{sum}_h$ .*
5. *The function  $f$  is  $\mathbf{AC}^0$ -reducible to  $\mathcal{L}_A^2 \cup \{\text{numones}\}$ .*

Therefore, to obtain new  $\mathbf{FTC}^0$  functions, and hence to extend conservatively the language of  $VTC^0$  with function symbols that can also be used in comprehension and induction axioms, we can define a function with a  $\Sigma_0^B$  formula in a language that contains  $\text{sum}_f$ , for  $f$  in  $\mathbf{FAC}^0$ , and possibly contains also other symbols already definable in  $V^0$ . Then, we can iterate this process a finite number of times, where now  $\text{sum}_f$  is defined also for  $f$  being a function defined in a previous

---

<sup>5</sup>Note that this is a definition in the metatheory (or in other words the standard two-sorted model).



iteration. Since a function is in  $\mathbf{FTC}^0$  iff it is  $\Sigma_1^B$ -definable in  $\mathbf{VTC}^0$ , new functions obtained in this way, are said to be  $\Sigma_1^B$ -definable in  $\mathbf{VTC}^0$ .

To extend the language of  $\mathbf{VTC}^0$  with new *relation* symbols, we can simply add new  $\Sigma_0^B$ -definable relations, using possibly relation and function symbols that were already added before to the language, and specifically the *numones* function. Such relations can then be used in induction and comprehension axioms, and we shall say that they are  $\Sigma_0^B$ -definable relations in  $\mathbf{VTC}^0$ .

### 3.2.2 Summation in $\mathbf{VTC}^0$

Here we show how to express and prove basic equalities and inequalities in the theory  $\mathbf{VTC}^0$ .

**Summation over natural and rational number sequences.** Given a sequence  $X$  of *natural* numbers, we define the function that sums the numbers in  $X$  until the  $y$ th position by  $\text{sum}_{\text{seq}}(y, X)$  which is equal to  $\sum_{i=0}^y \text{seq}(i, X)$ .

To sum sequences of *rational* numbers, on the other hand, we do the following. For our purposes it is sufficient to sum many small (that is, polynomially bounded) numbers (this is in contrast to additions of numbers encoded as *strings*). Recall that we assume that all rational numbers in the theory have the same denominator  $n^{2c}$ , for some global constant  $c$ , independent of  $n$ .

**Proposition 3.16** *Let  $X$  be a sequence of rational numbers with denominator  $n^{2c}$  and let  $\text{sum}_{\mathbb{Q}}(z, X)$  be the number function that outputs  $\sum_{i=0}^z X[i]$ . Then, the number function  $\text{sum}_{\mathbb{Q}}(z, X)$  is  $\Sigma_1^B$ -definable in  $\mathbf{VTC}^0$ .*

**Proof:** It suffices to show that there is a  $\Sigma_0^B$  formula that defines the number function  $\text{sum}_{\mathbb{Q}}(z, X)$  using only number summation functions and  $\mathbf{FAC}^0$  functions.

The  $\mathbf{AC}^0$  function  $\text{seq}(i, X)$  extracts the  $i$ th element (that is, rational number) from the sequence  $X$  (see Formula (7)). A rational number is a pair of integers, and hence is a pair of pairs. Thus,  $\text{gp}(i, X) := \text{left}(\text{left}(\text{seq}(i, X)))$  extracts the positive part of the integer numerator of the  $i$ th rational number in  $X$ , and  $\text{gn}(i, X) := \text{right}(\text{left}(\text{seq}(i, X)))$  extracts the negative part of the integer numerator of the  $i$ th rational number in  $X$ . Note that both  $\text{gp}(i, X)$  and  $\text{gn}(i, X)$  are  $\mathbf{FAC}^0$  functions. Therefore,  $\text{sum}_{\text{gp}}(z, X)$  equals the sum of all the positive parts in  $X$ , and  $\text{sum}_{\text{gn}}(z, X)$  equals the function that sums of all the negative parts of the numerators in  $X$ . We can now define  $\text{sum}_{\mathbb{Q}}(z, X)$  as follows:

$$w = \text{sum}_{\mathbb{Q}}(z, X) \leftrightarrow w = \langle \langle \text{sum}_{\text{gp}}(z, X), \text{sum}_{\text{gn}}(z, X) \rangle, \langle n^{2c}, 0 \rangle \rangle \quad (12)$$

Note indeed that  $\langle \langle \text{sum}_{\text{gp}}(z, X), \text{sum}_{\text{gn}}(z, X) \rangle, \langle n^{2c}, 0 \rangle \rangle$  is a pair of integers that encodes the desired rational number (with denominator  $n^{2c}$ ).  $\blacksquare$

**Notation:** As a corollary from Proposition 3.16, we can abuse notation as follows: for  $f(y, \vec{x}, \vec{X})$  a number function mapping to the rationals we write  $\text{sum}_f(n, \vec{x}, \vec{X})$  to denote the sum of *rationals*  $\sum_{i=0}^n f(i, \vec{x}, \vec{X})$ , for some fixed  $\vec{x}, \vec{X}$  and  $n$ . Abusing notation further, we can write in a formula in the theory simply  $\sum_{i=0}^n f(i, \vec{x}, \vec{X})$ .

**Expressing vectors and operations on vectors.** Vectors over  $\mathbb{Q}$  are defined as sequences of rational numbers (for simplicity we shall assume that the number at the 0 position of a vector is 0). Given two rational vectors  $\mathbf{v}, \mathbf{u}$  of size  $n$ , their inner product, denoted  $\langle \mathbf{v}, \mathbf{u} \rangle$ , is defined as follows (we identify here  $\mathbf{v}, \mathbf{u}$  with the string variables encoding  $\mathbf{v}, \mathbf{u}$ ): let  $f(y, \mathbf{v}, \mathbf{u})$  be the  $\mathbf{FAC}^0$  number function defined by  $f(y) := \mathbf{v}[y] \cdot \mathbf{u}[y]$ . Then the inner product of  $\mathbf{v}$  and  $\mathbf{u}$  is defined by

$$\text{innerprod}(\mathbf{v}, \mathbf{u}) := \text{sum}_{\mathbb{Q}} (\text{length}(\mathbf{v}) + 1, \text{Sequence}_f(\text{length}(\mathbf{v}) + 1)).$$

The function that adds two rational vectors is easily seen to be in  $\mathbf{FAC}^0$  (use Definition 3.11 to construct a sequence, where each entry in the sequence is the addition of the corresponding entries of the two vectors).

**Expressing product of matrices and vectors.** Let  $\mathbf{v}$  be an  $n$ -dimensional rational vector and let  $M$  be an  $n \times n$  rational matrix. Assume that  $f(z, M, \mathbf{v}) := \text{innerprod}(\text{Row}(z, M), \mathbf{v})$ . We  $\Sigma_1^B$ -define in  $\mathbf{VTC}^0$  the product  $M\mathbf{v}$  as follows:

$$\text{Matvecprod}(M, \mathbf{v}) := \text{Sequence}_f(\text{length}(\mathbf{v}) + 1, M, \mathbf{v}).$$

**Notation:** When reasoning in the theory  $\mathbf{VTC}^0$  we sometimes abuse notation and write  $\mathbf{v} \cdot \mathbf{u}$  or  $\langle \mathbf{v}, \mathbf{u} \rangle$  instead of  $\text{innerprod}(\mathbf{u}, \mathbf{v})$ , and  $M\mathbf{v}$  instead of  $\text{Matvecprod}(M, \mathbf{v})$ , and  $\mathbf{u}^t M\mathbf{v}$  instead of  $\langle \mathbf{u}, M\mathbf{v} \rangle$ .

### 3.2.3 Counting in $\mathbf{VTC}^0$

Here we present basic statements involving counting of certain objects and sets, provable in  $\mathbf{VTC}^0$ .

**Notation:** When reasoning in the theory  $\mathbf{VTC}^0$ , we will say that a family of  $\Sigma_0^B$ -definable in  $\mathbf{VTC}^0$  sets  $B_0, \dots, B_\ell$  forms a partition of  $\bigcup_{i=0}^{\ell} B_i := \{r : \exists i \leq \ell, B_i(r)\}$  whenever  $\mathbf{VTC}^0$  proves that (i)  $\bigcup_{i=0}^{\ell} B_i = B$ , and (ii)  $B_i \cap B_j = \emptyset$ , for all  $0 \leq i \neq j \leq \ell$ .

**Proposition 3.17 (Some counting in  $\mathbf{VTC}^0$ )** *Let  $B_1, \dots, B_\ell$  be family of  $\Sigma_0^B$ -definable sets in  $\mathbf{VTC}^0$  that partition the set  $B$  ( $\ell$  may be a variable). Then,  $\mathbf{VTC}^0$  proves:*

$$\text{numones}(B) = \sum_{i=1}^{\ell} \text{numones}(B_i).$$

**Proof:** We proceed by induction on  $\ell$  to show that for every  $0 \leq y \leq \max\{B_1, \dots, B_\ell\}$ :

$$\text{numones}(y, B_1 \cup \dots \cup B_\ell) = \sum_{i=1}^{\ell} \text{numones}(y, B_i).$$

*Base case:*  $\ell = 1$ . Thus,  $B = B_1$  and so we need to prove only  $\text{numones}(y, B_1) = \sum_{i=1} \text{numones}(y, B_i)$ . Since  $\mathbf{VTC}^0$  proves that a summation that contains only one summand  $B_1$  equals  $B_1$  we are done.

*Induction step:*  $\ell > 1$ . We have  $B = \bigcup_{i=1}^{\ell} B_i = (\bigcup_{i=1}^{\ell-1} B_i) \cup B_\ell$ . Assume by way of contradiction that

$(\bigcup_{i=1}^{\ell-1} B_i) \cap B_\ell \neq \emptyset$ . Then  $\mathbf{VTC}^0$  can prove that this contradicts the assumption that  $B_i \cap B_j = \emptyset$ , for all  $i \neq j$  (which holds since the  $B_i$ 's form a partition of  $B$ ). Hence,  $(\bigcup_{i=1}^{\ell-1} B_i) \cap B_\ell = \emptyset$ , and by Claim 3.18 (proved below):

$$\text{numones}(y, B) = \text{numones}(y, \bigcup_{i=1}^{\ell-1} B_i) + \text{numones}(y, B_\ell) \quad (13)$$

$$= \sum_{i=1}^{\ell-1} \text{numones}(y, B_i) + \text{numones}(y, B_\ell) \quad (\text{by induction hypothesis}) \quad (14)$$

$$= \sum_{i=1}^{\ell} \text{numones}(y, B_i). \quad (15)$$

It remains to prove the following:

**Claim 3.18** (In  $\mathbf{VTC}^0$ ) let  $A, B$  be two sets such that  $A \cap B = \emptyset$ , then for all  $0 \leq y \leq \max\{|A|, |B|\}$ :

$$\text{numones}(y, A \cup B) = \text{numones}(y, A) + \text{numones}(y, B).$$

**Proof of claim:** We proceed by induction on  $y$ , using the defining axiom of  $\text{numones}$  (stating the existence of a counting sequence for the input string variable; see Equations (11) and (9)).

*Base case:*  $y = 0$ . The counting sequence  $Z$  for  $\text{numones}(A \cup B)$  is defined such that  $Z[0] = 0$ . Thus,

$$0 = \text{numones}(0, A \cup B) = \text{numones}(0, A) + \text{numones}(0, B) = 0 + 0 = 0.$$

*Induction step:*  $0 < y \leq \max\{|A|, |B|\}$ . By the defining axiom of  $\text{numones}$  we have:

$$\text{numones}(y, A \cup B) = \begin{cases} \text{numones}(y-1, A \cup B) + 1, & y \in A \cup B; \\ \text{numones}(y-1, A \cup B), & \text{otherwise.} \end{cases} \quad (16)$$

We have to consider the following three cases:

**Case 1:**  $y \in A$ . Thus, by assumption that  $A$  and  $B$  are disjoint, we have  $y \notin B$ . Also, we have  $y \in A \cup B$ . Therefore:

$$\begin{aligned} & \text{numones}(y, A) + \text{numones}(y, B) \\ &= \text{numones}(y-1, A) + 1 + \text{numones}(y, B) && (\text{since } y \in A) \\ &= \text{numones}(y-1, A) + 1 + \text{numones}(y-1, B) && (\text{since } y \notin B) \\ &= \text{numones}(y-1, A \cup B) + 1 && (\text{by induction hypothesis}) \\ &= \text{numones}(y, A \cup B) && (\text{since } y \in A \cup B). \end{aligned}$$

**Case 2:**  $y \in B$ . This is the same as Case 1.

**Case 3:**  $y \notin A \cup B$ . This is similar to the previous cases. We omit the details.  $\blacksquare_{\text{Claim}}$

■

**Proposition 3.19 (More counting in  $VTC^0$ )** Let  $\varphi(x)$  be a  $\Sigma_0^B$  formula (possibly in an extended language of  $VTC^0$ ). The theory  $VTC^0$  can prove that if  $Z = \{0 \leq i < m : \varphi(i)\}$  and for any  $0 \leq i < m$ ,

$$\gamma_i = \begin{cases} a, & \varphi(i); \\ b, & \neg\varphi(i), \end{cases}$$

then

$$\sum_{i < m} \gamma_i = a \cdot \text{numones}(Z) + b \cdot (m - \text{numones}(Z)).$$

**Proof:** Since  $\varphi(x)$  is a  $\Sigma_0^B$  formula, by Section 3.2.1, we can use the comprehension axiom scheme to define, for any  $0 \leq k \leq m - 1$ , the set:

$$Z_k := \{i \leq k : \varphi(i)\}.$$

The claim is proved by induction on  $k$ .

*Base case:*  $k = 0$ . If  $\varphi(0)$  is true, then  $Z_0 = \{0\}$ , and so  $\text{numones}(Z_0) = 1$ . By assumption we have  $\gamma_0 = a = a \cdot \text{numones}(Z_0) + b \cdot (1 - \text{numones}(Z_0))$ . Otherwise,  $\varphi(0)$  is false and so  $Z_0 = \emptyset$ , implying that  $\text{numones}(Z_k) = 0$ . By assumption again we have  $\gamma_0 = b = a \cdot \text{numones}(Z_0) + b(1 - \text{numones}(Z_0))$ .

*Induction step:*  $k > 0$ .

**Case 1:**  $\varphi(k)$  is true. Thus  $Z_k(k)$  is true and also

$$\text{numones}(Z_k) = \text{numones}(Z_{k-1}) + 1, \tag{17}$$

and by assumption  $\gamma_k = a$ . Therefore,

$$\begin{aligned} \sum_{i=0}^k \gamma_i &= \sum_{i=0}^{k-1} \gamma_i + \gamma_k = \sum_{i=0}^{k-1} \gamma_i + a \\ &= a \cdot \text{numones}(Z_{k-1}) + b \cdot (k - 1 - \text{numones}(Z_{k-1})) + a && \text{(by induction hypothesis)} \\ &= a \cdot (\text{numones}(Z_{k-1}) + 1) + b \cdot (k - 1 - \text{numones}(Z_{k-1})) && \text{(rearranging)} \\ &= a \cdot \text{numones}(Z_k) + b \cdot (k - \text{numones}(Z_k)) && \text{(by (17)).} \end{aligned}$$

**Case 2:**  $\varphi(k)$  is false. This is similar to Case 1. Specifically,  $Z_k(k)$  is false and also

$$\text{numones}(Z_k) = \text{numones}(Z_{k-1}), \tag{18}$$

and by assumption  $\gamma_k = b$ . Therefore

$$\begin{aligned} \sum_{i=0}^k \gamma_i &= \sum_{i=0}^{k-1} \gamma_i + \gamma_k = \sum_{i=0}^{k-1} \gamma_i + b \\ &= a \cdot \text{numones}(Z_{k-1}) + b \cdot (k - 1 - \text{numones}(Z_{k-1})) + b && \text{(by induction hypothesis)} \\ &= a \cdot \text{numones}(Z_{k-1}) + b \cdot (k - 1 - \text{numones}(Z_{k-1}) + 1) && \text{(rearranging)} \\ &= a \cdot \text{numones}(Z_k) + b \cdot (k - \text{numones}(Z_k)) && \text{(by (18)).} \end{aligned}$$

■

We shall use the following proposition in Section 5 (Lemma 5.8).

**Proposition 3.20** *The theory  $\mathbf{VTC}^0$  proves the following statement. Let  $F(x)$  be a string function. Let  $d < t$  be a natural number and assume that any number in any set  $F(1), \dots, F(t)$  occurs in at most  $d$  many sets in  $F(1), \dots, F(t)$ . Let  $g(x)$  be a number function such that  $g(1), \dots, g(t)$  are (not necessarily distinct) numbers with  $g(i) \in F(i)$  for all  $i \in [t]$ . Then  $\text{numones}(\{g(i) : i \in [t]\}) \geq \lceil t/d \rceil$ .*

**Proof:** Let  $\text{img}(g(x)) := \{i : g(x) \in F(i)\}$  be a string function (it is  $\Sigma_0^B$ -definable in  $\mathbf{V}^0$ ). By assumption

$$\forall z \in [t] (\text{numones}(\text{img}(g(z))) \leq d). \quad (19)$$

Since for any  $i \in [t]$ ,  $g(i) \in F(i)$ , we can prove in  $\mathbf{VTC}^0$  that  $\bigcup_{z \in [t]} \text{img}(g(z))$  equals  $\{1, 2, \dots, t\}$ , and so  $\mathbf{VTC}^0$  proves:

$$\text{numones} \left( \bigcup_{z \in [t]} \text{img}(g(z)) \right) = t. \quad (20)$$

**Claim 3.21** *(Under the assumptions of the proposition)  $\mathbf{VTC}^0$  proves:*

$$\text{numones} \left( \bigcup_{z \in [t]} \text{img}(g(z)) \right) \leq d \cdot \text{numones}(\{g(i) : i \in [t]\}).$$

**Proof of claim:** The proof follows from (19), by induction on  $t$ .

*Base case:*  $t = 1$ . We have

$$\begin{aligned} \text{numones}(\bigcup_{z \in [t]} \text{img}(g(z))) &= \text{numones}(\text{img}(g(1))) \\ &\leq d && \text{(by assumption)} \\ &= d \cdot \text{numones}(\{g(1)\}) \\ &= d \cdot \text{numones}(\{g(i) : i \in [t]\}). \end{aligned}$$

*Induction step:*

**Case 1:**  $g(t) \in \{g(i) : i \in [t-1]\}$ . Thus,

$$\{g(i) : i \in [t-1]\} = \{g(i) : i \in [t]\} \quad \text{and} \quad \bigcup_{i \in [t-1]} \text{img}(g(i)) = \bigcup_{i \in [t]} \text{img}(g(i)). \quad (21)$$

Thus,

$$\begin{aligned} \text{numones} \left( \bigcup_{i \in [t]} \text{img}(g(i)) \right) &= \text{numones} \left( \bigcup_{i \in [t-1]} \text{img}(g(i)) \right) \\ &\leq d \cdot \text{numones}(\{g(i) : i \in [t-1]\}) && \text{(by induction hypothesis)} \\ &= d \cdot \text{numones}(\{g(i) : i \in [t]\}) && \text{(by (21)).} \end{aligned}$$

**Case 2:**  $g(t) \notin \{g(i) : i \in [t-1]\}$ . Thus,

$$\text{numones}(\{g(i) : i \in [t-1]\}) + 1 = \text{numones}(\{g(i) : i \in [t]\}). \quad (22)$$

we have

$$\text{numones} \left( \bigcup_{z \in [t]} \text{Img}(g(z)) \right) \leq \text{numones} \left( \bigcup_{z \in [t-1]} \text{Img}(g(z)) \right) + \text{numones}(\text{Img}(g(t)))$$

and by induction hypothesis

$$\begin{aligned} &\leq d \cdot \text{numones}(\{g(i) : i \in [t-1]\}) + \text{numones}(\text{Img}(g(t))) \\ &\leq d \cdot (\text{numones}(\{g(i) : i \in [t]\}) - 1) + \text{numones}(\text{Img}(g(t))) \quad (\text{by (22)}) \\ &\leq d \cdot (\text{numones}(\{g(i) : i \in [t]\}) - 1) + d \quad (\text{by assumption}) \\ &= d \cdot \text{numones}(\{g(i) : i \in [t]\}). \end{aligned}$$

■ Claim

Thus, by Claim 3.21 and by (20), we get:

$$t \leq d \cdot \text{numones}(\{g(i) : i \in [t]\}),$$

which leads to  $t/d \leq \text{numones}(\{g(i) : i \in [t]\})$ , and since  $\text{numones}(\{g(i) : i \in [t]\})$  is an integer number we get:

$$\lceil t/d \rceil \leq \lceil \text{numones}(\{g(i) : i \in [t]\}) \rceil = \text{numones}(\{g(i) : i \in [t]\}).$$

■

### 3.2.4 Manipulating big sums in $\mathbf{VTC}^0$

We need to prove basic properties of summation (having a non-constant number of summands) like commutativity, associativity, distributivity, substitution in big sums, rearranging etc., in  $\mathbf{VTC}^0$ , to be able to carry out basic calculations in the theory. As a consequence of this section we will be able to freely derive inequalities and equalities between big summations (using rearranging, substitutions of equals, etc.) in  $\mathbf{VTC}^0$ .

**Proposition 3.22 (Basic properties of sums in  $\mathbf{VTC}^0$ )** *In what follows we consider the theory  $\mathbf{VTC}^0$  over an extended language (including possibly new  $\Sigma_1^B$ -definable function symbols in  $\mathbf{VTC}^0$  and their defining axioms). The function  $f(i)$  is a number function symbol mapping to the rationals or naturals (possibly with additional undisplayed parameters). The theory  $\mathbf{VTC}^0$  proves the following statements:*

**Substitution:** *Assume that  $u(i), v(i)$  are two terms (possibly with additional undisplayed parameters), such that  $u(i) = v(i)$  for any  $i \leq n$ , then*

$$\sum_{i=0}^n f(u(i)) = \sum_{i=0}^n f(v(i)).$$



**Distributivity:** Assume that  $u$  is a term that does not contain the variable  $i$ , then

$$u \cdot \sum_{i=0}^n f(i) = \sum_{i=0}^n u \cdot f(i).$$

**Rearranging:** Assume that  $I = \{0, \dots, n\}$  and let  $I_1, \dots, I_k$  be a definable partition of  $I$  (specifically, the sets  $I_1, \dots, I_k$  are all  $\Sigma_0^B$ -definable in  $\mathbf{VTC}^0$  and  $\mathbf{VTC}^0$  proves that the  $I_j$ 's form a partition of  $I$ ). Then

$$\sum_{i=0}^n f(i) = \sum_{j=1}^k \sum_{i \in I_j} f(i),$$

where  $\sum_{i \in I_j} f(i)$  denotes the term  $\sum_{i=0}^{|I_j|-1} f(\delta(i))$  where  $\delta(i)$  is the function that enumerates (in ascending order) the elements in  $I_j$ .

**Inequalities:** Let  $g(i)$  be a number function mapping to the rationals or naturals (possibly with additional undisplayed parameters), such that  $f(i) \leq g(i)$  for all  $0 \leq i \leq n$ , then

$$\sum_{i=0}^n f(i) \leq \sum_{i=0}^n g(i).$$

**Proof:**

**Substitution:** When we work in the theory  $\mathbf{VTC}^0$  we implicitly assume that we have equality axioms stating that if  $t = t'$ , for any two terms  $t, t'$ , then  $F(t) = F(t')$ , for any function  $F$  (including functions  $F$  that are from the extended language of  $\mathbf{VTC}^0$ ). Since we assume that  $f(i)$  is a  $\Sigma_1^B$ -definable number function in  $\mathbf{VTC}^0$ , the function  $g(n) := \sum_{i=0}^n f(i)$  is also  $\Sigma_1^B$ -definable in  $\mathbf{VTC}^0$ , and so we also have the equality axiom for  $g(n)$ , from we can derive that  $u(i) = v(i)$  for any  $i \leq n$  implies  $g(u(n)) = g(v(n))$ .

**Distributivity:** This is proved simply by induction on  $n$ . We omit the details.

**Rearranging:** Because  $I_1, \dots, I_k$  are  $\Sigma_0^B$ -definable sets in  $\mathbf{VTC}^0$  we can define the family of sequences  $S_1, \dots, S_k$ , each of length  $n + 1$ , such that

$$S_j[i] := \begin{cases} f(i), & i \in I_j; \\ 0, & \text{otherwise.} \end{cases}$$

The theory  $\mathbf{VTC}^0$  proves, by induction on  $n$ , that

$$\sum_{j=1}^k \sum_{i=0}^n S_j[i] = \sum_{i=0}^n f(i).$$

For any  $j = 1, \dots, k$ , we can  $\Sigma_1^B$ -define in  $\mathbf{VTC}^0$  the function  $\delta_j : \{0, \dots, |I_j| - 1\} \rightarrow \{0, \dots, n\}$  such that  $\delta_j(\ell) = i$  iff  $i$  is the  $(\ell + 1)$ th element in  $I_j$  (when the elements in  $I_j$  are ordered in ascending order). In other words, the  $\delta_j$ 's functions enumerate the elements in  $I_j$ .

We can now prove in  $\mathbf{VTC}^0$  that

$$\sum_{i=0}^n S_j[i] = \sum_{i=0}^{|I_j|-1} f(\delta_j(i)),$$

from which, by Substitution (proved above), we can prove:

$$\sum_{i=1}^k \sum_{i=0}^n S_j[i] = \sum_{i=1}^k \sum_{i=0}^{|I_j|-1} f(\delta_j(i)).$$

**Inequalities:** This can be proved in  $\mathbf{VTC}^0$  simply by induction on  $n$ . We omit the details.  $\blacksquare$

All the equalities and inequalities which contain big summations that we will derive in the theory, can be proved using Proposition 3.22. We shall not state this explicitly in the text, but continue to derive such equalities and inequalities freely.

### 3.2.5 The relation between $\mathbf{VTC}^0$ and $\mathbf{TC}^0$ -Frege

In this section we show how one can translate a  $\Sigma_0^B$  formula  $\varphi$  into a family of propositional formulas  $\llbracket \varphi \rrbracket$ . We then state the theorem showing that if the universal closure of a  $\Sigma_0^B$  formula  $\varphi$  is provable in  $\mathbf{VTC}^0$  then the propositional translation  $\llbracket \varphi \rrbracket$  has a polynomial-size proof in  $\mathbf{TC}^0$ -Frege.

**Definition 3.23 (Propositional translation  $\llbracket \cdot \rrbracket$  of  $\Sigma_0^B$  formulas)** *Let  $\varphi(\vec{x}, \vec{X})$  be a  $\Sigma_0^B$  formula. The propositional translation of  $\varphi$  is a family*

$$\llbracket \varphi \rrbracket = \{ \llbracket \varphi \rrbracket_{\vec{m}; \vec{n}} \mid m_i, n_i \in \mathbb{N} \}$$

*of propositional formulas in variables  $p_j^{X_i}$  for every  $X_i \in \vec{X}$ . The intended meaning is that  $\llbracket \varphi \rrbracket$  is a valid family of formulas if and only if the formula*

$$\forall \vec{x} \forall \vec{X} \left( \left( \bigwedge |X_i| = \underline{n}_i \rightarrow \varphi(\vec{m}, \vec{X}) \right) \right)$$

*is true in the standard model  $\mathbb{N}_2$  of two sorted arithmetic, where  $\underline{n}$  denotes the  $n$ th numeral, for any  $n \in \mathbb{N}$ .*

*For given  $\vec{m}, \vec{n} \in \mathbb{N}$  we define  $\llbracket \varphi \rrbracket$  by induction on the size of the formula  $\llbracket \varphi \rrbracket_{\vec{m}; \vec{n}}$ . We denote the value of a term  $t$  by  $\text{val}(t)$ .*

**Case 1:** *Let  $\varphi(\vec{x}, \vec{X})$  be an atomic formula.*

- *If  $\varphi(\vec{x}, \vec{X})$  is  $\top$  (or  $\perp$ ), then  $\llbracket \varphi \rrbracket_{\vec{m}; \vec{n}} := \top$  (or  $\perp$ ).*
- *If  $\varphi(\vec{x}, \vec{X})$  is  $X_i = X_i$ , then  $\llbracket \varphi \rrbracket_{\vec{m}; \vec{n}} := \top$ .*
- *If  $\varphi(\vec{x}, \vec{X})$  is  $X_i = X_j$  for  $i \neq j$ , then (using the fact that  $\mathbf{V}^0$  contains the extensionality axiom **SE**) instead of translating  $\varphi$ , we translate the  $\mathbf{V}^0$ -equivalent formula*

$$|X_i| = |X_j| \wedge \forall k \leq |X| (X_i(k) \leftrightarrow X_j(k)).$$

- *If  $\varphi(\vec{x}, \vec{X})$  is  $t_1(\vec{y}, |\vec{Y}|) = t_2(\vec{z}, |\vec{Z}|)$  for terms  $t_1, t_2$ , number variables  $\vec{y}, \vec{z}$  and string variables  $\vec{Y}, \vec{Z}$ , where  $\vec{y} \cup \vec{z} = \vec{x}$  and  $\vec{Y} \cup \vec{Z} = \vec{X}$ , and  $\vec{m}^y, \vec{m}^z$  and  $\vec{n}^Y, \vec{n}^Z$  denote the corresponding assignments of numerals  $\vec{m}, \vec{n}$  to the  $\vec{y}, \vec{z}$  and  $\vec{Y}, \vec{Z}$  variables, respectively. Then*

$$\llbracket \varphi \rrbracket_{\vec{m}; \vec{n}} := \begin{cases} \top & \text{if } \text{val}(t_1(\vec{m}^Y, \vec{n}^Y)) = \text{val}(t_2(\vec{m}^Z, \vec{n}^Z)) \text{ and} \\ \perp & \text{otherwise.} \end{cases}$$

- If  $\varphi(\vec{x}, \vec{X})$  is  $t_1(\vec{y}, |\vec{Y}|) \leq t_2(\vec{z}, |\vec{Z}|)$  for terms  $t_1, t_2$ , number variables  $\vec{y}, \vec{z}$  and string variables  $\vec{Y}, \vec{Z}$ , then

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \begin{cases} \top & \text{if } \text{val}(t_1(\vec{m}^Y, \vec{n}^Y)) \leq \text{val}(t_2(\vec{m}^Z, \vec{n}^Z)) \text{ and} \\ \perp & \text{otherwise.} \end{cases}$$

- If  $\varphi(\vec{x}, \vec{X})$  is  $X_i(t(\vec{x}, |\vec{X}|))$ , then

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \perp \quad \text{if } n_i = 0$$

and otherwise

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \begin{cases} p_{\text{val}(t(\vec{m}, \vec{n}))}^{X_i} & \text{if } \text{val}(t(\vec{m}, \vec{n})) < \underline{n_i - 1}, \\ \top & \text{if } \text{val}(t(\vec{m}, \vec{n})) = \underline{n_i - 1}, \\ \perp & \text{if } \text{val}(t(\vec{m}, \vec{n})) > \underline{n_i - 1}. \end{cases}$$

**Case 2:** The formula  $\varphi$  is not atomic.

- If  $\varphi \equiv \psi_1 \wedge \psi_2$  we let

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \llbracket \psi_1 \rrbracket_{\vec{m}, \vec{n}} \wedge \llbracket \psi_2 \rrbracket_{\vec{m}, \vec{n}}.$$

- If  $\varphi \equiv \psi_1 \vee \psi_2$  we let

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \llbracket \psi_1 \rrbracket_{\vec{m}, \vec{n}} \vee \llbracket \psi_2 \rrbracket_{\vec{m}, \vec{n}}.$$

- If  $\varphi \equiv \neg\psi$  we let

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \neg \llbracket \psi \rrbracket_{\vec{m}, \vec{n}}.$$

- If  $\varphi \equiv \exists y \leq t(\vec{x}, |\vec{X}|) \psi(y, \vec{x}, \vec{X})$  then

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \bigvee_{i=0}^{\text{val}(t(\vec{m}, \vec{n}))} \llbracket \psi(i, \vec{x}, \vec{X}) \rrbracket_{\vec{m}, \vec{n}}.$$

- If  $\varphi \equiv \forall y \leq t(\vec{x}, |\vec{X}|) \psi(y, \vec{x}, \vec{X})$  then

$$\llbracket \varphi \rrbracket_{\vec{m}, \vec{n}} := \bigwedge_{i=0}^{\text{val}(t(\vec{m}, \vec{n}))} \llbracket \psi(i, \vec{x}, \vec{X}) \rrbracket_{\vec{m}, \vec{n}}.$$

This concludes the translation for  $\Sigma_0^B$  formulas.

**Proposition 3.24 (Lemma VII.2.2 [13])** For every  $\Sigma_0^B$  formula  $\varphi(\vec{x}, \vec{X})$  there exists a constant  $d \in \mathbb{N}$  and a polynomial  $p(\vec{m}, \vec{n})$  such that for all  $\vec{m}, \vec{n} \in \mathbb{N}$ , the propositional translation  $\llbracket \varphi(\vec{x}, \vec{X}) \rrbracket_{\vec{m}, \vec{n}}$  has depth at most  $d$  and size at most  $p(\vec{m}, \vec{n})$ .

We can now state the relation between provability of an arithmetical statement  $\varphi$  in  $\mathbf{VTC}^0$  to the provability of the family  $\llbracket \varphi \rrbracket$  in  $\mathbf{TC}^0$ -Frege as follows.

**Theorem 3.25 (Section X.4.3. [13])** Let  $\varphi(\vec{x}, \vec{X})$  be a  $\Sigma_0^B$  formula. Then, if  $\mathbf{VTC}^0$  proves  $\varphi(\vec{x}, \vec{X})$  then there is a polynomial size family of  $\mathbf{TC}^0$ -Frege proofs of  $\llbracket \varphi \rrbracket$ .

## 4 Feige-Kim-Ofek witnesses and the main formula

In this section we define the main formula we are going to prove in the theory. We are concerned with proofs of 3CNF formulas. Let us fix the following notation. With  $n$  we will denote the number of propositional variables  $x_1, \dots, x_n$  and with  $m$  we will denote the number of clauses appearing in the 3CNF denoted  $\mathbf{C} = \bigwedge_{\alpha=0}^{m-1} C_\alpha$ . Each clause  $C_\alpha$  is of the form  $x_i^{\ell_1} \vee x_j^{\ell_2} \vee x_k^{\ell_3}$ , for  $\ell_1, \ell_2, \ell_3 \in \{0, 1\}$ , where  $x_i^1$  abbreviates  $x_i$  and  $x_i^0$  abbreviates  $\neg x_i$ . A clause  $C_\alpha$  is represented by the sequence  $\langle i, j, k, \langle \ell_1, \ell_2, \ell_3 \rangle, \alpha \rangle$ . The defining  $\Sigma_0^B$  formula of the relation is:

$$\begin{aligned} \text{CLAUSE}(x, n, m) &\leftrightarrow \exists i, j, k \leq n \exists \alpha < m \exists \ell \leq 8 \\ & (i > 0 \wedge j > 0 \wedge k > 0 \wedge \langle x \rangle_1^5 = i \wedge \langle x \rangle_2^5 = j \wedge \langle x \rangle_3^5 = k \wedge \langle x \rangle_4^5 = \ell \wedge \langle x \rangle_5^5 = \alpha). \end{aligned}$$

A 3CNF  $\mathbf{C} \equiv \bigwedge_{\alpha=0}^{m-1} C_\alpha$  is represented by the sequence  $(C_0, \dots, C_{m-1})$ . Since  $m$  is non-constant, we use a string variable to code  $\mathbf{C}$ . The defining  $\Sigma_0^B$  formula of this relation is

$$\text{3CNF}(\mathbf{C}, n, m) \leftrightarrow \forall i < m (\text{CLAUSE}(\mathbf{C}[i], n, m) \wedge \langle \mathbf{C}[i] \rangle_5^5 = i).$$

For a number variable  $x$ , we  $\Sigma_0^B$ -define  $\text{EVEN}(x)$  by the formula  $\exists y \leq x (2 \cdot y = x)$  (meaning that  $x$  is an even number). Accordingly, we define  $\text{ODD}(x)$  by  $\neg \text{EVEN}(x)$ .

For some clause  $C$  and a string variable  $A$  (interpreted as a Boolean assignment), we  $\Sigma_0^B$ -define the following predicate, stating that  $C$  is not satisfied under the assignment  $A$ :

$$\begin{aligned} \text{NOTSAT}(C, A) &\equiv \exists i, j, k \leq n \\ & (\langle C \rangle_1^5 = i \wedge (A(i) \leftrightarrow \langle \langle C \rangle_4^5 \rangle_1^3 = 0)) \\ & \wedge (\langle C \rangle_2^5 = j \wedge (A(j) \leftrightarrow \langle \langle C \rangle_4^5 \rangle_2^3 = 0)) \\ & \wedge (\langle C \rangle_3^5 = k \wedge (A(k) \leftrightarrow \langle \langle C \rangle_4^5 \rangle_3^3 = 0)). \end{aligned}$$

We need the following notations and definitions to facilitate the formalization of certain sets and objects:

**Notation:**

1. When considering a *set* of clauses, then a clause in  $\mathbf{C}$  will be referred to only by its index  $0 \leq i < m$ . Thus, a set of clauses from  $\mathbf{C}$  is a set of natural numbers less than  $m$ .
2. A set of literal positions from  $\mathbf{C}$  will be coded as a set of numbers  $\langle a, b \rangle$ , where  $0 \leq a < m$  is the index of a clause in  $\mathbf{C}$  and  $b = 1, 2, 3$  is the index of a literal in the clause.
3. For  $0 \leq i < m$  and  $\varepsilon = 0, 1$  and a sequence  $S$  of 3-clauses we define  $\text{LitPos}(S, i, \varepsilon)$  to be the string function that outputs the set of (positions of) literals  $x_i^\varepsilon$  in  $S$ . In other words, we have:

$$\text{LitPos}(S, i, \varepsilon) := \{ \langle j, \ell \rangle : j < \text{length}(S) \wedge \ell \leq 3 \wedge \langle S[j] \rangle_\ell^5 = i \wedge \langle \langle S[j] \rangle_4^5 \rangle_\ell^3 = \varepsilon \}.$$

4. Let  $\text{satLit}(A, \mathbf{C})$  be the string function that outputs the set of all literal positions in  $\mathbf{C}$  that are satisfied by  $A$ .
5. The function  $\text{Lit}(C, i)$  returns the  $i$ th literal  $x_i^\varepsilon$  of the clause  $C$ , for  $i = 1, 2, 3$ , in the form of a pair  $\langle j, \varepsilon \rangle$ .

6. If the literals of a clause are not all true or not all false under  $A$ , then we say that the clause is satisfied as NAE (standing for “not all equal”) by  $A$ . We can easily  $\Sigma_0^B$ -define the predicate  $\text{SATL}(z, A)$ , stating that the literal  $z$  is satisfied by the assignment  $A$  in  $\mathbf{VTC}^0$ . Let:

$$\text{NAE}(C, A) \leftrightarrow \text{CLAUSE}(C) \wedge \bigvee_{i=1,2,3} \text{SATL}(\text{Lit}(C, i), A) \wedge \bigvee_{i=1,2,3} \neg \text{SATL}(\text{Lit}(C, i), A)$$

be the  $\Sigma_0^B$  relation that states that the assignment  $A$  satisfies the 3-clause  $C$  as NAE. Let  $\text{satNAE}(A, \mathbf{C})$  be the string function that outputs the set of clauses in  $\mathbf{C}$  that are satisfied as NAE by  $A$ .

The functions  $\text{LitPos}(S, i, \varepsilon)$ ,  $\text{satLit}(A, \mathbf{C})$  and  $\text{satNAE}(A, \mathbf{C})$  above are all  $\mathbf{AC}^0$ -reducible to the language  $\mathcal{L}_A^2$  and so we can assume that we have these functions (along with their defining axioms) in  $\mathbf{VTC}^0$  (see Section 3.1.2). All the functions in this section will be  $\mathbf{AC}^0$ -reducible to  $\mathcal{L}_A^2 \cup \{\text{numones}\}$ , and all the relations in this section will have  $\Sigma_0^B$  definitions in the language  $\mathcal{L}_A^2$  extended to include both our new function symbols and  $\text{numones}$ .

**Definition 4.1 (Even  $k$ -tuple)** *For any given  $k$ , a sequence  $S$  of  $k$  clauses is an even  $k$ -tuple iff every variable appears an even number of times in the sequence. Formally, the predicate is denoted  $\text{TPL}(S, k)$ :*

$$\begin{aligned} \text{TPL}(S, k) \leftrightarrow & \text{length}(S) = k \wedge \\ & \forall i \leq n, \text{EVEN}(\text{numones}(\text{LitPos}(S, i, 0)) + \text{numones}(\text{LitPos}(S, i, 1))). \end{aligned} \quad (23)$$

Observe that if  $S$  is an even  $k$ -tuple then  $k$  is even (since the total number of variable occurrences  $N$  is even, by assumption that each variable occurs an even number of times; and  $k = N/3$ , since each clause has three variables).

**Definition 4.2 (Inconsistent  $k$ -tuple)** *An even  $k$ -tuple is said to be inconsistent if the total number of negations in its clauses is odd. Formally, the predicate is denoted by  $\text{ITPL}(S, k)$ :*

$$\text{ITPL}(S, k) \leftrightarrow \text{TPL}(S, k) \wedge \text{ODD} \left( \sum_{i=1}^n \text{numones}(\text{LitPos}(S, i, 1)) \right).$$

**Definition 4.3 (The imbalance  $\text{Imb}(S, y)$ )** *For a 3CNF  $S$  we define the function  $i$ -imbalance  $\text{ilmb}(S, i)$  to be the absolute value of the difference of negated occurrences of  $x_i$  and non-negated occurrences of  $x_i$  in the 3CNF  $S$  (where  $x_1, \dots, x_n$  are considered to be all the variables in  $S$ ). It is defined simply by the term:*

$$\text{ilmb}(S, i) := \text{abs}(\text{numones}(\text{LitPos}(i, 0, S)) - \text{numones}(\text{LitPos}(i, 1, S))).$$

For a 3CNF  $S$ , the predicate imbalance of  $S$ , denoted  $\text{IMB}(S, y)$ , is true iff  $y$  equals the sum over the  $i$ -imbalances of all the variables, that is:

$$\text{IMB}(S, y) \leftrightarrow y = \sum_{i=1}^n \text{ilmb}(S, i).$$

**Definition 4.4** ( $(t, k, d)$ -collection) *A  $(t, k, d)$ -collection  $\mathcal{D}$  of a 3CNF  $\mathbf{C}$  with  $m$  clauses is an array (coded as in Definition 3.10) of  $t$  many inconsistent  $k$ -tuples, which contain only clauses from  $\mathbf{C}$ , and each clause appears in at most  $d$  many such inconsistent  $k$ -tuples. The predicate is denoted  $\text{COLL}(t, k, d, \mathbf{C}, \mathcal{D})$  and is defined by the following formula:*

$$\begin{aligned} \text{length}(\mathcal{D}) &= t \wedge \\ \forall i < t &\text{ITPL}(\mathcal{D}^{[i]}, k) \wedge \\ \forall i < t \forall \ell < k &\exists j < |\mathbf{C}| (\mathcal{D}^{[i]}[\ell] = \mathbf{C}[j]) \wedge \\ \forall j < |\mathbf{C}| &\sum_{i=0}^{t-1} \sum_{\ell=0}^{k-1} \chi_{=(\langle \mathcal{D}^{[i]}[\ell] \rangle_5^5, j)} \leq d. \end{aligned}$$

**Definition 4.5** ( $\text{Mat}(M, \mathbf{C})$ ) *We define the predicate  $\text{MAT}(M, \mathbf{C})$  that holds iff  $M$  is an  $n \times n$  rational matrix such that  $M_{ij}$  equals  $\frac{1}{2}$  times the number of clauses in  $\mathbf{C}$  where  $x_i$  and  $x_j$  appear with different polarity minus  $\frac{1}{2}$  times the number of clauses where they appear with the same polarity. More formally, we have*

$$M_{ij} := \sum_{k=0}^{m-1} E_{ij}^{(k)}, \quad \text{for any } i, j \in [n], \quad (24)$$

where  $E_{ij}^{(k)}$  corresponds to the  $k$ th clause in  $\mathbf{C}$  as follows:

$$E_{ij}^{(k)} := \begin{cases} \frac{1}{2}, & x_i^{\varepsilon_i}, x_j^{\varepsilon_j} \in \mathbf{C}[k] \text{ and } \varepsilon_i \neq \varepsilon_j, \text{ for some } \varepsilon_i, \varepsilon_j \in \{0, 1\} \text{ and } i \neq j; \\ -\frac{1}{2}, & x_i^{\varepsilon_i}, x_j^{\varepsilon_j} \in \mathbf{C}[k] \text{ and } \varepsilon_i = \varepsilon_j, \text{ for some } \varepsilon_i, \varepsilon_j \in \{0, 1\} \text{ and } i \neq j; \\ 0, & \text{otherwise.} \end{cases} \quad (25)$$

Note that  $E_{ij}^{(k)}$  is definable by a  $\Sigma_0^B$  formula (in  $\mathcal{L}_A^2$ ), and so  $\text{MAT}(M, \mathbf{C})$  is a  $\Sigma_0^B$ -definable relation in  $\mathbf{VTC}^0$ .

Finally, we need a predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  that ensures that  $\vec{\lambda}$  is a collection of  $n$  rational approximations of the eigenvalues of the matrix  $M$  and that  $V$  is the rational matrix whose rows are the rational approximations of the eigenvectors of  $M$  (where the  $i$ th row in  $V$  is the approximation of the approximate eigenvector  $\lambda_i$ ). For the sake of readability we defer the formal definition of the predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  and all the lemmas that relate to it, including the proofs in the theory making use of this predicate, to Section 6.

**Notation:** 1. The notation  $o(1)$  appearing inside a formula in the proof within the theory, and specifically in Definition 4.6 below, stands for a term of the form  $b/n^c$ , for  $b$  a number symbol greater than 0, and  $c$  some positive constant (and where a rational number is encoded in the way described in Section 3.1.2).

2. Given two terms  $t$  and  $f(n)$  in the language  $\mathcal{L}_A^2$ , where  $n$  is a number variable, we say that  $\mathbf{VTC}^0$  proves  $t = O(f(n))$ , to mean that there exists some constant  $c$  (independent of  $n$ ) such that  $\mathbf{VTC}^0$  proves  $t \leq c \cdot f(n)$ , where  $c$  is a term without variables in the language  $\mathcal{L}_A^2$ .

We can now state the main formula that we are going to prove in  $\mathbf{VTC}^0$ . It says that if the Feige-Kim-Ofek witness fulfills the inequality  $t > \frac{d \cdot (I + \lambda n)}{2} + o(1)$  then there exists a clause in  $\mathbf{C}$  that is not satisfied by any assignment  $A$  (one can think of all the free variables in the formula as universally quantified):

**Definition 4.6 (The main formula)** *The main formula is the following formula ( $\vec{\lambda}$  denotes  $n$  distinct number parameters  $\lambda_1, \dots, \lambda_n$ ):*

$$\left( \begin{aligned} &3\text{CNF}(\mathbf{C}, n, m) \wedge \text{COLL}(t, k, d, \mathbf{C}, \mathcal{D}) \wedge \text{IMB}(\mathbf{C}, I) \wedge \text{MAT}(M, \mathbf{C}) \wedge \\ &\text{EIGVALBOUND}(M, \vec{\lambda}, V) \wedge \lambda = \max\{\lambda_1, \dots, \lambda_n\} \wedge t > \frac{d \cdot (I + \lambda_n)}{2} + o(1) \end{aligned} \right) \\ \longrightarrow \exists i < m \text{NOTSAT}(\mathbf{C}[i], A).$$

## 5 Proof of the main formula

In this section we prove our key theorem:

**Theorem 5.1 (Key)** *The theory  $\mathbf{VTC}^0$  proves the main formula (Definition 4.6).*

**Proof:** We reason inside  $\mathbf{VTC}^0$ . Assume by way of contradiction that the premise of the implication in the main formula holds and that there is an assignment  $A \in \{0, 1\}^n$  (construed as a string variable of length  $n$ ) that satisfies every clause in  $\mathbf{C}$ . Recall that  $\text{satLit}(A, \mathbf{C})$  is the set of all literal positions that are satisfied by  $A$ .

**Lemma 5.2** *(Assuming the premise of the main formula) the theory  $\mathbf{VTC}^0$  proves:*

$$\text{numones}(\text{satLit}(A, \mathbf{C})) \leq \frac{3m + I}{2}.$$

**Proof:** First observe that for any assignment  $A$  and any  $1 \leq i \leq n$  the set of satisfied literals of  $x_i$  is defined by  $\text{LitPos}(\mathbf{C}, i, A(i))$ . Therefore, the sets  $\text{LitPos}(\mathbf{C}, 1, A(1)), \dots, \text{LitPos}(\mathbf{C}, n, A(n))$  form a partition of  $\text{satLit}(A, \mathbf{C})$  (provably in  $\mathbf{VTC}^0$ ), and thus by Proposition 3.17,  $\mathbf{VTC}^0$  proves that

$$\text{numones}(\text{satLit}(A, \mathbf{C})) = \sum_{i=1}^n \text{numones}(\text{LitPos}(\mathbf{C}, i, A(i))). \quad (26)$$

By (26) we get

$$\text{numones}(\text{satLit}(A, \mathbf{C})) \leq \sum_{i=1}^n \max\{\text{numones}(\text{LitPos}(\mathbf{C}, i, 0)), \text{numones}(\text{LitPos}(\mathbf{C}, i, 1))\}. \quad (27)$$

For any  $1 \leq i \leq n$ , define the term

$$\text{LitPos}(\mathbf{C}, i) := \text{LitPos}(\mathbf{C}, i, 0) \cup \text{LitPos}(\mathbf{C}, i, 1).$$

Then by

$$\begin{aligned} \frac{\text{ilmb}(\mathbf{C}, i) + \text{numones}(\text{LitPos}(\mathbf{C}, i))}{2} &= \\ \frac{\text{ilmb}(\mathbf{C}, i) + \text{numones}(\text{LitPos}(\mathbf{C}, i, 0)) + \text{numones}(\text{LitPos}(\mathbf{C}, i, 1))}{2}, \end{aligned}$$



and since, by Definition 4.3,  $\text{ilmb}(\mathbf{C}, i) = \text{abs}(\text{numones}(\text{LitPos}(\mathbf{C}, i, 0)) - \text{numones}(\text{LitPos}(\mathbf{C}, i, 1)))$ , the theory  $\mathbf{VTC}^0$  proves that for any  $1 \leq i \leq n$ :

$$\max\{\text{numones}(\text{LitPos}(\mathbf{C}, i, 0)), \text{numones}(\text{LitPos}(\mathbf{C}, i, 1))\} = \frac{\text{ilmb}(\mathbf{C}, i) + \text{numones}(\text{LitPos}(\mathbf{C}, i))}{2}. \quad (28)$$

**Claim 5.3** (Assuming the premise of the main formula) the theory  $\mathbf{VTC}^0$  proves:

$$\sum_{i=1}^n \frac{\text{ilmb}(\mathbf{C}, i) + \text{numones}(\text{LitPos}(\mathbf{C}, i))}{2} = \frac{I + 3m}{2}.$$

**Proof of claim:** First recall the definition of imbalance (Definition 4.3)  $I = \sum_{i=1}^n \text{ilmb}(\mathbf{C}, i)$ . Thus it remains to prove that  $\sum_{i=1}^n \text{numones}(\text{LitPos}(\mathbf{C}, i)) = 3m$ . For this, note that  $\text{LitPos}(\mathbf{C}, i)$ , for  $i = 1, \dots, n$ , partition the set of all literal positions in  $\mathbf{C}$ . In other words, we can prove that: (i) if  $H$  is the set of all literal positions in  $\mathbf{C}$  (this set is clearly  $\Sigma_0^B$ -definable in  $\mathbf{VTC}^0$ ) then  $H = \cup_{i=1}^n \text{LitPos}(\mathbf{C}, i)$ ; and (ii)  $\text{LitPos}(\mathbf{C}, i) \cap \text{LitPos}(\mathbf{C}, j) = \emptyset$ , for all  $1 \leq i \neq j \leq n$ . Therefore, by Proposition 3.17 we can prove that:

$$\text{numones}(H) = \sum_{i=1}^n \text{numones}(\text{LitPos}(\mathbf{C}, i)). \quad (29)$$

Now, the set  $H$  of all literal position in  $\mathbf{C}$  can be partitioned (provably in  $\mathbf{VTC}^0$ ) by the sets  $T_1, \dots, T_m$ , where each  $T_j$ , for  $0 \leq j < m$ , is the set of the three literals in the  $j$ th clause in  $\mathbf{C}$ . Thus, again by Proposition 3.17, we can prove that  $\text{numones}(H) = 3m$ . By (29) we therefore have

$$\sum_{i=1}^n \text{numones}(\text{LitPos}(\mathbf{C}, i)) = 3m.$$

■ Claim

We conclude that:

$$\begin{aligned} & \text{numones}(\text{satLit}(A, \mathbf{C})) \\ & \leq \sum_{i=1}^n \max\{\text{numones}(\text{LitPos}(\mathbf{C}, i, 0)), \text{numones}(\text{LitPos}(\mathbf{C}, i, 1))\} && \text{(by (27))} \\ & = \sum_{i=1}^n \frac{\text{ilmb}(\mathbf{C}, i) + \text{LitPos}(\mathbf{C}, i)}{2} && \text{(by (28))} \\ & = \frac{I + 3m}{2}. && \text{(by Claim 5.3).} \end{aligned}$$

■

We now bound the number of clauses in  $\mathbf{C}$  that contain exactly two literals satisfied by  $A$ . We say that a 3-clause is satisfied by a given assignment as NAE (which stands for *not all equal*) if the literals in the clause do not all have the same truth values. That is, if either exactly one or exactly two literals in the clause are satisfied by the assignment.

For a definable set  $R$  in  $\mathbf{VTC}^0$  we denote by  $\mathcal{P}^R$  the *powerset* of  $R$  (we do not use  $\mathcal{P}^R$  as an object in the formal proof in the theory itself—this is just a convenient notation). Also, recall that  $\text{satNAE}(A, \mathbf{C})$  is the function that returns the set of all clauses (formally, indices  $< m$ ) that are satisfied as NAE by  $A$ .

**Lemma 5.4** (*Assuming the premise of the main formula*) the theory  $\mathbf{VTC}^0$  proves: let  $h$  be the number of clauses in  $\mathbf{C}$  that contain exactly two literals satisfied by  $A$ . Then

$$h \leq \frac{3m + I}{2} - 3m + 2 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})).$$

**Proof:** For  $i = 0, 1, 2, 3$ , let  $B_i$  be the set of clauses in  $\mathbf{C}$  that contain exactly  $i$  literals satisfied by  $A$ . For  $i = 0, 1, 2, 3$ , let  $F_i$  be the string function that maps a clause (index)  $C$  to the set of literal positions that are satisfied by  $A$  in case there are exactly  $i$  such literals and to the empty set otherwise:

$$F_i(j) = \begin{cases} \{l_1, \dots, l_i\}, & \text{if } j \in B_i ; \\ \emptyset, & \text{otherwise} \end{cases}$$

(where a literal  $l_k$  is coded, as before, by the pair  $\langle a, b \rangle$  for  $a$  an index of a clause in  $\mathbf{C}$  and  $b$  the position of the literal in the clause). Every such function  $F_i$  is  $\Sigma_0^B$ -defined in  $\mathbf{VTC}^0$ . We also  $\Sigma_0^B$ -define the image of  $F_i$  as follows:

$$\text{Img}(F_i) := \{x : \exists y < m (F_i(y))(x)\}.$$

**Claim 5.5** (*Assuming the premise of the main formula*) the theory  $\mathbf{VTC}^0$  proves:

$$\text{numones}(\text{satLit}(A, \mathbf{C})) = \sum_{i=1}^3 \text{numones}(\text{Img}(F_i)).$$

**Proof of claim:** In light of Proposition 3.17, it suffices to prove that  $\text{satLit}(A, \mathbf{C})$  is partitioned by  $\text{Img}(F_1), \text{Img}(F_2), \text{Img}(F_3)$  (note that  $\text{Img}(F_0) = \emptyset$  by definition), in the sense that:

- (i)  $\text{satLit}(A, \mathbf{C}) = \text{Img}(F_1) \cup \text{Img}(F_2) \cup \text{Img}(F_3)$ , and
- (ii)  $\text{Img}(F_i) \cap \text{Img}(F_j) = \emptyset$ , for all  $1 \leq i \neq j \leq 3$ .

We prove (i): consider a literal  $x \in \text{satLit}(A, \mathbf{C})$ , and let  $x = \langle a, b \rangle$ . We know that the clause  $C_a$  contains the literal  $x$ . Now, either zero, or one, or two of the remaining literals in  $C_a$  are satisfied by  $A$ . So  $x$  must be in either  $F_1(a)$  or in  $F_2(a)$  or in  $F_3(a)$ , respectively. Item (ii) is easy to prove by the definition of the  $F_i$ 's. We omit the details. ■<sub>Claim</sub>

**Claim 5.6** For any  $i = 1, 2, 3$ ,  $\text{numones}(\text{Img}(F_i)) = i \cdot \text{numones}(B_i)$ .

**Proof of claim:** Fix some  $i = 1, 2, 3$ . We prove the claim by induction on the number of clauses  $j < m$  (we can consider the sets  $B_i$  and the functions  $F_i$  having an additional parameter that determines until which clause to build the sets. That is,  $B_i(z)$  is the set of clauses from 0 to  $z$  that have  $i$  literals satisfied by  $A$ ; and similarly we add a parameter for the  $F_i$ 's). In the base case  $j = 0$  there is only one clause  $C_0$ . Depending on  $A$  we know how many literals in  $C_0$  are satisfied by  $A$ .

And so  $0 \in B_i$  iff  $i$  literals are satisfied by  $A$  in  $C_0$  iff  $\text{numones}(F_i(0)) = i = i \cdot 1 = i \cdot \text{numones}(B_i)$ . The induction step is similar and we omit the details.  $\blacksquare$ Claim

By Claim 5.5 and Claim 5.6 we get:

$$\begin{aligned} \text{numones}(\text{satLit}(A, \mathbf{C})) &= \sum_{i=1,2,3} \text{numones}(\text{Img}(F_i)) \\ &= \sum_{i=1,2,3} i \cdot \text{numones}(B_i). \end{aligned} \quad (30)$$

It is easy to show (in a similar manner to Claim 5.5) that  $B_1 \cup B_2 \cup B_3 = \{0, \dots, m-1\}$  and  $B_i \cap B_j = \emptyset$ , for any  $1 \leq i \neq j \leq 3$ . From this, using Proposition 3.17, we get that  $m = \text{numones}(B_1) + \text{numones}(B_2) + \text{numones}(B_3)$ , and so:

$$\text{numones}(B_1) = m - \text{numones}(B_2) - \text{numones}(B_3). \quad (31)$$

Thus, by (30):

$$\begin{aligned} \text{numones}(\text{satLit}(A, \mathbf{C})) &= m - \text{numones}(B_2) - \text{numones}(B_3) + 2 \cdot \text{numones}(B_2) + 3 \cdot \text{numones}(B_3) \\ &= m + 2 \cdot \text{numones}(B_3) + \text{numones}(B_2), \end{aligned}$$

and so

$$\text{numones}(B_2) = \text{numones}(\text{satLit}(A, \mathbf{C})) - m - 2 \cdot \text{numones}(B_3). \quad (32)$$

The set of clauses in  $\mathbf{C}$  that are NAE satisfied by  $A$  (i.e.,  $\text{satNAE}(A, \mathbf{C})$ ) is equal to the set of clauses having either one or two literals satisfied by  $A$ ; the latter two sets are just  $B_1$  and  $B_2$ , and since they are (provably in  $\mathbf{VTC}^0$ ) disjoint we have (using also (31)):

$$\text{numones}(B_3) = m - (\text{numones}(B_1) + \text{numones}(B_2)) = m - \text{numones}(\text{satNAE}(A, \mathbf{C})).$$

Plugging this into (32), and using Lemma 5.2, we get:

$$\begin{aligned} \text{numones}(B_2) &= \text{numones}(\text{satLit}(A, \mathbf{C})) - 3m + 2 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})) \\ &\leq \frac{3m + I}{2} - 3m + 2 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})). \end{aligned}$$

This concludes the proof of Lemma 5.4  $\blacksquare$

The following lemma provides an upper bound on the number of clauses in  $\mathbf{C}$  that can be satisfied as NAE by the assignment  $A$ .

**Lemma 5.7** (*Assuming the premise of the main formula*) the theory  $\mathbf{VTC}^0$  proves:

$$\text{numones}(\text{satNAE}(A, \mathbf{C})) \leq (n\lambda + 3m)/4 + o(1).$$

The proof of this lemma involves a spectral argument. Carrying out this argument in the theory is fairly difficult because one has to work with rational approximations (as the eigenvalues and eigenvectors might be irrationals, and so undefined in the theory) and further the proof must be sufficiently constructive, in the sense that it would fit in the theory  $\mathbf{VTC}^0$ . We thus defer to a separate section (Section 6) all treatment of the spectral argument. Given the desired spectral inequality, we can prove Lemma 5.7—this is done in Section 5.2.

We can now finish the proof of the key theorem:

**Concluding the proof of the theorem (Theorem 5.1).** In  $VTC^0$  (and assuming the premise of the main formula), let  $h$  be the number of clauses in  $\mathbf{C}$  that contain exactly two literals satisfied by  $A$ . We have:

$$\begin{aligned}
h &\leq \frac{3m + I}{2} - 3m + 2 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})) && \text{(by Lemma 5.4)} \\
&\leq \frac{3m + I}{2} - 3m + \frac{3m + \lambda n}{2} + o(1) && \text{(by Lemma 5.7)} \\
&= \frac{I + \lambda n}{2} + o(1). && (33)
\end{aligned}$$

Since we assumed that  $A$  satisfies  $\mathbf{C}$ , then every clause in  $\mathbf{C}$  has at least one literal satisfied by  $A$ . Thus, the clauses in  $\mathbf{C}$  that are not satisfied as 3XOR by  $A$  are precisely the clauses that have exactly two literals satisfied by  $A$ . By (33), the number of clauses that have exactly two literals satisfied by  $A$  is at most  $\frac{I + \lambda n}{2} + o(1)$ . We now use Lemma 5.9 (proved in the next subsection) to prove the following lemma:

**Lemma 5.8** (*Assuming the premise of the main formula*) the theory  $VTC^0$  proves that the number of clauses in  $\mathbf{C}$  that are not satisfied as 3XOR by  $A$  is at least  $\lceil t/d \rceil$ .

**Proof:** Consider the collection  $\text{COLL}(t, k, d, \mathbf{C}, \mathcal{D})$  in the premise of the main formula. Then,  $\mathcal{D}$  is a sequence of  $t$  inconsistent  $k$ -tuples from  $\mathbf{C}$ , and every pair of  $k$ -tuples in  $\mathcal{D}$  intersect<sup>6</sup> on at most  $d$  clauses from  $\mathbf{C}$ . By Lemma 5.9, each of the  $t$  inconsistent  $k$ -tuples contains a clause which is unsatisfied as 3XOR by  $A$ . Since each such clause may appear in at most  $d$  other inconsistent  $k$  tuples, using Proposition 3.20 the theory  $VTC^0$  proves that the total number of distinct clauses not satisfied as 3XOR by  $A$  is at least  $\lceil t/d \rceil$ . ■

Using this Lemma, we can finish the proof of the key Theorem 5.1, as follows: by Lemma 5.8 and the fact that the number of clauses in  $\mathbf{C}$  that are not satisfied as 3XOR by  $A$  is at most  $\frac{I + \lambda n}{2} + o(1)$ , we get

$$t = d \cdot \frac{t}{d} \leq d \cdot \left\lceil \frac{t}{d} \right\rceil \leq d \cdot \frac{I + \lambda n}{2} + o(1), \quad (34)$$

which contradicts our assumption (in the main formula) that  $t > \frac{d(I + \lambda n)}{2} + o(1)$ . Formally, we need to take care here for the “ $o(1)$ ” notation. Recall that  $o(1)$  stands for a term  $b/n^c$  for some constants number term  $b$  and a constant  $c$ . Therefore, it is enough to require that if our assumption (in the premise of the main formula) is  $t > \frac{d(I + \lambda n)}{2} + b/n^c$ , then in (34) above we have  $t \leq d \cdot \left\lceil \frac{t}{d} \right\rceil \leq d \cdot \frac{I + \lambda n}{2} + b'/n^{c'}$ , so that  $b/n^c \leq b'/n^{c'}$ . (This requirement will be easily satisfied when applying our theorem (see Corollary 7.3).) ■

## 5.1 Formulas satisfied as 3XOR

Here we prove the missing lemma that was used in the proof of Lemma 5.8.

**Notation:** For a sequence  $S$  of  $k$  many 3-clauses, and for  $0 \leq \alpha < k$ , we denote the three variables in the clause  $S[\alpha]$  by  $x_{i_\alpha}, x_{j_\alpha}, x_{h_\alpha}$ , and abbreviate  $\langle\langle S[\alpha] \rangle\rangle_4^5 \rangle_t^3$ , which is the polarity of the  $t$ th variable

<sup>6</sup>Where a clause is identified with its index  $0, \dots, m - 1$  in  $\mathbf{C}$ , so that two identical clauses with a different index are considered as two different clauses.

in  $S[\alpha]$ , by  $\ell_t^\alpha$ , for  $t = 1, 2, 3$ . Thus,  $x_i^{\ell_1^\alpha}, x_j^{\ell_2^\alpha}, x_h^{\ell_3^\alpha}$ , are the three literals in  $S[\alpha]$  and the values of  $\neg A(i) \oplus \ell_1^\alpha, \neg A(j) \oplus \ell_2^\alpha, \neg A(h) \oplus \ell_3^\alpha$  are the values that  $A$  assigns to  $x_i^{\ell_1^\alpha}, x_j^{\ell_2^\alpha}, x_h^{\ell_3^\alpha}$ , respectively, where  $\oplus$  is the XOR operator. We also abuse notation and write  $\neg A(i)$  inside a term to mean the *characteristic function* of the predicate  $\neg A(i)$ , that is, the function that returns 1 if  $\neg A(i)$  is true, and 0 otherwise.

For a clause  $C$  and an assignment  $A$  the predicate  $3\text{XOR}(C, A)$  says that  $A$  satisfies exactly one or three of the literals in  $C$ . If we denote by  $x_i, x_j, x_h$  the three variables in  $C$  and by  $\ell_1, \ell_2, \ell_3$  their respective polarities, we have:

$$3\text{XOR}(C, A) \quad \text{iff} \quad \neg A(i) \oplus \ell_1 + \neg A(j) \oplus \ell_2 + \neg A(h) \oplus \ell_3 = 1 \pmod{2},$$

and formally the predicate  $3\text{XOR}$  is  $\Sigma_0^B$ -definable by the following formula:

$$3\text{XOR}(C, A) := \text{ODD}(\neg A(i) + \ell_1 + \neg A(j) + \ell_2 + \neg A(h) + \ell_3).$$

**Lemma 5.9** *The theory  $\mathbf{VTC}^0$  proves that if  $S$  is an inconsistent (even)  $k$ -tuple, then for every assignment  $A$  to its variables there exists  $\alpha \leq k$  such that  $A$  satisfies exactly zero or exactly two literals in the clause  $S[\alpha]$ . More formally,  $\mathbf{VTC}^0$  proves:*

$$\forall A \leq n \forall k \leq n \forall S \leq p(n) \exists \alpha < k (|A| = n \wedge \text{ITPL}(S, k) \rightarrow \neg 3\text{XOR}(S[\alpha], A)),$$

for some (polynomial) term  $p(\cdot)$ .

**Proof:** We need the following claim:

**Claim 5.10** *Let  $f(y)$  be a number function definable in  $\mathbf{VTC}^0$ . Then  $\mathbf{VTC}^0$  proves the following statements:*

1.  $(\forall \alpha < k, \text{ODD}(f(\alpha))) \wedge \text{EVEN}(k) \rightarrow \text{EVEN}\left(\sum_{\alpha=0}^{k-1} f(\alpha)\right);$
2.  $(\forall \alpha < k, \text{EVEN}(f(\alpha))) \rightarrow \text{EVEN}\left(\sum_{\alpha=0}^{k-1} f(\alpha)\right);$
3.  $(\forall \alpha < k, \text{ODD}(f(\alpha))) \wedge \text{ODD}(k) \rightarrow \text{ODD}\left(\sum_{\alpha=0}^{k-1} f(\alpha)\right).$

**Proof of claim:** Consider Item 1 (the other items are similar). The proof is by induction on  $k$ , showing that

$$((\forall \alpha < k \exists y(2y + 1 = f(\alpha))) \wedge \exists y(2y = k)) \rightarrow \exists y \sum_{\alpha=0}^{k-1} f(\alpha) = 2y,$$

and using the fact that  $\mathbf{V}^0$  proves that  $\text{ODD}(x) \leftrightarrow \exists y \leq x(2y + 1 = x)$  (e.g., by induction on  $x$ ). We omit the details.  $\blacksquare_{\text{Claim}}$

Now, assume by way of contradiction that  $A$  satisfies all the clauses in  $S$  as  $3\text{XOR}$ s. Thus, for any  $\alpha < k$ , if we define  $f(\alpha) := \neg A(i_\alpha) + \ell_1^\alpha + \neg A(j_\alpha) + \ell_2^\alpha + \neg A(h_\alpha) + \ell_3^\alpha$ , then  $\text{ODD}(f(\alpha))$ . Hence, because  $\text{EVEN}(k)$ , by Claim 5.10 we can prove that:

$$\sum_{\alpha=0}^{k-1} (\neg A(i_\alpha) \oplus \ell_1^\alpha + \neg A(j_\alpha) \oplus \ell_2^\alpha + \neg A(h_\alpha) \oplus \ell_3^\alpha) = 0 \pmod{2}. \quad (35)$$

Recall that every variable appears an even number of times in  $S$ . Thus, if a variable has an odd number of negative appearances then it also has an odd number of positive appearances. Similarly, if a variable has an even number of negative appearances then it also has an even number of positive appearances. Let  $I_0 \in \{0, \dots, n-1\}$  be the indices of variables having an even number of positive (and thus negative) appearances in  $S$  and let  $I_1 = \{0, \dots, n-1\} \setminus I_0$  be the indices of variables having an odd number of positive (and thus negative) appearances in  $S$ . Thus, the left hand side of (35), can be written as follows (for  $\varepsilon = 0, 1$ , we denote by  $x_i^\varepsilon(A)$  the truth value of the literal  $x_i^\varepsilon$  under  $A$ ):

$$\begin{aligned} & \sum_{i \in I_0} \left( \underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{even times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{even times}} \right) + \\ & \sum_{i \in I_1} \left( \underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{odd times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{odd times}} \right). \end{aligned} \tag{36}$$

**Claim 5.11** *For any  $i \in I_0$  (and any string variable  $A$  of size  $n$ ) the theory  $\mathbf{VTC}^0$  proves that*

$$\underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{even times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{even times}}$$

*is an even number.*

**Proof of claim:** Reason in  $\mathbf{VTC}^0$  as follows: assume that  $A(i) = 0$ . Then  $x_i^1(A) = 0$  and  $x_i^0(A) = 1$  and so by Claim 5.10 the sum of evenly many  $x_i^1(A)$ 's is even and the sum of evenly many  $x_i^0(A)$ 's is also even. The sum of two even numbers is even, and so we are done. (The case where  $A(i) = 1$  is similar.) ■**Claim**

By Claims 5.10 and 5.11, the theory  $\mathbf{VTC}^0$  proves

$$\text{EVEN} \left( \sum_{i \in I_0} \left( \underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{even times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{even times}} \right) \right). \tag{37}$$

Similarly to the above claims we have:

**Claim 5.12** *For any  $i \in I_1$  (and any string variable  $A$  of size  $n$ ) the theory  $\mathbf{VTC}^0$  proves that*

$$\underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{odd times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{odd times}}$$

*is an odd number.*

Since by assumption  $S$  is an inconsistent  $k$ -tuple, the number of negative literals is odd (Definition 4.2), and so (provably in  $\mathbf{VTC}^0$ ) the number of variables that has an odd number of negative appearances must be odd, in other words,  $|I_1|$  is odd. Therefore, by Claims 5.12 and 5.10,  $\mathbf{VTC}^0$  proves:

$$\text{ODD} \left( \sum_{i \in I_1} \left( \underbrace{x_i^1(A) + \dots + x_i^1(A)}_{\text{odd times}} + \underbrace{x_i^0(A) + \dots + x_i^0(A)}_{\text{odd times}} \right) \right). \quad (38)$$

Since  $\mathbf{VTC}^0$  proves both (37) and (38),  $\mathbf{VTC}^0$  proves that (36) is odd, which contradicts (35). This implies that not all the clauses in  $S$  are satisfied as 3XOR by the assignment  $A$ .  $\blacksquare$

## 5.2 Bounding the number of NAE satisfying assignments

Here we prove Lemma 5.7 used to prove the key theorem (Theorem 5.1). Recall that  $\text{satNAE}(A, \mathbf{C})$  is the string function that outputs the set of clauses in  $\mathbf{C}$  that are satisfied as NAE by  $A$  (see Section 4). The proof of the following lemma is based on the spectral inequality proved in Section 6.

**Lemma 5.7** (*Assuming the premise of the main formula*)  $\mathbf{VTC}^0$  proves

$$\text{numones}(\text{satNAE}(A, \mathbf{C})) \leq (n\lambda + 3m)/4 + o(1).$$

**Proof:** Let  $\mathbf{a}$  be a vector from  $\{-1, 1\}^n$  such that  $\mathbf{a}(i) = 2A(i) - 1$ . Thus,  $\mathbf{a}(i) = 1$  if  $A(i) = 1$  and  $\mathbf{a}(i) = -1$  if  $A(i) = 0$ . We can prove in  $\mathbf{VTC}^0$  (by definition of inner products and a product of a matrix and a vector—*innerprod* and *Matvecprod* function symbols, respectively, as defined in Section 3.2.2) the following:

$$\mathbf{a}^t M \mathbf{a} = \sum_{i=1}^n \sum_{j=1}^n M_{ij} \mathbf{a}(i) \mathbf{a}(j). \quad (39)$$

By assumption  $\text{MAT}(M, \mathbf{C})$  holds (see Definition 4.5) and so by definition 4.5 and by (39) we can prove in  $\mathbf{VTC}^0$  that:

$$\mathbf{a}^t M \mathbf{a} = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=0}^{m-1} E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j), \quad (40)$$

where  $E_{ij}^{(k)}$ , for any  $i, j \in [n]$ , is:

$$E_{ij}^{(k)} := \begin{cases} +\frac{1}{2}, & x_i^{\varepsilon_i}, x_j^{\varepsilon_j} \in \mathbf{C}[k] \text{ and } \varepsilon_i \neq \varepsilon_j, \text{ for some } \varepsilon_i, \varepsilon_j \in \{0, 1\} \text{ and } i \neq j; \\ -\frac{1}{2}, & x_i^{\varepsilon_i}, x_j^{\varepsilon_j} \in \mathbf{C}[k] \text{ and } \varepsilon_i = \varepsilon_j, \text{ for some } \varepsilon_i, \varepsilon_j \in \{0, 1\} \text{ and } i \neq j; \\ 0, & \text{otherwise.} \end{cases} \quad (41)$$

By rearranging (40) we get

$$\mathbf{a}^t M \mathbf{a} = \sum_{k=0}^{m-1} \sum_{i=1}^n \sum_{j=1}^n E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j),$$



and since  $E_{ij}^{(k)} = 0$  whenever either  $x_i \notin \mathbf{C}[k]$  or  $x_j \notin \mathbf{C}[k]$ , we get

$$= \sum_{k=1}^{m-1} \sum_{i,j \in \{r : x_r \in \mathbf{C}[k]\}} E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j),$$

and further, since  $E_{ij}^{(k)} = 0$  if  $i = j$ , and  $E_{ij}^{(k)} = E_{ji}^{(k)}$ , for any  $i, j$ , we have

$$= \sum_{k=0}^{m-1} \sum_{i < j \in \{r : x_r \in \mathbf{C}[k]\}} 2E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j). \quad (42)$$

**Claim 5.13** *The theory  $\mathbf{VTC}^0$  (in fact already  $\mathbf{V}^0$ ) proves that for any  $k = 0, \dots, m-1$ :*

$$\sum_{i < j \in \{r : x_r \in \mathbf{C}[k]\}} 2E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j) = \begin{cases} +1, & \text{NAE}(\mathbf{C}[k], A); \\ -3, & \text{-NAE}(\mathbf{C}[k], A). \end{cases}$$

**Proof of claim:** For any  $i < j \in \{r : x_r \in \mathbf{C}[k]\}$ , if  $A(i) \neq A(j)$  (which means that  $\mathbf{a}(i) \neq \mathbf{a}(j)$ ) then  $\mathbf{a}(i) \mathbf{a}(j) = -1$ , and if  $A(i) = A(j)$  (which means that  $\mathbf{a}(i) = \mathbf{a}(j)$ ) then  $\mathbf{a}(i) \mathbf{a}(j) = 1$ . Thus, by (41), For any  $i < j \in \{r : x_r \in \mathbf{C}[k]\}$ :

$$E_{ij}^{(k)} = \begin{cases} +\frac{1}{2}, & \text{if } x_i^{\varepsilon_i} \neq x_j^{\varepsilon_j} \text{ under } \mathbf{a}; \\ -\frac{1}{2}, & \text{if } x_i^{\varepsilon_i} = x_j^{\varepsilon_j} \text{ under } \mathbf{a}. \end{cases} \quad (43)$$

Note that if  $\text{NAE}(\mathbf{C}[k], A)$  is true then there are exactly two pairs of literals  $x_i^{\varepsilon_i}, x_j^{\varepsilon_j}$ ,  $i < j$ , for which  $x_i^{\varepsilon_i}$  and  $x_j^{\varepsilon_j}$  get different values under the assignment  $\mathbf{a}$  (if  $A$  assigns 1 (i.e.,  $\top$ ) to one literal and 0 (i.e.,  $\perp$ ) to the other two literals, then two pairs have different values and one pair has the same value; and similarly if  $A$  assigns 0 to one literal and 1 to the other two literals). Therefore, if  $\text{NAE}(\mathbf{C}[k], A)$  is true then

$$\sum_{i < j \in \{r : x_r \in \mathbf{C}[k]\}} 2E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j) = 2 \left( \frac{1}{2} + \frac{1}{2} - \frac{1}{2} \right) = 1.$$

On the other hand, if  $\text{NAE}(\mathbf{C}[k], A)$  is false then all pairs of literals  $x_i^{\varepsilon_i}, x_j^{\varepsilon_j}$ ,  $i < j$ , get the same value under the assignment  $A$ , and so:

$$\sum_{i < j \in \{r : x_r \in \mathbf{C}[k]\}} 2E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j) = 2 \left( -\frac{1}{2} - \frac{1}{2} - \frac{1}{2} \right) = -3.$$

■ Claim

Let  $Z = \{i < m : \text{NAE}(\mathbf{C}[i], A)\}$  (note that  $Z = \text{satNAE}(A, \mathbf{C})$ ), and for any  $k = 0, \dots, m-1$ , let  $\gamma_k = \sum_{i < j \in \{r : x_r \in \mathbf{C}[k]\}} 2E_{ij}^{(k)} \mathbf{a}(i) \mathbf{a}(j)$ . Then, by Claim 5.13 and Proposition 3.19:

$$\begin{aligned} \sum_{i=0}^{m-1} \gamma_i &= 1 \cdot \text{numones}(Z) - 3 \cdot (m - \text{numones}(Z)) \\ &= 4 \cdot \text{numones}(Z) - 3m \\ &= 4 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})) - 3m. \end{aligned} \quad (44)$$

By (42) we have

$$\sum_{i=0}^{m-1} \gamma_i = \mathbf{a}^t M \mathbf{a}, \quad (45)$$

and by the spectral inequality proved in Lemma 6.7 in the next section, we have:

$$\mathbf{a}^t M \mathbf{a} \leq \lambda n + o(1).$$

By (44) we thus get

$$4 \cdot \text{numones}(\text{satNAE}(A, \mathbf{C})) - 3m \leq \lambda n + o(1),$$

which leads to

$$\text{numones}(\text{satNAE}(A, \mathbf{C})) \leq \frac{\lambda n + 3m}{4} + o(1).$$

■

## 6 The spectral bound

In this section we show how to prove inside  $\mathbf{VTC}^0$  the desired spectral inequality, used in the proof of the key theorem (Theorem 5.1; specifically, it was used in Lemma 5.7 in Section 5.2).

Since the original matrix associated to a 3CNF is a real symmetric matrix, and its eigenvectors and eigenvalues also might be real, and thus cannot be represented in our theory  $\mathbf{VTC}^0$ , we shall need to work with *rational approximations* of real numbers. We will work with polynomially small approximations. Specifically, a real number  $r$  in the real interval  $[-1, 1]$  is represented with precision  $1/n^c$ , where  $n$  is the number of variables in the 3CNF and  $c$  is a constant natural number independent of  $n$  (that is, if  $\tilde{r}$  is the approximation of  $r$ , we shall have  $|r - \tilde{r}| \leq 1/n^c$ ). Recall that we will assume that all rational numbers have in fact the same denominator  $n^{2c}$  for some specific global constant  $c$  (see the Preliminaries, Section 3.1.2 on this).

**Idea of proving the eigenvalue bound in  $\mathbf{VTC}^0$ .** We explain here informally how we proceed to prove the eigenvalue bound  $\mathbf{a}^t M \mathbf{a} \leq \lambda n$ , for any  $\mathbf{a} \in \{-1, 1\}^n$ , in the theory  $\mathbf{VTC}^0$ , assuming that  $\text{MAT}(M, \mathbf{C})$  and  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  hold (Lemma 6.7). The idea of the proof of this inequality is as follows: in the predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  we certify that the rows of a given matrix  $V$  are rational approximations of the normalized eigenvector basis of  $M$ . Since  $M$  is symmetric and real,  $V$  will approximate an orthonormal matrix, and  $V^t$  will *approximate*  $V^{-1}$  (this is where we circumvent the need to prove the correctness of inverting a matrix in the theory  $\mathbf{VTC}^0$ ). Thus,  $V^{-1}$  approximates the matrix of the basis transformation from the standard basis to the eigenvector basis. Note that  $\mathbf{a}$  (as a  $\{-1, 1\}$  vector) is already almost described in the standard basis. Hence, it will be possible to prove in the theory that  $V^t \mathbf{a}$  is the representation of  $\mathbf{a}$  in the (approximate) eigenvector basis, i.e., we shall have an equality  $\mathbf{a} = \sum_{i=1}^n \gamma_i \mathbf{v}_i + o(1)$ , for  $\mathbf{v}_i$ 's the approximate eigenvectors of  $M$  and rationals  $\gamma_i$ 's. After plugging-in this equality in  $\mathbf{a}^t M \mathbf{a}$ , to prove (54) we only need to *validate computations*—using also the fact that we know the inequalities  $M \mathbf{v}_i \leq \lambda \mathbf{v}_i + o(1)$ , for any  $i \in [n]$  (since this will be witnessed in the predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  as well).

## 6.1 Notations

Here we collect the notation we use in this section. We denote by  $e_1, \dots, e_n$  the standard basis vectors spanning  $\mathbb{Q}^n$ . That is, for any  $1 \leq i \leq n$  the vector  $e_i \in \mathbb{Q}^n$  is 1 in the  $i$ th coordinate and all other coordinates are 0. For a vector  $\mathbf{v}$  we denote by  $\mathbf{v}(j)$  the  $j$ th entry in  $\mathbf{v}$ . Given a real symmetric matrix  $M$  we denote by  $\mathbf{u}_1, \dots, \mathbf{u}_n \in \mathbb{R}^n$  the normalized eigenvectors of  $M$ . It is known that the collection of normalized eigenvectors of a symmetric  $n \times n$  real matrix  $M$  forms an orthonormal basis for  $\mathbb{R}^n$ , called *the eigenvector basis of  $M$*  (cf. [24]). The (rational) approximation of the eigenvectors will be denoted  $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{Q}^n$  and we define  $v_{ij} := \mathbf{v}_i(j)$ . Recall that for a real or rational vector  $v = (v_1, \dots, v_n)$  we denote by  $\|v\|^2$  the squared Euclidean norm of  $v$ , that is,  $\|v\|^2 = v_1^2 + \dots + v_n^2$ . We also define  $\|\mathbf{v}\|_\infty := \max\{v_i : 1 \leq i \leq n\}$ .

## 6.2 Rational approximations of real numbers, vectors and matrices

**Definition 6.1 (Rational  $\varepsilon$ -approximation of a real number)** For  $r \in \mathbb{R}$ , we say that  $q \in \mathbb{Q}$  is a rational  $\varepsilon$ -approximation of  $r$  (or just  $\varepsilon$ -approximation), if  $|r - q| \leq \varepsilon$ .

**Claim 6.2** For any real number  $r \in [-1, 1]$  and any natural number  $m$  there exists a  $1/m$ -approximation of  $r$  whose numerator and denominator have values linearly bounded in  $m$ .

**Proof of claim:** By assumption, there exists an integer  $0 \leq k < 2m$ , such that  $r \in [-1 + \frac{k}{m}, -1 + \frac{k+1}{m}]$ . Then  $-1 + \frac{k}{m}$  is a rational  $1/m$ -approximation of  $r$ .  $\blacksquare$ Claim

In a similar fashion we have:

**Definition 6.3 (Rational  $\varepsilon$ -approximation of (sets of) real vectors)** Let  $0 < \varepsilon < 1$ . For  $\mathbf{u} \in \mathbb{R}^n$ , we say that  $\mathbf{v} \in \mathbb{Q}^n$  is an  $\varepsilon$ -approximation of  $\mathbf{u}$ , if  $\mathbf{v}(i)$  is an  $\varepsilon$ -approximation of  $\mathbf{u}(i)$ , for all  $i = 1, \dots, n$ . Accordingly, for a set  $U = \{\mathbf{u}_1, \dots, \mathbf{u}_k\} \subseteq \mathbb{R}^n$ , we say that  $V = \{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subseteq \mathbb{Q}^n$  is a (rational)  $\varepsilon$ -approximation of  $U$  if every  $\mathbf{v}_i \in \mathbb{Q}^n$  is an  $\varepsilon$ -approximation of the vector  $\mathbf{u}_i$ ,  $i = 1, \dots, k$ .

## 6.3 The predicate EigValBound

We define the predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  which is meant to express the properties needed for the main proof. Basically,  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  expresses the fact that  $V$  is a rational  $1/n^c$ -approximation (Definition 6.3) of the eigenvector basis of  $M$ , whose  $1/n^c$ -approximate eigenvalues (in decreasing order with respect to value) are  $\vec{\lambda}$ , for a sufficiently large constant  $c \in \mathbb{N}$ .

**Note:** For a number or a number term in the language, we sometimes use  $|t|$  to denote the absolute value of  $t$ . This should not be confused with the length  $|T|$  of a string term  $T$ .

**Definition 6.4 (EigValBound predicate)** The predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  is a  $\Sigma_0^B$ -definable relation in  $\mathbf{VTC}^0$  that holds (in the standard two-sorted model) iff all the following properties hold (where  $c \in \mathbb{N}$  is a sufficiently large global constant):

1.  $V$  is a sequence of  $n$  vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{Q}^n$  with polynomially small entries. That is, for any  $1 \leq i, j \leq n$ , the rational number

$$v_{ij} := \mathbf{v}_i(j) \in \mathbb{Q}$$

is polynomial in  $n$  (meaning that both its denominator and numerator are polynomially bounded in  $n$ ).

2. For any  $1 \leq i, j \leq n$  it holds that the absolute value  $|v_{ij}| \leq 2$ .
3. For any  $1 \leq i \leq n$ , define:

$$\tilde{e}_i := \sum_{j=1}^n v_{ij} \cdot \mathbf{v}_j.$$

Then, there exists  $\mathbf{r}_i \in \mathbb{Q}^n$  for which

$$\tilde{e}_i = e_i + \mathbf{r}_i \quad \text{and} \quad \|\mathbf{r}_i\|_\infty = O(1/n^{c-1}).$$

To formalize the existence of such an  $\mathbf{r}_i$  we do not use an existential second-sort quantifier here; instead, we simply assert that for any  $\ell = 1, \dots, n$ :

$$|\tilde{e}_i(\ell) - e_i(\ell)| = O(1/n^{c-1}).$$

4. The vectors in  $V$  are “almost” orthonormal, in the following sense:

$$\begin{aligned} \langle \mathbf{v}_i, \mathbf{v}_j \rangle &= O(1/n^{c-1}), & \text{for all } 1 \leq i \neq j \leq n, \\ \langle \mathbf{v}_i, \mathbf{v}_i \rangle &= 1 + O(1/n^{c-1}), & \text{for all } 1 \leq i \leq n. \end{aligned}$$

5. The parameter  $\vec{\lambda}$  is a sequence  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  of rational numbers such that for every  $1 \leq i \leq n$ , there exists a vector  $\mathbf{t}_i \in \mathbb{Q}^n$  for which  $\|\mathbf{t}_i\|_\infty = O(1/n^{c-3})$ , and

$$M\mathbf{v}_i = \lambda_i \mathbf{v}_i + \mathbf{t}_i.$$

(Similar to Item 3 above, we do not use an existential second-sort quantifier for  $\mathbf{t}_i$  here.)

It should be easy to check that  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  is a  $\Sigma_0^B$ -definable relation in  $\mathbf{VTC}^0$ .

Now we show that there exist objects  $M, \vec{\lambda}, V$  that satisfy the predicate  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$ .

**Proposition 6.5 (Suitable approximations of eigenvector bases exist)** *Let  $M$  be an  $n \times n$  real symmetric matrix whose entries are quadratic in  $n$ . Let  $U = \{\mathbf{u}_1, \dots, \mathbf{u}_n\} \subseteq \mathbb{R}^n$  be the orthonormal basis consisting of the eigenvectors of  $M$ , let  $c \in \mathbb{N}$  be positive and constant (independent of  $n$ ). If  $V = \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq \mathbb{Q}^n$  is an  $1/n^c$ -approximation of  $U$  (Definition 6.3),  $\vec{\lambda} = \{\lambda_1, \dots, \lambda_n\}$  is the collection of rational  $1/n^c$ -approximations of the real eigenvalues of  $M$  such that  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ , then  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  holds (as before, the predicate holds in the standard two-sorted model, for the appropriate encodings of its parameters).<sup>7</sup>*

**Proof:** Let  $u_{ij}$  be an abbreviation of  $\mathbf{u}_i(j)$ , that is, the  $j$ th element in the vector  $\mathbf{u}_i$ , and similarly for  $v_{ij}$ . We proceed by checking each of the conditions in Definition 6.4.

<sup>7</sup>This is an existence statement. We do not claim that the statement of the proposition is provable in the theory (although some of the computations can be carried out inside the theory).

**Condition (1):** Holds by the definition of an approximation of a real vector and by Claim 6.2, stating that the  $\varepsilon$ -approximation of a real number in  $[-1, 1]$  is a rational number whose both denominator and numerator are of value  $O(n^c)$ .

**Condition (2):** Since  $v_{ij}$  is a rational  $1/n^c$ -approximation of  $u_{ij}$ , and  $|u_{ij}| \leq 1$  (because  $\|\mathbf{u}_i\| = 1$ ) for any  $1 \leq i, j \leq n$ , we have  $|v_{ij}| \leq 2$ .

**Condition (3):** By orthonormality of the real matrix  $U$ , we have that  $U^t = U^{-1}$ , that is:

$$\sum_{i=1}^n u_{ij} \mathbf{u}_i = e_j, \text{ for any } j = 1, \dots, n, \quad (46)$$

By assumption, for any  $1 \leq i \leq n$  there exists  $\mathbf{s}_i = (s_{i1}, \dots, s_{in}) \in \mathbb{R}^n$  such that  $\|\mathbf{s}_i\|_\infty \leq 1/n^c$  and  $\mathbf{v}_i = \mathbf{u}_i + \mathbf{s}_i$ . Therefore, for any  $1 \leq j \leq n$ , we have:

$$\begin{aligned} \tilde{e}_j &:= \sum_{i=1}^n v_{ij} \mathbf{v}_i = \sum_{i=1}^n (u_{ij} + s_{ij}) \cdot (\mathbf{u}_i + \mathbf{s}_i) \\ &= \underbrace{\sum_{i=1}^n u_{ij} \mathbf{u}_i}_{=e_j \text{ by (46)}} + \sum_{i=1}^n u_{ij} \mathbf{s}_i + \sum_{i=1}^n s_{ij} \cdot (\mathbf{u}_i + \mathbf{s}_i). \end{aligned} \quad (47)$$

We define

$$\mathbf{r}_j := \sum_{i=1}^n u_{ij} \mathbf{s}_i + \sum_{i=1}^n s_{ij} \cdot (\mathbf{u}_i + \mathbf{s}_i),$$

which gives us

$$\tilde{e}_j = e_j + \mathbf{r}_j.$$

Note that since  $\sum_{i=1}^n v_{ij} \mathbf{v}_i = \tilde{e}_j$  is a rational vector then  $\mathbf{r}_j$  is also a rational vector.

It remains to show that  $\|\mathbf{r}_j\|_\infty = O(1/n^{c-1})$ . Since  $1 = \|\mathbf{u}_i\|^2 = \sum_{j=1}^n u_{ij}^2$ , we have  $|u_{ij}| \leq 1$ . By this, and by the fact that  $\|\mathbf{s}_i\|_\infty \leq 1/n^c$ , we get  $\|\sum_{i=1}^n u_{ij} \mathbf{s}_i\|_\infty = O(1/n^{c-1})$ , and  $\|\sum_{i=1}^n s_{ij} \cdot (\mathbf{u}_i + \mathbf{s}_i)\|_\infty = O(1/n^{c-1})$ . This means that  $\|\mathbf{r}_j\|_\infty = O(1/n^{c-1})$ .

**Condition (4):** This is similar to the proof of Condition (3). By assumption, for any  $1 \leq i \leq n$  there exists  $\mathbf{s}_i = (s_{i1}, \dots, s_{in}) \in \mathbb{R}^n$  such that  $\|\mathbf{s}_i\|_\infty \leq 1/n^c$ , and  $\mathbf{v}_i = \mathbf{u}_i + \mathbf{s}_i$ . Thus, we have

$$\begin{aligned} \langle \mathbf{v}_i, \mathbf{v}_j \rangle &= \langle \mathbf{u}_i + \mathbf{s}_i, \mathbf{u}_j + \mathbf{s}_j \rangle \\ &= \langle \mathbf{u}_i, \mathbf{u}_j \rangle + \langle \mathbf{s}_i, \mathbf{u}_j + \mathbf{s}_j \rangle + \langle \mathbf{u}_i, \mathbf{s}_j \rangle. \end{aligned} \quad (48)$$

The first term in (48) is 0 since  $U$  is an orthonormal basis, and the second and third terms in (48) are both  $O(1/n^{c-1})$  (by calculations similar to that in the proof of Condition (3)).

The proof of  $\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 1 + O(1/n^{c-1})$ , for all  $1 \leq i \leq n$ , is similar.

**Condition (5):** Similar to the proof of previous conditions, we define  $\mathbf{s}_i = (s_{i1}, \dots, s_{in}) \in \mathbb{R}^n$  such that  $\|\mathbf{s}_i\|_\infty \leq 1/n^c$ , and  $\mathbf{v}_i = \mathbf{u}_i + \mathbf{s}_i$ , for any  $1 \leq i \leq n$ . We have

$$\begin{aligned} M\mathbf{v}_i &= M(\mathbf{u}_i + \mathbf{s}_i) \\ &= M\mathbf{u}_i + M\mathbf{s}_i. \end{aligned} \tag{49}$$

Since  $\mathbf{u}_i \in \mathbb{R}^n$  is the eigenvector of  $M$  and  $\lambda_i$  is a  $1/n^c$ -approximation of the eigenvalue of  $\mathbf{u}_i$ , we have that (49) equals

$$(\lambda_i + \epsilon)\mathbf{u}_i + M\mathbf{s}_i \tag{50}$$

for some  $|\epsilon| \leq 1/n^c$ ,

$$\begin{aligned} &= \lambda_i\mathbf{u}_i + \epsilon\mathbf{u}_i + M\mathbf{s}_i \\ &= \lambda_i(\mathbf{v}_i - \mathbf{s}_i) + \epsilon\mathbf{u}_i + M\mathbf{s}_i \\ &= \lambda_i\mathbf{v}_i - \lambda_i\mathbf{s}_i + \epsilon\mathbf{u}_i + M\mathbf{s}_i. \end{aligned}$$

We put

$$\mathbf{t}_i := -\lambda_i\mathbf{s}_i + \epsilon\mathbf{u}_i + M\mathbf{s}_i.$$

It remains to show that  $\|\mathbf{t}_i\|_\infty = O(1/n^{c-3})$ .

**Claim 6.6** *For every  $1 \leq i \leq n$ ,  $\lambda_i = O(n^3)$ .*

**Proof of claim:** Since  $\|\mathbf{u}_i\|_\infty = 1$  and, by assumption, every entry in  $M$  is  $O(n^2)$ , we have:

$$\|M\mathbf{u}_i\|_\infty = O(n^3). \tag{51}$$

Observe that

$$M\mathbf{u}_i = (\lambda_i + \epsilon)\mathbf{u}_i = \lambda_i\mathbf{u}_i + \epsilon\mathbf{u}_i. \tag{52}$$

Because  $|\epsilon| \leq 1/n^c$  and  $\|\mathbf{u}_i\|_\infty = 1$ , we have  $\|\epsilon\mathbf{u}_i\|_\infty = O(1/n^c)$ . Therefore, by (51) and (52) we have  $\lambda_i = O(n^3)$ .  $\blacksquare$ Claim

We have  $\|\mathbf{s}_i\|_\infty \leq 1/n^c$ , and so by Claim 6.6 we get that  $\|-\lambda_i\mathbf{s}_i\|_\infty = O(1/n^{c-3})$ . Now,  $\|\epsilon\mathbf{u}_i\|_\infty = O(1/n^c)$  and since  $M$  has entries which are  $O(n^2)$  we have  $\|M\mathbf{s}_i\|_\infty = O(1/n^{c-3})$ . We conclude that

$$\begin{aligned} \|\mathbf{t}_i\|_\infty &= \|-\lambda_i\mathbf{s}_i + \epsilon\mathbf{u}_i + M\mathbf{s}_i\|_\infty \\ &\leq \|-\lambda_i\mathbf{s}_i\|_\infty + \|\epsilon\mathbf{u}_i\|_\infty + \|M\mathbf{s}_i\|_\infty \\ &= O(1/n^{c-3}). \end{aligned}$$

■

## 6.4 Certifying the matrix identity

In this section we show that the theory  $VTC^0$  can prove that, if  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  holds, then the desired eigenvalue inequality also holds.

**Note on coding and formalizing the proof in  $VTC^0$ :** In what follows we will write freely terms such as matrices, vectors, inner products, products of a matrix by a vector (of the appropriate dimensions), addition of vectors, and big sums. We also use freely basic properties of these objects; like transitivity of inequalities, distributivity of a product over big sums, associativity of addition and product, etc. We showed how to formalize these objects, and how to prove their basic properties within  $VTC^0$  in Sections 3.2.2 and 3.2.4 (see Proposition 3.22).

For an assignment  $A \in \{0, 1\}^n$  we define its associated vector  $\mathbf{a} \in \{-1, 1\}^n$  such that  $\mathbf{a}(i) = 1$  if  $A(i) = 1$  and  $\mathbf{a}(i) = -1$  if  $A(i) = 0$ . In other words we define  $\mathbf{a}(i) = 2A(i) - 1$ . Note that

$$\mathbf{a} = \sum_{i=1}^n \mathbf{a}(i) \cdot e_i.$$

We define

$$\tilde{\mathbf{a}} := \sum_{i=1}^n \mathbf{a}(i) \cdot \tilde{e}_i, \quad (53)$$

and recall that  $\tilde{e}_i := \sum_{j=1}^n v_{ij} \cdot \mathbf{v}_j$  is a rational approximation of  $e_i$  (Definition 6.4). We let  $\mathbf{a}^t M \mathbf{a}$  abbreviate  $\langle \mathbf{a}, M \mathbf{a} \rangle$  (which is  $\Sigma_1^B$ -definable in  $VTC^0$ , by Section 3.2.2).

**Lemma 6.7 (Main spectral bound)** *The theory  $VTC^0$  proves that if  $A$  is an assignment to  $n$  variables (that is,  $A$  is a string variable of length  $n + 1$ ) and  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  holds, then*

$$\mathbf{a}^t M \mathbf{a} \leq \lambda n + o(1). \quad (54)$$

This is a corollary of Lemma 6.8 and Lemma 6.11 that follow.

**Lemma 6.8** *The theory  $VTC^0$  proves that for any assignment  $A$  to  $n$  variables,  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  implies:*

$$\mathbf{a}^t M \mathbf{a} \leq \tilde{\mathbf{a}}^t M \tilde{\mathbf{a}} + O(1/n^{c-5}),$$

where  $c$  is the constant from the  $\text{EIGVALBOUND}(M_K, \vec{\lambda}, V)$  predicate.

**Proof:** First note that  $A$  is a string variable of length  $n$ . By Definition 6.4 for any  $1 \leq j \leq n$  there exists a vector  $\mathbf{r}_j \in \mathbb{Q}^n$  such that  $\tilde{e}_j = e_j + \mathbf{r}_j$ , and where  $\|\mathbf{r}_j\|_\infty = O(1/n^{c-1})$ . Therefore, by (53):

$$\tilde{\mathbf{a}} = \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i = \sum_{i=1}^n \mathbf{a}(i) (e_i + \mathbf{r}_i) = \sum_{i=1}^n \mathbf{a}(i) e_i + \sum_{i=1}^n \mathbf{a}(i) \mathbf{r}_i.$$

Note that  $\sum_{i=1}^n \mathbf{a}(i) e_i = \mathbf{a}$ , and let

$$\mathbf{r} := \sum_{i=1}^n \mathbf{a}(i) \mathbf{r}_i.$$

Then,

$$\tilde{\mathbf{a}} = \mathbf{a} + \mathbf{r},$$



and since  $\mathbf{a}(i) \in \{-1, 1\}$ , we have  $\|\mathbf{r}\|_\infty = O(1/n^{c-2})$ . Now, proceed as follows:

$$\begin{aligned} \mathbf{a}^t M \mathbf{a} &= (\tilde{\mathbf{a}} - \mathbf{r})^t M (\tilde{\mathbf{a}} - \mathbf{r}) \\ &= \tilde{\mathbf{a}}^t M \tilde{\mathbf{a}} - \tilde{\mathbf{a}}^t M \mathbf{r} - \mathbf{r}^t M \tilde{\mathbf{a}} + \mathbf{r}^t M \mathbf{r}. \end{aligned} \quad (55)$$

We now claim that (provably in  $\mathbf{VTC}^0$ ) the three right terms in (55) are  $o(1)$ :

**Claim 6.9** *The theory  $\mathbf{VTC}^0$  proves that for any assignment  $A$  to  $n$  variables,  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  implies:*

$$-\tilde{\mathbf{a}}^t M \mathbf{r} - \mathbf{r}^t M \tilde{\mathbf{a}} + \mathbf{r}^t M \mathbf{r} = O(1/n^{c-5}).$$

**Proof of claim:** Consider  $-\tilde{\mathbf{a}}^t M \mathbf{r}$ . Since  $\|\tilde{\mathbf{a}}\|_\infty \leq 2$  and since (by construction) each entry in  $M$  is at most  $O(n^2)$ , we have  $\|\tilde{\mathbf{a}}^t M\|_\infty = O(n^3)$ . Therefore, since  $\|\mathbf{r}\|_\infty \leq 1/n^{c-2}$ , we get  $-\tilde{\mathbf{a}}^t M \mathbf{r} = O(\frac{1}{n^{c-5}})$ . Similarly, we have  $-\mathbf{r}^t M \tilde{\mathbf{a}} = O(\frac{1}{n^{c-5}})$ .

Considering  $\mathbf{r}^t M \mathbf{r}$ , we have  $\|\mathbf{r}^t M\|_\infty = O(1/n^{c-4})$  and so  $\mathbf{r}^t M \mathbf{r} = O(1/n^{c-5} \cdot 1/n^{c-2} \cdot n) = O(1/n^{2c-8}) = O(1/n^{c-5})$ .  $\blacksquare$ Claim

Claim 6.9 concludes the proof of Lemma 6.8.  $\blacksquare$

**Claim 6.10** *There is a constant  $c'$  such that the theory  $\mathbf{VTC}^0$  proves that  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  implies that:*

$$\begin{aligned} \langle \tilde{e}_i, \tilde{e}_i \rangle &= 1 + O(1/n^{c'}), & \text{for any } 1 \leq i \leq n, \text{ and} \\ \langle \tilde{e}_i, \tilde{e}_j \rangle &= O(1/n^{c'}), & \text{for any } 1 \leq i \neq j \leq n. \end{aligned}$$

**Proof of claim:** By assumption for any  $1 \leq i \leq n$ ,  $\tilde{e}_i = e_i + \mathbf{r}_i$  for some  $\|\mathbf{r}_i\|_\infty = O(1/n^{c-1})$ . Thus

$$\begin{aligned} \langle \tilde{e}_i, \tilde{e}_i \rangle &= \langle e_i + \mathbf{r}_i, e_i + \mathbf{r}_i \rangle \\ &= \|e_i\|^2 + 2\langle e_i, \mathbf{r}_i \rangle + \|\mathbf{r}_i\|^2 \\ &= 1 + o(1), \end{aligned} \quad \begin{aligned} (56) \\ (57) \end{aligned}$$

where the last equation holds since  $2\langle e_i, \mathbf{r}_i \rangle$  and  $\|\mathbf{r}_i\|^2$  can be easily proved to be  $o(1)$  in  $\mathbf{VTC}^0$ .

Proving  $\langle \tilde{e}_i, \tilde{e}_j \rangle = O(1/n^{c'})$  for any  $1 \leq i \neq j \leq n$ , is similar.  $\blacksquare$ Claim

**Lemma 6.11** *The theory  $\mathbf{VTC}^0$  proves that for any assignment  $A$  to  $n$  variables,  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  implies:*

$$\tilde{\mathbf{a}}^t M \tilde{\mathbf{a}} \leq \lambda n + o(1). \quad (58)$$

**Proof:** We have:

$$\begin{aligned}
\tilde{\mathbf{a}}^t M \tilde{\mathbf{a}} &= \tilde{\mathbf{a}}^t M \left( \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i \right) && \text{(by definition of } \tilde{\mathbf{a}}) \\
&= \tilde{\mathbf{a}}^t M \left( \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{v}_j \right) \right) && \text{(by definition of } \tilde{e}_i) \\
&= \tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} M \mathbf{v}_j \right) && \text{(rearranging)} \\
&= \tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} (\lambda_j \mathbf{v}_j + \mathbf{r}_j) \right) && \text{(by Definition 6.4)} \\
&= \tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n \lambda_j v_{ji} \mathbf{v}_j \right) + \underbrace{\tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{r}_j \right)}_{\textcircled{1}} && \text{(rearranging)} \tag{59}
\end{aligned}$$

We claim (inside  $\mathbf{VTC}^0$ ) that the second term above, denoted  $\textcircled{1}$ , is of size  $o(1)$ :

**Claim 6.12** *The theory  $\mathbf{VTC}^0$  proves that for any assignment  $A$  to  $n$  variables,  $\text{EIGVALBOUND}(M, \vec{\lambda}, V)$  implies*

$$\tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{r}_j \right) = O(1/n^{c-6}).$$

**Proof of claim:** The proof is similar to the proof of Claim 6.9. Specifically, by Definition 6.4, for any  $1 \leq j \leq n$ , we have  $\|\mathbf{r}_j\|_\infty \leq 1/n^{c-1}$ , and for any  $1 \leq i, j \leq n$ , we have  $|v_{ji}| \leq 2$ . Thus,  $\mathbf{VTC}^0$  proves that  $\|\sum_{j=1}^n v_{ji} \mathbf{r}_j\|_\infty = O(1/n^{c-2})$ , for any  $1 \leq i \leq n$ . Since  $\mathbf{a}(i) \in \{-1, 1\}$ , for any  $1 \leq i \leq n$ , the theory  $\mathbf{VTC}^0$  proves  $\|\mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{r}_j\|_\infty = O(1/n^{c-2})$ , for any  $1 \leq i \leq n$ , and therefore also proves

$$\left\| \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{r}_j \right) \right\|_\infty = O(1/n^{c-3}). \tag{60}$$

Now consider  $\tilde{\mathbf{a}} = \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i = \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ji} \mathbf{v}_j \right)$ . Since, for any  $1 \leq i, j \leq n$  we have  $|v_{ji}| \leq 2$  we have  $\|\sum_{j=1}^n v_{ji} \mathbf{v}_j\|_\infty = O(n)$ . Thus, since  $\mathbf{a}(i) \in \{-1, 1\}$ ,  $\mathbf{VTC}^0$  can prove that  $\tilde{\mathbf{a}} = O(n^2)$ , and so by (60) the theory can finally prove

$$\tilde{\mathbf{a}}^t \sum_{i=1}^n \left( \mathbf{a}(i) \cdot \sum_{j=1}^n v_{ij} \mathbf{r}_j \right) = O(1/n^{c-6}).$$

■ Claim

It remains to bound the first term in (59):

$$\tilde{\mathbf{a}}^t \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \sum_{j=1}^n \lambda_j v_{ji} \mathbf{v}_j \right). \quad (61)$$

By the definition of  $\tilde{\mathbf{a}}$  in (53) and the definition of the  $\tilde{e}_i$ 's, we get that (61) equals:

$$\left( \sum_{i=1}^n \mathbf{a}(i) \sum_{j=1}^n v_{ji} \mathbf{v}_j^t \right) \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \sum_{j=1}^n \lambda_j v_{ji} \mathbf{v}_j \right). \quad (62)$$

We can prove in  $\mathbf{VTC}^0$  that for any vectors  $\mathbf{b}_1, \dots, \mathbf{b}_\ell \in \mathbb{Q}^n$  and any rational numbers  $c_1, \dots, c_\ell$  and  $\zeta_1, \dots, \zeta_\ell$ , such that  $\zeta = \max\{\zeta_i : 1 \leq i \leq \ell\}$ , we have

$$\left\langle \sum_{i=1}^{\ell} c_i \mathbf{b}_i, \sum_{i=1}^{\ell} \zeta_i c_i \mathbf{b}_i \right\rangle \leq \zeta \cdot \left\langle \sum_{i=1}^{\ell} c_i \mathbf{b}_i, \sum_{i=1}^{\ell} c_i \mathbf{b}_i \right\rangle.$$

Therefore, we can prove in  $\mathbf{VTC}^0$  that (62) is at most:

$$\begin{aligned} & \lambda \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \sum_{j=1}^n v_{ji} \mathbf{v}_j^t \right) \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \sum_{j=1}^n v_{ji} \mathbf{v}_j \right) \\ &= \lambda \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i^t \right) \cdot \left( \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i \right) \quad (\text{by definition of } \tilde{e}_i) \\ &= \lambda \cdot \left\langle \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i, \sum_{i=1}^n \mathbf{a}(i) \tilde{e}_i \right\rangle \\ &= \lambda \cdot \sum_{i=1}^n \langle \mathbf{a}(i) \tilde{e}_i, \mathbf{a}(i) \tilde{e}_i \rangle + \lambda \cdot \sum_{1 \leq i \neq j \leq n} \langle \mathbf{a}(i) \tilde{e}_i, \mathbf{a}(j) \tilde{e}_j \rangle \quad (\text{by rearranging}) \\ &= \lambda \cdot \sum_{i=1}^n \mathbf{a}(i)^2 \langle \tilde{e}_i, \tilde{e}_i \rangle + \lambda \cdot \sum_{1 \leq i \neq j \leq n} \mathbf{a}(i) \mathbf{a}(j) \langle \tilde{e}_i, \tilde{e}_j \rangle \quad (\text{by rearranging again}) \\ &= \lambda \cdot \sum_{i=1}^n 1 \cdot (1 + o(1)) + \lambda \cdot \sum_{1 \leq i \neq j \leq n} \mathbf{a}(i) \mathbf{a}(j) o(1) \quad (\text{by Claim 6.10}) \\ &= \lambda n + o(1) \quad (\text{for sufficiently large constant } c).^8 \quad (63) \end{aligned}$$

This concludes the proof of Lemma 6.11. ■

## 7 Wrapping up the proof: $\mathbf{TC}^0$ -Frege refutations of random 3CNFs

In this section we establish the main result of this paper, namely, polynomial-size  $\mathbf{TC}^0$ -Frege refutations for random 3CNF formulas with  $\Omega(n^{1.4})$  clauses.

<sup>8</sup>The constant  $c$  here is the global constant power of  $n$  (appearing in the  $1/n^c$ -approximation in Definition 6.4).

## 7.1 Converting the main formula into a $\forall\Sigma_0^B$ formula

Note that the main formula (Definition 4.6) is a  $\Sigma_0^B(\mathcal{L})$  formula, where the language  $\mathcal{L}$  contains function symbols not in  $\mathcal{L}_A^2$ , and in particular it contains the *numones* function. Since Theorem 3.25 relates  $\mathbf{VTC}^0$  proofs of  $\Sigma_0^B$  formulas to polynomial-size  $\mathbf{TC}^0$ -Frege proofs, in order to use this theorem we need to convert the main formula into a  $\Sigma_0^B$  formula (in the language  $\mathcal{L}_A^2$ ). It suffices to show that  $\mathbf{VTC}^0$  proves that the main formula is equivalent to a  $\forall\Sigma_0^B$  formula, since if  $\mathbf{VTC}^0$  proves a  $\forall\Sigma_0^B$  formula  $\forall\Phi$ , it also proves the  $\Sigma_0^B$  formula  $\Phi$  obtained by discarding all the universal quantifiers in  $\forall\Phi$ .

**Lemma 7.1** *The theory  $\mathbf{VTC}^0$  proves that the main formula is equivalent to a  $\forall\Sigma_0^B$  formula  $\forall\Phi$  where the universal quantifiers in the front of the formula all quantify over string variables that serve as counting sequences. Specifically,*

$$\forall\Phi := \forall Z_1 \leq t_1 \dots \forall Z_r \leq t_r \Phi(Z_1, \dots, Z_r), \quad (64)$$

where  $t_1, \dots, t_r$  are number terms and  $\Phi(Z_1, \dots, Z_r)$  has also free variables other than the  $Z_i$ 's, and every occurrence of every  $Z_i$  appears in  $\Phi$  in the form  $(\delta_{\text{NUM}}(|T|, T, Z_i) \wedge Z_i[t] = s)$ , for some string term  $T$  and number terms  $t, s$ , and where  $\delta_{\text{NUM}}(|T|, T, Z_i)$  states that  $Z_i$  is a counting sequence that counts the number of ones in  $T$  until position  $|T|$  (see Definition 3.12).

**Proof:** The following steps convert the main formula into a  $\forall\Sigma_0^B$  formula which is equivalent (provably in  $\mathbf{VTC}^0$ ) to the main formula:

1. All the functions in the main formula are  $\mathbf{AC}^0$ -reducible to  $\mathcal{L}_A^2 \cup \{\text{numones}\}$  (see Section 3.2.1). Thus, the defining axioms of all the function symbols in the main formula can be assumed to be  $\Sigma_0^B(\text{numones})$  formulas. Now, it is a standard procedure to substitute in the main formula all the function symbols by their  $\Sigma_0^B(\text{numones})$ -defining axioms.<sup>9</sup> The resulting formula is  $\Sigma_0^B(\text{numones})$ , and provably in  $\mathbf{VTC}^0$  is equivalent to the original main formula.
2. We now substitute all the *numones* function symbols by their  $\Sigma_1^B$ -defining axioms. Specifically, every occurrence of  $\text{numones}(t, T)$  in the formula, for  $t, T$  number and string terms, respectively, occurs inside some atomic formula  $\Psi := \Psi(\dots \text{numones}(t, T) \dots)$ . And so we substitute  $\Psi$  by the existential formula

$$\exists Z \leq 1 + \langle |T|, |T| \rangle (\delta_{\text{NUM}}(|T|, T, Z) \wedge Z[t] = z \wedge \Psi(\dots z \dots)).$$

3. Note that all the *numones* function symbols appear in the *premise* of the implication in the main formula, so we can take all these existential quantifiers out of the premise of the implication and obtain a universally quantified formula, where the universal quantifiers in the front of the formula all quantify over string variables that serve as counting sequences (as in Item 2 above). ■

---

<sup>9</sup>When the defining axiom of a string function  $F(\vec{x}, \vec{X})$  is a *bit-definition*  $i < r(\vec{x}, \vec{X}) \wedge \psi(i, \vec{x}, \vec{X})$ , we substitute an atomic formula like  $F(\vec{x}, \vec{X})(z)$ , by  $z < r(\vec{x}, \vec{X}) \wedge \psi(z, \vec{x}, \vec{X})$  (cf. Lemma V.4.15 in [13]).

## 7.2 Propositional proofs

We need to restate the main probabilistic theorem in [17]:

**Theorem 7.2** ([17], **Theorem 3.1**) *Let  $\mathbf{C}$  be a random 3CNF with  $n$  variables and  $m = \beta \cdot n$  clauses ( $\beta = c \cdot n^{0.4}$ ,  $c$  some fixed large constant). Then, with probability converging to 1, the following holds:*

- *The imbalance of  $\mathbf{C}$  is at most  $O(n\sqrt{\beta}) = O(n^{1.2})$ .*
- *The largest eigenvalue  $\lambda$  satisfies  $\lambda = O(\sqrt{\beta}) = O(n^{0.2})$ .*
- *There are  $k = O(\frac{n}{\beta^2}) = O(n^{0.2})$ ,  $t = \Omega(n\beta) = \Omega(n^{1.4})$ ,  $d = O(k) = O(n^{0.2})$  and  $\mathcal{C}$  with  $|\mathcal{C}| = t$  such that  $\text{COLL}(t, k, d, n, m, \mathbf{C}, \mathcal{C})$  holds.*

We need to rephrase the theorem in a manner that suites our needs, as follows:

**Corollary 7.3** *Let  $\mathbf{C}$  be random 3CNF with  $n$  variables and  $m = c \cdot n^{1.4}$  clauses where  $c$  is sufficiently large constant. Then, with probability converging to 1, the following holds:<sup>10</sup>*

- *There exists an  $I = O(n^{1.2})$  such that  $\text{IMB}(\mathbf{C}, I)$ .*
- *The  $1/n^{c'}$ -rational approximation  $\lambda$  of the largest eigenvalue of  $M$  satisfies  $\lambda = O(n^{0.2})$ , where  $c' > 6$  is some constant. I.e.,  $\text{EIGVALBOUND}(M, \lambda, V)$  and  $\text{MAT}(M, \mathbf{C})$  hold.*
- *There are natural numbers  $k = O(n^{0.2})$ ,  $t = \Omega(n^{1.4})$ ,  $d = O(k) = O(n^{0.2})$  and a sequence  $\mathcal{D}$  of  $t$  inconsistent  $k$ -tuples such that  $\text{COLL}(t, k, d, n, m, \mathbf{C}, \mathcal{D})$  holds, and such that:*

$$t > \frac{d(I + \lambda n)}{2} + o(1).$$

The last inequality concerning  $t$  stems from direct computations, using the bounds in Theorem 7.2 with  $\beta = n^{0.4}$ .

Recall that that premise in the implication in the main formula:

$$\begin{aligned} & 3\text{CNF}(\mathbf{C}, n, m) \wedge \text{COLL}(t, k, d, n, m, \mathbf{C}, \mathcal{D}) \wedge \text{IMB}(\mathbf{C}, I) \wedge \text{MAT}(M, \mathbf{C}) \wedge \\ & \text{EIGVALBOUND}(M, \vec{\lambda}, V) \wedge \lambda = \max\{\vec{\lambda}\} \wedge t > \frac{d \cdot (I + \lambda n)}{2} + o(1). \end{aligned} \quad (65)$$

Let  $\text{PREM}(\mathbf{C}, n, m, t, k, d, \mathcal{D}, I, \vec{\lambda}, V, M, \lambda, \vec{Z})$  be the formula obtained from (65) after transforming the main formula into a  $\forall \Sigma_0^B$  formula, where the  $\vec{Z}$  string variables are the variables for counting sequences added after the transformation (as described in Lemma 7.1).

**Claim 7.4** *If a  $\Sigma_0^B$  formula  $\varphi(\vec{x}, \vec{X})$  can be evaluated to a true sentence in  $\mathbb{N}_2$  by assigning numbers  $\vec{x}$  and sets  $\vec{X}$  to the appropriate variables, then the translation  $\llbracket \varphi \rrbracket_{\vec{x}, \vec{X}}$  is satisfiable.*

<sup>10</sup>Formally speaking, we mean that the following three items hold in the standard two-sorted model  $\mathbb{N}_2$ , when all the second-sort objects (like  $\mathbf{C}$  and  $\mathcal{D}$ ) are in fact finite sets of numbers (encoding  $\mathbf{C}$  and  $\mathcal{D}$ ), natural numbers are treated as natural numbers in the standard two-sorted model and rational numbers are the corresponding natural numbers that encode them as pairs of natural numbers (as described in Section 3.1.2).

**Lemma 7.5** *For every  $m, n \in \mathbb{N}$  and every unsatisfiable 3CNF formula  $\mathbf{C}$  with  $m$  clauses and  $n$  variables such that  $\text{PREM}(\mathbf{C}, n, m, \dots)$  is true for some assignment to the remaining variables (i.e. to the unspecified variables denoted by  $\dots$ ; this also implies that  $\llbracket \text{PREM}(\mathbf{C}, n, m, \dots) \rrbracket$  is satisfiable), there exists a polynomially bounded  $\mathbf{VTC}^0$ -Frege proof of  $\neg \mathbf{C}$  (i.e. the sequent  $\longrightarrow \neg \mathbf{C}$  can be derived).*

**Proof:** Recall that for given  $m, n \in \mathbb{N}$ , 3CNF formula  $\mathbf{C} = (\mathbf{C}[\alpha])_{\alpha < m}$  and assignment  $A$ , the formula  $\exists \alpha \leq m \text{NOTSAT}(\mathbf{C}[i], A)$  (which is the consequence of the implication in the main formula 4.6) is the statement:

$$\begin{aligned} \exists \alpha < m \exists i, j, k \leq n ( & \langle \mathbf{C}[\alpha] \rangle_1^5 = i \wedge (A(i) \leftrightarrow \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_1^3 = 0) \\ & \wedge \langle \mathbf{C}[\alpha] \rangle_2^5 = j \wedge (A(j) \leftrightarrow \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_2^3 = 0) \\ & \wedge \langle \mathbf{C}[\alpha] \rangle_3^5 = k \wedge (A(k) \leftrightarrow \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_3^3 = 0)). \end{aligned}$$

The propositional translation of this formula (Definition 3.23) contains the variables  $p_{\langle i, j, k, \ell, \alpha \rangle}^{\mathbf{C}}$  with  $i, j, k \leq n$ ,  $\alpha < m$ . Additionally it contains variables  $p_i^A$  for  $i \leq n$  stemming from the assignment  $A$ . It is not necessary to show the full translation of the formula, since we intend to plug-in propositional constants ( $\top, \perp$ ) for some of the variables. In other words, parts of the formula will consist of only constants and so it is unnecessary to give these parts in full detail. Having this in mind, the translation  $\llbracket \exists \alpha < m \text{NOTSAT}(\mathbf{C}[\alpha], A) \rrbracket_{m, n}$  is

$$\begin{aligned} \bigvee_{\alpha=0}^{m-1} \bigvee_{i, j, k=1}^n ( & (\llbracket \langle \mathbf{C}[\alpha] \rangle_1^5 = i \rrbracket_{m, n} \wedge (p_i^A \leftrightarrow \llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_1^3 = 0 \rrbracket_{m, n})) \\ & \wedge (\llbracket \langle \mathbf{C}[\alpha] \rangle_2^5 = j \rrbracket_{m, n} \wedge (p_j^A \leftrightarrow \llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_2^3 = 0 \rrbracket_{m, n})) \\ & \wedge (\llbracket \langle \mathbf{C}[\alpha] \rangle_3^5 = k \rrbracket_{m, n} \wedge (p_k^A \leftrightarrow \llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_3^3 = 0 \rrbracket_{m, n}))). \end{aligned} \quad (66)$$

Here, the variables  $p_{\langle i, j, k, \ell, \alpha \rangle}^{\mathbf{C}}$  all implicitly appear in the parts inside  $\llbracket \cdot \rrbracket$ .

Now assume we have a fixed 3CNF  $\underline{\mathbf{C}}$  with  $n$  variables and  $m$  clauses. Then for every  $\alpha < m$  there exists  $1 \leq i, j, k \leq n$  such that the formulas  $\llbracket \langle \underline{\mathbf{C}}[\alpha] \rangle_1^5 = i \rrbracket_{m, n}$  and  $\llbracket \langle \underline{\mathbf{C}}[\alpha] \rangle_2^5 = j \rrbracket_{m, n}$  and  $\llbracket \langle \underline{\mathbf{C}}[\alpha] \rangle_3^5 = k \rrbracket_{m, n}$  are all satisfied (in fact they are polynomial-size in  $n$  propositional tautologies consisting of only constants  $\top, \perp$ ). From now on we will only concentrate on the disjuncts where this is the case (as the other disjuncts are falsified, or in other words they are propositional contradictions consisting of only constants).

By plugging  $\underline{\mathbf{C}}$  into  $\llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_1^3 = 0 \rrbracket_{m, n}$  and  $\llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_2^3 = 0 \rrbracket_{m, n}$  and  $\llbracket \langle \langle \mathbf{C}[\alpha] \rangle_4^5 \rangle_3^3 = 0 \rrbracket_{m, n}$  we get that  $\llbracket \exists \alpha < m \text{NOTSAT}(\mathbf{C}[\alpha], A) \rrbracket_{m, n}$  is evaluated to

$$\bigvee_{\alpha < m} \left( (p_i^A)^{\ell_1^\alpha} \wedge (p_j^A)^{\ell_2^\alpha} \wedge (p_k^A)^{\ell_3^\alpha} \right), \quad (67)$$

where  $\ell_r^\alpha$  is an abbreviation of  $\llbracket \langle \langle \underline{\mathbf{C}}[\alpha] \rangle_4^5 \rangle_r^3 = 0 \rrbracket_{m, n}$ , and thus we can observe that (67) gets evaluated to  $\neg \underline{\mathbf{C}}(p_1^A/x_1, \dots, p_n^A/x_n)$ , where  $p_i^A/x_i$  means substitution of  $x_i$  by  $p_i^A$ .

By Theorem 5.1 the theory  $\mathbf{VTC}^0$  proves the main formula and so by Lemma 7.1 there is a  $\mathbf{VTC}^0$  proof of

$$\text{PREM}(\mathbf{C}, n, m, t, k, d, \mathcal{D}, I, \vec{\lambda}, V, M, \lambda, \vec{Z}) \rightarrow \exists i < m \text{NOTSAT}(\mathbf{C}[i], A).$$

Thus, by Theorem 3.25 we can derive a polynomially bounded  $\mathbf{TC}^0$ -proof of the formula

$$\llbracket \text{PREM}(\mathbf{C}, \dots) \rrbracket_{m,n} \rightarrow \llbracket \exists \alpha < m \text{NOTSAT}(\mathbf{C}[\alpha], A) \rrbracket_{m,n}$$

and thus also of the *sequent*

$$\llbracket \text{PREM}(\mathbf{C}, \dots) \rrbracket_{m,n} \longrightarrow \llbracket \exists \alpha < m \text{NOTSAT}(\mathbf{C}[\alpha], A) \rrbracket_{m,n}.$$

By Claim 7.4 and the assumption that  $\text{PREM}(\underline{\mathbf{C}}, n, m, \dots)$  is true in  $\mathbb{N}_2$  for an assignment to the remaining variables we know that  $\llbracket \text{PREM}(\underline{\mathbf{C}}, \dots) \rrbracket_{m,n}$  is satisfiable. Plugging-in such a satisfying assignment  $\vec{a}$  into  $\llbracket \text{PREM}(\underline{\mathbf{C}}, \dots) \rrbracket_{m,n}$ , Lemma 2.7 yields a polynomially bounded  $\mathbf{TC}^0$ -Frege proof of

$$\llbracket \text{PREM}(\underline{\mathbf{C}}, \vec{a}) \rrbracket_{m,n}$$

and of the sequent

$$\llbracket \text{PREM}(\underline{\mathbf{C}}, \vec{a}) \rrbracket_{m,n} \longrightarrow \llbracket \exists \alpha < m \text{NOTSAT}(\underline{\mathbf{C}}[\alpha], A) \rrbracket_{m,n}.$$

Using the Cut rule (Definition 2.4) we get a polynomially bounded  $\mathbf{TC}^0$ -Frege proof of the formula

$$\llbracket \exists \alpha < m \text{NOTSAT}(\underline{\mathbf{C}}[\alpha], A) \rrbracket_{m,n}.$$

As we showed before, this gets evaluated to

$$\neg \underline{\mathbf{C}}(p_1^A/x_1, \dots, p_n^A/x_n)$$

as desired. Because of Claim 2.7, this proof is only polynomially longer than the one of the translation of the main formula. Since that proof was polynomially bounded, the above proof of  $\neg \underline{\mathbf{C}}(p_i^A/x_i)$  also is.  $\blacksquare$

We can now conclude:

**Corollary 7.6** *With probability converging to 1, a random 3CNF  $\mathbf{C}$  with  $n$  variables and  $m \geq c \cdot n^{1.4}$  clauses,  $c$  a sufficiently large constant,  $\neg \mathbf{C}$  has polynomially bounded  $\mathbf{TC}^0$ -Frege proofs, while  $\mathbf{C}$  has no sub-exponential size resolution refutations (as long as  $m = O(n^{1.5-\epsilon})$ , for  $0 < \epsilon < 1/2$ ).*

**Proof:** By Corollary 7.3, with probability converging to 1 there exists an assignment of numbers and strings  $\vec{\alpha}$  (including also the appropriate counting sequences assigned to the  $Z_i$  string variables introduced in Lemma 7.1) such that  $\text{PREM}(\mathbf{C}, \vec{\alpha})$  holds (in the standard two-sorted model). Therefore, with probability converging to 1 we can apply Lemma 7.5 to establish that  $\neg \mathbf{C}$  has a short  $\mathbf{TC}^0$ -Frege proof. That with probability converging to 1 there are no sub-exponential size resolution refutations of  $\mathbf{C}$  follows from [11, 5, 8].  $\blacksquare$

## Acknowledgments

We wish to thank Jan Krajíček for very helpful discussions on the topic of this paper and Emil Jeřábek and Neil Thapen for answering many of our questions about theories of weak arithmetic and for many other insightful comments.



## References

- [1] Michael Alekhnovich. Lower bounds for  $k$ -DNF resolution on random 3-CNFs. In *Proceedings of the Annual ACM Symposium on the Theory of Computing*, pages 251–256, 2005.
- [2] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: non-binomial case. In *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001)*, pages 190–199. IEEE Computer Soc., Los Alamitos, CA, 2001.
- [3] Michael Alekhnovich and Alexander A. Razborov. Resolution is not automatizable unless W[P] is tractable. *SIAM J. Comput.*, 38(4):1347–1363, 2008.
- [4] A. Atserias, Maria Luisa Bonet, and J. Esteban. Lower bounds for the weak pigeonhole principle and random formulas beyond resolution. *Information and Computation*, 176:152–136, August 2002.
- [5] Paul Beame, Richard Karp, Toniann Pitassi, and Michael Saks. The efficiency of resolution and Davis-Putnam procedures. *SIAM J. Comput.*, 31(4):1048–1075 (electronic), 2002.
- [6] Eli Ben-Sasson. *Expansion in Proof Complexity*. PhD thesis, Hebrew University, Jerusalem, Israel, September 2001.
- [7] Eli Ben-Sasson and Russell Impagliazzo. Random CNF’s are hard for the polynomial calculus. *Computational Complexity*, pages 1–19, 2010.
- [8] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *J. ACM*, 48(2):149–169, 2001. (A preliminary version appeared in Proceedings of the 31th Annual ACM Symposium on the Theory of Computing (Atlanta, GA, 1999)).
- [9] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. *SIAM J. Comput.*, 29(6):1939–1967, 2000.
- [10] Samuel R. Buss and Peter Clote. Cutting planes, connectivity, and threshold logic. *Arch. Math. Logic*, 35(1):33–62, 1996.
- [11] Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. Assoc. Comput. Mach.*, 35(4):759–768, 1988.
- [12] Stephen Cook. *Theories for Complexity Classes and Their Propositional Translations*, pages 175–227. Complexity of computations and proofs, Jan Krajíček, ed. Quaderni di Matematica, 2005.
- [13] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. ASL Perspectives in Logic. Cambridge University Press, 2010. Draft available at url: <http://www.cs.toronto.edu/~sacook/>.
- [14] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem proving. *Communications of the ACM*, 5(7), 1962.
- [15] Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *Journal of the ACM*, 7(3):201–215, 1960.

- [16] Uriel Feige. Refuting smoothed 3CNF formulas. In *Proceedings of the IEEE 48th Annual Symposium on Foundations of Computer Science*, pages 407–417. IEEE Computer Society, 2007.
- [17] Uriel Feige, Jeong Han Kim, and Eran Ofek. Witnesses for non-satisfiability of dense random 3CNF formulas. In *Proceedings of the IEEE 47th Annual Symposium on Foundations of Computer Science*, 2006.
- [18] Uriel Feige and Eran Ofek. Easily refutable subformulas of large random 3cnf formulas. *Theory of Computing*, 3(1):25–43, 2007.
- [19] Joel Friedman, Andreas Goerdt, and Michael Krivelevich. Recognizing more unsatisfiable random  $k$ -SAT instances efficiently. *SIAM J. Comput.*, 35(2):408–430, 2005.
- [20] Nicola Galesi and Massimo Lauria. Optimality of size-degree trade-offs for polynomial calculus. *ACM Trans. Comput. Log.*, 12(1), 2011 (to appear).
- [21] A. Goerdt and M. Krivelevich. Efficient recognition of random unsatisfiable  $k$ -SAT instances by spectral methods. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 294–304, 2001.
- [22] Andreas Goerdt and André Lanka. Recognizing more random unsatisfiable 3-SAT instances efficiently. *Electronic Notes in Discrete Mathematics*, 16:21–46, 2003.
- [23] Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985.
- [24] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.
- [25] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. *The Journal of Symbolic Logic*, 59(1):73–86, 1994.
- [26] Alexis Maciel and Toniann Pitassi. On  $\text{ACC}^0[p^k]$  Frege proofs. In *Proceedings of the Annual ACM Symposium on the Theory of Computing 1997 (El Paso, TX)*, pages 720–729 (electronic). ACM, New York, 1999.
- [27] Phuong Nguyen. Proving infinitude of prime numbers using binomial coefficients. In *22nd International Workshop on Computer Science Logic, (Bertinoro, Italy)*, volume 5213 of *Lecture Notes in Computer Science*, pages 184–198. Springer, 2008.
- [28] Phuong Nguyen and Stephen A. Cook. Theories for  $TC^0$  and other small complexity classes. *Logical Methods in Computer Science*, 2(1), 2006.
- [29] Robert Reckhow. *On the lengths of proofs in the propositional calculus*. PhD thesis, University of Toronto, 1976. Technical Report No . 87.
- [30] Nathan Segerlind, Samuel R. Buss, and Russel Impagliazzo. A switching lemma for small restrictions and lower bounds for  $k$ -DNF resolution. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pages 604–613. 2002.
- [31] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. *Ann. Pure Appl. Logic*, 130(1-3):277–323, 2004.

- [32] Domenico Zambella. Notes on polynomially bounded arithmetic. *The Journal of Symbolic Logic*, 61(3):942–966, 1996.