UNIVERSITY OF CALIFORNIA, SAN DIEGO

New Separations in Propositional Proof Complexity

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Computer Science

by

Nathan Segerlind

Committee in charge:

Professor Samuel R. Buss, Co-Chair
Professor Russell Impagliazzo, Co-Chair
Professor Daniele Micciancio
Professor Ramamohan Paturi
Professor Nolan Wallach

2003

The dissertation of Nathan Segerlind is approved, and it is acceptable in quality and form for publication on microfilm:

_____

_____

_____

_____
Co-chair

_____
Co-chair

University of California, San Diego

2003

DEDICATION

Surely all that I ever achieve is because of (and nothing without) my family. My parents, Gerald and Christine Segerlind, instilled a love of learning and a work ethic within me while giving me the freedom to pursue my own goals and dreams. My siblings, Adam, David and Sarah, have always been there for me in good times and bad, and while I cannot say that they played much of a role in this dissertation, my life is certainly richer for their presence. Finally, I must thank my wife Li Chen, who supported and encouraged me throughout the long years of graduate school. She was also a PhD student at UCSD, and we were able to support one another during the dark days of insecurity and uncertainty that all graduate students face. Li, I love you very much, and I look forward to living the rest our life side by side.

At this time, in the final hours before I file my dissertation with the Office of Graduate Studies and Research, I would like explain how I came to the unusual arrangement having two advisors. Usually such arrangements are lopsided, with a "real advisor" and an "official advisor", or with one advisor at the student's location and the other afar. In my case, the two functioned as equals and I met with each weekly. Either Sam or Russell would make an outstanding advisor in the area of propositional proof complexity, but of course the two have very different styles and personalities. Their respective strengths complement one another very well. When the department said that I had to get an advisor, I decided "Why should I have the best advisor when I could have the two best advisors?". In the end, it seems that my estimation was correct and I could not have asked for more.

TABLE OF CONTENTS

LIST OF TABLES

I would like to acknowledge my coauthors Sam Buss and Russell Impagliazzo for their contributions to the research that makes up the body of this dissertation.

Most of the material in chapters III and IV was previously published in the Proceedings of the Forty-third Annual IEEE Symposium on the Foundations of Computer Science [41]. Sam and Russell were my coauthors on this paper.

Most of the material in chapter V was previously published in the Proceedings of the Twenty-ninth Annual Colloquium on Automata, Languages and Programming [80]. Russell was my coauthor on this paper.

Most of the material in chapter VI was previously published in the Proceedings of the Forty-second Annual IEEE Symposium on the Foundations of Computer Science [68]. Russell was my coauthor on this paper.

VITA

1996	B.S. Carnegie Mellon University
1998	M.S. Carnegie Mellon University
1998–1999	MICRO Fellowship Scholar University of California, San Diego
1999–2003	Research Assistant University of California, San Diego
2003	Doctor of Philosophy University of California, San Diego

PUBLICATIONS

R. Impagliazzo and N. Segerlind, Counting Axioms Do Not Polynomially Simulate Counting Gates. Appeared in *the Forty-Second Annual Symposium on Foundations of Computer Science*, October, 2001.

R. Impagliazzo and N. Segerlind, Bounded Depth Frege with Counting Axioms Polynomially Simulates Nullstellensatz Refutations. Appeared in *the Twenty-Ninth Annual International Colloquium on Automata, Languages and Programming*, July, 2002.

N. Segerlind, S. Buss and R. Impagliazzo, A Switching Lemma for Small Restrictions and Lower Bounds for k-DNF Resolution. Appeared in *the Forty-third Annual Symposium on Foundations of Computer Science*, November, 2002.

ABSTRACT OF THE DISSERTATION

New Separations in Propositional Proof Complexity

by

Nathan Segerlind
Doctor of Philosophy in Computer Science
University of California, San Diego, 2003
Professors Samuel R. Buss and Russell Impagliazzo, Chairs

The problem of recognizing satisfiable formulas and propositional tautologies is ubiquitous in computer science. Propositional proof systems are methods for establishing that a propositional formula is a tautology. In general, proof systems correspond to algorithms for satisfiability so that lower bounds on proof sizes in a given system correspond to lower bounds on the run time of the related satisfiability algorithms. Moreover, the question of proof sizes is intimately connected to questions such as NP versus $coNP$.

In this dissertation, we study the sizes of proofs in different propositional proof systems. We prove new lower bounds on the sizes of proofs in the Res(k) systems, we prove that constant-depth Frege systems with counting axioms do not polynomially simulate constant-depth Frege systems with counting gates, and we prove that constant-depth Frege systems with counting axioms polynomially simulate Nullstellensatz refutations. As corollaries to these results, we obtain the first separation of the Nullstellensatz and polynomial calculus systems with respect to *size*, and an exponential separation between constant-depth Frege systems and constant-depth Frege systems with counting axioms with respect to constant-width CNFs. The lower bounds for the Res(k) systems include:

1. The $2n$ to n weak pigeonhole principle requires size $2^{\Omega(n^\epsilon)}$ to refute in $\mathrm{Res}(\sqrt{\log n / \log\log n})$.
2. For each k, there exists a constant $w > k$ so that random w-CNFs in n variables require size $2^{\Omega(n^\epsilon)}$ to refute in $\mathrm{Res}(k)$.
3. We demonstrate sets of clauses on n variables that have polynomial size $\mathrm{Res}(k+1)$ refutations, but require size $2^{\Omega(n^\epsilon)}$ to refute in $\mathrm{Res}(k)$.

Our lower bounds for proof sizes are proved using extensions of the switching lemma technique. The lower bound proofs for the $\mathrm{Res}(k)$ systems use a method we call *switching with small restrictions*, and the lower bound proof for constant-depth Frege with counting axioms uses a switching lemma that makes random *substitutions* rather than 0/1 restrictions. The switching lemma for small restrictions allows us to prove the first separation between depth d circuits of bottom fan-in $k+1$ and depth d circuits of bottom fan-in k.

Chapter I

Introduction

Propositional logic is the science of reasoning about statements that are either true or false. **Propositional formulas** (also called **Boolean formulas**) are expressions built up from variables that take the values TRUE and FALSE using connectives such as *and*, *or*, *implies*, and *not*; for example, *(A or B) implies (C and(not D))*. Some formulas are always true, no matter how truth assignments are made to the variables; for example, *(A and B) implies A* and *((A and C) implies B) implies ((C implies A) implies (C implies B))*. Such formulas are called **tautologies**. The recognition of tautologies is a central task in logic and computer science and there are many systems for establishing that a given formula is a tautology. This dissertation quantitatively compares the relative efficiency of various systems for establishing that a formula is a tautology.

In computer science, the problem of recognizing tautologies often appears in the guise of recognizing satisfiable formulas. A formula is said to be **satisfiable** if there exists a truth assignment to the variables that makes the formula true. Notice that a formula is a tautology if and only if its negation is *not* satisfiable. This is the foundation of an important duality: any algorithm that can decide if a formula is satisfiable corresponds to an algorithm that can decide if a formula is a tautology and any algorithm that can decide if a formula is tautology corresponds an algorithm that can decide if a formula is satisfiable.

The satisfiability problem is ubiquitous in both theoretical and applied computer science. The famous P versus NP problem asks whether a polynomial-time algorithm can recognize satisfiable formulas [77]. The recognition of satisfiable formulas also has applications in areas such as artificial intelligence [8, 6, 7] and the verification of hardware systems [5, 4]. For example, in hardware testing, it is common to take a description of a circuit and compute a formula which is satisfiable if and only if it is possible for a certain fault in production to cause a run-time error. Indeed, because of its central role in the theory of NP-complete problems, a vast host of computational problems, such as the solvability of systems of polynomial equations over a finite field and the traveling salesman problem, are equivalent to recognizing satisfiable formulas [84].

Propositional proof systems are methods for certifying that a propositional formula is a tautology. There are many propositional proof systems, but all provide a straightforward, mechanistic procedure for verifying the correctness of proofs. This is the defining characteristic of proof systems: it may not be easy to find a proof that a formula is a tautology, but it should always be easy to check that a proof is correct. Furthermore, we will consider only **complete** proof systems. A proof system is complete if it has a proof for every tautology.

The best known propositional proof systems are ones in which the prover begins with a small set of self-evident axioms and repeatedly applies inference rules, such as "from A and A *implies* B infer B", to successively derive new formulas until the desired tautology is obtained. These systems are known in the proof complexity literature as **Frege systems** [74]. There are proof systems that are not Frege systems. For example, any algorithm which solves the satisfiability problem for Boolean formulas also functions as a propositional proof system: a transcript of the algorithm's run on an input that outputs "unsatisfiable" provides a proof that the input is the negation of a tautology. In general, any polynomial time mapping f from strings onto the set of tautologies is viewed as a propositional proof system: if $f(S) = \tau$ then S is a proof of τ [74]. The requirement that f is polynomial-time

computable captures the principle that the proofs should be easy to check, and the requirement that f is onto captures the requirement the proof system is complete. Systems of this form are called **abstract propositional proof systems**. The sizes of proofs in abstract propositional proof systems is of great interest because there exists such a system in which every tautology has a proof whose size is at most polynomially larger than the size of the tautology if and only if NP is equal to $coNP$ [74].

While every Frege system is an abstract proof system, it is not known whether or not every abstract proof system can have its proofs transformed into Frege proofs with only a polynomial (or even subexponential) increase in size. This problem, whether or not Frege systems can **polynomially simulate** [74] all abstract propositional proof systems, has important consequences. If Frege systems polynomially simulate every abstract proof system, then the NP versus $coNP$ problem is more concrete than is currently thought – it would be a question about a specific Frege system rather than a question about all abstract proof systems. If there exists an abstract proof system which is not polynomially simulated by Frege systems, then this method for certifying tautologies would be more efficient than classical propositional proof systems, possibly leading to new satisfiability algorithms.

Most researchers believe that Frege systems cannot polynomially simulate all abstract proof systems. However, proving lower bounds for the sizes of Frege proofs seems to be a very difficult problem and at present there are no proven superpolynomial size lower bounds for Frege proofs.

I.A Circuit Complexity and Restricted Frege Systems

One of the difficulties for proving lower bounds on the sizes of Frege proofs is that currently there is little understanding of the expressive power of the propositional formulas used in Frege proofs. It is consistent with our current

knowledge that every function in NP could be computed by a small Boolean formula. Without knowing which concepts can be expressed by small formulas, it seems impossible to know what tautologies have small Frege proofs.

Some restricted classes of formulas are known to require exponential size to compute certain functions. One such class is the class of constant-depth[1] formulas with the connectives AND, OR and NOT. Circuits of this form are known to require exponential size to compute functions involving counting, such as modular sums or whether a majority of the input variables is to TRUE [11, 66, 14]. Another class of circuits with proven size lower bounds for specific functions is the class of constant-depth formulas with the connectives AND, OR, NOT and counting gates[2] modulo a prime p. When p and q are distinct primes, constant-depth circuits with counting modulo p gates are known to require exponential size to compute sums modulo q [83, 82]. By limiting Frege systems to use formulas only from these classes, we obtain **constant-depth Frege systems** and **constant-depth Frege systems with counting gates** [57].

Although the name "restricted Frege systems" suggests weakness, constant-depth Frege systems are actually quite powerful and can simulate many of the algorithms used by automated theorem provers and satisfiability solvers. Size lower bounds for these proof systems imply run time lower bounds for the related satisfiability algorithms. For example, satisfiability algorithms such as the Davis-Putnam-Logemann-Loveland algorithm (DPLL) implicitly create proofs in resolution, a depth-one Frege system. Common extensions of these algorithms, such as formula caching [81], also generate constant-depth Frege proofs. The Gröbner basis algorithm (over a finite field) can be simulated by constant-depth Frege systems with counting gates [70].

Although there are some proven size lower bounds for constant-depth Frege systems, many issues remain open. All known lower bounds for constant-

[1] Formula depth is essentially the maximum number of alternations of AND and OR from an input to the output. See section I.E for a more formal treatment.

[2] These gates have an unlimited number of Boolean (0/1) inputs and are true if the sum of the inputs is divisible by p. See section I.E for a more formal treatment.

depth Frege systems exploit the inability of constant-depth formulas to express counting functions.

Tautologies known to require exponential size constant-depth Frege proofs include the **pigeonhole principle**, which expresses the impossibility of placing $n+1$ pigeons in n holes without collisions [48, 50, 51], the **modular counting principles**, which express the impossibility of partitioning a set of size N into pieces of size m when N is indivisible by m [54, 58, 56, 57], and the **Tseitin graph tautologies**, which generalize the fact that the sum of the degrees of a graph cannot be odd [9]. The proof sizes needed for tautologies that do not involve counting or involve it only weakly remain a mystery. Notable open problems of this flavor are proving size lower bounds for constant-depth Frege proofs of **weak pigeonhole principles** (the impossibility of placing $2n$ or n^2 many pigeons into n holes without collision), finding constant depth tautologies that require superpolynomial depth d proofs but have polynomial size depth $d+1$ proofs, and proving lower bounds on the expected size of a proof of unsatisfiability for a randomly generated 3-CNF. The sizes of proofs of unsatisfiability for random 3-CNFs is especially important because it addresses whether difficult tautologies are common or exceptional, and it has connections to the complexity of computing approximate solutions to min-bisection and other NP-complete problems [78].

For constant-depth Frege systems with counting gates, there are no proven size lower bounds. Because constant-circuits with counting gates modulo a prime are known to require exponential size to compute certain functions, such as majority or sums modulo another prime, it seems that proof size lower bounds for these systems should be within our grasp. For this reason, there has been much interest regarding proof systems that utilize modular counting in limited ways. Three such systems are: **constant-depth Frege systems with counting axioms** [53, 54, 55, 56, 57, 58, 59, 68] (counting axioms state that a set of size N cannot be partitioned into sets of size m when N is indivisible by m), the **Nullstellensatz system** [56, 57, 59, 61, 60], which captures static polynomial reasoning,

and the **polynomial calculus** [70, 71, 63, 72, 73], which captures iterative polynomial reasoning. One motivation for this line of research is the possibility that constant-depth Frege proofs with counting gates might be efficiently simulated by a subsystem, one with proven size lower bounds. For example, in circuit complexity, any constant-depth circuit of ANDs, ORs, NOTs and sums modulo a prime can be transformed into an equivalent OR-of-ANDs-of-polynomials with only a quasipolynomial[3] increase in the size [79]. It is not known if the analogous depth reduction result holds for Frege systems because it is not known if the translation can be done in a way that preserves proof structure.

This dissertation furthers our knowledge of both lower bounds for proof sizes in constant-depth Frege systems and the relationship between constant-depth Frege systems with counting gates and its subsystems. We establish new lower bounds for weak pigeonhole principles and random, constant-width CNFs in constant-depth Frege systems known as the Res(k) systems. We also establish that constant-depth Frege systems with counting axioms can polynomially simulate Nullstellensatz refutations, but cannot polynomially simulate constant-depth Frege systems with counting gates or even the polynomial calculus.

I.A.1 The Res(k) Systems

Technically speaking, the Res(k) systems are not proof systems, but *refutation systems*. A **refutation system** is a proof system that proves the input formula is unsatisfiable. Because a formula is unsatisfiable if and only if its negation is a tautology, a refutation is a proof that the negation of the input formula is a tautology. **Res(k)** is a propositional refutation system whose formulas are ORs of ANDs where each AND contains at most k variables (although some variables may be negated) [4] [45].

The Res(k) systems can be viewed as intermediate between resolution

[3] A **quasipolynomial** function in n is on of the form $n^{O(\log^c n)}$ where c is a constant.

[4] A formula of this form is called a k-DNF and the Res(k) systems are sometimes called **k-DNF resolution**.

and constant depth Frege systems. Resolution can be thought of as Res(1) and depth two Frege can be thought of as Res(n) (where n is the number of variables). An interesting phenomenon is that increasing the size of the conjunctions allowed can affect the ability of the systems to prove tautologies that involve some counting. The weak pigeonhole principle, which states that it is impossible to place $2n$ pigeons into n holes without collisions, has quasipolynomial size Res($n^{O(log^{O(1)}n)}$) refutations whereas it requires exponential size resolution refutations. Therefore, there must be a critical range for k between 1 and $polylog(n)$ where these arguments become possible in sub-exponential size.

I.B Contributions

In this dissertation, we present several new results on the sizes of propositional proofs. One of our lower bound techniques also establishes a new separation in circuit complexity.

1. **The 2n to n weak pigeonhole principle requires size $2^{\Omega(n^{\epsilon})}$ to refute in Res($\sqrt{\text{logn/loglogn}}$).**

   Our lower bounds for refutations of the $2n$ to n weak pigeonhole principle are the first for Res(k) with $k \geq 3$. The weak pigeonhole principle (for any number of pigeons) is known to require an exponential number of steps to refute in resolution [29, 75, 17, 42, 24, 15, 16, 23, 20]. Atserias, Bonet and Esteban [47] gave exponential lower bounds for Res(2) refutations of the $2n$ to n weak pigeonhole principle. Moreover, because there exist Res(polylog(n)) refutations of the $2n$ to n weak pigeonhole principle of quasipolynomial size [37], our result brings the size of conjuncts allowed close to the range when sub-exponential size proofs are known to be possible.

   After this result appeared in conference [41], our techniques were extended by Alexander Razborov to show that the weak pigeonhole principle requires exponential size to refute in Res($\epsilon \log n / \log\log n$), where ϵ is a constant [21].

2. **For each k, there exists a constant w > k so that random w-CNFs in n variables require size $2^{\Omega(n^\epsilon)}$ to refute in Res(k).**

   Our lower bounds for Res(k) refutations of random w-CNFs are the first such lower bounds for Res(k) with $k \geq 3$. Resolution refutations of randomly chosen sets of clauses were known to require exponential size [27, 24, 39]. Atserias, Bonet and Esteban [47] gave exponential lower bounds for random 3-CNFs in Res(2). We extend these results to Res(k), although the width of the CNFs increases with k (it is $4k^2+2$). At present, the Res(k) systems are the strongest fragments of constant-depth Frege systems for which we know there are superpolynomial size lower bounds for refutations of random sets of clauses.

3. **We demonstrate sets of clauses on n variables that have polynomial size Res(k + 1) refutations, but require size $2^{\Omega(n^\epsilon)}$ to refute in Res(k).**

   Our separation between Res($k+1$) and Res(k) is the first for $k \geq 3$. Atserias, Bonet and Esteban [47] proved a quasi-polynomial separation between Res(2) and resolution; this separation was later strengthened to almost-exponential by Atserias and Bonet [22]. Our result further improves this separation to $2^{O(n^\epsilon)}$.

4. **Constant-depth Frege systems with counting axioms do not polynomially simulate constant-depth Frege systems with counting gates.**

   The relative power of constant-depth Frege systems with counting axioms and constant-depth Frege systems with counting axioms had been open for some time. The motivation for this question is that while there are yet no proven superpolynomial size lower bounds for proof sizes in constant-depth Frege systems with counting gates, there are exponential lower bounds for the sizes of proofs for some tautologies in constant-depth Frege systems with counting axioms [53, 54, 55, 56, 57, 58, 59]. An efficient simulation of

constant-depth Frege systems with counting gates by constant-depth Frege systems with counting axioms would give the desired proof size lower bounds for the former system.

Our lower bounds shows that a polynomial simulation is not possible. Moreover, the tautologies for which we prove the lower bound for have polynomial size proofs in the polynomial calculus, so we obtain the slightly stronger result of a separation between proof sizes for the polynomial calculus and constant-depth Frege systems with counting axioms.

5. **Constant-depth Frege systems with counting axioms polynomially simulate Nullstellensatz refutations.**

   We define a notion of reducibility from Boolean formulas to sets of polynomials and show that if a Boolean formula reduces in small size to a set of polynomials with a small Nullstellensatz refutation, then the formula has a small constant-depth Frege with counting-axioms refutation.

   This simulation has four consequences: It provides a general method for finding small proofs in constant-depth Frege systems with counting axioms. It shows that there are constant width CNFs that require exponential size constant-depth Frege refutations but have polynomial size constant-depth Frege with counting axioms refutations. When combined with result 4, it establishes a size separation between Nullstellensatz and polynomial calculus refutations. Moreover, it shows that techniques previously used to establish lower bounds for constant-depth Frege systems with counting axioms are not only sufficient but necessary.

   The proofs of size lower bounds for constant-depth Frege systems with counting axioms that appeared in papers such as [56, 57, 59, 68] followed the strategy of converting an alleged small proof into a low degree Nullstellensatz refutation and then proving that the low degree Nullstellensatz refutation cannot exist. Low degree Nullstellensatz refutations are small because there

are $O(n^d)$ monomials of degree d. Therefore, our simulation shows that if there were a low degree Nullstellensatz refutation, there would be a small constant-depth Frege with counting axioms proof.

6. **Nullstellensatz refutations do not polynomially simulate polynomial calculus refutations with respect to size.**

   Previously, it had been known that there are systems of polynomials in n variables that have constant degree polynomial calculus refutations, but require degree $\Omega(n/\log n)$ Nullstellensatz refutations [42, 60]. However, it was conceivable that the Nullstellensatz system could simulate the polynomial calculus efficiently with respect to *size* using refutations of high degree and small size. Our separation shows that this is not the case.

7. **For each constant d and k, we give a function that is computable by polynomial size depth d, bottom fan-in k + 1 circuits and requires exponential size to be computed by depth d, bottom fan-in k circuits.**

   Our result refines results of Cai, Chen and Håstad [12]. They showed that for each constant d, there exist functions computable with polynomial size, depth $d+1$, bottom fan-in 2 circuits that require exponential size to compute with depth d circuits, and that for each constant k, there exists a function of n variables computable by depth d circuits of polynomial size and bottom fan-in $O(\log n)$ that requires exponential size to compute with depth d circuits of bottom fan-in k.

Our lower bounds for proof and circuit sizes are proved using extensions of the switching lemma technique. A **switching lemma** is a guarantee that after randomly setting some of the variables to 0 and 1, with high probability, a disjunction of small ANDs can be represented by a conjunction of small ORs, thus "switching" an OR into an AND [11, 66, 14, 65]. Repeated application of such a lemma allows one to decrease the depth of a circuit until it is either a CNF or a

DNF. Such arguments were first developed to show that constant-depth circuits require exponential size to compute the parity function. Switching lemmas are used in the study of propositional proofs to transform small, constant-depth Frege proofs into proofs in another system for which we can show that the proofs in question do not exist.

The lower bound proofs for the Res(k) systems use a method we call *switching with small restrictions*, and the lower bound proof for constant-depth Frege with counting axioms uses a switching lemma that makes random *substitutions* rather than 0/1 restrictions.

I.C Credits and Coauthors

The results on Res(k) refutations and circuit bottom fan-in was done jointly with Sam Buss and Russell Impagliazzo and appeared previously in FOCS 2002 [41].

The separation between constant-depth Frege systems with counting gates and constant-depth Frege systems with counting axioms was done jointly with Russell Impagliazzo and appeared previously in FOCS 2001 [68].

The simulation of Nullstellensatz refutations by constant-depth Frege with counting axioms refutations was done jointly with Russell Impagliazzo and appeared previously in ICALP 2002 [80].

I.D Outline of the Dissertation

We define the propositional proof systems used in this dissertation and summarize the relevant in chapter II

In chapter III, we prove the switching lemma for small restrictions and use it to prove the separation between depth d, bottom fan-in $k+1$ circuits and depth d, bottom fan-in k circuits. This chapter uses no proof theory and may be read independently of the other chapters.

The lower bounds for the Res(k) proof systems are proved in chapter IV. These results are proved using the switching lemma of chapter III and that chapter is necessary prerequisite reading for this chapter.

In chapter V, we show that constant-depth Frege systems with counting axioms can polynomially simulate Nullstellensatz refutations. This chapter stands apart from chapters III and IV and can be read before either of those chapters.

The separation between constant-depth Frege systems with counting gates and constant-depth Frege systems with counting axioms is proved in chapter VI. It may be advisable to read chapters III and V before reading this chapter, depending on how familiar the reader is with switching lemmas and proof systems such as the Nullstellensatz system or constant-depth Frege with counting axioms. The earlier chapters introduce these tools in a gentler way.

I.E Notation and Background

I.E.1 Boolean Formulas and Circuits

A **literal** is a variable or its negation. A **term** is a constant 0 or 1 or a conjunction (AND) of literals. Our convention is that a term is specified as a set of literals, with 1 corresponding to the empty set and 0 to any literal and its negation. We say that a term T contains a literal l if $l \in T$, and that a term T contains a variable x if either $x \in T$ or $\neg x \in T$. We will often identify literals with terms of size one, and will write l instead of $\{l\}$. A **DNF** is a disjunction (OR) of terms, specified as a set of terms. A **k-DNF** is a DNF whose terms are each of size at most k. A **clause** is a 1-DNF, i.e. a disjunction of literals. The width of a clause C, written $w(C)$, is the number of literals appearing in C. The width of a set of clauses is the maximum width of any clause in the set. A **CNF** is a conjunction of clauses, specified as a set of clauses. A k-**CNF** is a CNF whose clauses are each of width at most k. Two terms t and t' are **consistent** if there is no literal l such that $l \in t$ and $\neg l \in t'$.

When we study constant-depth circuits and constant-depth Frege systems, we need to use AND and OR gates of **unbounded fan-in**. An OR gate of unbounded fan-in has any number of inputs and evaluates to 1 if at least one of the inputs evaluates to 1, and evaluates to 0 otherwise. Similarly, an AND gate of unbounded fan-in has any number of inputs and evaluates to 0 if at least one of the inputs evaluates to 0, and evaluates to 1 otherwise. An equivalent approach we do not use in this dissertation is to use fan-in two gates and measure depth in terms of the number of quantifier alternations.

By convention, all circuits are organized into alternating layers of AND and OR gates, with connections appearing only between adjacent levels. NOT gates may have only variables as their inputs. The output gate is said to be at level one, the gates feeding into the output gate are said to be at level two, and so forth. The depth of a circuit is the maximum level of an AND or OR gate in the circuit. The size of a circuit is the number of AND and OR gates appearing in it. The **bottom fan-in** of a depth d circuit is the maximum number of inputs to a gate at level d.

A common augmentation of constant-depth circuits is the addition of **modular gates**. While we will not use them directly in any of our results, such systems motivate several of our results, and we include their definition for completeness. Let p and a be integers. A $\mathbf{MOD}_{p,a}$ **gate** is a Boolean connective which outputs true if the sum of its inputs is a modulo p and outputs false if the sum of its inputs is not a modulo p. Constant-depth circuits with AND, OR and MOD p gates are organized into levels so that all gates in the same level are of the same type. The depth of a circuit is the maximum level of an AND, OR, or MOD p gate in the circuit.

For more detail on the basics of constant depth circuits, the reader is advised to consult the survey by Boppana and Sipser [13].

A **restriction** is a map from a set of variables to $\{0, 1, *\}$. For a formula F, **the restriction of F by a restriction** ρ**,** $\mathbf{F} \restriction_\rho$**,** is defined as usual, replacing

each gate whose value becomes determined by that value. For any restriction ρ, let $\mathrm{dom}(\rho)$ denote the set of variables to which ρ assigns the value 0 or 1.

I.E.2 Miscellaneous Mathematical Notation

For graphs $G = (V, E)$ and $S \subseteq V$ we will write $G - S$ to denote the induced subgraph on $V \setminus S$.

In this dissertation, we perform many manipulations on partitions of sets into pieces of a fixed size. We make use of the following definitions:

Definition I.E.1 *Let S be a set. The set $[\mathbf{S}]^{\mathbf{m}}$ is the collection of m element subsets of S; $[S]^m = \{e \mid e \subseteq S,\ |e| = m\}$. For $e, f \in [S]^m$, we say that* **e conflicts with f, $\mathbf{e \perp f}$,** *if $e \neq f$ and $e \cap f \neq \emptyset$.*

When N is a positive integer, we write $[N]$ for the set of integers $\{i \mid 1 \leq i \leq N\}$. The collection of m element subsets of $[N]$ are denoted by $[N]^m$, *not* by $[[N]]^m$.

Throughout this dissertation, the word polynomial is used to mean "multivariate polynomial."

Definition I.E.2 *A* **monomial** *is a product of variables. A* **term** *is scalar multiple of a monomial.*

I.E.3 Chernoff Bounds

In this dissertation, we make use of a simplified form of the Chernoff bounds. These formulations come from standard references on applying such bounds in algorithmics, (c.f. [32, 33]).

Lemma 1 *Let $X_1, \ldots, X_n$ be independent random indicator variables. Let $\mu = E[\sum_{i=1}^n X_i]$, then $Pr\left[\sum_{i=1}^n X_i < \frac{\mu}{2}\right] \leq e^{-\mu/8}$ and $Pr[\sum_{i=1}^n X_i > 2\mu] \leq e^{-\mu/4}$.*

Chapter II

A Survey of Propositional Proof Systems

In this chapter, we summarize the propositional proof systems that are the principal objects of study of this dissertation.

To allow for more elegant comparisons between different proof systems, we treat all proof systems as *refutation systems*. Propositional proof systems are usually viewed as deriving tautologies by applying inference rules to a set of axioms. However, it is useful to take the dual view that proof systems establish that a set of hypotheses is unsatisfiable by deriving FALSE from the hypotheses. Such systems are called **refutation systems**. The Nullstellensatz and polynomial calculus systems demonstrate that sets of polynomials have no common solution, and are inherently refutation systems. Frege systems are traditionally viewed as deriving tautologies, but for ease of comparison, we treat them as refutation systems. This is especially appropriate when proving that a CNF is unsatisfiable, as an unsatisfiable CNF may be viewed as a set of clauses such that no assignment satisfies every clause.

To facilitate the comparison between refutation systems that work with Boolean formulas, such as constant depth Frege, and refutation systems that work with sets of polynomials, such as the Nullstellensatz system, we identify the logical

constant FALSE with the field element 0 and the logical constant TRUE with the field element 1. This way, there is no confusion when discussing propositional formulas and polynomials in the same variables.

II.A Resolution

Resolution is a refutation system for propositional logic. It is one of the most studied proof systems, and is used as the basis for many satisfiability algorithms. Back-tracking algorithms such as DPLL that branch on a single variable provide tree-like resolution refutations on unsatisfiable formulas. General resolution proofs correspond to adding a limited form of memoization (previously refuted subproblems are saved for reuse rather than refuted again) to DPLL.

Definition II.A.1 Resolution *is the refutation system whose lines are clauses and whose only inference rule is*

$$\textit{Resolution: } \frac{A \vee x \quad \neg x \vee B}{A \vee B}$$

Let $\mathcal{C}$ be a set of clauses. A **resolution derivation from $\mathcal{C}$** *is a sequence of clauses $F_1, \ldots, F_m$ so that each F_i either belongs to $\mathcal{C}$ or follows from the preceding lines by an application of the resolution rule. For a set of clauses $\mathcal{C}$, a* **resolution refutation of $\mathcal{C}$** *is a derivation from $\mathcal{C}$ whose final line is the empty clause. The* **size** *of a resolution refutation is the number of lines it contains. $S(\mathcal{C})$ denotes the minimum size of a resolution refutation of $\mathcal{C}$. If $\mathcal{C}$ is satisfiable, then $\mathcal{C}$ has no refutation and we use the convention that $S(\mathcal{C})$ is ∞. $\mathbf{w_R}(\mathcal{C})$ denotes the minimum width of a resolution refutation of $\mathcal{C}$; if $\mathcal{C}$ is satisfiable then there is no refutation and we use the convention that $w_R(\mathcal{C})$ is ∞.*

In this dissertation, we make use of the following well-known property of resolution.

Lemma 2 *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be unsatisfiable sets of clauses on disjoint sets of variables. If there is a resolution refutation Γ of $\mathcal{C}_1 \cup \mathcal{C}_2$, then there is a refutation Γ' of either $\mathcal{C}_1$ or $\mathcal{C}_2$. Moreover, $w(\Gamma') \leq w(\Gamma)$.*

Because of the simplicity of the resolution system, a great deal is known about the refutation sizes required for many CNFs. The first lower bounds for resolution refutations were proved by Tseitin who showed that a fragment known as *regular resolution* requires exponential size to prove the pigeonhole principle [29]. About fifteen years later, Haken showed that the resolution system requires exponential size to refute the pigeonhole principle [75]. Subsequently, it was shown that resolution requires exponential size to refute the pigeonhole principle, the impossibility of placing m pigeons into n holes when $m > n$, regardless of the value of m [42, 24, 15, 16, 23, 20]. Also, resolution refutations of randomly chosen sets of clauses are known to require exponential size with high probability [27, 24, 39].

The resolution system plays a supporting role in chapter IV. The lower bound proofs for the sizes of Res(k) refutations all have the following outline: Suppose for the sake of contradiction there is a small Res(k) refutation. We apply a switching lemma and convert the small Res(k) refutation into a narrow resolution refutation, contradicting the results of [39].

II.B The Res(k) Systems

The Res(k) refutation system is a generalization of resolution that reasons with k-DNFs. As resolution refutations correspond to satisfiability algorithms that branch on a single variable, Res(k) refutations correspond to algorithms that branch on more general conditions: the value of any function of up to k variables. The sizes of Res(k) refutations were first studied by Krajíček [45], who was motivated by the connection between Res(polylog(n)) and the provability of combinatorial statements in the arithmetic theory $T_2^2(\alpha)$ (a fragment of Peano's arithmetic that allows induction only on certain bounded formulas). The first

non-trivial lower bounds for Res(k) with $k > 1$ (that do not follow from known lower bounds for constant-depth Frege systems) were proved by Atserias, Bonet and Esteban [47], who gave exponential lower bounds for Res(2) refutations of the $2n$ to n weak pigeonhole principle and of random 3-CNFs.

Definition II.B.1 **Res(k)** *is the refutation system whose lines are k-DNFs and whose inference rules are given below (A, B are k-DNF's, $1 \leq j \leq k$, and $l, l_1, \ldots, l_j$ are literals):*

$$\textit{Subsumption:}\quad \frac{A}{A \vee l} \qquad \textit{AND-introduction:}\quad \frac{A \vee l_1 \cdots A \vee l_j}{A \vee \bigwedge_{i=1}^{j} l_i}$$

$$\textit{Cut:}\quad \frac{A \vee \bigwedge_{i=1}^{j} l_i \quad B \vee \bigvee_{i=1}^{j} \neg l_i}{A \vee B} \qquad \textit{AND-elimination:}\quad \frac{A \vee \bigwedge_{i=1}^{j} l_i}{A \vee l_i}$$

Let $\mathcal{C}$ be a set of k-DNFs. A **Res(k) derivation from** $\mathcal{C}$ *is a sequence of k-DNFs $F_1, \ldots, F_m$ so that each F_i either belongs to $\mathcal{C}$ or follows from the preceding lines by an application of one of the inference rules. For a set of k-DNFs $\mathcal{C}$, a* **Res(k) refutation of** $\mathcal{C}$ *is a derivation from $\mathcal{C}$ whose final line is the empty clause. The* **size** *of a Res(k) refutation is the number of lines it contains. $S_k(\mathcal{C})$ denotes the minimum size of a Res(k) refutation of $\mathcal{C}$. If $\mathcal{C}$ is satisfiable, then $\mathcal{C}$ has no refutation and we use the convention that $S_k(\mathcal{C})$ is ∞.*

We do not use the exact definition of the $Res(k)$ system in our arguments; the main property we use is **strong soundness**: if F is inferred from $F_1, \ldots, F_j$, and $t_1, \ldots, t_j$ are consistent terms of $F_1, \ldots, F_j$ respectively, then there is a term t of F implied by $\bigwedge_{i=1}^{j} t_i$. In other words, any reason why $F_1, \ldots, F_k$ are true implies a reason why F is true. This is stronger than mere soundness[1]

Lemma 3 *Res(k) is strongly sound.*

[1] An example of an inference rule that is sound but not strongly sound is $\frac{y}{x \vee \neg x}$. The rule is sound because the conclusion is always true, but the term y does not imply x nor does it imply $\neg x$.

II.C Constant-Depth Frege Systems

Constant-depth Frege systems arise naturally in three settings. The first is as a generalization of proof systems such as resolution: whereas resolution allows the formation of only clauses, constant-depth Frege systems are able to form constant-depth formulas. The second is as a proof-theoretic analog of the circuit class AC^0 of constant-depth formulas. The third is in the study of first-order theories of arithmetic. Paris and Wilkie showed that proofs in $I\Delta_0$ (a fragment of Peano's arithmetic that allows induction only on bounded formulas) can be translated into small constant-depth Frege proofs [62]. Hence, establishing size lower bounds for constant-depth Frege proofs is a way of obtaining independence results for these arithmetic theories.

A **Frege system** is a sound, implicationally complete propositional proof system over a finite set of connectives with a finite number of axiom schemata and inference rules. By the methods of Cook and Reckhow [74], any two Frege systems simulate one another up to a polynomial factor in size and a linear factor in depth. For concreteness, the reader can keep in mind the following Frege system.

Definition II.C.1 *Let $\mathcal{F}$ be the proof system whose connectives are NOT gates, $\neg$, and unbounded fan-in OR gates, $\bigvee$, and whose inference rules are:*

$$\textit{Axioms: } \frac{}{A \vee \neg A} \qquad \textit{Weakening: } \frac{A}{A \vee B} \qquad \textit{Cut: } \frac{A \vee B \quad (\neg A) \vee C}{B \vee C}$$

$$\textit{Merging: } \frac{\bigvee X \vee \bigvee Y}{\bigvee (X \cup Y)} \qquad \textit{Unmerging: } \frac{\bigvee (X \cup Y)}{\bigvee X \vee \bigvee Y}$$

Let $\mathcal{H}$ be a set of formulas. A **derivation** *from $\mathcal{H}$ is a sequence of formulas $f_1, \ldots, f_m$ so that for each $i \in [m]$, either f_i is a substitution instance of an axiom, f_i is an element of $\mathcal{H}$, or there exist $j, k < i$ so that f_i follows from f_j and f_k by the application of an inference rule to f_j and f_k. For a given formula F, a* **proof of F** *is a derivation from the empty set of hypotheses whose final formula is F. For fixed set of hypotheses $\mathcal{H}$, a* **refutation of $\mathcal{H}$** *is a derivation from $\mathcal{H}$ whose*

final formula is FALSE. The **size** *of a derivation is the total number of symbols appearing in it. We say that a family of tautologies (unsatisfiable formulas) τ_n, each of size $s(n)$, has* **polynomial size constant-depth Frege proofs (refutations)** *if there are constants c and d so that for all n, there is a proof (refutation) of τ_n so that each formula in the proof has depth at most d, and the proof (refutation) has size $O(s^c(n))$.*

In general, tautologies that involve counting are known to require large constant-depth Frege proofs. Intuitively, this is because constant-depth formulas cannot compute functions that involve counting. For example, the pigeonhole principle, the modular counting principles, and the Tseitin graph tautologies, are all known to require exponential size constant-depth Frege proofs [48, 50, 51, 9]. It is not currently known if there are polynomial size constant-depth Frege refutations of the weak pigeonhole principle (the impossibility of placing $2n$ pigeons into n holes), or if a random 3-CNF can be expected to require exponential size constant-depth Frege refutation.

II.D Constant-depth Frege Systems with Counting Gates

The proof systems whose lines are constant-depth circuits with modular counting gates are called constant-depth Frege systems with counting gates. From the perspective of mathematical logic, these systems correspond to fragments of Peano's arithmetic which allow counting quantifiers [62, 52].

Definition II.D.1 *Fix a constant m. Let $\mathcal{F}_m$ be the proof system whose connectives are NOT gates, unbounded fan-in OR gates, and unbounded fan-in $MOD_{m,a}$ gates, for $0 \leq a \leq m-1$. The inference rules of $\mathcal{F}_m$ are those of $\mathcal{F}$, with the addition of the following axiom schema: $MOD_{m,0}(\emptyset)$, for $1 \leq a \leq m-1$, $\neg MOD_{m,a}(\emptyset)$, and for each a,*

$$\begin{aligned} MOD_{m,a}(A_1, \ldots, A_k,\ A_{k+1}) \quad \leftrightarrow \quad & (MOD_{m,a}(A_1, \ldots, A_k) \wedge \neg A_{k+1}) \\ & \vee (MOD_{m,a-1}(A_1, \ldots, A_k) \wedge A_{k+1}) \end{aligned}$$

The sizes of proofs and refutations are defined analogously as for the Frege system $\mathcal{F}$.

Note that these systems augment constant-depth Frege systems not only with modular counting gates, but with *infinitely many* axiom schema. While these axioms have polynomial-size Frege proofs, they do not have polynomial-size constant-depth Frege proofs. This is why the simulation of [74] does not show that constant-depth Frege systems can simulate constant-depth Frege systems with counting axioms with a polynomial increase in size and a linear increase in depth. If we were to simply add counting gates to a constant-depth Frege system without these axioms, the simulation would apply and the new system could be simulated by constant-depth Frege systems with only a small increase in size.

Despite the successes for proving size lower bounds for constant-depth circuits with counting gates [82], there are no known superpolynomial lower bounds for constant-depth Frege systems with counting gates.

II.E Constant-depth Frege Systems with Counting Axioms Modulo m

Constant-depth Frege systems with counting axioms are a powerful fragment of constant-depth Frege systems with counting gates. One of the central results of this dissertation is that constant-depth Frege systems with counting axioms do not polynomially simulate constant-depth Frege systems with counting gates.

After the discovery of lower bounds on the sizes of constant-depth Frege proofs of the pigeonhole principle, it was discovered that there exist counting principles that are stronger than the pigeonhole principle in a proof-theoretic sense. Consider the "parity principle": when n is odd, it is impossible to partition a set of N elements into sets of size two. Because a perfect matching from a set of size $n+1$ to a set of size n provides exactly such a partition, this principle implies the

pigeonhole principle. However, constant-depth Frege proofs of the parity principle require exponential size even when the pigeonhole principle is allowed as an axiom [53, 55]. This launched a study of the sizes of proofs needed when modular counting axioms are added to constant-depth Frege systems.

Definition II.E.1 *Let $m > 1$ and $N \not\equiv_m 0$ be given. Let V be a set of N elements. For each $e \in [V]^m$, let there be a variable x_e.*

$$\mathbf{Count_m^V} = \bigvee_{v \in V} \left(\bigwedge_{\substack{e \in [V]^m \\ e \ni v}} \neg x_e \right) \quad \vee \bigvee_{\substack{e,f \in [V]^m \\ e \perp f}} (x_e \wedge x_f)$$

Constant-depth Frege with counting axioms modulo m *are constant-depth Frege systems that allow the use of substitution instances of $Count_m^{[N]}$ (with $N \not\equiv_m 0$) as axioms. The sizes of proofs and refutations are defined analogously as for the Frege system $\mathcal{F}$.*

It is known that constant-depth Frege systems with counting axioms modulo p require exponential size to prove counting axioms modulo q when q has a prime factor that is not a factor of p [54, 55, 56, 57, 58, 59].

II.F Nullstellensatz Refutations

One way to prove that a system of polynomials $f_1, \ldots, f_k$ has no common roots is to give a list of polynomials $p_1, \ldots, p_k$ so that $\sum_{i=1}^{k} p_i f_i = 1$. Because we are interested in translations of propositional formulas, we add the polynomials $x^2 - x$ as hypotheses to guarantee all roots are zero-one roots. This method, known as the **Nullstellensatz system**, was first introduced as a tool for proving lower bounds for constant-depth Frege systems with counting axioms [56]. The Nullstellensatz system is efficient in the sense that if there is a low-degree Nullstellensatz refutation of a system of polynomials, then such a refutation can be found by solving a system of linear equations.

Definition II.F.1 *For a system of polynomials $f_1, \ldots, f_k$ in variables $x_1, \ldots, x_n$ over a field F, a* **Nullstellensatz refutation** *is a list of polynomials $p_1, \ldots, p_k$, $r_1, \ldots, r_n$ satisfying the following equation:*

$$\sum_{i=1}^{k} p_i f_i + \sum_{j=1}^{n} r_j \left(x_j^2 - x_j\right) = 1$$

For a polynomial q, **Nullstellensatz derivation of q from $\mathbf{f_1}, \ldots, \mathbf{f_k}$** *is a list of polynomials $p_1, \ldots, p_k$, $r_1, \ldots, r_n$ satisfying the following equation:*

$$\sum_{i=1}^{k} p_i f_i + \sum_{j=1}^{n} r_j \left(x_j^2 - x_j\right) = q$$

The **degree** *of the refutation (derivation) is the maximum degree of the polynomials $p_i f_i$, $r_j \left(x_j^2 - x_j\right)$. We define the* **size** *of a Nullstellensatz refutation (derivation) to be the number of monomials appearing in $p_1, \ldots, p_k$ and $f_1, \ldots, f_k$.*

Hilbert's weak Nullstellensatz guarantees that over a field, all unsatisfiable systems of polynomials have Nullstellensatz refutations [3]. We can define Nullstellensatz refutations over any ring, but such systems are no longer complete. In this dissertation, we work with Nullstellensatz refutations of polynomials over $\mathbb{Z}_m$, and for the sake of generality, we make no assumptions on m unless otherwise stated.

Nullstellensatz refutations modulo p are known to require super-constant degree to refute polynomial versions of the pigeonhole principle [71, 63], counting principles of modulus q when q is coprime with p [56, 57], and the linear induction principles (if x_1 is true, and x_i implies x_{i+1} for all i, then x_n must be true) [61, 60].

II.G The Polynomial Calculus

The polynomial calculus is a method for demonstrating that a system of polynomials $f_1, \ldots, f_k$ has no roots by expressing the polynomial 1 by iteratively taking linear combinations of previously derived polynomials or multiplying previously derived polynomials by arbitrary polynomials [70]. The system is efficient

in that if there exists a degree d polynomial calculus refutation of a system of polynomials in n variables, then the refutation can be found in time $n^{O(d)}$ by a variant of the Gröbner basis algorithm.

Definition II.G.1 *Let $f_1, \ldots, f_k$ be polynomials over a field F. A* **polynomial calculus refutation of** $f_1, \ldots, f_k$ **over** F *is a sequence of polynomials $g_1, \ldots, g_m$ so that, $g_m = 1$, and for each $i \in [m]$, either g_i is f_l for some $l \in [k]$, g_i is ${x_l}^2 - x_l$ for some $l \in [n]$, g_i is $ag_j + bg_l$ for some $j, l < i, a, b \in F$, or g_i is $x_l g_j$ for some $j < i$, $l \in [n]$.*

The **size** *of a polynomial calculus refutation is the total number of monomials appearing in the polynomials of the refutation. The* **degree** *of a polynomial calculus refutation is the maximum degree of a polynomial that appears in the refutation.*

The polynomial calculus is known to require exponential size to refute the pigeonhole principle [71, 63] and the algebraic translations of random 3-CNFs [72, 69].

The polynomial calculus system can simulate Nullstellensatz refutations with no increase in size or degree. Moreover, the polynomial calculus is more efficient than the Nullstellensatz system in with respect to *degrees* [61, 60]. The polynomial calculus can refute the linear induction principles in constant degree whereas this system requires super-constant degree Nullstellensatz refutations. One of the results of this dissertation is that the polynomial calculus can prove principles in polynomial size that require super-polynomial size Nullstellensatz refutations.

Chapter III

A Switching Lemma for Small Restrictions

A switching lemma is a guarantee that after the application of a randomly chosen restriction, a disjunction of small ANDs can be represented by a conjunction of small ORs, thus "switching" an OR into an AND [11, 66, 14, 65]. One thing that all of these switching lemmas had in common was that the random restrictions used set a majority of the variables.

In this chapter, we prove a switching lemma that is allowed to set a small number of the variables, even as few as $n^{1-\epsilon}$ out of n. The trade-off is that ORs of *extremely* small ANDs are transformed into ANDs of modestly small ORs. Therefore, our switching lemma cannot be iterated to prove lower bounds for proof systems of depth more than two. However, one application of our switching lemma suffices to prove lower bounds for the Res(k) proof systems, because each line in such a proof is of depth two with small bottom fan-in.

At the end of this chapter, we apply our switching lemma to obtain an exponential separation between depth d circuits of bottom fan-in $k+1$ and depth d circuits of bottom fan-in k.

III.A Switching with Small Restrictions

A common formulation of switching lemmas is that after the application of a random restriction, a DNF can be represented by a short decision tree. Functions represented by a height h decision tree can be computed by an h-CNF and by an h-DNF, so this formulation allows OR gates to be switched to an AND gates. The decision tree formulation of the switching lemma is especially useful for proving size lower bounds for Res(k) refutations because of a connection between decision trees and resolution refutations that we prove in chapter IV, section IV.A.

Definition III.A.1 *A* **decision tree** *is a rooted binary tree in which every internal node is labeled with a variable, the edges leaving a node correspond to whether the variable is set to* 0 *or* 1*, and the leaves are labeled with either* 0 *or* 1*. Every path from the root to a leaf may be viewed as a partial assignment. For a decision tree T and $v \in \{0,1\}$, we write the set of paths (partial assignments) that lead from the root to a leaf labeled v as $Br_v(T)$. For a partial assignment ρ, $T \restriction_\rho$ is the decision tree obtained by deleting from T every edge whose label conflicts with ρ and contracting along each edge whose label belongs to ρ. We say that a decision tree T* **strongly represents** *a DNF F if for every $\pi \in Br_0(T)$, for all $t \in F$, $t \restriction_\pi = 0$ and for every $\pi \in Br_1(T)$, there exists $t \in F$, $t \restriction_\pi = 1$. The representation height of F, $h(F)$, is the minimum height of a decision tree strongly representing F.*

If a function is computed by a height h decision tree, then we can compute the function with an h-CNF: for each branch that leads to a leaf labeled 0, include the clause stating that that branch is *not* taken. In chapter VI we use the fact that if F is strongly represented by a height h decision tree, then it can be computed by a degree h polynomial over any field.

Our switching lemma will exploit a trade-off based on the minimum size of a set of variables that meets each term of a k-DNF. When this quantity is small, we can build a decision tree by querying these variables and recursing on

the $(k-1)$-DNFs created. When this quantity is large, the DNF has many disjoint terms and is likely to be satisfied by a random restriction.

Definition III.A.2 *Let F be a DNF, and let S be a set of variables. If every term of F contains a variable from S, then we say that* **S is a cover of F.** *The* **cover number of F, c(F),** *is the minimum cardinality of a cover of F.*

For example, the 3-DNF $xyz \vee \neg x \vee yw$ has cover number two.

The switching lemma is shown to hold for all distributions which satisfy certain properties. When we apply the switching lemma, we will show that the random restrictions used satisfy these properties.

Theorem 4 *Let $k \geq 1$, let $s_0, \ldots, s_{k-1}$ and $p_1, \ldots, p_k$ be sequences of positive numbers, and let $\mathcal{D}$ be a distribution on partial assignments so that for every $i \leq k$ and every i-DNF G, if $c(G) > s_{i-1}$, then $Pr_{\rho \in \mathcal{D}}[G \restriction_\rho \neq 1] \leq p_i$. Then for every k-DNF F:*

$$Pr_{\rho \in \mathcal{D}}\left[h(F \restriction_\rho) > \sum_{i=0}^{k-1} s_i\right] \leq \sum_{i=1}^{k} 2^{\left(\sum_{j=i}^{k-1} s_j\right)} p_i$$

Proof: We proceed by induction on k. First consider $k = 1$. If $c(F) \leq s_0$, then at most s_0 variables appear in F. We can construct a height $\leq s_0$ decision tree that strongly represents $F \restriction_\rho$ by querying all of the variables of $F \restriction_\rho$. On the other hand, if $c(F) > s_0$ then $\Pr_{\rho \in \mathcal{D}}[F \restriction_\rho \neq 1] \leq p_1$. Therefore, $h(F \restriction_\rho)$ is non-zero with probability at most $p_1 2^{\sum_{j=1}^{k-1} s_j} = p_1$ (because $k = 1$).

For the induction step, assume that the theorem holds for all k-DNFs, and let F be a $(k+1)$-DNF. If $c(F) > s_k$, then by the conditions of the lemma, $\Pr_{\rho \in \mathcal{D}}[F \restriction_\rho \neq 1] \leq p_{k+1}$. Because $p_{k+1} \leq \sum_{i=1}^{k+1} 2^{\sum_{j=i}^{k} s_j} p_i$, we have that $h(F \restriction_\rho)$ is non-zero with probability at most $\sum_{i=1}^{k+1} 2^{\sum_{j=i}^{k} s_j} p_i$.

Consider the case when $c(F) \leq s_k$. Let S be a cover of F of size at most s_k. Let π be any assignment to the variables in S. Because each term of F contains at least one variable from S, $F \restriction_\pi$ is a k-DNF. By combining the induction

hypothesis with the union bound (and the fact $F \restriction_\rho \restriction_\pi = F \restriction_\pi \restriction_\rho$), we have that

$$\begin{aligned} \Pr_{\rho\in\mathcal{D}}\left[\exists\pi\in\{0,1\}^S \;\; h((F\restriction_\rho)\restriction_\pi) > \textstyle\sum_{i=0}^{k-1} s_i\right] &\leq 2^{s_k}\left(\textstyle\sum_{i=1}^{k} 2^{\left(\sum_{j=i}^{k-1} s_j\right)} p_i\right) \\ &< \textstyle\sum_{i=1}^{k+1} 2^{\left(\sum_{j=i}^{k} s_j\right)} p_i \end{aligned}$$

In the event that $\forall\pi\in\{0,1\}^S$, $h((F\restriction_\rho)\restriction_\pi) \leq \sum_{i=0}^{k-1} s_i$, we construct a decision tree for $F\restriction_\rho$ as follows. First, query all variables in S unset by ρ, and then underneath each branch, β, simulate a decision tree of minimum height strongly representing $(F\restriction_\rho)\restriction_\beta$. For each such β, let $\pi = (\rho\cup\beta)\restriction_S$, and note that $h((F\restriction_\rho)\restriction_\beta) = h((F\restriction_\rho)\restriction_\pi)$. Therefore the height of the resulting decision tree is at most $s_k + \max_{\pi\in\{0,1\}^S} h((F\restriction_\rho)\restriction_\pi) \leq \sum_{i=0}^{k} s_i$.

Now we show that the decision tree constructed above strongly represents $F\restriction_\rho$. Let π be a branch of the tree. Notice that $\pi = \beta\cup\sigma$, where β is an assignment to the variables in $S\setminus \mathrm{dom}(\rho)$ and σ is a branch of a tree that strongly represents $(F\restriction_\rho)\restriction_\beta$. Consider the case that π leads to a leaf labeled 1. In this case, σ satisfies a term t' of $(F\restriction_\rho)\restriction_\beta$. We may choose a term t of F so that $t' = (t\restriction_{\rho\cup\beta})$, and $\pi = \beta\cup\sigma$ satisfies the term $t\restriction_\rho$ of $F\restriction_\rho$. Now consider the case that π leads to a leaf labeled 0. There are two cases, $(F\restriction_\rho)\restriction_\beta = 0$ and $(F\restriction_\rho)\restriction_\beta \neq 0$. If $(F\restriction_\rho)\restriction_\beta = 0$, then for every term t of $F\restriction_\rho$, t is inconsistent with β and hence with π. If $(F\restriction_\rho)\restriction_\beta \neq 0$ then because the sub-tree underneath β strongly represents $(F\restriction_\rho)\restriction_\beta$, for every term t of $(F\restriction_\rho)\restriction_\beta$, t is inconsistent with σ. Therefore, every term of $F\restriction_\rho$ is inconsistent with either β or σ, and thus with $\pi = \beta\cup\sigma$. ∎

We usually use this theorem in the following normal form for the parameters:

Corollary 5 *Let k, s and d be positive integers, let γ and δ be real numbers from the range $(0,1]$ and let $\mathcal{D}$ be a distribution on partial assignments so that for every k-DNF G, $Pr_{\rho\in\mathcal{D}}[G\restriction_\rho \neq 1] \leq d2^{-\delta(c(G))^\gamma}$. For every k-DNF F:*

$$Pr_{\rho\in\mathcal{D}}[h(F\restriction_\rho) > 2s] \leq dk2^{-\delta' s^{\gamma'}}$$

where $\delta' = 2(\delta/4)^k$ and $\gamma' = \gamma^k$.

Proof: Let $s_i = (\delta/4)^i(s^{\gamma^i})$, and $p_i = d2^{-4s_i}$. Note that $s_{i-1}/4 \geq (\delta/4)s_{i-1} = (\delta/4)(\delta/4)^{i-1}s^{\gamma^{i-1}} \geq (\delta/4)^i s^{\gamma^i} = s_i$. It follows that $\sum_{j=i}^{k} s_j \leq \sum_{j \geq i} s_i/4^{j-i} \leq 2s_i$. Also, for any i-DNF G, with $c(G) \geq s_{i-1}$, $\Pr_{\rho \in \mathcal{D}}[G \restriction_\rho \neq 1] \leq d2^{-\delta(c(G))^\gamma} \leq d2^{-\delta s_{i-1}^\gamma} = 2^{-\delta(\delta/4)^{i-1}(s^{\gamma^{i-1}})^\gamma} = d2^{-4s_i}$. Thus, we can apply theorem 4 with parameters $p_1, \ldots, p_k, s_0, \ldots, s_{k-1}$. For every k-DNF F:

$$\begin{array}{rcccl} \Pr_{\rho \in \mathcal{D}}[h(F \restriction_\rho) > 2s] & \leq & \Pr_{\rho \in \mathcal{D}}\left[h(F \restriction_\rho) > \sum_{i=0}^{k-1} s_i\right] & \leq & \sum_{i=1}^{k} 2^{\left(\sum_{j=i}^{k-1} s_j\right)} p_i \\ & \leq & \sum_{i=1}^{k} 2^{2s_i}(d2^{-4s_i}) & \leq & dk2^{-2s_k} = dk2^{-\delta' s^{\gamma'}} \end{array}$$

■

III.A.1 Switching with Small Restrictions

In this subsection, we show that small, uniform restrictions meet the conditions for the switching lemma. Using corollary 5, k-DNFs can then be converted into decision trees – *using restrictions that set only a polynomially small fraction of the bits.* We include it here for comparison with previous switching lemmas. Later, it will be used to prove the lower bound on Res(k) refutations of random CNFs. More complicated distributions are used for our other results.

Definition III.A.3 *Let $n > 0$ and $p \in [0, 1]$. Define $\mathcal{D}_p$ to be the family of random restrictions which arises by assigning variables $*$ with probability $1 - p$, and 0, 1 each with probability $\frac{p}{2}$.*

Lemma 6 *Let $i \geq 1$, G be an i-DNF, and ρ be chosen from $\mathcal{D}_p$. Then $Pr[G \restriction_\rho \neq 1] \leq e^{-\frac{c(G)p^i}{i2^i}}$.*

Proof: Because every covering set of G has size at least $c(G)$, there is a set of variable-disjoint terms of size at least $c(G)/i$ (such a set can be found by greedily choosing a maximal set of disjoint terms). Each of these variable-disjoint terms is satisfied with independent probability at least $(p/2)^i$. Therefore,

$$\Pr_{\rho \in \mathcal{D}_p}[G \restriction_\rho \neq 1] \leq \left(1 - \left(\frac{p}{2}\right)^i\right)^{\frac{c(G)}{i}} \leq e^{-\left(\frac{p}{2}\right)^i \frac{c(G)}{i}} = e^{-\frac{c(G)p^i}{i2^i}}$$

■

Combining this with the switching lemma shows that a k-DNF is strongly represented by a short decision tree when restricted.

Corollary 7 *Let $k \geq 1$ be given. There exists $\gamma > 0$ so that for any k-DNF F, $w > 0$, $p \geq n^{-1/(2k^2)}$, $Pr_{\rho \in \mathcal{D}_p}[h(F \restriction_\rho) > w] \leq k2^{-\gamma w n^{-1/2}}$.*

Proof: In the notation of corollary 5, set $p = n^{-1/2k^2}$, $d = 1$, $\gamma = 1$, $s = w/2$ and $\delta = (\log e)\frac{p^k}{k2^k} = (\log e)\frac{n^{-1/2k}}{k2^k}$. Combining lemma 6 with corollary 5 shows that for every k-DNF F:

$$\Pr_{\rho \in \mathcal{D}_p}[h(F \restriction_\rho) > w] \leq k2^{-2(w/2)(\delta^k/4^k)} = k2^{-w(\log e)^k n^{-1/2}/(4^k k^k 2^{k^2})}$$

Because k is fixed, we may take $\gamma = (\log e)^k/(4^k k^k 2^{k^2})$. ∎

We take a moment to contrast corollary 7 with Håstad's switching lemma. Recall that whenever $F \restriction_\rho$ is strongly represented by a height w decision tree, it is also computed by a w-CNF.

Theorem 8 *([14], c.f. [13, 65]) Let positive integers k and w be given. Setting $\phi = (1+\sqrt{5})/2$ and $\gamma = 2/\ln\phi$ (note that $\gamma > 4$), we have that for any k-DNF F,*

$$Pr_{\rho \in \mathcal{D}_p}[F \restriction_\rho \text{ cannot be computed by a } w\text{-CNF}] \leq (\gamma(1-p)k)^w$$

To collapse a k-DNF to a w-CNF using theorem 8, it is necessary for $1-p$, the probability of a variable being unset, to be strictly less than $\frac{1}{\gamma k}$. On the other hand, corollary 7 will collapse a k-DNF to a w-CNF when the probability of a variable being unset is as large as $1 - n^{-\epsilon}$.

III.B An Application to Circuit Bottom Fan-in

Our first application of the switching lemma is an exponential size separation between depth d circuits of bottom fan-in k and depth d circuits of bottom fan-in $k+1$.

Our circuits are organized into alternating layers of AND and OR gates, with connections appearing only between adjacent levels. NOT gates may have only variables as their inputs. The output gate is said to be at level one, the gates feeding into the output gate are said to be at level two and so forth. The depth of a circuit is the maximum depth of an AND or OR gate in the circuit. The size of a circuit is the number of AND and OR gates appearing in it. The **bottom fan-in** of a depth d circuit is the maximum number of inputs of a gate at level d. For more detail on the basics of constant depth circuits, consult the survey by Boppana and Sipser [13].

III.B.1 The Functions

Definition III.B.1 *[10, 13] Let integers d and $m_1, \ldots, m_d$ be given, and let there be variables $x_{i_1,\ldots,i_d}$ for $1 \leq i_j \leq m_j$.*

$$\mathbf{f_d^{m_1,\ldots,m_d}} = \bigwedge_{i_1 \leq m_1} \bigvee_{i_2 \leq m_2} \cdots \bigodot_{i_d \leq m_d} x_{i_1,\ldots,i_d}$$

Where $\bigodot = \bigvee$ if d is even, and $\bigodot = \bigwedge$ if d is odd.

The **Sipser function $\mathbf{f_d^m}$** *is $f_d^{m_1,\ldots,m_d}$ with $m_1 = \sqrt{m/\log m}$, $m_2 = \cdots = m_{d-1} = m$ and $m_d = \sqrt{dm \log m/2}$.*

The **modified Sipser function $\mathbf{g_d^{m,k}}$** *is $f_{d+1}^{m_1,\ldots,m_d,k}$, with $m_1 = \sqrt{m/\log m}$, $m_2 = \cdots = m_{d-1} = m$, and $m_d = 4\sqrt{dm \log m/2}$.*

Notice that the function f_d^m depends on $m^{d-1}\sqrt{d/2}$ many variables and it can be computed by a circuit of depth d and size linear in the number of variables. Furthermore, we will often identify these functions with the circuits defining them.

Our result builds upon the earlier result that it is impossible to decrease the bottom fan-in of a circuit computing a Sipser function without without increasing the size or the depth. Moreover, Σ_d circuits of small bottom fan-in circuits require exponential size to compute f_d^m.

Theorem 9 *[14] For all $d \geq 1$, there exists $\epsilon_d > 0$ so that if a depth d, bottom fan-in k circuit with an AND gate at the output and at most S gates in levels 1 through $d-1$ computes f_d^m, then either $k \geq m^{\epsilon_d}$ or $S \geq 2^{m^{\epsilon_d}}$.*

For all $d \geq 1$, there exists $\beta_d > 0$ so that if a depth $d+1$, bottom fan-in k circuit with an OR gate at the output and at most S gates in levels 1 through d computes f_d^m, then either $S \geq 2^{m^{\beta_d}}$ or $k \geq m^{\beta_d}$.

We use the modified Sipser function $g_d^{m,k+1}$ to obtain the exponential separation between depth $d+1$, bottom fan-in $k+1$ and depth $d+1$, bottom fan-in k circuits. Notice that the function $g_d^{m,k}$ has $4m^{d-1}\sqrt{d/2}$ many blocks and $4km^{d-1}\sqrt{d/2}$ many variables. Moreover, it can be computed by a circuit of depth $d+1$, bottom fan-in k and size linear in the number of variables. For each $i_1, \ldots, i_d$, we say that the variables $x_{i_1,\ldots,i_d,1}, \ldots, x_{i_1,\ldots,i_d,k}$ come from **block** $(\mathbf{i_1}, \ldots, \mathbf{i_d})$. Variables in the same block occur in the same bottom-level conjunction of $g_d^{m,k}$.

III.B.2 The Lower Bounds

We will show that depth $d+1$ circuits with bottom fan-in k require exponential size to compute $g_d^{m,k+1}$. In light of theorem 9, it suffices to consider only circuits with an AND gate at the output level. Furthermore, we consider only the case when d is even. This ensures that all gates at depth d are OR gates. The case for odd d is dual and we simply invert the random restriction used. Each gate at depth d computes a k-DNF, and we will apply a random restrictions which almost certainly collapse all of the k-DNFs to narrow CNFs and thus collapse the circuits to depth d circuits with small bottom fan-in. On the other hand, the random restrictions will probably leave $g_d^{m,k+1}$ containing f_d^m as a sub-function, and thus we obtain a contradiction to theorem 9.

Definition III.B.2 *Let m, d and k be given. Set $m_1 = \sqrt{m/logm}$, $m_2 = \cdots = m_{d-1} = m$ and $m_d = 4\sqrt{dm \log m/2}$.*

Let $\mathcal{B}^{\mathbf{m,k+1}}_{\mathbf{d,0}}$ *be the random distribution on partial assignments given by the following experiment: for each* $i_1 \leq m_1, \ldots, i_d \leq m_d$*, with independent probability probability* $\frac{1}{2}$ *either set* $x_{i_1,\ldots,i_d,j} = *$*, for all* $j \in [k+1]$*, or uniformly choose a* $0/1$ *assignment to* $\{x_{i_1,\ldots,i_d,j} \mid j \in [k+1]\}$ *which sets at least one of the variables to* 0*. The dual distribution,* $\mathcal{B}^{\mathbf{m,k+1}}_{\mathbf{d,1}}$*, selects a restriction according to* $\mathcal{B}^{m,k+1}_{d,0}$ *and then inverts the* 0*s and* 1*s.*

Lemma 10 *Let* $k \geq 1$ *be given. There exists a constant* $\gamma_k > 0$ *so that for every* k*-DNF* F*:*

$$Pr_{\rho \in \mathcal{B}^{m,k+1}_{d,0}} [F \restriction_\rho \neq 1] \leq 2^{-\gamma_k c(F)}$$

Proof: We say that two terms T and T' are **block-disjoint** if no variable of T shares a block with a variable of T'. More formally, whenever a variable $x_{i_1,\ldots,i_{d+1}}$ appears in T and a variable $x_{j_1,\ldots,j_{d+1}}$ appears in T', we have that $(i_1, \ldots, i_d) \neq (j_1, \ldots, j_d)$. Because each term involves at most k variables, there must be a set of $c(F)/k$ many variable-disjoint terms, and hence a set of $c(F)/(k(k+1))$ many block-disjoint terms.

We now show that each term is satisfied with probability at least $\frac{1}{6^k}$. Because the literals of a term come from at most k distinct blocks, the chance that every variable in the term is set to 0 or 1 is at least $1/2^k$. Conditioned on this event, the probability of satisfying the term is at least $1/3^k$. To see this, consider the chance of satisfying each literal of the term in turn, conditioned on the event of satisfying the previous literals. If a variable from that block has already been set to 0, then clearly the probability of satisfying the current literal is $1/2$. If not, then suppose there l variables in the block of the current variable that have not yet been set to a value. The probability of satisfying the current literal is at least $(2^{l-1}-1)/(2^l-1)$. Because there are $k+1$ variables and the term has size at most k, $l \geq 2$, and thus the probability is at least $1/3$.

The events of satisfying block-disjoint terms are independent, therefore we have:

$$\Pr_{\rho \in \mathcal{B}_{d,0}^{m,k+1}} [F \restriction_\rho \neq 1] \leq \left(1 - \frac{1}{6^k}\right)^{c(F)/(k(k+1))}$$

Set $\gamma_k = -\log_2(1 - \frac{1}{6^k})/(k(k+1))$. ∎

Symmetrically, the dual result holds for k-CNFs when we apply a random restriction from $\mathcal{B}_{d,1}^{m,k+1}$.

Lemma 11 *Let $k \geq 1$ be given. There exists a constant ϵ_k so that for all d, for all w sufficiently large with respect to k, and for every depth $d+1$, bottom fan-in k circuit C of size $S \leq 2^{\epsilon_k w}$, when by ρ is chosen from $\mathcal{B}_{d,0}^{m,k+1}$ ($\mathcal{B}_{d,1}^{m,k+1}$), with probability at least $3/4$, $C \restriction_\rho$ is is equivalent to a depth d, bottom fan-in w circuit with at most S gates in levels 1 through $d-1$.*

Proof: We will solve for the particular values of ϵ_k and w after going through the calculations.

We consider the case when d is even; the case when d is odd is handled by using the restrictions $\mathcal{B}_{d,1}^{m,k+1}$ instead of $\mathcal{B}_{d,0}^{m,k+1}$. Each gate at depth d is an OR gate and its inputs are AND gates of fan-in at most k. For each gate g at depth d, we let F_g denote the k-DNF computed by the sub-circuit at g.

Suppose that there is a partial assignment $\rho \in \mathcal{B}_{d,0}^{m,k}$ so that for each depth d gate g of C, $h(F_g \restriction_\rho) < w$. For each g at depth d, let T_g be the shortest decision tree representing $F_g \restriction_\rho$. We can compute $C \restriction_\rho$ with a depth d, bottom fan-in w circuit with at most S gates in levels 1 through $d-1$ by starting with C, replacing each level d gate g with the conjunction of the negated branches of $\mathrm{Br}_0(T_g)$ and then merging these conjuncts with the AND gate at depth $d-1$ to which g sends its output.

We now show that for ρ chosen according to the distribution $\mathcal{B}_{d,0}^{m,k}$, with probability at least $3/4$, every depth d gate g of C has $h(F_g \restriction_\rho) < w$.

Let g be a depth d gate of the circuit. By combining lemma 10 with corollary 5, setting $d = 1$, $\gamma = 1$ $s = w/2$ and $\delta = \gamma_k$ shows that

$$\Pr_{\rho \in \mathcal{B}_{d,0}^{m,k}}[h(F_g) > w] \leq k2^{-w\gamma_k^k/4^k}$$

Because there are at most $S = 2^{\epsilon_k w}$ many gates at depth d, by the union bound, there exists a gate with $h(F_g) > w$ with probability at most $2^{w(\epsilon_k - \gamma_k^k/4^k)+\log k}$. We simply take ϵ_k sufficiently small so that this probability is less than $1/4$. ∎

Theorem 12 *For all $k \geq 1$, $d \geq 1$, there exists $\epsilon_k, \epsilon_d > 0$ so that for every m sufficiently large, every size S, depth $d+1$ bottom fan-in k circuit for $g_d^{m,k+1}$ has $S \geq 2^{\epsilon_k m^{\epsilon_d}}$.*

Proof: We will have to take m sufficiently large to apply theorem 9 and lemma 11, and large enough for an application of the Chernoff bounds. Set $w = m^{\epsilon_d}$ (with ϵ_d from theorem 9) and $S = 2^{\epsilon_k w}$ (with ϵ_k from lemma 11). Furthermore, we consider the case when d is even; the case when d is odd is handled by using the restrictions $\mathcal{B}_{d,1}^{m,k+1}$ instead of $\mathcal{B}_{d,0}^{m,k+1}$.

Suppose, for the sake of contradiction, that C is a size S, depth d, bottom fan-in k circuit computing $g_d^{m,k+1}$.

Fix an OR gate at depth d in $g_d^{m,k+1}$. When ρ is chosen from the distribution $\mathcal{B}_{d,0}^{m,k+1}$, the expected number of blocks underneath this gate that are left unset is $2\sqrt{dm \log m/2}$. By the Chernoff bounds, with probability at most $e^{-\sqrt{dm \log m/2}/4}$ are there fewer than $\sqrt{dm \log m/2}$ blocks left unset by ρ underneath this gate.

Because there are $m^{d-3/2}/\sqrt{\log m}$ many depth d gates in $g_d^{m,k+1}$, by the union bound, the probability that there exists a depth d gate underneath which there are fewer than $\sqrt{dm \log m/2}$ many blocks unset is at most $(m^{d-3/2}/\sqrt{\log m})e^{-\sqrt{dm \log m/2}/4}$, and this tends to 0 as m tends to infinity.

On the other hand, by lemma 11, with probability at least $3/4$, $C \restriction_\rho$ is is equivalent to a depth d, bottom fan-in w circuit with at most S gates in levels 1 through $d-1$.

Therefore we may choose $\rho \in \mathcal{B}_{0,d}^{m,k+1}$ so that underneath each depth d gate of $g_d^{m,k+1}$ there are at least $\sqrt{dm \log m/2}$ many blocks unset by ρ, and $C \restriction_\rho$ is equivalent to a depth d, bottom fan-in w circuit with $\leq S$ gates in levels $1, \ldots, d-1$.

Because $C \restriction_\rho$ computes $g_d^{m,k+1} \restriction_\rho$, a restriction of it computes f_d^m: set some blocks to 0 and collapse the other blocks to a single variable. This gives a depth d circuit with $\leq S$ gates in levels $1, \ldots, d-1$, and bottom fan-in w that computes f_d^m, a contradiction to theorem 9. ∎

III.C Acknowledgements

Much of the text of this chapter was previously published as part of [41] in the proceedings of the Forty-third Annual IEEE Symposium on the Foundations of Computer Science. I was the primary researcher and author of this publication which forms the basis for this chapter.

Chapter IV

Lower Bounds for the Res(k) Refutation Systems

Our lower bounds are proved using the small restriction switching lemma of chapter III. In section IV.A we show how to transform a Res(k) refutation of a set of clauses whose lines are represented by short decision trees into a narrow resolution refutation of that same set of clauses. This conversion is used in combination with the switching lemma to show prove lower bounds for Res(k) refutations. Lower bounds for Res(k) refutations of the weak pigeonhole principle are proved in section IV.B and lower bounds for Res(k) refutations of random CNFs are proved in section IV.C. The separations between Res($k+1$) and Res(k) are proved in sections IV.D and IV.E.

IV.A Decision Trees and Res(k) Refutations

All of our lower bounds for Res(k) refutations use the fact that when the lines of a Res(k) refutation can be strongly represented by short decision trees, the Res(k) refutation can be converted into a narrow resolution refutation.

Theorem 13 *Let $\mathcal{C}$ be a set of clauses of width $\leq h$. If $\mathcal{C}$ has a Res(k) refutation so that for each line F of the refutation, $h(F) \leq h$, then $w_R(\mathcal{C}) \leq kh$.*

Proof: We will use the short decision trees to construct a narrow refutation of $\mathcal{C}$ in resolution augmented with subsumption inferences: whenever $A \subseteq B$, infer B from A. These new inferences simplify our proof, but they may be removed from the resolution refutation without increasing the size or the width.

For each initial clause $C \in \mathcal{C}$, we let T_C be the decision tree that queries the (at most h) variables in C, stopping with a 1 if the clause becomes satisfied and stopping with a 0 if the clause becomes falsified. For a line F of the Res(k) refutation that is not a hypothesis, let T_F be a decision tree of minimum height that strongly represents F.

For any partial assignment π let C_π be the clause of width $\leq h$ that contains the negation of every literal in π, i.e., the clause that says that branch π was not taken. We construct a resolution refutation of width $\leq kh$ by deriving C_π for each line F of the refutation and each $\pi \in \mathrm{Br}_0(T_F)$.

Notice that for $\pi \in \mathrm{Br}_0(T_\emptyset)$, $C_\pi = \emptyset$, and for each $C \in \mathcal{C}$, for the unique $\pi \in \mathrm{Br}_0(T_C)$, $C_\pi = C$.

Let F be a line of the refutation that is inferred from previously derived formulas $F_1, \ldots, F_j$, $j \leq k$. Assume we have derived all $C_\pi \in \mathrm{Br}_0(T_{F_i})$ for $1 \leq i \leq j$. To guide the derivation of $\{C_\pi \mid \pi \in \mathrm{Br}_0(T_F)\}$, we construct a decision tree that represents $\bigwedge_{i=1}^{j} F_i$. The tree (call it T) begins by simulating, T_{F_1} and outputting 0 on any 0-branch of T_{F_1}. On any 1-branch, it then simulates T_{F_2}, etc. If all j branches are 1, T outputs 1; otherwise T outputs 0. The height of T is at most $jh \leq kh$, so the width of any such C_π, with $\pi \in \mathrm{Br}(T)$ is at most kh. The set of clauses $\{C_\sigma \mid \sigma \in \mathrm{Br}_0(T)\}$ can be derived from the previously derived clauses by subsumption inferences because every $\sigma \in \mathrm{Br}_0(T)$ contains some $\pi \in \bigcup_{i=1}^{j} \mathrm{Br}_0(T_{F_i})$.

We now show that for every $\sigma \in \mathrm{Br}_1(T)$, there exists a $t \in F$ so that σ satisfies t. Choose $\pi_1 \in \mathrm{Br}_1(T_{F_1}), \ldots, \pi_j \in \mathrm{Br}_1(T_{F_j})$ so that $\pi_1 \cup \cdots \cup \pi_j = \sigma$. Because the decision trees $T_{F_1}, \ldots, T_{F_j}$ strongly represent the k-DNFs $F_1, \ldots, F_j$, there exist terms $t_1 \in F_1, \ldots, t_j \in F_j$ so that $\bigwedge_{i=1}^{j} t_i$ is satisfied by σ. By strong

soundness of Res(k), there exists $t \in F$ so that σ satisfies t.

Let $\sigma \in \mathrm{Br}_0(T_F)$ be given. Because T_F strongly represents F, σ falsifies all terms of F. By the preceding paragraph, for all $\pi \in \mathrm{Br}(T)$, if π is consistent with σ, then $\pi \in \mathrm{Br}_0(T)$ (otherwise, σ would not falsify the term of F satisfied by π). For each node v in T, let π_v be the path (viewed as a partial assignment) from the root to v. Bottom-up, from the leaves to the root, we recursively derive $C_{\pi_v} \vee C_\sigma$, for each v so that π_v is consistent with σ. When we reach the root, we will have derived C_σ. If v is a leaf, then $\pi_v \in \mathrm{Br}_0(T)$ so it has already been derived. If v is labeled with a variable that appears in σ, call it x, then there is a child u of v with $\pi_u = \pi_v \cup \{x\}$. Therefore, $C_{\pi_v} \vee C_\sigma = C_{\pi_u} \vee C_\sigma$. By induction, the clause $C_{\pi_u} \vee C_\sigma$ has already been derived. If v is labeled with a variable x that does not appear in σ, then for both of the children of v, call them v_1, v_2, the paths π_{v_1} and π_{v_2} are consistent with σ. Moreover, $C_{\pi_{v_1}} \vee C_\sigma = x \vee C_{\pi_v} \vee C_\sigma$ and $C_{\pi_{v_2}} \vee C_\sigma = \neg x \vee C_{\pi_v} \vee C_\sigma$. Resolving these two previously derived clauses gives us $C_{\pi_v} \vee C_\sigma$. ∎

We will use this theorem after we apply a random restriction which simultaneously collapses every line of a Res(k) refutation to a short decision tree. Hence, we can use a width lower bound for resolution refutations of a restricted tautology to give a size lower bound for Res(k) refutations of the original tautology.

Corollary 14 *Let $\mathcal{C}$ be a set of clauses of width $\leq h$, let Γ be a Res(k) refutation of $\mathcal{C}$, and let ρ be a partial assignment so that for every line F of Γ, $h(F \restriction_\rho) \leq h$. Then $w_R(\mathcal{C} \restriction_\rho) \leq kh$.*

IV.B Lower Bounds for the Weak Pigeonhole Principle

Definition IV.B.1 *The* **m to n pigeonhole principle, $\mathbf{PHP^m_n}$,** *is the following set of clauses:*

1. *For each $i \in [m]$, $\bigvee_{j \in [n]} x_{i,j}$.*

2. *For each* $i, i' \in [m]$ *with* $i \neq i'$, $\neg x_{i,j} \vee \neg x_{i',j}$.

Theorem 15 *For every* $c > 1$, *there exists* $\epsilon > 0$ *so that for all* n *sufficiently large, if* $k \leq \sqrt{\log n / \log\log n}$, *then every Res*$(k)$ *refutation of* PHP_n^{cn} *has size at least* 2^{n^ϵ}.

The idea of the proof for Theorem 15 is as follows: Suppose there is a small Res(k) refutation of the weak pigeonhole principle. Then, by applying a random restriction we obtain a low width resolution refutation of the restricted pigeonhole principle. By the well-known lower bounds on the width of resolution refutations of the pigeonhole principle, this is impossible.

In order to make the random restriction method work, we prove lower bounds for for the pigeonhole principle restricted to a low degree graph. Because these principles reduce to the pigeonhole principle by setting some variables to 0, this suffices to prove lower bounds for the pigeonhole principle. The difficulty with applying random restrictions directly to the clauses of the pigeonhole principle is that there are clauses of high width which are not satisfied with very high probability. If we were to choose random subset of the holes and place into each hole a randomly chosen pigeon, then a clause of the form $\bigvee_{i=1}^{m} x_{i,j}$ would be satisfied with probability no better than the chance that hole j is in the random subset (this will be no better than a constant in our proof). At the heart of this problem is that each hole j appears in cn distinct variables, $x_{1,j}, \ldots, x_{cn,j}$, and restricting the principle to low degree graph solves this.

Definition IV.B.2 *Let* $G = (U \cup V, E)$ *be a bipartite graph. The* **pigeonhole principle of** G, **PHP(G),** *is the set of clauses*

1. *For each* $u \in U$

$$\bigvee_{\substack{v \in V \\ \{u,v\} \in E}} x_{u,v}$$

2. *For each* $u, u' \in [m]$, *with* $u \neq u'$, *and each* $v \in V$ *with* $\{u, v\} \in E$ *and* $\{u', v\} \in E$

$$\neg x_{u,v} \vee \neg x_{u',v}$$

Definition IV.B.3 *Let* $G = (U \cup V, E)$ *be a bipartite graph. The* **maximum degree of G, $\Delta(G)$,** *is defined to be* $\max_{v \in V} deg(v)$.

Furthermore, we assume that all Res(k) refutations have been put into a normal form in which no term of any DNF asks that two pigeons be mapped to the same hole. See, for example, [47].

Definition IV.B.4 *Let* $G = (U \cup V, E)$ *be a bipartite graph. A term is said to be in* **pigeon-normal-form** *if it does not contain two literals* $x_{u,v}$ *and* $x_{u',v}$ *with* $u \neq u'$. *A DNF is said to be in pigeon-normal-form if all of its terms are in pigeon-normal-form and a Res(k) refutation is said to be in pigeon normal form if every line is in pigeon-normal-form.*

Every Res(k) refutation of $PHP(G)$ can be transformed into a refutation in pigeon normal form which at must doubles the number of lines in the proof. When there is an AND-introduction inference that creates a line not in pigeon normal form, say

$$\frac{A \vee x_{u,v} \quad A \vee x_{u',v} \quad \cdots \quad A \vee l_j}{A \vee x_{u,v} \wedge x_{u',v} \wedge \bigwedge_{i=3}^{j} l_i}$$

Replace the inference by a derivation that cuts $A \vee x_{u',v}$ with $\neg x_{u,v} \vee \neg x_{u',v}$ to obtain $A \vee \neg x_{u,v}$. Cut this with $A \vee x_{u,v}$ to obtain A. We may proceed through the rest of the proof with A because it subsumes $A \vee x_{u,v} \wedge x_{u',v} \wedge \bigwedge_{i=3}^{j} l_i$.

IV.B.1 Random Restrictions

Definition IV.B.5 *For a bipartite graph* $G = (U \cup V, E)$ *and a real number* $p \in [0, 1]$, *let* $\mathcal{M}_p(G)$ *denote the distribution on partial assignments which arises from the following experiment:*

Independently, for each $v \in V$, with probability $1-p$ choose to match v and with probability p leave v unmatched. If v is matched, uniformly select a neighbor u of v, set $x_{u,v}$ to 1, and for every $w \neq u$ that is a neighbor of v, set $x_{w,v}$ to 0.

Let V_ρ be the set of vertices of V matched by ρ, let U_ρ be the set of vertices of U matched by ρ, and let $S_\rho = U_\rho \cup V_\rho$.

These restrictions randomly associate pigeons with holes in an injective way. While some pigeons can be associated with multiple holes, no two pigeons can be associated with the same hole. It is easy to check that for any $\rho \in \mathcal{M}_p(G)$, we have that $PHP(G) \restriction_\rho = PHP(G - S_\rho)$.

Lemma 16 *Let $p \in [0,1]$, $i \in [k]$ be given. Let $G = (U \cup V, E)$ be a bipartite graph with $\Delta = \Delta(G)$. Let F be an i-DNF in pigeon-normal-form.*

$$Pr_{\rho \in \mathcal{M}_p(G)}[F \restriction_\rho \neq 1] \leq 2^{-\frac{(\log e)(1-p)^i c(F)}{i\Delta^{i+1}}}$$

Proof: For a term T, define the **holes of T** as $\text{Holes}(T) = \{v \mid x_{u,v} \in T \text{ or } \neg x_{u,v} \in T\}$. We say that two terms T and T' are **hole-disjoint** if $\text{Holes}(T) \cap \text{Holes}(T') = \emptyset$.

Because F contains at least $c(F)/i$ many variable-disjoint terms, and each hole $v \in V$ appears in at most Δ many variables, F must contain at least $c(F)/i\Delta$ many hole-disjoint terms.

The events of satisfying hole-disjoint terms are independent, and for a given term, T, the probability that $T \restriction_\rho = 1$ is at least $(1-p)^i/\Delta^i$. This is because with probability $(1-p)^i$, every hole of T is matched, and with probability at least $1/\Delta^i$ the holes are matched in a way that satisfies T (here we use that F is in pigeon-normal-form). Therefore, we have the following inequalities:

$$\Pr_\rho[F \restriction_\rho \neq 1] \leq \left(1 - (1-p)^i/\Delta^i\right)^{\frac{c(F)}{i\Delta}} \leq \left(e^{-(1-p)^i/\Delta^i}\right)^{\frac{c(F)}{i\Delta}} = 2^{-\frac{(\log e)(1-p)^i c(F)}{i\Delta^{i+1}}}$$

■

IV.B.2 Width Lower Bounds for Resolution

For the lower bound proof to work, we need a graph G so that after the application of a random restriction ρ , with high probability, $PHP(G) \restriction_\rho$ requires high width to refute in resolution. We call such graphs **robust**, and in this subsection we probabilistically demonstrate robust, low degree graphs.

Definition IV.B.6 *A bipartite graph G is said to be* $(\mathbf{p}, \mathbf{w})$**-robust**, *if when ρ is selected from $\mathcal{M}_p(G)$, with probability at least $\frac{1}{2}$, $w_R(PHP(G) \restriction_\rho) \geq w$.*

All we need for the size lower bound is the following lemma, we prove in the next sub-subsection. Readers who believe that random graphs should be robust can skip to the proof of the lower bound.

Lemma 17 *For all $c > 1$, there exists $d > 0$, so that for n sufficiently large, there exists a $(3/4, n/24)$-robust graph with $\Delta(G) \leq d \log n$ on the vertex sets $[cn]$ and $[n]$.*

Existence of Robust Graphs

As a starting point, we use a now standard lower bound of $w_R(PHP(G))$ in terms of the expansion of G.

Definition IV.B.7 *For a vertex $u \in U$, let $N(u)$ be its set of neighbors. For a subset $V' \subseteq V$, let its* **boundary** *be $\partial \mathbf{V}' = \{u \in U \mid |N(u) \cap V'| = 1\}$. A bipartite graph G is said to be an $(\mathbf{m}, \mathbf{n}, \mathbf{r}, \mathbf{f})$-expander if $|V| = m$, $|U| = n$, and for all $V' \subseteq V$, $|V'| \leq r$, $|\partial V'| \geq f|V'|$.*

Theorem 18 *[39] If G is a bipartite graph that is an (m, n, r, f)-expander, then $w_R(PHP(G)) \geq rf/2$.*

Definition IV.B.8 *Let $\mathbf{G_{m,n,p}}$ be the distribution on bipartite graphs with vertex sets $[m]$ and $[n]$ in which every edge is included with independent probability p.*

The following lemma was proven by Atserias, Bonet and Esteban [47].

Lemma 19 *[47] Let $m = cn$, $q = \frac{48c \ln m}{m}$, $\alpha = \frac{1}{mq}$ and $f = \frac{nq}{6}$. Let G be selected according to the distribution $G_{m,n,q}$.*

$$Pr_G[G \text{ is an } (m, n, \alpha m, f) \text{ expander }] \geq \frac{2}{3}$$

Lemma 20 *Let $m = cn$, let $q \geq \frac{48c \ln m}{m}$ and let G be selected according to the distribution $G_{m,n,q}$.*

$$Pr_G[w_R(PHP(G)) \geq n/12] \geq \frac{2}{3}$$

Proof: Let $\alpha = \frac{1}{mq}$ and $f = \frac{nq}{6}$. Because $\alpha m f/2 = (1/mq)m(nq/6)/2 = n/12$, an application of theorem 18 shows that when G is selected according to $G_{m,n,\frac{48c \ln m}{m}}$, with probability at least $2/3$, $w_R(PHP(G)) \geq n/12$.

Now consider G selected according to $G_{m,n,q}$, with $q \geq \frac{48c \ln m}{m}$. Whenever G_0 is an edge-induced subgraph of G_1, $w_R(PHP(G_1)) \geq w_R(PHP(G_0))$ because a refutation of $PHP(G_1)$ can always be transformed into a refutation of $PHP(G_0)$ by setting some variables to 0. Therefore, by increasing the probability of including an edge, the probability of having no small resolution refutation for $PHP(G)$ only increases. ∎

We now prove lemma 17.

Proof: Set $m = cn$, $p = 3/4$ and $q = \frac{192c \ln m}{m}$. Consider the joint distribution that arises by selecting G according to $G_{m,n,q}$ and ρ according to $\mathcal{M}_{3/4}(G)$. We will bound the probability that the degree is too large, that too many holes are matched, and that the restricted graph is expanding.

By the Chernoff bounds, for each $v \in [n]$ the probability that v has degree in excess of $2mq$ is at most $e^{-mq/4}$. By the union bound, the probability that there exists some $v \in [n]$ of degree in excess of $2mq$ is at most $ne^{-mq/4}$. Similarly, the probability that there exists some $v \in [m]$ of degree in excess of $2mq$ is at most $me^{-nq/4}$. Therefore, the probability that the maximum degree of G exceeds $2mq$ is bounded as follows:

$$ne^{-mq/4} + me^{-nq/4} = ne^{-m192c \ln m/m} + me^{-n192c \ln m/m} = O(n^{-191})$$

Remember that V_ρ is the set of holes matched by the restriction ρ. By the Chernoff bounds, the probability that $|V_\rho| \geq 2n(1-p) = n/2$ is at most $e^{-\frac{n(1-p)}{4}} = e^{-n/16}$.

We now bound the probability that $G - S_\rho$ is an expander. First, up to renaming vertices, $G - S_\rho$ is distributed as $G_{m_\rho,n_\rho,q}$, with $n_\rho = n - |V_\rho|$ and $m_\rho = m - |U_\rho|$. This is because for fixed sets of vertices $V_0 \subseteq V$ and $U_0 \subseteq U$, when we condition on the event that $V_\rho = V_0$ and $U_\rho = U_0$, the edges $\{u, v\}$ with $u \in U \setminus U_0$ and $v \in V \setminus V_0$ are included in $G - S_\rho$ with independent probability q. Now, condition on the event that $|V_\rho| \leq n/2$. We have that $m_\rho = m - |U_\rho| \geq m - n/2 \geq m/2$ and thus $q = 192c \ln m/m \geq 192c \ln m_\rho/m \geq 192c \ln m_\rho/2m_\rho = 48 \cdot 2c \ln m_\rho/m_\rho$. Because $\frac{m_\rho}{n_\rho} \leq \frac{cn}{n/2} = 2c$, we can apply lemma 20 and deduce that $w_R(PHP(G - S_\rho)) \geq n_\rho/12$ with probability at least $\frac{2}{3}$. Because $n_\rho \geq n/2$, with the same probability, $w_R(G - S_\rho) \geq n/24$.

Combining the three inequalities from the preceding paragraphs shows that the probability that G contains a vertex of degree in excess of $192c \ln m$, that V_ρ contains more than $n/2$ vertices, or that $w_R(PHP(G - S_\rho)) < n/24$, is at most

$$\frac{1}{3} + O(n^{-191}) + e^{-n/16}$$

For sufficiently large n, this probability is bounded above by $\frac{1}{2}$. By averaging over the choices of the edges, there exists a bipartite graph G on vertex sets $[cn]$ and $[n]$ with $\Delta(G) \leq 2mq = 384c \ln(cn)$, so that upon selection of $\rho \in \mathcal{R}_{3/4}(G)$, $w_R(G - S_\rho) \geq n/24$ with probability at least $\frac{1}{2}$. ∎

IV.B.3 Size Lower Bounds for Res(k)

To prove the size lower bounds for Res(k) refutations of PHP_n^{cn} we first prove size lower bounds for the weak pigeonhole principle restricted to a robust graph, and then we reduce these principles to PHP_n^{cn}.

Lemma 21 *For any $c > 1$ and $d > 0$, there exists $\epsilon > 0$ so that for all n sufficiently large, if $k \leq \sqrt{\log n / \log\log n}$ and G is a $(3/4, n/24)$-robust bipartite graph with vertex sets of sizes cn and n and $\Delta(G) \leq d \log n$, then $S_k(PHP(G)) \geq 2^{n^\epsilon}$.*

Proof: By lemma 16, for each $i \in [k]$ and every i-DNF F,

$$\Pr_{\rho \in \mathcal{M}_{3/4}(G)} [F \restriction_\rho \neq 1] \leq 2^{-\frac{(\log e)(1-3/4)^i c(F)}{i(d \log n)^{i+1}}} = 2^{-\frac{(\log e) c(F)}{i \cdot 4^i (d \log n)^{i+1}}}.$$

In the interest of obtaining a better bound, we will not appeal to corollary 5, but directly apply the theorem 4. We define sequences $s_0, \ldots, s_k$ and $p_1, \ldots, p_k$ for use in the switching lemma. Set $s_0 = \frac{3}{4k}(n/24 - 1)$. For each $i \in [k]$, set

$$s_i = \left(\frac{\log e}{2i 4^i (d \log n)^{i+1}} \right) s_{i-1}$$

For each $i \in [k]$ set $p_i = 2^{-2s_i}$. For any i-DNF F so that $c(F) > s_{i-1}$, we have the following inequality:

$$\Pr_{\rho \in \mathcal{M}_{3/4}(G)} [F \restriction_\rho \neq 1] < 2^{-\frac{(\log e) s_{i-1}}{i \cdot 4^i (d \log n)^{i+1}}} = 2^{-2\frac{(\log e) s_{i-1}}{2i 4^i (d \log n)^{i+1}}} = 2^{-2s_i} = p_i$$

It can be shown that there exists $\epsilon > 0$ so that for sufficiently large n, $s_k \geq n^\epsilon$. To avoid distraction, we show this in in lemma 23, at the end of this subsection. Suppose that Γ is a $\mathrm{Res}(k)$ refutation of $PHP(G)$ of size less than 2^{n^ϵ}.

By an application of theorem 4 and the union bound, we have:

$$\Pr_{\rho \in \mathcal{M}_{3/4}(G)} \left[\exists F \in \Gamma,\ h(F \restriction_\rho) > \sum_{i=0}^{k-1} s_i \right] \leq 2^{n^\epsilon} \sum_{i=1}^{k} p_i 2^{\sum_{j=i}^{k-1} s_j}$$

$$\leq 2^{s_k} \sum_{i=1}^{k} p_i 2^{\sum_{j=i}^{k-1} s_j} = \sum_{i=1}^{k} p_i 2^{\sum_{j=i}^{k} s_j}$$

We now bound $p_i 2^{\sum_{j=i}^{k} s_j}$ for each $i > 0$. For each i, $s_{i+1} < \frac{1}{4} s_i$ so $\sum_{j=i}^{k-1} s_j \leq \frac{4}{3} s_i$. This gives us the following inequality:

$$p_i 2^{\sum_{j=i}^{k-1} s_j} = 2^{\sum_{j=i}^{k-1} s_j - 2s_i} \leq 2^{(4/3-2)s_i} = 2^{-(2/3)s_i} \leq 2^{-(2/3)s_k} \leq 2^{-(2/3)n^\epsilon}$$

Therefore:

$$\begin{aligned}
&\Pr_{\rho\in\mathcal{M}_{3/4}(G)}\left[\exists F\in\Gamma,\ h(F\restriction_\rho) > (n/24-1)/k\right] \\
&\leq \Pr_{\rho\in\mathcal{M}_{3/4}(G)}\left[\exists F\in\Gamma,\ h(F\restriction_\rho) > \sum_{i=0}^{k-1} s_i\right] \\
&\leq \sum_{i=1}^{k} p_i 2^{\sum_{j=i}^{k-1} s_j} \leq \sum_{i=1}^{k} 2^{-(2/3)n^\epsilon} \leq k2^{-(2/3)n^\epsilon} = 2^{\log k-(2/3)n^\epsilon}
\end{aligned}$$

For n sufficiently large, this probability is strictly less than $1/2$. Because G is $(3/4, n/24)$-robust, for $\rho \in \mathcal{M}_{3/4}(G)$, with probability at least $1/2$, $w_R(PHP(G)\restriction_\rho) \geq n/24$. Thus, there is a ρ so that $w_R(PHP(G)\restriction_\rho) \geq n/24$ and $\forall F \in \Gamma,\ h(F\restriction_\rho) \leq \frac{1}{k}(n/24-1)$. This is a contradiction because by corollary 14, there is a resolution refutation of $PHP(G)\restriction_\rho$ of width $\leq n/24-1$. ∎

Theorem 22 *For each $c > 1$, there exists $\epsilon > 0$ so that for all n sufficiently large, if $k \leq \sqrt{\log n/\log\log n}$, then every Res($k$) refutation of PHP_n^{cn} has size at least 2^{n^ϵ}.*

Proof:

Apply lemma 17 and choose d so that for sufficiently large n, there exists a $(3/4, n/24)$-robust graph G on vertex sets cn and n, with $\Delta(G) \leq d\log n$. By lemma 21, there exists $\epsilon > 0$ so that for $k \leq \sqrt{\log n/\log\log n}$, $S_k(PHP(G)) \geq 2^{n^\epsilon}$. Because $PHP(G)$ can be obtained by setting some of the variables of PHP_n^{cn} to 0, every Res(k) refutation of PHP_n^{cn} can be converted into a Res(k) refutation of $PHP(G)$ of the same or lesser size. Therefore, all Res(k) refutations of PHP_n^{cn} must have size at least 2^{n^ϵ}. ∎

Now we prove the lower bound on the number s_k that we used in lemma 21. The constants are *not* optimized.

Lemma 23 *There exists $\epsilon > 0$, so that all n sufficiently large, with $k \leq \sqrt{\log n/\log\log n}$ and $s_0, \ldots, s_k$ defined as in the proof of lemma 21, $s_k \geq n^\epsilon$.*

Proof: Unwinding the recursive definition of the s_i's, gives the following equality:

$$s_k = \frac{1}{2^k}(\log e)^k \frac{1}{k!}\left(\frac{1}{4}\right)^{\sum_{j=1}^{k} j}\left(\frac{1}{d\log n}\right)^{\sum_{j=2}^{k+1} j}\frac{3}{4k}(n/24-1)$$

Because $k \leq \sqrt{\log n/\log\log n}$, we have that $\frac{1}{2^k}(\log e)^k \frac{1}{k!}\left(\frac{1}{4}\right)^{\sum_{j=1}^{k} j}\frac{3}{4k} = n^{-o(1)}$.

$$s_k = n^{-o(1)}(1/d\log n)^{(k+2)(k+1)/2}(n/24-1) = n^{-o(1)}2^{-(\log(d\log n))(k^2+3k+2)/2}(n/24-1)$$

Because $k \leq \sqrt{\log n/\log\log n}$ and d is a constant, for n sufficiently large, $(\log(d\log n))(k^2+3k+2)/2 = (\log n)(1+o(1))/2$. Therefore,

$$s_k = n^{-o(1)}2^{-(\log n)(1+o(1))/2}(n/24-1)$$

and thus there exists $\epsilon > 0$ so that for all n sufficiently large, $s_k \geq n^{\epsilon}$. ∎

IV.C Lower Bounds for Random CNFs

It is well-known that, in some cases, randomly generated sets of clauses require exponentially large resolution refutations, see [27, 24, 39]. We extend these results by giving exponential lower bounds for the size of Res(k) refutations of randomly chosen sets of width $4k^2+2$ clauses.

Definition IV.C.1 *Let n, Δ and w be given. The distribution $\mathcal{F}_w^{n,\Delta}$ is defined by choosing $\Delta \cdot n$ many clauses independently, with repetitions, from the set of all $\binom{n}{w}2^w$ clauses of width w.*

Our main result for this section is:

Theorem 24 *For any $\epsilon \in [0, \frac{1}{6})$, there exists $\delta > 0$, so that for n sufficiently large and for $\Delta = n^{\epsilon}$,*

$$Pr_{F \in \mathcal{F}_{4k^2+2}^{n,\Delta}}\left[S_k(F) \leq 2^{n^{\delta}}\right] = o(1).$$

The reason that our proof does not give lower bounds for refutations of random 3-CNFs in Res(k) is that on one hand, we want our random restrictions to have a good chance of satisfying a fixed k-term (so we can apply the switching lemma), but on the other hand, the restrictions should have little probability of falsifying any of the initial clauses (this would make the restricted set of clauses trivial to refute). Because satisfying a k-term is equivalent to falsifying a k-clause, we can only work with initial clauses width larger than k.

A set of clauses that, with constant probability, requires high width to refute after random restriction is called **robust**. Recall the distribution $\mathcal{D}_p$ from definition III.A.3.

Definition IV.C.2 *Let F be a CNF in variables $x_1, \ldots, x_n$. We say that F is* $(\mathbf{p}, \mathbf{r})$ **robust** *if*
$Pr_{\rho \in \mathcal{D}_p}[w_R(F \restriction_\rho) \geq r] \geq 1/2$.

It turns out that for sufficiently large w, a random w-CNF is almost surely robust. We state the result below and prove it in the following subsection.

Lemma 25 *There exists a constant c so that for any constants w and t, $w \geq 2t+2$, for every n sufficiently large, and every $\epsilon \in [0, 1/2]$, if we set $\Delta = n^\epsilon$ then the following inequality holds:*

$$Pr_{F \in \mathcal{F}_w^{n,\Delta}}\left[F \text{ is not } \left(n^{-1/t}, cn^{\frac{1-2\epsilon}{1+2\epsilon}}\right)\text{-robust}\right] = o(1)$$

We now prove the size lower bound. We set bits with probability $n^{-1/2k^2}$ so we can collapse k-DNFs but still have that most $4k^2+2$ CNFs are robust. For each $k \geq 1$, let γ_k be the constant of corollary 7.

Lemma 26 *Let n, r, w, and k be given. For sufficiently large n, if F is a $(n^{-1/2k^2}, r)$-robust w-CNF, then $S_k(F) \geq \frac{1}{4k} 2^{(\gamma_k(r-1)/k\sqrt{n})}$.*

Proof: Suppose that Γ is a Res(k) refutation of F of size at most $\frac{1}{4k} 2^{(\gamma_k(r-1)/k\sqrt{n})}$. By corollary 7, with $p = n^{-1/2k^2}$ and $w = (r-1)/k$, we have that for every line F

of Γ, $\Pr_{\rho\in\mathcal{D}_p}[h(F\restriction_\rho) > (r-1)/k] \leq k2^{-\gamma_k(r-1)/k\sqrt{n}}$. By the union bound we have that

$$\Pr_{\rho\in\mathcal{D}_p}[\exists F\in\Gamma\ h(F\restriction_\rho) > (r-1)/k] \leq |\Gamma|\cdot k\cdot 2^{-\gamma_k(r-1)/k\sqrt{n}}$$

$$\leq \frac{1}{4k}2^{(\gamma_k(r-1)/k\sqrt{n})}\cdot k\cdot 2^{-\gamma_k(r-1)/k\sqrt{n}} = \frac{1}{4}$$

Because F is (p,r)-robust, with probability at least $1/2$ over choices of ρ, $w_R(F\restriction_\rho)\geq r$. Therefore, we may choose $\rho\in\mathcal{D}_p$ so that $w_R(F\restriction_\rho)\geq r$ and for all $F\in\Gamma$, $h(F\restriction_\rho)\leq (r-1)/k$. This is a contradiction because by corollary 14 there should be a width $r-1$ resolution refutation of $F\restriction_\rho$. ∎

Combining lemmas 25 and 26 with $t=2k^2$, $w=4k^2+2$ and $r=cn^{\frac{1-2\epsilon}{1+2\epsilon}}$ shows that a random $(4k^2+2)$-CNF almost surely requires exponential size to refute in Res(k).

Corollary 27 *There exists a constant c so that for every k, for every n sufficiently large and $\epsilon\in[0,1/2]$, if we set $\Delta=n^\epsilon$, then the following inequality holds.*

$$Pr_{F\in\mathcal{F}^{n,\Delta}_{4k^2+2}}\left[S_k(F)\leq 2^{\gamma_k(cn^{\frac{1-2\epsilon}{1+2\epsilon}}-1)/k\sqrt{n}}\right] = o(1)$$

This gives an exponential lower bound only when $\frac{1-2\epsilon}{1+2\epsilon} > \frac{1}{2}$. This holds exactly for $\epsilon\in[0,\frac{1}{6})$.

Theorem 28 *For any $\epsilon\in[0,\frac{1}{6})$, there exists $\delta>0$, so that for n sufficiently large and for $\Delta=n^\epsilon$,*

$$Pr_{F\in\mathcal{F}^{n,\Delta}_{4k^2+2}}\left[S_k(F)\leq 2^{n^\delta}\right] = o(1)$$

IV.C.1 Robustness of Random CNFs

In this section we show for appropriate clause densities, a random w-CNF is almost surely robust.

We begin with a width bound for resolution refutations of random 3-CNFs given by Ben-Sasson and Wigderson.

Theorem 29 *[39] There exists a constant c, so that for all n, and all* $\epsilon \in [0, 1/2]$ *with* $\Delta = n^{\epsilon}$*, the following inequality holds.*

$$Pr_{F \in \mathcal{F}_3^{n,\Delta}} \left[w_R(F) \leq cn^{\frac{1-2\epsilon}{1+2\epsilon}} \right] = o(1)$$

Lemma 30 *There exists a constant c so that for any constants w and t with* $w \geq 2t + 2$*, for every n sufficiently large and* $\epsilon \in [0, 1/2]$*, if we set* $\Delta = n^{\epsilon}$ *and* $p = n^{-1/t}$*, then the following inequality holds:*

$$Pr_{\substack{F \in \mathcal{F}_w^{n,\Delta} \\ \rho \in \mathcal{D}_p}} \left[w_R(F \restriction_\rho) \leq cn^{\frac{1-2\epsilon}{1+2\epsilon}} \right] = o(1)$$

Proof: Let w, t, n, ϵ be given as above and set $\Delta = n^{\epsilon}$ and $p = n^{-1/t}$.

Because the expected size of $\mathrm{dom}(\rho)$ is pn, the Chernoff bounds show that the size of $\mathrm{dom}(\rho)$ exceeds $2pn = 2n^{1-\frac{1}{t}}$ with probability at most $e^{-n^{1-1/t}/4} = o(1)$.

Let C be a fixed clause of width w that contains no opposite literals. When we choose $\rho \in \mathcal{D}_p$, the probability that the domain of ρ contains at least $w - 2$ variables of C is at most $\binom{w}{2} p^{w-2}$. Because w is a constant, this probability is $O\left(n^{-(w-2)/t}\right)$. Because $w \geq 2t + 2$, this probability is $O\left(n^{-2}\right)$. For any fixed w-CNF F on Δn many clauses, an application of the the union bound shows that there is some clause with $\geq w-2$ of its variables in the restriction with probability $O(\Delta n \cdot n^{-2}) = o(1)$. Because this calculation holds for every w-CNF of Δn many clauses, we have that

$$\Pr_{\substack{F \in \mathcal{F}_w^{n,\Delta} \\ \rho \in \mathcal{D}_p}} \left[\exists C \in F,\ |vars(C) \setminus \mathrm{dom}(\rho)| \leq 2 \right] = o(1)$$

Let $n' = n - |\mathrm{dom}\rho|$. Conditioned on the events that $\mathrm{dom}(\rho) \leq 2n^{1-\frac{1}{t}}$ and $\forall i \in [\Delta],\ |vars(C_i) \setminus \mathrm{dom}(\rho)| \geq 3$, $F \restriction_\rho$ is subsumed by a random 3-CNF distributed as $\mathcal{F}_3^{n',\Delta}$. (To see this, consider the distribution on 3-CNFs that chooses three literals unset by ρ from each C_i). Choose ϵ' so that $n^{\epsilon} = (n')^{\epsilon'}$. By theorem 30 we have

$$\Pr_{\substack{F \in \mathcal{F}_w^{n,\Delta} \\ \rho \in \mathcal{D}_p}} \left[w_R(F \restriction_\rho) \leq c(n')^{\frac{1-2\epsilon'}{1+2\epsilon'}} \right] = o(1)$$

Because $n' \geq n - 2n^{1-1/t}$, we may choose c' so that

$$\Pr_{\substack{F \in \mathcal{F}_w^{n,\Delta} \\ \rho \in \mathcal{D}_p}} \left[w_R(F \restriction_\rho) \leq c'(n)^{\frac{1-2\epsilon}{1+2\epsilon}} \right] = o(1)$$

■

From lemma 30, an averaging argument yields the following phrasing of lemma 25.

Lemma 31 *There exists a constant c so that for any constants w and t, $w \geq 2t+2$, for every n sufficiently large and $\epsilon \in [0, 1/2]$, if we set $\Delta = n^\epsilon$ and let $p = n^{-1/t}$, then the following inequality holds:*

$$Pr_{F \in \mathcal{F}_w^{n,\Delta}} \left[Pr_{\rho \in \mathcal{D}_p} \left[w_R(F \restriction_\rho) \leq cn^{\frac{1-2\epsilon}{1+2\epsilon}} \right] \geq 1/2 \right] = o(1)$$

IV.D Separation Between Res(k) and Res($k+1$)

In this section we show that for each constant k, there is an $\epsilon_k > 0$ and a family of unsatisfiable CNFs which have polynomial size Res($k+1$) refutations but which require size $2^{n^{\epsilon_k}}$ to refute in Res(k). The unsatisfiable clauses are a variation of the graph ordering tautologies [43, 44].

Definition IV.D.1 *Let G be an undirected graph. For each vertex u of G, let $N(u)$ denote the set of neighbors of u in G. For each ordered pair of vertices $(u, v) \in V(G)^2$, with $u \neq v$, let there be a propositional variable $X_{u,v}$.*

The **graph ordering principle for G, GOP(G),** *is the following set of clauses: (1) The relation X is transitive: for all $u, v, w \in V(G)$, $X_{u,v} \wedge X_{v,w} \rightarrow X_{u,w}$ (2) The relation X is anti-symmetric: for all $u, v \in V(G)$ with $u \neq v$, $\neg X_{u,v} \vee \neg X_{v,u}$ (3) There is no locally X-minimal element: for every $u \in V(G)$, $\bigvee_{v \in N(u)} X_{v,u}$.*

The **k-fold graph ordering principle of G, GOP$^{\mathbf{k}}$(G),** *is obtained by replacing each variable $X_{u,v}$ by a conjunction of k variables, $X_{u,v}^1, \ldots, X_{u,v}^k$, and then using the distributive rule and DeMorgan's law to express this as a set of clauses.*

Notice that for a graph G on n vertices with maximum degree d, the principle $GOP(G)$ consists of $O(n^3)$ many clauses each of width at most $\max\{3, d\}$. Therefore, for any graph G on n vertices with maximum degree d, the principle $GOP^k(G)$ has size $O(n^3k^d)$.

It is readily shown that, for any graph G, the principle $GOP(G)$ has polynomial size resolution refutations. Furthermore, these refutations can be transformed into Res$(k+1)$ refutations of $GOP^{k+1}(G)$, as show in lemma 34. On the other hand, we will also prove that Res(k) refutations of $GOP^{k+1}(G)$ require exponential size for certain graphs:

Theorem 32 *Let k be a positive integer. There exist constants $c > 0$ and $\epsilon_k > 0$, and a family of graphs G on n vertices (for n sufficiently large) with maximum degree $c \log n$ so that Res(k) refutations of $GOP^{k+1}(G)$ require size at least $2^{O(n^{\epsilon_k})}$.*

IV.D.1 The Upper Bounds

We build Res(k) refutations for $GOP^k(G)$ from resolution refutations of $GOP(G)$. The resolution refutation of $GOP(G)$ is a slight variation of the resolution refutation of GT_n [43, 44].

Lemma 33 *Let G be an n vertex graph. There is a resolution refutation of $GOP(G)$ of size $O(n^3)$.*

Proof: To construct the resolution refutation of $GOP(G)$, we iteratively derive the formulas $\bigvee_{\substack{i\in[l,n]\\ i\neq j}} X_{i,j}$ for all i, j with $1 \leq l \leq j \leq n$. The clauses $\bigvee_{\substack{i\in[n]\\ i\neq j}} X_{i,j}$ are derived by weakening the hypotheses. We proceed in stages as l ranges from 1 up to n. At stage l, for $j = l$, we have $\bigvee_{i\in[l+l,n]} X_{i,l}$. For $j \neq l$, we resolve $\bigvee_{i\in[l+1,n]} X_{i,l}$ with the transitivity axioms $\neg X_{i,l} \vee \neg X_{l,j} \vee X_{i,j}$ to obtain $\neg X_{l,j} \vee X_{j,l} \bigvee_{\substack{i\in[l+1,n]\\ i\neq j}} X_{i,j}$. This clause is resolved with $\neg X_{l,j} \vee \neg X_{j,l}$ and $\bigvee_{\substack{i\in[l,n]\\ i\neq j}} X_{i,j}$ to obtain $\bigvee_{i=l+1}^{n} X_{i,j}$. At stage n, with $j = n$, we have derived the empty clause. This refutation clearly has size $O(n^3)$. ∎

Lemma 34 *For each k, and every G with n vertices and degree at most $d \geq 3$, $GOP^k(G)$ has a Res(k) refutation of size $O(n^3 k^d)$.*

Proof: Let τ be the operation that replaces $X_{u,v}$ by $\bigwedge_{i=1}^{k} X_{u,v}^i$ and $\neg X_{u,v}$ by $\bigvee_{i=1}^{k} \neg X_{u,v}^i$.

Let Γ be the size $O(n^3)$ resolution refutation of $GOP(G)$ given above, and remove all of its weakening inferences. If we apply the transformation τ to the refutation, we obtain a Res(k) refutation of $\tau(GOP(G))$.

From the clauses of $GOP^k(G)$ we can derive the k-DNFs of $\tau(GOP(G))$ by a sequence of $O(k^d)$ many AND-introduction inferences per formula. Thus, we have a Res(k) refutation of $GOP^k(G)$ of the claimed size. ∎

IV.D.2 Random Restrictions

In this subsection we define a distribution on partial assignments so that i-DNFs with high cover number are satisfied with high probability. The idea is to randomly color the graph with $4k$ many colors, and then between vertices u and v of distinct color classes, uniformly choose an assignment to $X_{u,v}^1, \ldots, X_{u,v}^{k+1}, X_{v,u}^1, \ldots, X_{v,u}^{k+1}$ which makes both $\bigwedge_{i=1}^{k+1} X_{u,v}^i$ and $\bigwedge_{i=1}^{k+1} X_{v,u}^i$false.

Definition IV.D.2 *Let $k \geq 1$ be given. Let G be a graph. The distribution $\mathcal{P}_{\mathbf{k+1}}(\mathbf{G})$ on partial assignments ρ to the variables of $GOP^{k+1}(G)$ is given by the following experiment.*

For each $(u,v) \in V(G)^2$, let $\sigma_\rho^{u,v}$ be chosen uniformly among $0,1$ assignments to $X_{u,v}^1, \ldots, X_{u,v}^{k+1}$ so that for at least one $i \in [k+1]$, $\sigma_\rho^{u,v}(X_{u,v}^i) = 0$.

Select a random coloring of $V(G)$ by $4k$ many colors, $c_\rho : V(G) \to [4k]$.

The **partial assignment** *ρ is defined as:*

$$\rho = \bigcup_{\substack{(u,v) \in V(G)^2 \\ c_\rho(u) \neq c_\rho(v)}} \sigma_\rho^{u,v}$$

The **auxiliary total assignment** σ_ρ *is defined as:*

$$\sigma_\rho = \bigcup_{(u,v)\in V(G)^2} \sigma_\rho^{u,v}$$

If we let B_ρ be the set of edges which are bichromatic under the coloring c_ρ, then $GOP^{k+1}(G) \restriction_\rho$ is $GOP^{k+1}(G \setminus B_\rho)$. Moreover, we have the following lemma, which the reader can easily check.

Lemma 35 *Let G be a graph. Let $\rho \in \mathcal{P}_{k+1}(G)$ be given. Let B_ρ be the set of edges of G that are bichromatic under c_ρ. Let $G_1, \ldots, G_m$ be the connected components of $G \setminus B_\rho$.*

$$GOP^{k+1}(G) \restriction_\rho = \bigcup_{j=1}^{m} GOP^{k+1}(G_j)$$

Formulas with high cover number contain many variable-disjoint terms, but the events of satisfying these terms with $\rho \in \mathcal{P}_{k+1}(G)$ are not necessarily independent. To obtain independence, we look at the pairs of vertices involved with the literals of the terms. Remember that in the definition of $GOP(G)$, there are no variables $X_{u,u}$.

Definition IV.D.3 *Let $X^i_{u,v}$ be a variable of $GOP^{k+1}(G)$. The* **underlying pair** *of $X^i_{u,v}$ is the set $\{u, v\}$. The* **underlying ordered pair** *of $X^i_{u,v}$ is (u, v). Let T be a term. The set of* **vertex pairs of T, $\mathbf{P_T}$,** *is defined as*

$$P_T = \{\{u, v\} \mid \{u, v\} \text{ is the underlying pair of a variable in } T\}$$

The **set of vertices of T, $\mathbf{S_T}$,** *is defined as $S_T = \bigcup P_T$.*

We use combinatorial sunflowers to obtain independence between the events of satisfying terms of an i-DNF with high cover number. To guarantee that such a system exists, we apply the Erdös-Rado lemma.

Definition IV.D.4 *A* **($\mathbf{p}, \mathbf{l}$) sunflower** *is a collection of sets $P_1, \ldots, P_p$, each of size $\leq l$, so that there exists a set C so that $P_i \cap P_j = C$ for all $i, j \in [p]$, $i \neq j$. The set C is called the* **core** *of the sunflower.*

Theorem 36 *([31], c.f. [67]) Let l be given. Let $\mathcal{Z}$ be a family of M distinct sets, each with cardinality $\leq l$. $\mathcal{Z}$ contains a (p, l) sunflower where $p \geq \left(\frac{M}{l!}\right)^{\frac{1}{l}}$.*

Definition IV.D.5 *Let $T_1, \ldots, T_t$ be terms in the variables of $GOP^{k+1}(G)$. We say that the terms are* **sufficiently independent** *if the following conditions hold:*

1. *For $i, j \in [t]$, if $i \neq j$ then $S_{T_i} \neq S_{T_j}$.*

2. *The family $\{S_{T_i} \mid 1 \leq i \leq t\}$ forms a sunflower with core C.*

3. *For each $i \in [t]$, each $\{u, v\} \in P_i$, $\{u, v\} \not\subseteq C$.*

Lemma 37 *Let $T_1, \ldots, T_t$ be a sufficiently independent set of terms. The sets P_{T_i}, $1 \leq i \leq t$, are disjoint.*

Proof: Let i, j, $1 \leq i < j \leq t$ be given and let C denote the core of the sunflower. Suppose that $\{u, v\} \in P_{T_i} \cap P_{T_j}$. We then have that $\{u, v\} \subseteq S_{T_i} \cap S_{T_j}$, so $\{u, v\} \subseteq C$. Therefore, by the third property of sufficient independence, $\{u, v\} \notin P_{T_i}$ – contradiction. ∎

We begin the task of showing that a DNF with high cover number is likely to be satisfied by a random restriction. The quality of our bounds is most affected by the use of the sunflower lemma, and the particular constants we obtain at other points have limited impact. Therefore, to conserve space and readability, we will not optimize many of the probabilities involved.

Lemma 38 *Let k be given. There exist a constants $\beta_k > 0$ and $c_k > 0$ so that for every k-DNF F in the variables of $GOP^{k+1}(G)$, F contains a sufficiently independent set of size at least $\beta_k (c(F))^{\frac{1}{2k}} - c_k$.*

Proof: F contains a set of $s = c(F)/k$ many variable-disjoint terms, $T_1, \ldots, T_s$. It is possible that $S_{T_m} = S_{T_l}$ for some $m \neq l$. However, because all terms have size at most k, for each i, $|S_{T_i}| \leq 2k$, and a set of $\leq 2k$ many vertices can be the underlying set of fewer than $\left((k+1)4k^2\right)^k$ many different variable-disjoint terms

(since a variable $X^i_{u,v}$ is determined by an ordered pair $(u,v) \in [S_T]^2$ and $i \in [k+1]$). Therefore, there is a sub-collection of of $\frac{s}{((k+1)4k^2)^k}$ many variable-disjoint terms whose underlying sets of vertices are distinct.

Because the underlying sets of vertices have size at most $2k$, we can apply the sunflower lemma to find $s' = \left(\frac{s}{((k+1)4k^2)^k(2k)!}\right)^{\frac{1}{2k}} = \left(\frac{c(F)}{k((k+1)4k^2)^k(2k)!}\right)^{\frac{1}{2k}}$ many terms whose sets of underlying vertices form an $(s', 2k)$ sunflower. We rename these terms $T_1, \ldots, T_{s'}$.

Let C be the core of the sunflower $S_{T_1}, \ldots, S_{T_{s'}}$. Notice that $|C| \leq 2k$. Call a variable **bad** if both of its underlying vertices belong to C. There are fewer than $2k^2$ many unordered pairs of vertices contained in C, and each is the underlying pair of exactly $2(k+1)$ many variables. Therefore, there are fewer than $2(k+1) \cdot 2k^2 = 4k^2(k+1)$ many variables whose underlying vertices are both in C. The terms $T_1, \ldots, T_{s'}$ are variable-disjoint, so each bad variable appears in at most one term, and when we remove all terms containing a bad variable, we obtain a sufficiently independent set of terms of size $s' - 4k^2(k+1) = \left(\frac{c(F)}{k(2k)!((k+1)4k^2)^k}\right)^{\frac{1}{2k}} - 4k^2(k+1)$. ∎

Before we bound the probability of satisfying a DNF with high cover number, we make a few observations.

Fact 1 *Let T be a term, and let $\rho \in \mathcal{P}_{k+1}(G)$ be given. $T \restriction_\rho = 1$ if and only if the following two events occur: (i) $T \restriction_{\sigma_\rho} = 1$ and (ii) For each $\{u,v\} \in P_T$, $c_\rho(u) \neq c_\rho(v)$.*

Lemma 39 *Let T be a term of size at most k.*

$$Pr_{\rho \in \mathcal{P}_{k+1}(G)}\left[T \restriction_{\sigma_\rho} = 1\right] \geq \frac{1}{3^k}$$

Proof: Order the literals of T as $l_1, \ldots, l_k$. For each j, $1 \leq j \leq k$, if we condition on the event that each of $l_1, \ldots, l_{j-1}$ is satisfied, then the probability of l_j being satisfied is at least $1/3$. This is because in the worst case, l_j is a literal $X^{ij}_{u,v}$ and

the other literals are $X_{u,v}^{i_1}, \ldots, X_{u,v}^{i_{j-1}}$, and in this case, the probability that $X_{u,v}^{i_j}$ is satisfied by σ_ρ is at least $1/3$. ∎

Lemma 40 *Let G be graph and let k be a positive integer. Let F be a k-DNF which contains contains t sufficiently independent terms.*

$$Pr_{\rho \in \mathcal{P}_{k+1}(G)} [F \restriction_\rho \neq 1] \leq \left(1 - \frac{1}{3^k 2^{2k}}\right)^t$$

Proof: Let $T_1, \ldots, T_t$ be the sufficiently independent terms of F. Let C be the core of the sunflower $S_{T_1}, \ldots, S_{T_t}$. Fix a coloring of the vertices in the core, $\chi : C \to [4k]$. Condition on the event that $c_\rho \restriction_C = \chi$.

We now lower-bound the probability that a given term T of the sufficiently independent set is satisfied. First, we bound the probability that every underlying edge of T is bichromatic. Note that by property (3) of sufficient independence, for all $\{u, v\} \in P_T$, $\{u, v\} \not\subseteq C$, so it suffices to bound the probability that the vertices in $S_T \backslash C$ receive distinct colors not in the range of χ. Therefore, the probability that every pair in P_T is bichromatic, conditioned on $c_\rho \restriction_C = \chi$, is at least $1/2^{2k}$. Because T contains at most k literals, the probability that $T \restriction_{\sigma_\rho} = 1$ is at least $\frac{1}{3^k}$. These two events are independent, so we have $\Pr_{\rho \in \mathcal{P}_{k+1}(G)} [T \restriction_\rho = 1 \mid c_\rho \restriction_C = \chi] \geq \frac{1}{2^{2k}} \frac{1}{3^k}$.

Now we show that (when we condition on the event that $c_\rho \restriction_C = \chi$) the events $T_i \restriction_\rho = 1$ are totally independent. Because the terms share no underlying pairs, the events $T_i \restriction_{\sigma_\rho}$ are independent of the satisfaction of other terms. The events "for each $\{u, v\} \in P_{T_i}$, $c_\rho(u) \neq c_\rho(v)$" are independent of the satisfaction of other terms. This is because once we condition on the event $c_\rho \restriction_C = \chi$, the probability that every pair of P_{T_i} is bichromatic under c_ρ depends only on the values that c_ρ takes on $S_{T_i} \setminus C$ and, for all $i \neq j$, $S_{T_i} \cap S_{T_j} = C$.

Combining the results of the previous two paragraphs shows that $\Pr_{\rho \in \mathcal{P}_{k+1}(G)} [F \restriction_\rho \neq 1 \mid c_\rho \restriction_C = \chi] \leq \left(1 - \frac{1}{3^k 2^{2k}}\right)^t$. Because this holds for all colorings $\chi : C \to [4k]$, we have that $\Pr_{\rho \in \mathcal{P}_{k+1}(G)} [F \restriction_\rho \neq 1] \leq \left(1 - \frac{1}{3^k 2^{2k}}\right)^t$ ∎

We now have the lemma relating cover number to the probability that a restriction satisfies a k-DNF.

Lemma 41 *For each k there exist positive constants δ, γ and d so that for any k-DNF F:*

$$Pr_{\rho \in \mathcal{P}_{k+1}(G)} [F \restriction_\rho \neq 1] \leq d2^{-\delta(c(F))^\gamma}$$

Proof:

By lemma 38 F contains a sufficiently independent set of at size at least $\beta_k(c(F))^{\frac{1}{2k}} - c_k$ By lemma 40:

$$\Pr_{\rho \in \mathcal{P}_{k+1}(G)} [F \restriction_\rho \neq 1] \leq \left(1 - \frac{1}{3^k 2^{2k}}\right)^{\beta_k(c(F))^{\frac{1}{2k}} - c_k}$$

Because k is fixed, this concludes the proof with $\delta = -\beta_k \log\left(1 - \frac{1}{3^k 2^{2k}}\right)$, $\gamma = 1/2k$ and $d = \left(1 - \frac{1}{3^k 2^{2k}}\right)^{-c_k}$.

■

IV.D.3 Width Lower Bound for Resolution

In this subsection we show that for each n, if G is a graph on n vertices satisfying a certain expansion-like property, then $w_R(GOP^{k+1}(G)) = \Omega(n)$. Combining this with a probabilistic calculation that there exist graphs G so that for $\rho \in \mathcal{P}_{k+1}(G)$, with probability at least $1/2$, $w_R(GOP^{k+1}(G) \restriction_\rho) = \Omega(n)$.

The proof of the resolution width bound is similar to the one used by Bonet and Galesi for the GT_n principles [44]. They worked with complete graphs, but we do not because the principles $GOP^2(K_n)$ have size in excess of 2^n. Fortunately, for the proof technique to work, G need not be complete but instead have the following property:

Definition IV.D.6 *Let G be an undirected graph on n-vertices. We say that G is ϵ-neighborly if between every pair of disjoint sets of vertices, $A, B \subseteq V(G)$ with $|A|, |B| \geq \epsilon n$, there exists an edge joining A and B.*

We now show that resolution refutations of $GOP(G)$ require large width when G is a connected, neighborly graph.

Lemma 42 *If G is a connected graph of n vertices that is ϵ-neighborly, then every resolution refutation of $GOP(G)$ contains a clause of width $\left(\frac{1-3\epsilon}{6}\right) n$.*

Proof: We begin by defining the "measure" of a clause. A **critical truth assignment** is an assignment to the variables of $GOP(G)$ which forms a total order on $V(G)$. For each $v \in V(G)$, let $C_v := \bigvee_{u \in N(v)} X_{u,v}$, and for each $I \subseteq V(G)$, $C_I := \bigwedge_{v \in I} C_v$. Let C be a clause. The **measure of C, $\mu(\mathbf{C})$,** is the minimum cardinality of a set $I \subseteq V(G)$ so that for every critical truth assignment α, if α satisfies C_I then α satisfies C.

Notice that if a clause $A \vee B$ is the resolvent of $A \vee x$ and $B \vee \neg x$ then $\mu(A \vee B) \leq \mu(A \vee x) + \mu(A \vee \neg x)$. Because of this, we say that μ is **subadditive with respect to resolution**. If $A \subseteq B$, then we have that $\mu(B) \leq \mu(A)$, so μ is **decreasing with respect to subsumption**.

We now show that $\mu(\{\}) = n$. Suppose otherwise, and let I be a subset of $V(G)$ with $|I| \leq n-1$. Choose one vertex $v_0 \in V(G) \setminus I$ and let α be a total order which arises by taking a depth-first search of G starting with v_0. Clearly α satisfies C_I but α does not satisfy $\{\}$.

Because every clause of $GOP(G)$ has measure either 0 or 1, the empty clause has measure n and the measure is both subadditive with respect to resolution and decreasing with respect to subsumption, there must exist a clause C so that $\frac{n}{3} \leq \mu(C) \leq \frac{2n}{3}$. Suppose for the sake of contradiction that $w(C) < \frac{n-3\epsilon n}{6}$.

Let I be a minimal subset of $V(G)$ so that for every critical truth assignment α, if α satisfies C_I then α satisfies C. Let $J = V(G) \setminus I$. Notice that $|I|, |J| \geq \frac{n}{3}$.

Let S be the set of vertices mentioned by variables of C. Clearly, $|S| \leq 2w(C) < 2\left(\frac{n-3\epsilon n}{6}\right) = \frac{n-3\epsilon n}{3}$. Therefore, $|I \setminus S| \geq \frac{n}{3} - \frac{n-3\epsilon n}{3} = \epsilon n$. Similarly, $|J \setminus S| \geq \epsilon n$. Because G is ϵ-neighborly, we may choose $u \in I \setminus S$ and $v \in J \setminus S$ so

that $\{u, v\}$ is an edge of G.

Let α be a critical truth assignment so that α satisfies $C_{I\setminus\{u\}}$ but α does not satisfy C_u and α does not satisfy C. Let β be the critical truth assignment which arises by moving v to the front of the order given by α. For $w \in I,\ w \neq u$, β satisfies C_w because every predecessor of w in α is a predecessor of w in β. For u, β satisfies C_u because β satisfies $X_{v,u}$. However, β does not satisfy C because α does not satisfy C and no variable mentioning u or v appears in C. Therefore, β satisfies C_I but β does not satisfy C, a contradiction to the choice of I. ∎

A resolution refutation of $GOP^k(G)$, $k \geq 1$, can be transformed into a resolution refutation of $GOP(G)$ by setting the appropriate variables to 1. Applying a restriction does not increase the width of a resolution refutation, so we have the following corollary:

Corollary 43 *If G is a connected graph of n vertices that is ϵ-neighborly, then for all $k \geq 1$, $w_R(GOP^k(G)) \geq \left(\frac{1-3\epsilon}{6}\right) n$.*

IV.D.4 Robust Graphs

Definition IV.D.7 *We say that a graph G is r-robust if for ρ selected at random by $\mathcal{P}_{k+1}(G)$, with probability at least $\frac{3}{4}$, $w_R(GOP(G)\restriction_\rho) \geq r$.*

To guarantee that the restricted principle will require high width to refute, it suffices that the graph obtained by deleting the bichromatic edges should consist of large, neighborly connected components. Random graphs of degree $\Theta(\log n)$ have this property with high probability. This is shown in the following subsection.

Lemma 44 *There exists a constant c, so that for sufficiently large n, there exists an $\frac{n}{96k}$-robust graph G on n vertices with degree at most $c \log n$.*

The proof of this lemma is a standard probabilistic argument. The reader may skip its proof in the following sub-subsection, and move directly to the proof of the lower bound in the next subsection.

Demonstration of Robust Graphs

An easy probabilistic argument shows that with very high probability, a random graph of expected degree $\Theta((1/\epsilon)\log n)$ is almost surely ϵ-neighborly.

Lemma 45 *Let n and d be positive integer so that $d \leq n$ and let $p = d/n$. Let $G_{n,p}$ be the distribution on graphs on n vertices in which every edge is included with independent probability p. With probability $\leq e^{2\epsilon n(1+\ln(1/\epsilon))-d\epsilon^2 n}$, a graph selected according to $G_{n,p}$ is* not *ϵ-neighborly.*

Proof: There are fewer than $\binom{n}{\epsilon n}^2 \leq \left(\frac{en}{\epsilon n}\right)^{2\epsilon n} = e^{2\epsilon n(1+\ln(1/\epsilon))}$ many pairs of disjoint sets of ϵn many vertices. Each such pair has a chance of at most $(1-p)^{\epsilon^2 n^2}$ of being unconnected. However, $(1-p)^{\epsilon^2 n^2} = (1-\frac{d}{n})^{\epsilon^2 n^2} \leq e^{-d\epsilon^2 n}$, so by the union bound the probability is at most $e^{2\epsilon n(1+\ln(1/\epsilon))}e^{-d\epsilon^2 n} = e^{2\epsilon n(1+\ln(1/\epsilon))-d\epsilon^2 n}$. ∎

We now show that a random graph will probably have each component large and neighborly if we randomly partition it into vertex-induced subgraphs.

Lemma 46 *For all $\epsilon > 0$, and all integers $k \geq 1$, there exists a constant c, so that for sufficiently large n, there exists graph G so that upon the random partition of G into $4k$ many vertex-induced subgraphs, with probability at least $1/2$, each component has size at least $n/8k$ and is ϵ-neighborly.*

Proof: Let $p = \frac{c\log n}{n}$. We will solve for the value of c at the end. Consider the following experiment: select a graph G according to the distribution $G_{n,p}$, and then independently color each vertex with one of $4k$ colors, then remove all bichromatic edges to form $4k$ vertex induced subgraphs, $G_1, \ldots, G_{4k}$.

Let P be the probability that G has a vertex of degree $> 2c\log n$, or that one of the induced subgraphs has size $< \frac{n}{8k}$, is disconnected or is not ϵ-neighborly. We now bound this probability.

Consider the probability that G has a vertex of degree $\geq 2c\log n$. By the Chernoff bounds, the probability of any one vertex having degree in excess of

$2p(n-1)$ is no more than $e^{-p(n-1)/4} = e^{-c(\log n)(n-1)/4n}$. Therefore, the probability of there existing a vertex with degree in excess of $2p(n-1)$ is no more than $ne^{-c(\log n)(n-1)/4n}$.

The Chernoff bounds also allow us to bound the probability that any of the G_i's contain too few vertices. The probability that a given color class of the partition contains fewer than $\frac{1}{2} \cdot \frac{n}{4k} = \frac{n}{8k}$ vertices is bounded by $e^{-\frac{n}{64k}}$.

Once we condition upon all pieces of the partition containing at least $\frac{n}{8k}$ vertices, we can bound the probability that any induced subgraph is disconnected. Consider a fixed set of $s \geq \frac{n}{8k}$ many vertices, and condition upon the event those vertices receive the same color in the partition. Each edge internal to the set is included with probability $\frac{c \log n}{n} = \frac{(cs/n)\log n}{s} \geq \frac{(c/8k)\log s}{s}$. By a standard result on the connectivity of random graphs (c.f. [46]), each color class is disconnected with probability bounded by $O\left(1/n^{(c/8k)-1}\right)$.

Finally, we consider the probability that each of the components G_i is ϵ-neighborly. For a fixed set of $s \geq \frac{n}{8k}$ vertices, if we condition on the event that set forms a component after partition, each internal edge is included with probability $\frac{c \log n}{n} \geq \frac{(c/8k)\log s}{s}$. By lemma 45, that means that the component is *not* ϵ-neighborly with probability at most $e^{2\epsilon s(1+\ln(1/\epsilon))-(c/8k)(\log s)\epsilon^2 s} = e^{-\Omega(n \log n)}$.

Therefore,

$$P \leq ne^{-c(\log n)(n-1)/4n} + 4ke^{-\frac{n}{64k}} + O\left(4k/n^{(c/8k)-1}\right) + e^{-\Omega(n \log n)}$$

For a sufficiently large constant c, dependent only on k and ϵ, this is below $\frac{1}{4}$.

Therefore, by an averaging argument on the edge choices, there exists a graph G of maximum degree $\leq 2c \log n$ so that upon random partition of its vertices into $4k$ color classes, its induced subgraphs are each connected, of size $\geq \frac{n}{8k}$, and ϵ-neighborly with probability $\geq \frac{3}{4}$. ∎

We now prove lemma 44.

Proof: Using lemma 46, choose c so that for sufficiently large n, there exists graph G so that upon the random partition of G into $4k$ many vertex-induced subgraphs, with probability at least $3/4$, each component has size at least $n/8k$ and is $(1/6)$-neighborly. Therefore we may choose $\rho \in \mathcal{P}_{k+1}(G)$ so that for each $i \in [4k]$, $w_R(GOP^{k+1}(G_i)) \geq \left(\frac{n}{8k}\right)\left(\frac{1-3\frac{1}{6}}{6}\right) = \frac{n}{96k}$ (by lemma 43).

Let Γ be a resolution refutation of $GOP^{k+1}(G) \restriction_\rho$. By lemma 35, $GOP^{k+1}(G) \restriction_\rho = \bigcup_{i=1}^{4k} GOP^{k+1}(G_i)$. However, for each $i, j \in [4k]$, $i \neq j$, we have that $GOP^{k+1}(G_i)$ and $GOP^{k+1}(G_j)$ are variable disjoint. Therefore, by lemma 2, for some $i \in [4k]$, there exists a resolution refutation of $GOP^{k+1}(G_i)$ of width is at most $w(\Gamma)$. However, by the preceding paragraph, each $GOP^{k+1}(G_i)$ requires width $\frac{n}{96k}$ to refute in resolution. Therefore $w(\Gamma) \geq \frac{n}{96k}$. ∎

IV.D.5 The Lower Bound

Theorem 47 *Let k be given. There exist constants $c > 0$ and $\epsilon_k > 0$, and a family of graphs G on n vertices (for n sufficiently large) with maximum degree $c \log n$ so that Res(k) refutations of $GOP^{k+1}(G)$ require size at least $2^{O(n^{\epsilon_k})}$.*

Proof: Let k be given. Apply lemma 44 and choose c so that for sufficiently large n, there exists a $\frac{n}{96k}$-robust graph G on n vertices with degree at most $c \log n$. By lemma 41, there are positive constants d, δ and γ so that for every k-DNF F $\Pr_{\rho \in \mathcal{P}_{k+1}(G)}[F \restriction_\rho \neq 1] \leq d2^{-\delta(c(F))^\gamma}$. By corollary 5, with $s = (\frac{n}{96k} - 1)/k$, for every k-DNF F:

$$\Pr_{\rho \in \mathcal{P}_{k+1}(G)}[h(F \restriction_\rho) > (n/96k - 1)/k] \leq dk2^{-2\delta^k((n/96k-1)/k)^{\gamma^k}/4^k}$$

Because d, γ and δ depend only on k, there exists ϵ_k so that

$$\Pr_{\rho \in \mathcal{D}}[h(F \restriction_\rho) > (n/96k - 1)/k] \leq \frac{1}{2}2^{-n^{\epsilon_k}}$$

Suppose for the sake of contradiction that Γ is a Res(k) refutation of $GOP^{K+1}(G)$ of size less than $2^{n^{\epsilon_k}}$, By the union bound, with probability at least

$1/2$, every line F of Γ has $h(F \restriction_\rho) \leq (n/96k-1)/k$. On the other hand, because G is $(n/96k)$-robust, $w_R(GOP^{k+1}(G) \restriction_\rho) \geq n/96k$ with probability at least $3/4$. So we may choose $\rho \in \mathcal{P}_{k+1}(G)$ so that $w_R(GOP^{k+1}(G) \restriction_\rho) \geq n/96k$, and for all lines F of Γ, $h(F \restriction_\rho) \leq (n/96k-1)/k$. By corollary 14, $GOP^{k+1}(G) \restriction_\rho$ has a resolution refutation of width at most $n/96k-1$. Contradiction. ∎

IV.E Improved Separation Between Res(k) and Res($k+1$)

The separation between Res($k+1$) and Res(k) given by theorem 47 uses sets of clauses whose maximum width is $\Theta(\log n)$. In this section we present an improvement which separates Res(k) and Res($k+1$) using constant width clauses. The width of the clauses does, however, depend doubly-exponentially on the constant k.

Definition IV.E.1 *Let $X_1, \ldots, X_k$ be propositional variables. The formula $Odd(X_1, \ldots, X_k)$ is the k-DNF expressing that the number of satisfied variables of $X_1, \ldots, X_k$ is odd. The formula $Even(X_1, \ldots, X_k)$ is the k-DNF expressing that the number of satisfied variables of $X_1, \ldots, X_k$ is even.*

The **k-parity graph ordering principle of G, $\mathbf{GOP^{\oplus k}(G)}$,** *is obtained by replacing each literal $X_{u,v}$ by $Odd(X^1_{u,v}, \ldots, X^k_{u,v})$, replacing each literal $\neg X_{u,v}$ by $Even(X^1_{u,v}, \ldots, X^k_{u,v})$, and then using the distributive rule and DeMorgan's law to express this set of k-DNFs as a set of clauses.*

Notice that for a graph G on n vertices with maximum degree $d \geq 3$, the principle $GOP^{\oplus k}(G)$ consists of $O(k^{d2^{k-1}}n^3)$ many clauses each of width at most $d2^{k-1}$.

For any graph G, the polynomial-size refutations of $GOP(G)$ can be transformed into Res($k+1$) refutations of $GOP^{\oplus(k+1)}(G)$. On the other hand, Res(k) refutations of $GOP^{\oplus(k+1)}(G)$ require exponential size for certain graphs:

Theorem 48 *Let k be given. There exist constants $d > 0$ and $\epsilon_k > 0$, and a*

family of graphs G on n vertices (for n sufficiently large) with maximum degree d so that Res(k) refutations of $GOP^{\oplus(k+1)}(G)$ require size at least $2^{O(\epsilon_k n)}$.

IV.E.1 The Upper Bounds

We build Res(k) refutations for $GOP^{\oplus k}(G)$ from resolution refutations of $GOP(G)$.

Definition IV.E.2 *Let k be a positive integer and let $X_1, \ldots, X_n$ be propositional variables. Let $X_1^1, \ldots, X_1^k, X_2^1, \ldots, X_n^k$ be new variables. Let σ be the mapping given by $\sigma(X_i) = Even(X_i^1, \ldots, X_i^k)$ and $\sigma(\neg X_i) = Odd(X_i^1, \ldots, X_i^k)$. For a clause $C = \bigvee_i l_i$, let $\sigma(C) = \bigvee_i \sigma(l_i)$.*

Lemma 49 *Let k be a constant. There exists a constant c (dependent only on k) so that for all clauses $A \vee X_i$ and $B \vee \neg X_i$ be clauses in the variables $X_1, \ldots, X_n$, there is a derivation of $\sigma(A) \vee \sigma(B)$ from $\{\sigma(A) \vee \sigma(X_i), \sigma(B) \vee \sigma(\neg X_i)\}$ of size $\leq c$.*

Proof: By the completeness of Res(k), there is a Res(k) refutation of the pair of k-DNFs $\{\text{Even}(X_1, \ldots, X_k), \text{Odd}(X_1, \ldots, X_k)\}$. Let c be the minimum size of such a refutation. Because $\sigma(X_i) = \text{Odd}(X_i^1, \ldots, X_i^k)$ and $\sigma(\neg X_i) = \text{Even}(X_i^1, \ldots, X_i^k)$, there is a derivation of $\sigma(A) \vee \sigma(B)$ from $\{\sigma(A) \vee \sigma(X_i), \sigma(B) \vee \sigma(\neg X_i)\}$ of size $\leq c$. ∎

Lemma 50 *For each k, there exists a constant c so that for every G with n vertices and degree at most $d \geq 3$, $GOP^{\oplus k}(G)$ has a Res(k) refutation of size $O(cn^3 + k^{d2^{k-1}} n^3)$.*

Proof: With the repeated application of AND-introduction inferences, $\sigma(GOP(G))$ can be derived from $GOP^{\oplus k}(G)$ in $O(k^{d2^{k-1}} n^3)$ many inferences. By lemma 33, $GOP(G)$ has a refutation of size $O(n^3)$ so by lemma 49, $\sigma(GOP(G))$ has a Res(k)

refutation of size $O(cn^3)$. Therefore, $GOP^{\oplus k}(G)$ has a refutation of size $O(cn^3 + k^{d2^{k-1}}n^3)$. ∎

IV.E.2 Random Restrictions

Definition IV.E.3 *Let $k \geq 1$ be given. Let G be a graph. The distribution $\mathcal{P}_{k+1}(G)$ on partial assignments ρ to the variables of $GOP^{\oplus(k+1)}(G)$ is given by the following experiment:*

For each $(u,v) \in V(G)^2$, choose $i \in \{1,\ldots,k+1\}$ uniformly and independently. For each $j \in \{1,\ldots,k\}$, $j \neq i$, set $X^j_{u,v}$ to 0 or 1, uniformly and independently.

Lemma 51 *Let k be given, and let F be a k-DNF in the variables of $GOP^{\oplus(k+1)}(G)$. There exist constants $\delta > 0$, dependent only on k, so that $Pr_{\rho\in\mathcal{P}_{k+1}(G)}[F \restriction_\rho \neq 1] \leq 2^{-\delta\cdot c(F)}$*

Proof: We will say that two terms T and T' are **underlying-variable-disjoint** if whenever $X^i_{u,v} \in T$ and $X^{i'}_{u',v'} \in T'$ we have that $(u,v) \neq (u',v')$. Because F is a k-DNF, it contains at least $c(F)/k(k+1)$ many underlying-variable-disjoint terms. Each of these terms is satisfied with independent probability at least $1/4^k$ (consider setting each variable of a term in turn, the probability that a variable is set to 0 or 1 is always $\geq 1/(k+1-(k-1)) = 1/2$). Therefore, $\Pr_{\rho\in\mathcal{P}_{k+1}(G)}[F \restriction_\rho \neq 1] \leq (1-1/4^k)^{c(F)/k(k+1)}$. ∎

When we apply a random restriction from $\mathcal{P}_{k+1}(G)$ to $GOP^{\oplus(k+1)}(G)$, we do not necessarily obtain an instance of $GOP(G)$. It possible that some of the edge variables will become inverted. However, inverting the variables does not affect the width required for a resolution refutation.

Corollary 52 *If G is a connected graph that is ϵ-neighborly, then for all $k \geq 1$, for all $\rho \in \mathcal{P}_{k+1}(G)$, $GOP^{\oplus(k+1)}(G) \restriction_\rho$ requires width $\frac{1-3\epsilon}{6}$.*

IV.E.3 The Lower Bound

Theorem 53 *Let k be given. There exist constants $d > 0$ and $\epsilon_k > 0$, and a family of graphs G on n vertices (for n sufficiently large) with maximum degree c so that Res(k) refutations of $GOP^{\oplus(k+1)}(G)$ require size at least $2^{O(\epsilon_k n)}$.*

Proof: Let k be given. Set $p = 15 \ln 6/n$. Consider a random graph selected according to $G_{n,p}$; by lemma 45, G is almost certainly $\frac{1}{6}$-neighborly and by the Chernoff bounds, it has maximum degree $\leq 2pn = 26 \ln 6$. Let G be a graph that is both $\frac{1}{6}$-neighborly and has maximum degree $\leq 26 \ln 6$.

By lemma 51, we have that for every k-DNF F $\Pr_{\rho \in \mathcal{P}_{k+1}(G)}[F \restriction_\rho \neq 1] \leq 2^{-\delta \cdot c(F)}$. Now apply corollary 5 with $s = (n/12 - 1)/k$, $d = 1$. For every k-DNF F:

$$\Pr_{\rho \in \mathcal{P}_{k+1}(G)}[h(F \restriction_\rho) > (n/12 - 1)/k] \leq k 2^{-2\delta^k((n/12-1)/k)/4^k}$$

Because k is fixed and δ depends only on k, there exists ϵ_k so that $\Pr_{\rho \in \mathcal{D}}[h(F \restriction_\rho) > (n/12 - 1)/k] < 2^{-\epsilon_k n}$.

Suppose for the sake of contradiction that Γ is a Res(k) refutation of $GOP^{\oplus(k+1)}(G)$ of size less than $2^{\epsilon_k n}$, By the union bound, with probability > 0, every line F of Γ has $h(F \restriction_\rho) \leq (n/12 - 1)/k$. By corollary 14, $GOP^{k+1}(G) \restriction_\rho$ has a resolution refutation of width at most $n/12 - 1$. On the other hand, because G is $\frac{1}{6}$-neighborly, $w_R(GOP(G)) \geq \left(\frac{1-3(1/6)}{6}\right) n = n/12$, and therefore $w_R(GOP^{\oplus(k+1)}(G) \restriction_\rho) \geq w_R(GOP(G)) \geq n/12 - 1$. Contradiction.

■

IV.F Acknowledgements

Much of the text of this chapter was previously published as part of [41] in the proceedings of the Forty-third Annual IEEE Symposium on the Foundations of Computer Science. I was the primary researcher and author of this publication which forms the basis for this chapter.

Chapter V

Simulation of Nullstellensatz Refutations

In this chapter, we show that constant-depth Frege systems with counting axioms modulo m polynomially simulate Nullstellensatz refutations modulo m. This allows us to transform Nullstellensatz refutations into constant-depth Frege with counting axioms proofs with a small increase in size, and to infer size lower bounds for Nullstellensatz refutations from size lower bounds for constant-depth Frege with counting axioms proofs. In particular, this method establishes the first superpolynomial size separation between Nullstellensatz and polynomial calculus refutations.

It is not immediately clear how to compare constant-depth Frege systems with Nullstellensatz refutations because Frege systems prove propositional formulas in connectives such as $\bigwedge$, $\bigvee$ and $\neg$, and the Nullstellensatz system shows that systems of polynomials have no common roots. Moreover, constant-depth Frege systems use only constant-depth formulas and such formulas cannot express sums. We propose a definition of reducibility from propositional formulas to systems of polynomials: a formula F reduces to a system of polynomials over $\mathbb{Z}_m$ if we can use F to define an m-partition (a partition in which every class consists of exactly m elements) on the satisfied monomials of the polynomials. The simulation

shows that if a formula has a small reduction to a set of polynomials with a small Nullstellensatz refutation, then the formula has a small constant-depth Frege with counting axioms refutation. This notion of reduction seems natural in that for previously studied translations of formulas into systems of polynomials, a formula reduces to its translation.

The simulation of Nullstellensatz refutations modulo m by constant-depth Frege systems with counting axioms modulo m works by defining two different m-partitions on the satisfied monomials in the expansion of the Nullstellensatz refutation. One covers the satisfied monomials perfectly, and the other leaves out exactly one satisfied monomial. In section V.B, we show that Frege systems with counting axioms can prove in constant depth and polynomial size that such a partition cannot exist. Section V.C formalizes our definition of reducibility from propositional formulas to systems of polynomials and proves the main simulation theorem. In section V.D we show that, for several methods of translating propositional formulas into systems of polynomials, a formula efficiently reduces to its translation.

We explore some applications of the simulation in section V.E. First, we obtain small constant-depth Frege with counting axioms refutations for unsolvable systems of linear equations in which each equation contains a small number of variables. This class of tautologies includes the Tseitin tautologies and the "τ formulas" for Nisan-Wigderson pseudorandom generators built from the parity function [1, 2]. The Tseitin tautologies on a constant degree expander can be expressed as an unsatisfiable set of constant-width clauses, and are known to require exponential size to refute in constant-depth Frege systems [9]. Therefore, as a corollary, we obtain an exponential separation of constant-depth Frege systems with counting axioms and constant-depth Frege systems with respect to constant-width CNFs.

V.A Definitions, Notation and Conventions

Definition V.A.1 *For a monomial* $t = \prod_{i \in I} x_i^{\alpha_i}$*, its* **multilinearization,** $\bar{\mathbf{t}}$**,** *is defined as* $\bar{t} = \prod_{i \in I} x_i$*. Let* $f = \sum_t c_t t$ *be a polynomial. The* **multilinearization of f,** $\bar{\mathbf{f}}$**,** *is defined as* $\bar{f} = \sum_t c_t \bar{t}$*. We say that a polynomial* f *is* **multilinear** *if* $f = \bar{f}$*.*

Definition V.A.2 *Let* $n > 0$ *be given, and let* $x_1, \ldots, x_n$ *be variables. Let* $I \subseteq [n]$ *be given. The monomial* $\mathbf{x_I}$ *is defined to be* $\prod_{i \in I} x_i$*.*

Notice that a multilinear polynomial f in the variables $x_1, \ldots, x_n$ can be written as $\sum_{I \subseteq [n]} a_I x_I$.

V.B Contradictory Partitions of Satisfied Variables

To simulate Nullstellensatz refutations in constant-depth Frege systems with counting axioms, we construct two partitions on the satisfied monomials of the refutation: one which covers the satisfied monomials exactly, and another which covers the satisfied monomials with $m - 1$ new points. This is impossible, and in this section, we show that constant-depth Frege systems with counting axioms can prove that this is impossible with polynomial size proofs.

Definition V.B.1 *Let positive integers* n *and* k *be given. Let* $u_1, \ldots, u_n$ *be a set of Boolean variables. For each* $e \in [n]^m$*, let* y_e *be a variable, and for each* $e \in [n+k]^m$*, let* z_e *be a variable.* $\mathbf{CP^{n,k}_m}(\vec{\mathbf{u}}, \vec{\mathbf{y}}, \vec{\mathbf{z}})$ *is the negation of the conjunction of the following formulas:*

"every variable covered by the first partition is satisfied"

for each $e \in [n]^m$*,* $y_e \to \bigwedge_{i \in e} u_i$

"every satisfied variable is covered by the first partition"

for each $i \in [n]$*,* $u_i \to \bigvee_{e \ni i} y_e$

"no two overlapping edges are used by the first partition"

for each $e, f \in [n]^m$ *with* $e \perp f$, $\neg y_e \vee \neg y_f$

"every variable covered by the second partition is satisfied"

for each $e \in [n+k]^m$, $z_e \rightarrow \bigwedge_{\substack{i \in e \\ i \leq n}} u_i$

"every satisfied variable is covered by the second partition"

for each $i \in [n]$, $u_i \rightarrow \bigvee_{e \ni i} z_e$

"every extra point is covered by the second partition"

for each i, $n+1 \leq i \leq n+k$, $\bigvee_{e \ni i} z_e$

"no two overlapping edges are used by the second partition"

for each $e, f \in [n+k]^m$ *with* $e \perp f$, $\neg z_e \vee \neg z_f$

Lemma 54 *Fix* m *and* k *so that* m *is not divisible by* k. *For all* n, *the tautology* $CP_m^{n,k}$ *has a constant depth, size* $O(n^m)$ *proof in constant-depth Frege with counting modulo* m *axioms.*

Proof: Fix m, n and k. The proof of $\mathrm{CP}_m^{n,k}$ is by contradiction. We define a set U of size $mn+k$ and formulas ϕ_e for each $e \in [U]^m$ so that we can derive $\left(\neg\mathrm{Count}_m^U\right)[x_e \leftarrow \phi_e]$ in size $O(n^m)$ from the hypothesis $\neg\mathrm{CP}_m^{n,k}$.

Let U be the set consisting of the following points: $p_{r,i}$, $r \in [m]$, $i \in [n]$ (the r'th copy of the row of variables) and $p_{m,i}$, $n+1 \leq i \leq k$ (the extra points.)

"when u_i is unset, we group together its copies"

for each $i \in [n]$, $\phi_{\{p_{1,i},\ldots,p_{m,i}\}} = \neg u_i$

"in the first $m-1$ rows, use the partition given by the y_e's"

for each $r \in [m-1]$, each $i_1, \ldots, i_m \in [n]$, $\phi_{\{p_{r,i_1},\ldots,p_{r,i_m}\}} = y_{\{i_1,\ldots,i_m\}}$

"in the last row, use the the partition given by the z_e's"

for each $i_1, \ldots, i_m \in [n+k]$, $\phi_{\{p_{m,i_1},\ldots,p_{m,i_m}\}} = z_{\{i_1,\ldots,i_m\}}$

other edges are not used

for all other $e \in [U]^m$, $\phi_e = 0$

Now we sketch the derivation of $\left(\neg\mathrm{Count}_m^U\right)[x_e \leftarrow \phi_e]$ from $\neg\mathrm{CP}_m^{n,k}$. It is easily verified that the derivation has constant depth and size $O((mn+k)^m) = O(n^m)$.

"Every point of U is covered by the partition."

Let $p_{r,i} \in U$ with $i \in [n]$, $r \in [m-1]$ be given. From $\neg\mathrm{CP}_m^{n,k}$ derive $u_i \to \bigvee_{\substack{f \in [n]^m \\ f \ni i}} y_f$. Because $\bigvee_{\substack{f \in [n]^m \\ f \ni i}} y_f$ is a sub-disjunction of $\bigvee_{\substack{e \in [U]^m \\ e \ni p_{r,i}}} \phi_e$, we may derive $u_i \to \bigvee_{\substack{e \in [U]^m \\ e \ni p_{r,i}}} \phi_e$ with a weakening inference. Because $\phi_{\{p_{1,i},\ldots,p_{m,i}\}} = \neg u_i$, we may derive $\neg u_i \to \bigvee_{\substack{e \in [U]^m \\ e \ni p_{r,i}}} \phi_e$. Combining these two formulas yields $\bigvee_{\substack{e \in [U]^m \\ e \ni p_{r,i}}} \phi_e$. The case for $p_{m,i}$, $i \in [n]$ is similar.

For a point $p_{m,i}$, $n+1 \leq i \leq n+k$, from $\neg\mathrm{CP}_m^{n,k}$ derive $\bigvee_{\substack{f \in [n+k]^m \\ f \ni i}} z_f$. A weakening inference applied to this derives $\bigvee_{e \ni p_{m,i}} \phi_e$.

"No overlapping edges are used."

Let $e_1, e_2 \in [U]^m$ be given so that $e_1 \perp e_2$, and neither ϕ_{e_1} nor ϕ_{e_2} is identically 0.

If $\phi_{e_1} = \neg u_i$ and $\phi_{e_2} = y_f$, then e_1 is $\{p_{r,i} \mid r \in [m]\}$ and e_2 is $\{p_{r,j} \mid j \in f\}$ for some $r \in [m]$ and $f \in [n]^m$ so that $i \in f$. From $\neg\mathrm{CP}_m^{n,k}$ derive $y_f \to u_i$. From this, derive $\neg\neg u_i \vee \neg y_f = \neg\phi_{e_1} \vee \neg\phi_{e_2}$.

If $\phi_{e_1} = y_{f_1}$ and $\phi_{e_2} = y_{f_2}$, then e_1 is $\{p_{r_1,i} \mid i \in f_1\}$ and e_2 is $\{p_{r_2,i} \mid i \in f_2\}$ with $r_1 = r_2$ and $f_1 \perp f_2$. From $\neg\mathrm{CP}_m^{n,k}$ derive $\neg y_{f_1} \vee \neg y_{f_2} = \neg\phi_{e_1} \vee \neg\phi_{e_2}$.

The only other cases are when $\phi_{e_1} = \neg u_i$ and $\phi_{e_2} = z_f$ or $\phi_{e_1} = z_{f_1}$ and $\phi_{e_2} = z_{f_2}$, and these are handled similarly.

■

V.C The Simulation

Because we work over $\mathbb{Z}_m$, a polynomial vanishes on a given assignment if and only if there is an m-partition on its satisfied monomials (recall that we treat a monomial with coefficient a as having a distinct copies.) The definability of this partition is the connection between refuting a propositional formula and refuting a system of polynomials.

V.C.1 Reducing Formulas to Systems of Equations

The method we use to reduce a formula to a system of polynomials is to define a partition on the satisfied monomials of the polynomials with small, constant-depth formulas and prove that these formulas define a partition using the formula as a hypothesis.

Because of the central role played by the sets of monomials appearing in each polynomial, we take a moment to define this notion precisely. First of all, because we are concerned only with 0/1 assignments, a polynomial vanishes if and only if its multilinearization vanishes. For this reason, we restrict our attention to multilinear polynomials. We treat a term ax_I as a distinct copies of the monomial x_I. For this reason, when we talk about the "set of monomials" of a polynomial, we do not mean the set of monomials that appear in the polynomial, but a set which includes a copies of each monomial with coefficient a. We will generally identify ax_I with a objects $m_{1,I}, \ldots, m_{a,I}$. Think of $m_{c,I}$ as the c'th copy of the monomial x_I. There should be little confusion of the dual use of the symbol "m" because when the symbol appears without a subscript it denotes the modulus, and when it appear with a subscript it denotes a monomial.

Definition V.C.1 *Let $f = \sum_{I \subseteq [n]} a_I x_I$ be a multilinear polynomial over $\mathbb{Z}_m$. The* **set of monomials of f** *is the following set:*

$$M_f = \{m_{c,I} \mid I \subseteq [n],\ c \in [a_I]\}$$

Definition V.C.2 *Let $x_1, \ldots, x_n$ be Boolean variables. Let f be a multilinear polynomial in the variables $x_1, \ldots, x_n$. For each $E \in [M_f]^m$, let θ_E be a formula in $\vec{x}$. We say that* **the θ's form an m-partition the satisfied monomials of f** *if the following formula holds:*

$$\bigwedge_{E \in [M_f]^m} \left(\theta_E \rightarrow \bigwedge_{m_{c,I} \in E} \bigwedge_{k \in I} x_k \right) \ \wedge \ \left(\bigwedge_{\substack{E,F \in [M_f]^m \\ E \perp F}} \neg\theta_E \vee \neg\theta_F \right)$$

$$\wedge \bigwedge_{m_{c,I} \in M_f} \left(\left(\bigwedge_{k \in I} x_k \right) \rightarrow \bigvee_{\substack{E \in [M_f]^m \\ E \ni m_{c,I}}} \theta_E \right)$$

Definition V.C.3 *Let $x_1, \ldots, x_n$ be Boolean variables. Let $\Gamma(\vec{x})$ be a propositional formula. Let $F = \{f_1, \ldots, f_k\}$ be a system of polynomials over $\mathbb{Z}_m$ with a Nullstellensatz refutation $p_1, \ldots, p_k$, $r_1, \ldots, r_n$. If, for each $i \in [k]$, there are formulas $\beta_E^i(\vec{x})$, $E \in \left[M_{\bar{f}_i}\right]^m$, so that there is a size T, depth d Frege derivation from $\Gamma(\vec{x})$ that, for each i, the β^i's form an m-partition on the satisfied monomials of $\bar{f}_i$, then we say that* **Γ reduces to F in depth d and size T**.

V.C.2 The Simulation

Theorem 55 *Let $m > 1$ be an integer. Let $x_1, \ldots, x_n$ be Boolean variables. Let $\Gamma(\vec{x})$ be a propositional formula, and let F be a system of polynomials over $\mathbb{Z}_m$ so that Γ reduces to F in depth d and size T. If there is a Nullstellensatz refutation of F with size S, then there is a depth $O(d)$ Frege with counting axioms modulo m refutation of $\Gamma(\vec{x})$ with size $O(S^{2m}T)$.*

Proof: Let $p_1, \ldots, p_k$, $r_1, \ldots, r_n$ be a size S Nullstellensatz refutation of F. Let $\beta_E^i(\vec{x})$, for $i \in [k]$, $E \in [M_{\bar{f}_i}]^m$, be formulas so that from Γ there is a size T, depth d proof that for each i the $\beta_E^i(\vec{x})$'s form an m-partition on the satisfied monomials of $\bar{f}_i$.

We obtain contradictory partitions of the the monomials that appear in the expansion of $\sum_{i=1}^k \bar{p}_i \bar{f}_i$ in which polynomials are multiplied and multilinearized, but no terms are collected. In other words, the set is the collection, over $i \in [k]$, of all pairs of monomials from $\bar{p}_i$ and $\bar{f}_i$.

$$V = \bigcup_{i=1}^{k} \{(m_{c,I}, m_{d,J}, i) \mid m_{c,I} \in M_{\bar{p}_i},\ m_{d,J} \in M_{\bar{f}_i}\}$$

Notice that $|V| = O(S^2)$.

For each $v \in V$, $v = (m_{c,I}, m_{d,J}, i)$, let $\gamma_v = \bigwedge_{k \in I \cup J} x_k$. Think of these as the monomials. We will give formulas θ_E, that define a partition on the satisfied

monomials with $m-1$ many extra points, and η_E, that define a partition on the satisfied monomials with no extra points. We will give a $O(|V|^m+T) = O(S^{2m}+T)$ derivation from Γ of the following:

$$\neg \mathrm{CP}_m^{|V|,m-1}\left[u_v \leftarrow \gamma_v,\ y_E \leftarrow \theta_E,\ z_E \leftarrow \eta_E\right]$$

On the other hand, by lemma 54, $\mathrm{CP}_m^{|V|,m-1}$ has constant depth Frege proofs of size $O(|V|^m)$, so $\mathrm{CP}_m^{|V|,m-1}\left[u_v \leftarrow \gamma_v,\ y_E \leftarrow \theta_E,\ z_E \leftarrow \eta_E\right]$ has a constant depth Frege proof of size $O(|V|^m T)$. Therefore, Γ has a depth $O(d)$ Frege refutation of size $O(S^{2m}T)$.

The Partition with $m-1$ Extra Points

Notice that we have the following equation:

$$\overline{\sum_{i=1}^{k} \bar{p}_i \bar{f}_i} = \overline{\sum_{i=1}^{k} p_i f_i + \sum_{j=1}^{n} r_j (x_j^2 - x_j)} = 1$$

So when we collect terms after expanding $\sum_{i=1}^{k} \bar{p}_i \bar{f}_i$ and multilinearizing, the coefficient of every nonconstant term is 0 modulo m, and the constant term is 1 modulo m.

For each $S \subseteq [n]$, let $V_S = \{(m_{c,I}, m_{d,J}, i)) \in V \mid I \cup J = S\}$. Think of these as the occurrences of x_S in the multilinearized expansion.

For each $S \subseteq [n]$, $S \neq \emptyset$, there is an m-partition on V_S, call it $\mathcal{P}_S$. Likewise, there is an m-partition on $V_\emptyset \cup [m-1]$, call it $\mathcal{P}_\emptyset$.

Define the formulas θ_E as follows: for each $E \in ([V] \cup [m-1])^m$, if $E \in \mathcal{P}_S$ for some $S \subseteq [n]$ then $\theta_E = \bigwedge_{k \in S} x_k$, otherwise $\theta_E = 0$.

Constant-depth Frege can prove that this is a m-partition of the satisfied monomials of $\sum_{i=1}^{k} \overline{\bar{p}_i \bar{f}_i}$ with $m-1$ extra points. The proof has size $O(|V|^m)$ and depth $O(1)$. It is trivial from the definition of θ_E that the edges cover only satisfied monomials. That every satisfied monomial $\bigwedge_{k \in S} x_k$ is covered is also trivial: the edge from $\mathcal{P}_S$ is used if and only if the term x_S is satisfied. Finally, it easily shown that the formulas for two overlapping edges are never both satisfied: only edges

from $\mathcal{P}_S$ are used (regardless of the values of the x's), so for any pair of overlapping edges, $E \perp F$, one of the two formulas θ_E or θ_F is identically 0.

The Partition with No Extra Points

The idea is that an m-partition on the satisfied monomials on $\bar{f}_i$ can be used to build an m-partition on the satisfied monomials of $t\bar{f}_i$, for any monomial t.

For each $E \in [V]^m$, define η_E as follows: if $E = \{(m_{c,I}, m_{d_l,J_l}, i) \mid l \in [m]\}$ for some $i \in [k]$, $m_{c,I} \in M_{f_i}$, then $\eta_E = \bigwedge_{k\in I} x_k \wedge \beta_{\{m_{d_l,J_l} | l\in[m]\}}$, otherwise, $\eta_E = 0$.

There is a size $O(S + |V|^m)$, depth $O(d)$ Frege derivation from Γ that the η_E's form an m-partition on the satisfied monomials of $\sum_{i=1}^{k} \overline{\bar{p}_i \bar{f}_i}$. We briefly sketch how to construct the proof. Begin by deriving from Γ, for each i, that the β^i_E's form an m-partition on the satisfied monomials of $\bar{f}_i$.

"Every satisfied monomial is covered." Let $(m_{c,I}, m_{d,J}, i) \in V$ be given. If $\bigwedge_{k\in I\cup J} x_k$ holds, then so do $\bigwedge_{k\in I} x_k$ and $\bigwedge_{k\in J} x_k$. Because the β^i's form an m-partition on the satisfied monomials of $\bar{f}_i$, we may derive $\bigvee_{F\in[M_{f_i}]^m} \beta^i_F$. From this derive $\bigvee_{F\in[M_{f_i}]^m} \bigwedge_{k\in I} x_k \wedge \beta^i_F$. A weakening inference applied to this yields $\bigvee_{E\in[V]^m} \eta_E$.

"Every monomial covered is satisfied." Let $v = (m_{c,I}, m_{d,J}, i) \in V$ be given so that $v \in E$ and η_E holds. For this to happen, $E = \{(m_{c,I}, m_{d_l,J_l}, i) \mid l \in [m]\}$. By definition,, $\eta_E = \bigwedge_{k\in I} x_k \wedge \beta^i_{\{m_{d_l,J_l} | l\in[m]\}}$, and therefore $\bigwedge_{k\in I} x_k$ holds. Because the β^i's form an m-partition on the satisfied monomials of $\bar{f}_i$, we have that $\bigwedge_{k\in J} x_k$ holds. Therefore $\bigwedge_{k\in I\cup J} x_k$ holds.

"No two conflicting edges E and F can have η_E and η_F simultaneously satisfied." If $E \perp F$, and neither θ_E nor θ_F is identically 0, then they share the same $\bar{p}_i$ component. That is, there exists i, $m_{c,I} \in M_{\bar{p}_i}$ so that $E = \{(m_{c,I}, m_{d_l,J_l}, i) \mid l \in [m]\}$, and $F = \{(m_{c,I}, m_{d'_l,J'_l}, i) \mid l \in [m]\}$. Because $E \perp F$, we have $\{m_{d_l,J_l} \mid l \in [m]\} \perp \{m_{d'_l,J'_l} \mid l \in [m]\}$. Because the β^i's form an m-partition on the satisfied monomials of $\bar{f}_i$, we can derive $\neg\beta^i_{\{m_{d_l,J_l} | l\in[m]\}} \vee \neg\beta^i_{\{m_{d'_l,J'_l} | l\in[m]\}}$. We weaken this formula to obtain $\neg\beta^i_{\{m_{d_l,J_l} | l\in[m]\}} \vee \neg\beta^i_{\{m_{d'_l,J'_l} | l\in[m]\}} \vee \bigvee_{k\in I} \neg x_k$, and from that derive

$$\neg\left(\bigwedge_{k\in I} x_k \wedge \beta^i_{\{m_{d_l,J_l}|l\in[m]\}}\right) \vee \neg\left(\bigwedge_{k\in I} x_k \wedge \beta^i_{\{m_{d'_l,J'_l}|l\in[m]\}}\right) = \neg\eta_E \vee \neg\eta_F.$$

■

V.D Translations of Formulas into Polynomials

V.D.1 Direct Translation of Clauses

For sets of narrow clauses, a common way to translate the clauses into polynomials is to map x to $1-x$, $\neg x$ to x and replace "OR" by multiplication. This is most commonly used for constant-width CNFs, and in this case, we show that clauses efficiently reduce to their translations.

Definition V.D.1 *[44] For a a clause C in variables $\vec{x}$, the* **direct translation of C, tr(C),** *is defined recursively as follows: (i) $tr(\emptyset) = 1$ (ii) $tr(A \vee x) = tr(A)(1-x)$ (iii) $tr(A \vee \neg x) = tr(A)x$*

For a CNF F, the **direct translation of F, tr(F),** *is the set $\{tr(C) \mid C \in F\}$.*

It is easily verified by induction that an for any clause C, a Boolean assignment satisfies C if and only if it is a root of $tr(C)$.

Whenever C is satisfied, there exists an m-partition on the satisfied monomials of $tr(C)$. Moreover, if C contains at most w variables, then the m-partition can be defined by depth two formulas of size $O(2^w)$, and by the completeness of constant-depth Frege systems, there is a constant depth derivation from C of size $2^{O(w)}$ that these formulas define an m-partition on the satisfied monomials of $tr(C)$. Therefore, C reduces to $tr(C)$ in constant depth and size $O(2^w)$.

Lemma 56 *If F is an unsatisfiable CNF of m clauses of width w, then F is reducible to $tr(F)$ in size $m2^{O(w)}$ and depth $O(1)$.*

V.D.2 Translations That Use Extension Variables

More involved translations of formulas into sets of polynomials use extension variables that represent sub-formulas. The simplest way of doing this would be to reduce an unbounded fan-in formula Γ to a bounded fan-in formula, and then introduce one new variable y_g per gate g, with the polynomial that says y_g is computed correctly from its inputs. It is easy to give a reduction from Γ to this translation, of depth $depth(\Gamma)$ and size $poly(|\Gamma|)$. (We can define y_g by the subformula rooted at g and every polynomial would have constant size, so defining the partition is trivial.) However, this translation reveals little for our purposes because there is usually no small degree Nullstellensatz refutation of the resulting system of polynomials, even for trivial Γ. For example, say that we translated the formula $x_1, \neg((((x_1 \vee x_2) \vee \cdots \vee x_n)$ this way. The resulting system of polynomials is weaker than the induction principles (see the end of this section) which require $\Omega(\log n)$ degree **NS** refutations [61].

We give an alternative translation of formulas into sets of polynomials so that the formula is unsatisfiable if the set of polynomials has no common root. A formula f reduces to the set of polynomials with depth $O(\text{depth}(f))$ and size $O(|f|)$. Moreover, for many previously studied unsatisfiable CNFs (such as the negated counting principles), this translation is the same as the previously studied translations (up to constant-degree Nullstellensatz derivations).

Definition V.D.2 *Let f be a formula in the variables $x_1, \ldots, x_n$ and the connectives $\{\bigvee, \neg\}$. For each pair of subformulas g_1 and g_2 of f, we write $\mathbf{g_1 \to g_2}$ if g_1 is an input to g_2. Canonically order the subformulas of f, and write $\mathbf{g_1 < g_2}$ if g_1 precedes g_2 in this ordering. For each subformula g of f, let there be a variable y_g* - the value of g. *For each pair of subformulas of f, g_1 and g_2, so that the top connective of g_2 is $\bigvee$ and $g_1 \to g_2$, let there be a variable z_{g_1,g_2}* - "g_1 is the first satisfied input of g_2". *The* **polynomial translation of f, POLY(f),** *is the following set of polynomials:*

For each variable x_i*:*

"The value of subformula x_i *is equal to* x_i*"*

$y_{x_i} - x_i$

For each subformula g *whose top connective is* $\bigvee$*:*

"if $g_1 < g_2$*,* $g_1 \to g$*,* $g_2 \to g$*, and* g_1 *is satisfied ,*

then g_2 *is not the first satisfied input of* g*"*

$y_{g_1} z_{g_2,g}$

"if g_1 *is the first satisfied input of* g*,*

then g_1 *is satisfied"*

$z_{g_1,g} y_{g_1} - z_{g_1,g}$

"g *is satisfied if and only if the some input to* g

is the first satisfied input of g*"*

$y_g - \sum_{g_1 \to g} z_{g_1,g}$

For each subformula g *whose top connective is* $\neg$*:*

Let g_1 *the unique input of* g*,*

"if g_1 *is satisfied if and only if* g *is not satisfied"*

$y_{g_1} + y_g - 1$

The formula f *is satisfied:*

$y_f - 1$

One can show by induction that if f is satisfiable then POLY(f) has a common root. By the contrapositive, if POLY(f) has no common roots, then f is unsatisfiable.

Lemma 57 *Let* f *be a Boolean formula in the variables* $x_1, \ldots, x_n$*. If* f *is satisfiable, then POLY*(f) *has a common* 0/1 *root.*

Proof: Let α be a 0/1 assignment to $x_1, \ldots, x_n$. For any propositional formula g, let $\alpha(g)$ denote the value of g under the assignment α.

Suppose that $\alpha(f) = 1$. We extend α to the variables of POLY(f) as follows: For each subformula g of f, let $\alpha(y_g) = \alpha(g)$. When $g = \bigvee g_i$ and

$\alpha(g) = 1$, let i_0 be the first input to g so that $\alpha(g_i) = 1$. Set $\alpha(z_{g_{i_0}}) = 1$ and for $i \neq i_0$, set $\alpha(z_{g_i}) = 0$. When $g = \bigvee g_i$ and $\alpha(g) = 0$, $\alpha(z_{g_i,g}) = 0$ for all i.

We now show by induction that α is a root of POLY(f). Clearly, for each variable x_i, α is a root of $y_{x_i} - x_i$. Consider a subformula $\neg g$. Because $\alpha(y_{\neg g}) = \alpha(\neg g)$ and $\alpha(y_g) = \alpha(g) = 1 - \alpha(\neg g)$, α is a root of $y_{\neg g} + y_g - 1$. Consider a subformula $g = \bigvee_i g_i$. If $\alpha(g) = 0$, then for all i, $\alpha(z_{g_i,g}) = 0$, $\alpha(y_{g_i}) = 0$ and $\alpha(y_g) = 0$. In this case, α is clearly a root to $z_{g_i,g}y_{g_i} - z_{g_i,g}$, $y_{g_i}z_{g_j,g}$ and $y_g - \sum_i z_{g_i,g}$. In the case when $\alpha(g) = 1$, there exists i_0 so that $\alpha(z_{g_{i_0},g}) = 1$ and for all $j \neq i_0$, $\alpha(z_{g_j,g}) = 0$. Moreover, $\alpha(y_{g_{i_0}}) = 1$, $\alpha(y_g) = 1$ and for all $j < i_0$, $\alpha(y_{g_j}) = 0$. Therefore, α is a root to $y_{g_j}z_{g_i,g}$ for all $i < j$, $z_{g_i,g}y_{g_i} - z_{g_i,g}$ for all i, and $y_g - \sum_i z_{g_i,g}$. Finally, α is a root of $y_f - 1$ because $\alpha(f) = 1$ by assumption. ∎

The argument of lemma 57 can be carried in Frege systems with depth $O(\text{depth}(f))$ and size $O(|f|)$.

Theorem 58 *If f is a formula in the variables $x_1, \ldots, x_n$ and the connectives $\{\bigvee, \neg\}$, then f is reducible to POLY(f) in depth $O(depth(f))$ and size polynomial in $|f|$.*

Proof: We proceed in two stages. First, we give a set of formulas, EXT(f), that is in the variables x_i, y_g and z_{g_1,g_2} and is analogous to the translation of f into polynomials. We show that this translation has a constant depth, polynomial size reduction to POLY(f) and then show that f has a depth $O(\text{depth}(f))$ reduction to EXT(f) of size polynomial in $|f|$.

Let EXT(f) be the following set of formulas:

For each variable x_i:

$y_{x_i} \leftrightarrow x_i$

For each subformula g whose top connective is $\bigvee$:

"if $g_1 < g_2$, $g_1 \rightarrow g$, $g_2 \rightarrow g$, and g_1 is satisfied ,

then g_2 is not the first satisfied input of g"

$\neg y_{g_1} \vee \neg z_{g_2,g}$

"if g_1 is the first satisfied input of g,

then g_1 is satisfied"

$z_{g_1,g} \rightarrow y_{g_1}$

"g is satisfied if and only if some input to g

is the first satisfied input of g

$y_g \leftrightarrow \bigvee_{g_1 \rightarrow g} z_{g_1,g}$

For each subformula g whose top connective is $\neg$:

Let g_1 the unique input of g,

"if g_1 is satisfied then g is not satisfied"

$y_{g_1} \leftrightarrow \neg y_g$

The formula f is satisfied:

y_f

There is a straightforward constant-depth, polynomial-size reduction of EXT(f) to POLY(f). For each polynomial of POLY(f), there is a formula of EXT(f) that reduces to the polynomial; the formula associated with each polynomial is given in table V.1. For the constant-size polynomials of POLY(f), the corresponding formula of EXT(f) implies that there is an m-partition on the satisfied variables of the polynomial. Because the polynomial involves a constant number of variables, the partition may be defined and proved correct in constant size, depth two.

Table V.1: Polynomials and their Associated Formulas

polynomial	associated formula
$y_{x_i} - x_i$	$y_{x_i} \leftrightarrow x_i$
$y_{g_1} z_{g_2,g}$	$\neg y_{g_1} \vee \neg z_{g_2,g}$
$z_{g_1,g} y_{g_1} - z_{g_1,g}$	$z_{g_1,g} \rightarrow y_{g_1}$
$y_{g_1} + y_g - 1$	$y_{g_1} \leftrightarrow \neg y_g$
$y_f - 1$	y_f

The only polynomials of POLY(f) that involve a non-constant number

of variables are those of the form $y_g - \sum_{g_1 \to g} z_{g_1,g}$, and from the hypotheses of EXT(f) it can be shown that y_g is satisfied if only if exactly one of the $z_{g_1,g}$'s is satisfied. Because there are $(m-1)$ copies of each $z_{g_1,g}$ in such a polynomial, we can group y_g with these copies of $z_{g_1,g}$ whenever $z_{g_1,g}$ is satisfied.

To reduce f to EXT(f), it is easy to check to that there is a polynomial size, depth $O(\text{depth}(f))$ derivation of the following substitution instance of EXT(f) from the hypothesis f. (The substitution instances of each formula are given in table V.2.)

$$\text{EXT}(f)[y_g \leftarrow g,\ z_{g_1,g} \leftarrow (g_1 \wedge \bigwedge_{\substack{g_2 < g_1 \\ g_2 \to g}} \neg g_2)]$$

Table V.2: Formulas and their Substitution Instances

formula	substitution instance	comment
$y_{x_i} \leftrightarrow x_i$	$x_i \leftrightarrow x_i$	
$\neg y_{g_1} \vee \neg z_{g_2,g}$	$\neg g_1 \vee \neg(g_2 \wedge \bigwedge_{\substack{g_3 < g_2 \\ g_3 \to g}} \neg g_3)$	$g_1 < g_2$
$z_{g_1,g} \to y_{g_1}$	$(g_1 \wedge \bigwedge_{\substack{g_2 < g_1 \\ g_2 \to g}} \neg g_2) \to g_1$	
$y_g \leftrightarrow \vee_{g_1 \to g} z_{g_1,g}$	$g \leftrightarrow \vee_{g_1 \to g}(g_1 \wedge \bigwedge_{\substack{g_2 < g_1 \\ g_2 \to g}} \neg g_2)$	$g = \vee_{g_1 \to g} g_1$
$y_{g_1} \leftrightarrow \neg y_g$	$g_1 \leftrightarrow \neg g$	$g = \neg g_1$
y_f	f	

■

Example: We illustrate our translation with a the clauses of the negated counting principles. The translation of this set of clauses turns out to be same (up to constant degree Nullstellensatz derivations) as the polynomial formulation of the counting principles previously studied.

Let V be a set of cardinality indivisible by m. The clauses are $F_v = \bigvee_{e \ni v} x_e$ for $v \in V$ and $G_{e,f} = \neg x_e \vee \neg x_f$ for $e, f \in [V]^m$ with $e \perp f$. The standard translation of these systems has the polynomials $\sum_{e \ni v} x_e$, for $v \in V$, and $x_e x_f$, for $e \perp f$.

The polynomials introduced by the translation of $G_{e,f}$ are: $y_{x_e} - x_e$, $y_{x_f} - x_f$, $y_{\neg x_e} + y_{x_e} - 1$, $y_{\neg x_f} + y_{x_f} - 1$, $y_{\neg x_e} z_{\neg x_f, G_{e,f}}$, $z_{\neg x_e, G_{e,f}} y_{\neg x_e} - z_{\neg x_e, G_{e,f}}$, $z_{\neg x_f, G_{e,f}} y_{\neg x_f} -$

$z_{\neg x_f, G_{e,f}}$, $y_{G_{e,f}} - z_{\neg x_e, G_{e,f}} - z_{\neg x_f, G_{e,f}}$ and $y_{G_{e,f}} - 1$. It is easy to check that thee is a constant degree derivation of $x_e x_f$ from these polynomials (in particular, a non-optimal but constant-degree derivation is given by the completeness of the Nullstellensatz system).

The polynomials introduced by the translation of F_v are: $y_{x_e} - x_e$, $z_{y_{x_e}, F_v} y_f$ (for $e, f \ni v$ and $e < f$), $z_{y_{x_e}, F_v} y_{x_e} - z_{y_{x_e}, F_v}$ (for $e \ni v$), $y_{F_v} - \sum_{e \ni v} z_{y_{x_e}, F_v}$ and $y_{F_v} - 1$. With a degree two Nullstellensatz derivation we may derive $\sum_{e \ni v} z_{e, F_v} x_e - 1$. Multiplying this by $\sum_{e \ni v} x_e$, and reducing using the previously derived polynomials $x_e x_f$ and the axioms $x_e^2 - x_e$, yields $\sum_{e \ni v} z_{e, F_v} x_e - \sum_{e \ni v} x_e$. Subtracting this from $\sum_{e \ni v} z_{e, F_v} x_e - 1$ yields $\sum_{e \ni v} x_e$.

A Note on Translations of Formulas to Polynomials Using Extension Variables

Definition V.D.3 *The* **induction principle of length M, IND(M),** *is the following system of polynomials:* y_1, $y_{r+1} y_r - y_{r+1}$ *(for* $r < M$*) and* $y_M - 1$.

Theorem 59 *[61, 60] The IND(M) system has Nullstellensatz refutations of degree* $O(\log M)$ *over any field. Moreover, over any field the system requires degree* $\Omega(\log M)$ *Nullstellensatz refutations.*

The "standard" translation of $x_n, \neg(((((x_n \vee x_{n-1}) \vee \cdots \vee x_1))))$ into polynomials using extension variables introduces new variables $z_1, \ldots, z_{n-1}$, with polynomials $x_n - 1$, $1 - (1 - x_n)(1 - x_{n-1}) - z_{n-1}$, $1 - (1 - z_{n-1})(1 - x_{n-2}) - z_{n-2}$, $\ldots$, $1 - (1 - z_2)(1 - x_1) - z_1$, and z_1. (The indices have been reversed from those of subsection V.D.1 to ease the reduction.)

We may define this set of polynomials from IND(n) using the following definitions: $x_i := y_i$ for i, $1 \leq i \leq n$, and $z_i := y_i$, for $i \leq n - 1$. The polynomials $z_1 = y_1$ and $x_n - 1 = y_n - 1$ are belong to IND(n), and for each r, $1 \leq r \leq n - 2$,

$$\begin{aligned} 1 - (1 - z_{r+1})(1 - x_r) - z_r &= 1 - (1 - y_{r+1})(1 - y_r) - y_r \\ = 1 - (1 + y_{r+1} y_r - y_r - y_{r+1}) - y_r &= -(y_{r+1} y_r - y_{r+1}) \end{aligned}$$

Similarly, $1-(1-x_n)(1-x_{n-1})-z_{n-1} = -(y_n y_{n-1} - y_n)$.

Because there is a constant degree reduction from IND(n) to the standard translation of $x_n, \neg(((((x_n \vee x_{n-1}) \vee \ldots x_1))))$ into polynomials, this translation requires super-constant degree to refute in the Nullstellensatz system.

V.E An Application to Unsatisfiable Systems of Constant-Width Linear Equations

Many tautologies studied in propositional proof complexity, such as Tseitin's tautologies [9] and the τ formulas of Nisan-Wigderson generators built from parity functions, can be expressed as inconsistent systems of linear equations over a field $\mathbb{Z}_q$ in which each equation involves only a small number of variables. We show that in such situations, constant-depth Frege with counting axioms modulo q can prove these principles with polynomial size proofs.

Fix a prime number q. Let A be an $m \times n$ matrix over $\mathbb{Z}_q$, let $x_1, \ldots, x_n$ be variables and let $\vec{b} \in \mathbb{Z}_q^m$ be so that $A\vec{x} = \vec{b}$ has no solutions. Let w be the maximum number of non-zero entries in any row of A.

For each $i \in [m]$, let A_i be the i'th row of A, and let p_i be the polynomial $A_i\vec{x} - b_i$. Let C_i the CNF that is satisfied if and only $p_i(\vec{x}) = 0$. Notice that C_i has size at most 2^w. The **explicit encoding of $\mathbf{A\vec{x} = \vec{b}}$** is the CNF $\bigwedge_{i=1}^m C_i$.

The methods of subsection V.D.1 show that $\bigwedge_{i=1}^m C_i$ is reducible to the system of polynomials $\{p_1, \ldots, p_m\}$ via a constant depth reduction of size $m2^{O(w)}$. Moreover, the system of polynomials $\{p_1, \ldots, p_m\}$ has a degree one Nullstellensatz refutation given by Gaussian elimination. Moreover, degree one refutations are of size $O(mn)$. Thus we have the following theorem:

Theorem 60 *Fix a prime number q. Let A be an $m \times n$ matrix, let $x_1, \ldots, x_n$ be variables and let $\vec{b} \in \mathbb{Z}_q^m$ be so that $A\vec{x} = \vec{b}$ has no solutions. Let w be the maximum number of non-zero entries in any row of A.*

There is a constant depth Frege with counting axioms modulo q refutation

of the explicit encoding of $A\vec{x} = \vec{b}$ *of size polynomial in m,n and* 2^w.

The Tseitin graph tautologies on an expander graph are known to require exponential size constant-depth Frege proofs [9]. Because these principles can be represented as an unsatisfiable system of linear equations, they have polynomial size constant-depth Frege with counting axioms proofs.

Corollary 61 *There exists a family of unsatisfiable sets of constant width clauses that require exponential size constant-depth Frege refutations, but have polynomial size constant-depth Frege with counting axioms refutations.*

V.F Acknowledgements

Much of the text of this chapter was previously published as part of [80] in the proceedings of the Twenty-ninth Annual Colloquium on Automata, Languages and Programming. I was the primary researcher and author of this publication which forms the basis for this chapter.

Chapter VI

Separation of Counting Gates and Counting Axioms

In this chapter, we demonstrate a family of unsatisfiable sets of clauses that have polynomial size refutations in constant-depth Frege systems with counting gates, but do not have polynomial size refutations in constant-depth Frege systems with counting axioms. The lower bound is proved by a combination of switching lemma and degree arguments. The analogous circuit result is proving a separation between circuits with modular gates and sums of AC^0 circuits. One can prove this circuit separation using a combination of random restrictions and degree arguments: Consider the OR of n modular sums, each on disjoint sets of n variables. Look at any sum of AC^0 functions that supposedly computes this function. A random restriction to the variables will, with high probability, reduce the above circuit to a sum of small decision trees, and hence, to a low degree polynomial. However, the function will with high probability still have one variable unset from each block of n, and so will still have degree n, that of the OR. Thus, the circuit cannot compute the function.

The sets of clauses for which we obtain the separation are analogous to the OR of sums in the preceding example. We replace the OR by a tautology that is easy for the polynomial calculus but hard for Nullstellensatz, the linear induction

principles: $S_1, S_r \rightarrow S_{r+1}, 1 \leq r \leq M-1, \neg S_M$. Linear induction tautologies are known to have constant degree, polynomial size proofs in the polynomial calculus and to require logarithmic degree to proof in Nullstellensatz [61, 60].

Of course, constant-depth Frege systems have linear size proofs of the linear induction tautologies, so we must obfuscate the S_r's so that they are not definable by constant-depth formulas. Consider the case of sums modulo two. We replace each S_r by the parity of disjoint sets of N variables, $\{x_{r,i} \mid 1 \leq i \leq N\}$. S_r is true if and only if an even number of the $x_{r,i}$'s are satisfied. We wish to use the fact that it is difficult with AC^0 formulas to compute S_r from $x_{r,i}$. A delicate point is to express the constraints $S_r \rightarrow S_{r+1}$ without making S_r definable as a constant-depth formula; the standard use of intermediate variables allows such a definition. Instead, we think of $S_r \rightarrow S_{r+1}$ as the following equation modulo two: $\sum_i x_{r,i} = S_i = S_i S_{i+1} = \sum_i \sum_j x_{r,i} x_{r+1,j}$. This can be expressed using auxiliary variables representing a perfect matching on the satisfied monomials of $\sum_{i,j} x_{r,i} x_{r+1,j}$ and $\sum_j x_{r,j}$. We call these sets of clauses the "induction on sums principles".

In the polynomial calculus (and hence in constant-depth Frege systems with counting gates) we can define each S_r from $x_{r,i}$, prove the implications using the matchings, and then apply the proof for the induction principles to the S_r's.

The overall structure of the lower bound proof is analogous to our circuit bound sketch, and very similar to that of other lower bounds for constant-depth Frege with counting axioms (c.f. [59]). First, given an alleged polynomial-size constant depth Frege proof with counting axioms, we construct a interpretation of the subformulas of the proof so that each formula is associated with a small depth decision tree. This is constructed using the iterated application of a switching lemma. Next, the short decision trees of the interpretation are used to create a low-degree Nullstellensatz refutation of the algebraic translation of our tautology. Finally, we prove a degree lower bound for the algebraic system by giving a constant degree reduction of the linear induction tautologies to our tautologies and appealing to

the known degree lower bounds for Nullstellensatz refutations of linear induction [61, 60].

The technical novelty and difficulty of this separation is in the switching lemma. In the process of collapsing formulas to short decision trees, the proofs of [50, 51, 59] apply random 0/1 partial assignments to the variables that reduce the tautologies to smaller tautologies of the same family. For the induction on sums principles, no 0/1 partial assignment that does not set every variable in each row can collapse a DNF into a short decision tree with high probability. For this reason, we simplify the tautologies by not only setting many variables to 0s and 1s, but also substituting one variable for another.

VI..1 Outline of the Chapter

In section VI.A, we define the sets of clauses (the induction on sums principles) that provide the separation. Section VI.B shows that these principles have small polynomial calculus refutations.

The principle tasks of this chapter are the proof of the switching lemma and its use to construct a shallow interpretation for the formulas in the proof. Section VI.C introduces a modification of the induction on sums principles that is needed for the proof of the switching lemma. Sections VI.D and VI.E describe the basics of restrictions and decision trees. Because our switching lemma applies random substitutions, not just random 0/1 restrictions, we need to define a method for applying such substitutions to decision trees. We call this process simplification, and we show how to simplify decision trees in section VI.F.

The switching lemma, theorem 79, is proved in section VI.G. Finally, the switching lemma is used to construct a shallow interpretation of the formulas in the proof (called a "k-evaluation") in section VI.H.

Section VI.I uses the k-evaluation to construct a low-degree Nullstellensatz refutation of the algebraic induction on sums principles. Section VI.J uses a reduction from the linear induction principles to prove a degree lower bound for

the algebraic induction on sums principles.

Section VI.K puts everything together to prove the lower bound. Finally, in section VI.L, we apply the simulation of chapter V to obtain quasi-polynomial size refutations of the induction on sums principles modulo m using constant-depth Frege systems with counting axioms modulo m.

Convention: Throughout this chapter m denotes a fixed integer modulus with $m \geq 2$.

VI.A The Induction on Sums Principles

Suppose that we have M rows of N Boolean variables. There is no assignment to these variables so that the modular sum of the first row is 0, the sum of the final row is 1, and for each non-final row r, if the sum of row r is zero, then the sum of row $r+1$ is also zero. This is the idea behind the unsatisfiable sets of clauses we call the **induction on sums principles**.

Let M and N be positive integers. Let $R_1, \ldots, R_M$ be disjoint sets of N elements, for each $i \in \bigcup_{r=1}^{M} R_i$ we have a Boolean variable X_i. The variables $\{X_i \mid i \in R_r\}$ are identified as the "the r'th row of Boolean variables". Because constant depth circuits require exponential size to compute modular sums, it takes some care to represent the principles as an unsatisfiable set of clauses. It is helpful to view the constraints as a system of $M+1$ many quadratic equations modulo m.

Equation 0:	$\sum_{i \in R_1} X_i = 0$
Equation r, for $1 \leq r < M$:	$(\sum_{i \in R_r} X_i)(\sum_{j \in R_{r+1}} X_j) - \sum_{j \in R_{r+1}} X_j = 0$
Equation M:	$\sum_{i \in R_M} X_i - 1 = 0$

To give a set of propositional clauses which are satisfied only when these equations are satisfied, we add extension variables and constraints expressing "in each equation, the number of satisfied monomials satisfied is 0 modulo m." For shorthand, we define *multi-sets* U_r corresponding to the monomials in equation r. $U_0 = \{\{i\} \mid i \in R_1\}$, for $r \in \{1, \ldots, M-1\}$, $U_r = \{\{i,j\} \mid i \in R_r,\ j \in$

$R_{r+1}\} \cup (m-1) \times \{\{j\} \mid j \in R_{r+1}\}$, and $U_M = \{\{i\} \mid i \in R_M\} \cup (m-1) \times \{\emptyset\}$. (The notation $(m-1) \times S$ denotes the multi-set with $m-1$ copies of each element from S.)

For each equation, we add a set of "partitioning variables", Y_e for $e \in [U_i]^m$. The induction on sums principles state that for each equation, these variables define a two-partition on the satisfied monomials.

Because the particular index sets play no role except for their sizes, we refer to all such principles as the **M by N induction on sums principle**.

Definition VI.A.1 *Let M and N be positive integers, and let $R_1, \ldots, R_M$ and $U_0, \ldots, U_m$ be given as in the preceding paragraphs. The* **M by N induction on sums principle, IS(M, N)**, *is the following set of clauses:*

For each r, $0 \leq r \leq M$,

for each $I \in U_r$,	$\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$
for each $I \in U_r$, $e \in [U_r]^m$, $i \in I$,	$\neg Y_e \vee X_i$
for each $e, f \in [U_r]^m$, $e \perp f$,	$\neg Y_e \vee \neg Y_f$

We will also need to treat this set of a clauses as a set of polynomials. Let $\mathbf{AIS_m(M, N)}$ *denote the following set of polynomials:*

For each r, $0 \leq r \leq M$,

for each $I \in U_r$,	$\prod_{i \in I} X_i \left(\sum_{e \ni I} Y_e - 1\right)$
for each $I \in U_r$, $e \in [U_r]^m$, $i \in I$,	$Y_e(X_i - 1)$
for each $e, f \in [U_r]^m$, $e \perp f$,	$Y_e Y_f$

VI.B An Upper Bound for the Polynomial Calculus

Theorem 62 *The $AIS_m(M, N)$ system of polynomials has a degree 3, size $O(MN^3)$ polynomial calculus refutation.*

Proof: The polynomial calculus refutation proceeds as follows. First, we use the axioms to derive polynomials stating that the number of monomials satisfied in each equation is zero modulo m. Then we iteratively derive $\sum_{i \in R_r} X_i$ for each row r. After $\sum_{i \in R_M} X_i$ is derived, we subtract the initial polynomial $\sum_{i \in R_M} X_i - 1$ from it to derive 1.

For each r and each $I \in U_r$, $e \in [U_r]^m$ with $e \ni I$, let $q_{I,e} = Y_e \prod_{i \in I} X_i - Y_e$. When $|I| = 1$, $q_{I,e} = X_i Y_e - Y_e$ belongs to $\mathrm{AIS}_m(M, N)$, and when $I = \{i, j\}$, there is a degree 3 derivation of $q_{I,e}$ from $\mathrm{AIS}_m(M, N)$:

$$X_i(X_j Y_e - Y_e) + X_i Y_e - Y_e \;=\; X_i X_j Y_e - Y_e \;=\; q_{I,e}$$

For each r and each $I \in U_r$, let $p_I = \sum_{e \ni I} Y_e - \prod_{i \in I} X_i$. These polynomials have degree ≤ 3 derivations from $\mathrm{AIS}_m(M, N)$ and the $q_{I,e}$'s:

$$\begin{aligned} \left(\prod_{i \in I} X_i\right)\left(\sum_{e \ni I} Y_e - 1\right) - \sum_{e \ni I} q_{I,e} &= \sum_{e \ni I} \left(Y_e \prod_{i \in I} X_i - q_{I,e}\right) - \prod_{i \in I} X_i \\ &= \sum_{e \ni I} Y_e - \prod_{i \in I} X_i = p_I \end{aligned}$$

For each equation r, $0 \leq r \leq M$, when we negate the sum of all monomials, we discover that the sum of the satisfied monomials is zero modulo m. The final identity $\sum_{I \in U_r} \sum_{e \ni I} Y_e = 0$ is true because each variable Y_e appears exactly m times in the sum.

$$\begin{aligned} -\sum_{I \in U_r} p_I &= \sum_{I \in U_r} \left(\prod_{i \in I} X_i - \sum_{e \ni I} Y_e\right) \\ &= \sum_{I \in U_r} \prod_{i \in I} X_i - \sum_{I \in U_r} \sum_{e \ni I} Y_e \\ &= \sum_{I \in U_r} \prod_{i \in I} X_i \end{aligned}$$

We now iteratively derive $\sum_{i \in R_r} X_i$ for each r, $1 \leq r \leq M$. Because $U_0 = \{\{i\} \mid i \in R_1\}$, $\sum_{I \in U_0} \prod_{i \in I} X_i = \sum_{i \in R_1} X_i$. To derive $\sum_{j \in R_{r+1}} X_j$ from $\sum_{i \in R_r} X_i$, for $r < M$, we combine the initial polynomial $\sum_{I \in U_r} \prod_{i \in I} X_i$ with $\sum_{i \in R_r} X_i$ as follows:

$$\begin{aligned} &-\sum_{I \in U_r} \prod_{i \in I} X_i + \left(\sum_{j \in R_{r+1}} X_j\right)\left(\sum_{i \in R_r} X_i\right) \\ &= -\sum_{i \in R_r} \sum_{j \in R_{r+1}} X_i X_j - (m-1) \sum_{j \in R_{r+1}} X_j + \sum_{i \in R_r} \sum_{j \in R_{r+1}} X_i X_j \\ &= \sum_{j \in R_{r+1}} X_j \end{aligned}$$

Finally, notice that $\sum_{I \in U_M} \prod_{i \in I} X_i = \sum_{i \in R_M} X_i - 1$. We subtract this from $\sum_{i \in R_M} X_i$ to obtain 1.

■

Corollary 63 *The set of clauses $IS_m(M, N)$ has a polynomial size constant-depth Frege with counting gates modulo m refutation.*

VI.C Modified Induction on Sums Principles

To prove the size lower bounds for constant-depth Frege with counting axioms proofs of the induction on sums principles, we will not work directly with the induction on sums principles but with a variant more amenable to our proof method. There are two difficulties that make the induction on sums principles unwieldy. First, a restriction of the $\mathrm{IS}_m(M, N)$ principle usually does not yield an instance of some other $\mathrm{IS}_m(M', N')$. This kind of closure simplifies matters when working with decision trees. The second, and more substantial, difficulty is encountered in the proof of the switching lemma.

The modification restricts the partition variables, Y_e, so that each e can contain at most one monomial. This is done by adding a set of "extra-points" whose size is divisible by m, and placing an m-partition on the satisfied monomials and the extra points *with the restriction that each edge used contains at most one monomial.* Such a partition would imply that the equation is 0 modulo m because each satisfied monomial be grouped with $m - 1$ of extra points, and the total number of extra points is 0 modulo m.

Definition VI.C.1 *Fix a positive integer M. Let $R_1, \ldots, R_M$ be disjoint sets of size N. Let $U_0 = \{\{i\} \mid i \in R_1\}$, for $r \in \{1, \ldots, M-1\}$, let $U_r = \{\{i, j\} \mid i \in R_r,\ j \in R_{r+1}\} \cup (m-1) \times \{\{j\} \mid j \in R_{r+1}\}$, and let $U_M = \{\{i\} \mid i \in R_M\} \cup (m-1) \times \{\emptyset\}$. For each r, and let V_r be a set of distinct points so that $|V_r| = m|U_r|$. For each r, let $E_r = \{e \in [U_r \cup V_r]^m \mid |e \cap U_r| \leq 1\}$.*

For each $i \in \bigcup_{r=1}^{M} R_r$*, there is a propositional variable* X_i*, and for each* $e \in \bigcup_{r=0}^{M} E_r$*, there is a propositional variable* Y_e*.*

The **M by N modified induction on sums principle**, $\mathbf{MIS_m(M, N)}$, *is:*

For each r, $0 \leq r \leq M$,

for each $I \in U_r$,	$\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$
for each e *with* $I \in e$ *and* $i \in I$,	$\neg Y_e \vee X_i$
for each $p \in V_r$,	$\bigvee_{e \ni p} Y_e$
for each $e \perp f$,	$\neg Y_e \vee \neg Y_f$

To ease our constructions of decision trees and k-evaluations, we generalize the definition so that a restriction of MIS_m is also an instance of MIS_m on a different index set. When a variable X_i is set to false, it is removed from its row, however, when a variable X_i is set to true, it must later be covered with a matching variable Y_e. For this reason, the modified principles include rows of satisfied variables that must be matched. Furthermore, when a matching variable Y_e is satisfied, we remove one satisfied monomial and $m-1$ extra points from consideration. Therefore, setting a variable Y_e maintains the invariant that the number of extra points is congruent modulo m to the number of satisfied monomials that have been matched. The modified principles need a substantial amount of bookkeeping to describe their index sets. The family of index sets describing an instance of a modified induction on sums principle is called a **universe**.

Definition VI.C.2 *Fix a positive integer* M*. Let* $R_1, \ldots, R_M, S_1, \ldots S_M$ *be disjoint sets. Let* $R = \bigcup_{r=1}^{M} R_r$*, and let* $S = \bigcup_{r=1}^{M} S_r$*. Let* $\mathcal{M}_0 = \{\{i\} \mid i \in R_1 \cup S_1\}$*, for* $r \in \{1, \ldots, M-1\}$*, let* $\mathcal{M}_r = \{\{i, j\} \mid i \in R_r \cup S_r,\ j \in R_{r+1} \cup S_{r+1}\} \cup (m-1) \times \{\{j\} \mid j \in R_{r+1} \cup S_{r+1}\}$*, and let* $\mathcal{M}_M = \{\{i\} \mid i \in R_M \cup S_M\} \cup (m-1) \times \{\emptyset\}$*. For each* r*, let* U_r *be a subset of* $\mathcal{M}_r$ *so that* $(I \in \mathcal{M}_r \backslash U_r) \rightarrow I \subseteq S$ *(i.e., the monomials not in* U_r *have been satisfied). For each* r*, and let* V_r *be a set of distinct points so*

that $|V_r| \equiv_m |\mathcal{M}_r \setminus U_r|$. *The tuple* $(R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *is called a* **universe**.

It is helpful to think of the monomials $I \in \mathcal{M}_r \setminus U_r$ as the satisfied monomials that have been covered by some matching variable Y_e with $I \in e$.

Definition VI.C.3 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *be a universe. For each* $i \in R$, *let there be a propositional variable* X_i, *and for each* $e \in \bigcup_{r=0}^{M} E_r$, *let there be a propositional variable* Y_e. *The* **modified induction on sums principle for** $\mathcal{U}$, $\mathbf{MIS_m}(\mathcal{U})$, *is the following set of clauses:*

For each r, $0 \leq r \leq M$,

for each $I \in U_r$,	$\bigvee_{i \in I \cap R} \neg X_i \vee \bigvee_{e \ni I} Y_e$
for each e, $I \in e \cap U_r$, $i \in I \cap R$,	$\neg Y_e \vee X_i$
for each $p \in V_r$,	$\bigvee_{e \ni p} Y_e$
for each $e \perp f$,	$\neg Y_e \vee \neg Y_f$

Let $\mathbf{AMIS_m}(\mathcal{U})$ *denote the following set of polynomials*

For each r, $0 \leq r \leq M$,

For each $I \in U_r$,	$\prod_{i \in I \cap R} X_i \left(\sum_{e \ni I} Y_e - 1\right)$
for each e, $I \in e \cap U_r$, $i \in I \cap R$,	$Y_e(1 - X_i)$
For $p \in V_r$,	$\sum_{e \ni p} Y_e - 1$
For each $e \perp f$,	$Y_e Y_f$

The $\mathrm{MIS}_m(M, N)$ principles are an instance of the $\mathrm{MIS}_m(\mathcal{U})$ principles with an appropriate choice of universe; such a universe is called an (M, N) universe.

Definition VI.C.4 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *be a universe. We say that* $\mathcal{U}$ *is an* (M, N) *universe if for each* r, $1 \leq r \leq M$, $S_r = \emptyset$, $U_0 = \{\{i\} \mid i \in R_1\}$, $|V_0| = m|U_0|$, *for* $r \in \{1, \ldots, M-1\}$, *let* $U_r = \{\{i, j\} \mid i \in$

$R_r,\ j \in R_{r+1}\} \cup (m-1) \times \{\{j\} \mid j \in R_{r+1}\}$, $|V_r| = m|U_r|$, $U_M = \{\{i\} \mid i \in R_M\} \cup (m-1) \times \{\emptyset\}$, *and* $|V_M| = m|U_M|$. *Because the sets* $S_1, \ldots, S_M$ *are empty, we will often write* (M, N) *universes as* $(R_1, \ldots, R_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$.

Definition VI.C.5 *Let* M *and* N *be positive integers.* $AIS_{\mathbf{m}}(\mathbf{M}, \mathbf{N})$ *denotes any system of polynomials* $AIS_m(\mathcal{U})$ *where* $\mathcal{U}$ *is an* (M, N) *universe.*

Definition VI.C.6 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *be a universe. The* **length of** $\mathcal{U}$, $\mathbf{l}(\mathcal{U})$, *is* M *and the* **width of** $\mathcal{U}$, $\mathbf{w}(\mathcal{U})$, *is defined as follows:*

$$w(\mathcal{U}) = \min\left(\{|R_r| \mid 1 \leq r \leq M\} \cup \{\lfloor V_r/m \rfloor \mid 0 \leq r \leq M\}\right)$$

VI.C.1 Reducing IS_m to MIS_m

We prove size lower bounds for refutations of the $\mathrm{MIS}_m(M, N)$ principles, and these lower bounds imply size lower bounds refutations for $\mathrm{IS}_m(M, N)$ as well.

Theorem 64 *There exists a substitution* Σ *so that for each clause* $H \in IS_m(M, (m+1)N + m(m-1))$, *either* $\Sigma(H) = 1$, $\Sigma(H) = X \vee \neg X$, *or* $\Sigma(H) \in MIS_m(M, N)$.

Proof: The idea is straightforward; in each row we will set $mN + m(m-1)$ of the variables to 1 and treat the newly created satisfied monomials as the extra points. Of course, this substitution results in a few too many extra points and there is the issue of what to do with monomials that have one variable set and the other unset. These issues are easily worked out.

Let $Q_1, \ldots, Q_M$ be index sets of size $(m+1)N + m(m-1)$ and let $T_0, \ldots, T_m$ be the sets of monomials for $\mathrm{IS}_m(M, (m+1)N + m(m-1))$. Partition each Q_r into two sets, R_r and S_r with $|R_r| = N$ and $|S_r| = mN + m(m-1)$. For each r, $1 \leq r \leq M-1$, $i \in R_r$, let $H^1_{r,i} = \{\{i, j\} \in T_r \mid j \in S_{r+1}\}$. Let $\mathcal{P}^1_{r,i}$ be an m-partition of $H^1_{r,i}$. For each $j \in R_{r+1}$, let $H^2_{r,j} = \{\{i, j\} \in T_r \mid i \in S_r\}$, and let

$\mathcal{P}^2_{r,j}$ be an m-partition of $H^2_{r,j}$. For $r,\ 0 \leq r \leq M$, let $U_r = \{I \in T_r \mid I \subseteq \bigcup_r R_r\}$, and let $V_r = \{I \in T_r \mid I \subseteq \bigcup_r S_r\}$. Set $E_r = \{e \in [U_r \cup V_r]^m \mid |e \cap U_r| \leq 1\}$. Let $\mathcal{U}$ be the universe $(R_1, \ldots, R_M, \emptyset, \ldots, \emptyset, U_0, \ldots, U_M, V_0, \ldots, V_M)$; this is not an (M, N) universe, but it is close and we will deal with it at the end.

Let Σ be the following substitution:

$$\Sigma(X_i) = \begin{cases} 1 & \text{if } i \in S_r \\ X_i & \text{if } i \in R_r \end{cases} \qquad \Sigma(Y_e) = \begin{cases} Y_e & \text{if } e \in [U_r \cup V_r]^m \text{ and } |e \cap U_r| \leq 1 \\ X_i & \text{if } e \in \mathcal{P}^1_{r,i} \\ X_j & \text{if } e \in \mathcal{P}^2_{r,j} \\ 0 & \text{otherwise} \end{cases}$$

Consider an axiom of the form $\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$, with $I \in T_r$.

Consider the case when $I \subseteq S$. In this case, $I \in V_r$. For each $i \in I$, $\Sigma(X_i) = 1$ and for each $e \ni I$, $\Sigma(Y_e) = Y_e$ if $e \in E_r$ and $\Sigma(Y_e) = 0$ otherwise. Therefore, $\Sigma(\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e) = \bigvee_{\substack{e \in E_r \\ e \ni I}} Y_e$.

Consider the case when $I \subseteq R$. In this case, $I \in U_r$. For each $i \in I$, $\Sigma(X_i) = X_i$ and for each $e \ni I$, $\Sigma(Y_e) = Y_e$ if $e \in E_r$, and otherwise $\Sigma(Y_e) = 0$. Therefore, $\Sigma(\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e) = \bigvee_{i \in I} \neg X_i \vee \bigvee_{\substack{e \in E_r \\ e \ni I}} Y_e$.

If $I = \{i, j\}$ with $i \in R_r$ and $j \in S_{r+1}$, then $\Sigma(X_i) = X_i$ and there is exactly one $e \in [T_r]^m$ so that $\Sigma(Y_e) = X_i$, for all other e, $\Sigma(Y_e) = 0$. Therefore, Therefore, $\Sigma(\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e) = \neg X_i \vee X_i$. The case for $I = \{i, j\}$ with $i \in S_r$ and $j \in S_{r+1}$ is handled similarly.

For each axiom $\neg Y_e \vee \neg Y_f$ with $e, f \in [U_r]^m,\ e \perp f$, a similar case analysis shows that $\Sigma(\neg Y_e \vee \neg Y_f) = 1$ or $\Sigma(\neg Y_e \vee \neg Y_f) \in \mathrm{MIS}_m(\mathcal{U})$.

The only issue remaining is that $\mathcal{U}$ is not an (M, N) universe. Notice that $|U_0| = N$, $|V_0| = mN + m(m-1)$, $|U_M| = N + m - 1$, $|V_M| = mN + m(m-1)$, and for $1 \leq r \leq M - 1$, $|U_r| = (m-1)N + N^2$ and $|V_r| = (m-1)(mN + m(m-1)) + (mN + m(m-1))^2$. For $r < M$, we group together some of the points of V_r by setting some Y_e's to 1 and obtain $V'_r \subseteq V_r$ with $|V'_r| = m|U_r|$.

■

Corollary 65 *If there is a size s, depth d refutation of $IS_m(M,(m+1)N+m(m-1))$ then there is a size s, depth d refutation of $MIS(M,N)$.*

VI.D Restrictions and Partial Assignments

We say that two literals are *inconsistent* if their conjunction implies the negation of some clause of $\mathrm{MIS}_m(\mathcal{U})$.

Definition VI.D.1 *Let $\mathcal{U}$ be a universe. The following pairs of literals in $Vars(\mathcal{U})$ are* **inconsistent***: $\neg X_i$ and Y_e, when $i \in I$ and $I \in e$, X_i and $\neg X_i$, Y_e and Y_f, when $e \perp f$, and Y_e and $\neg Y_e$. For a set of literals S, if there exist $l_1, l_2 \in S$ so that l_1 and l_2 are inconsistent, then S is said to be inconsistent.*

Definition VI.D.2 *Let $\mathcal{U}$ be a universe. Let S be a consistent set of literals from $Vars(\mathcal{U})$. For a formula F, the restriction of F by S, $F \restriction_S$, is defined in the usual way, replacing a literal l by 1 if $l \in S$ and replacing l by 0 if some $l' \in S$ is inconsistent with l. Compound expressions are simplified when explicitly satisfied or falsified.*

Definition VI.D.3 *Let $\mathcal{U}$ be a universe. Let B be a set of literals in $Vars(\mathcal{U})$. We say that B is* **closed** *if for every $Y_e \in B$, we have that for every $I \in e \cap U_r$, $i \in I$, $X_i \in B$.*

Here is an easy lemma we give without proof.

Lemma 66 *Let $\mathcal{U}$ be a universe, and let S, T, V be subsets of $Vars(\mathcal{U})$.*

1. $(S \restriction_T) \restriction_V = S \restriction_{(T \cup V)}$
2. *If S and T are consistent and S is closed then $S \cup T = S \cup (T \restriction_S)$.*

The motivation for the more complicated formulation of MIS_m with the universes is that we want the restriction of an MIS_m principle to be another instance of an MIS_m principle. In actuality, we only need this hold for restrictions that do not negate an edge variable.

Definition VI.D.4 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *be a universe. Let* $i \in \bigcup_{r=1}^{M} R_r$ *be given, and let* $e \in \bigcup_{r=0}^{M}$, *so that if there is* $I \in e \cap U_r$ *for some* r, *then* $I \subseteq S_r \cup S_{r+1}$.

1. *The* **restriction of** $\mathcal{U}$ **by** $\mathbf{X_i}$, $\mathcal{U} \restriction_{\mathbf{X_i}}$, *is defined as follows: for* $1 \leq r \leq M$, $i \notin R_r$, *let* $R'_r = R_r$, *and* $S'_r = S_r$, *for the* r *so that* $i \in R_r$, *let* $R'_r = R_r \setminus \{i\}$ *and* $S'_r = S_r \cup \{i\}$.

$$\mathcal{U} \restriction_{X_i} = (R'_1, \ldots, R'_M, S'_1, \ldots, S'_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$$

2. *The* **restriction of** $\mathcal{U}$ **by** $\neg\mathbf{X_i}$, $\mathcal{U} \restriction_{\neg\mathbf{X_i}}$, *is defined as follows: for* $1 \leq r \leq M$, $i \notin R_r$, *let* $R'_r = R_r$, *and* $S'_r = S_r$, *for the* r *so that* $i \in R_r$, *let* $R'_r = R_r \setminus \{i\}$ *and* $S_r = S_r$. *For* r, $0 \leq r \leq M$, *let* $U'_r = U_r \setminus \{I \in U_r \mid i \in I\}$.

$$\mathcal{U} \restriction_{\neg X_i} = (R'_1, \ldots, R'_M, S_1, \ldots, S_M, U'_0, \ldots, U'_M, V_0, \ldots, V_M)$$

3. *The* **restriction of** $\mathcal{U}$ **by** $\mathbf{Y_e}$, $\mathcal{U} \restriction_{\mathbf{Y_e}}$, *is defined as follows: For* r, $0 \leq r \leq M$, *so that* $e \notin E_r$, *let* $U'_r = U_r$ *and* $V'_r = V_r$, *for the* r *so that* $e \in E_r$, *let* $V'_r = V_r \setminus e$ *and let* $U'_r = U_r \setminus e$.

$$\mathcal{U} \restriction_{Y_e} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U'_0, \ldots, U'_M, V'_0, \ldots, V'_M)$$

Let π *be a consistent,* closed *set of literals containing only positive instances of* Y_e *variables. The* **restriction of** $\mathcal{U}$ **by** π, $\mathcal{U} \restriction_{\pi}$ *is defined by iteratively restricting by* $X_i \in \pi$, $\neg X_i \in \pi$, *and finally by* $Y_e \in \pi$.

Lemma 67 *Let* $\mathcal{U}$ *be a universe, and let* π *be a consistent, closed set of literals containing only positive instances of* Y_e *variables.* $MIS_m(\mathcal{U}) \restriction_{\pi} = MIS_m(\mathcal{U} \restriction_{\pi})$.

Lemma 68 *Let* $\mathcal{U}$ *be a universe, and let* π *be a consistent, closed set of literals containing only positive instances of* Y_e *variables.* $l(\mathcal{U} \restriction_{\pi}) = l(\mathcal{U})$ *and* $w(\mathcal{U} \restriction_{\pi}) \geq w(\mathcal{U}) - |\pi|$.

VI.E Decision Trees

The decision trees used for constructing our k-evaluation do not represent Boolean functions in the sense of definition III.A.1. A trees does not represent its function over all assignments to the variables, rather, only over assignments that are locally consistent with respect to the $\mathrm{MIS}_m(\mathcal{U})$ principles.

At each internal node of a decision tree, a query is made either of an underlying variable X_i, asking whether the variable is true, or to a monomial in U_r, asking "Is this monomial satisfied, and if so, what partition edge covers this monomial? Or, is the monomial not satisfied?", or to an extra point in V_r, asking "What partition edge covers the extra point?" The arcs leaving an internal node are labeled with answers to these queries. Moreover, the answers possible at a node are exactly those answers consistent with the answers labeling the branch to that node.

Notation: When X is a propositional variable, let $\mathbf{X^1}$ denote X and let $\mathbf{X^{-1}}$ denote $\neg X$.

Definition VI.E.1 *Let $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, V_0, \ldots, V_M)$ be a universe. The* **queries of $\mathcal{U}$**, *$Q(\mathcal{U})$, are* **value queries**, **Value(I)**, *for each $I \in \bigcup_{r=0}^{M} V_r$,* **extra point matching queries**, *Match(**p**), for each $r \in \{0, \ldots M\}$ and $p \in V_r$,* **monomial matching queries**, *Match(**I**), for each $r \in \{0, \ldots M\}$ and $I \in U_r$.*

Associated with each query is a set of answers. An answer is a closed set of literals telling what happens to a point or monomial. Answers appear as labels for branches in decision trees.

Definition VI.E.2 *Let $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, V_0, \ldots, V_M)$ be a universe. Let $R = \bigcup_{r=1}^{M} R_r$. Let Q a be query of $\mathcal{U}$. The* **answer to Q in $\mathcal{U}$**, *$\mathcal{ANS}^{\mathcal{U}}(\mathbf{Q})$, is defined as follows:*

1. *For $i \in \bigcup_{r=1}^{M} R_r$,* $\qquad \mathcal{ANS}^{\mathcal{U}}(\mathit{Value}(\{i\})) = \{\{X_i\}, \{\neg X_i\}\}$

2. *For* $I \in U_r$, $0 \leq r \leq M$,

$$\begin{aligned}\mathcal{ANS}^{\mathcal{U}}(Match(I)) &= \{\{X_i^{\epsilon_i} \mid i \in I \cap R\} \mid \epsilon \in \{-1,1\}^{I \cap R},\ \exists j\ \epsilon_j = -1\} \\ &\quad \cup \{\{Y_e\} \cup \{X_k \mid k \in I \cap R\} \mid e \in E_r,\ I \in e\}\end{aligned}$$

3. *For* $p \in V_r$, $0 \leq r \leq M$,

$$\mathcal{ANS}^{\mathcal{U}}(Match(p)) = \{\{Y_e\} \cup \{X_k \mid k \in I \cap R,\ I \in e \cap U_r\} \mid e \in E_r,\ p \in e\}$$

Definition VI.E.3 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, V_0, \ldots, V_M)$ *be a universe.* **BLits**$(\mathcal{U})$ *is the set containing exactly the following literals:* X_i*, for each* $i \in \bigcup_{r=1}^{M} R_r$, $\neg X_i$*, for each* $i \in \bigcup_{r=1}^{M} R_r$*, and* Y_e*, for each* $0 \leq r \leq M,\ e \in E_r$.

Lemma 69 *Let* $\mathcal{U}$ *be a universe and let* Q *be a query. If* π *is a consistent, closed subset of BLits*$(\mathcal{U})$ *so that* $|\pi| < w(\mathcal{U})$ *then there exists* $L \in \mathcal{ANS}^{\mathcal{U}}(Q)$ *so that* L *is consistent with* π.

Lemma 70 *Let* $\mathcal{U}$ *be a universe and* Q *be a query. If* π *is consistent, closed subset of BLits*$(\mathcal{U})$ *then* $\mathcal{ANS}^{\mathcal{U}\restriction_\pi}(Q) = \{A \restriction_\pi \mid A \in \mathcal{ANS}^{\mathcal{U}}(Q),\ A \restriction_\pi \neq 0\}$.

Definition VI.E.4 *Let* $\mathcal{U}$ *be a universe. Fix a set of values,* V. *A* **decision tree (over** $\mathcal{U}$**)** *is a rooted tree* T *that satisfies the following recursive definition:* T *can be a single node, labeled with a value from* V. *If* T *has height* > 0*, then the root is labeled with a query* $Q \in \mathcal{Q}(\mathcal{U})$. *For each* $L \in \mathcal{ANS}^{\mathcal{U}}(Q)$*, there is an arc labeled* L*, underneath which is a decision tree over* $\mathcal{U} \restriction_L$. *The* **height** *of a decision tree is its height as a tree.*

Definition VI.E.5 *Let* $\mathcal{U}$ *be a universe and let* k *be a positive integer.* $\mathcal{T}(\mathcal{U}, k)$ *is the set of decision trees in* $\mathcal{U}$ *of height* $\leq k$.

Definition VI.E.6 *Let T be a decision tree. For each path p in T from the root to a leaf, let B_p be the partial assignment obtained by taking the union of the edge labels along p.*

Because the distinct answers for any query are mutually inconsistent, the mapping $p \mapsto B_p$ is injective.

Definition VI.E.7 *Let T be a decision tree.* $\mathbf{Br(T)}$ *is defined as*

$$Br(\mathbf{T}) = \{B_p \mid \ p \text{ is a path in } T \text{ from the root to a leaf } \}$$

For each $v \in V$,

$$Br_{\mathbf{v}}(\mathbf{T}) = \{B_p \mid \ p \text{ is a path in } T \text{ from the root to a leaf with label } v \ \}$$

In particular, if T is a single node labeled with v, then $\mathrm{Br}_v(T) = \{1\}$, and for all $w \in V \setminus \{v\}$, $\mathrm{Br}_w(T) = \emptyset$.

We will often view $\mathrm{Br}(T)$ as a set of terms, with each branch corresponding to the conjunction of the literals it contains. Using this interpretation, $\bigvee \mathrm{Br}_v(T)$ is the disjunction of all branches that lead to a leaf labeled v, and for a collection of trees T_i, $i \in I$, $\bigvee_{i \in I} \mathrm{Br}_v(T_i)$ denotes the disjunction of branches that lead to a leaf labeled v in some tree T_i.

Definition VI.E.8 *Let F be a DNF in $Vars(\mathcal{U})$. Let T be a decision tree over $\mathcal{U}$. We say that* $\mathbf{T}$ **strongly represents** $\mathbf{F}$ *if each leaf of T is labeled with a 0 or 1, for each $\sigma \in Br_1(T)$, there exists a term C of F so that $C \restriction_\sigma = 1$, and for each $\sigma \in Br_0(T)$, for every term C of F, $C \restriction_\sigma = 0$.*

Lemma 71 *Let T be a decision tree over $\mathcal{U}$ of height h. Let π be a closed partial assignment. If $2Ht(T) + |\pi| < w(\mathcal{U})$, then there is a branch in T consistent with π.*

Proof: The proof is by induction on the height of T. The statement is trivial for trees consisting of a single node. Assume that the lemma holds for all trees of

height h. Let T be a tree of height $h+1$ over $\mathcal{U}$ and let π be a partial assignment so that $2h + 2 + |\pi| < w(\mathcal{U})$. Let Q be the query on the root of T, and for each $L \in \mathcal{ANS}^{\mathcal{U}}(Q)$, let T_L be the subtree immediately underneath the root, underneath the arc labeled L. Because $|\pi| < w(\mathcal{U})$, we may apply lemma 69 and choose $L \in \mathcal{ANS}^{\mathcal{U}}(Q)$ which is consistent with π. T_L is a decision tree over $\mathcal{U} \restriction_L$, and has height at most h. Moreover, $2h + ||\pi|| < w(\mathcal{U}) - 2 \leq w(\mathcal{U} \restriction_L)$, so by the induction hypothesis, we can find $\beta \in \mathrm{Br}(T_L)$ consistent with π. $L \cup \beta$ is the desired branch of T. ∎

Definition VI.E.9 *Let $\mathcal{U}$ be a universe. For each $v \in Vars(\mathcal{U})$, the* **query associated with v**, $\mathbf{Q_v}$, *is defined as follows: If $v = X_i$ then $Q_v = Value(i)$. If $v = Y_e$, then $Q_v = Match(p)$, where p is the lexicographically first element of e.*

VI.F Simplifications

The switching lemma requires us to not only apply a random restriction, but also to make substitutions of literals for variables. The process of applying such transformations to decision trees is called *simplification*. We use simplifications similarly to the way restrictions are used in other proofs of lower bounds for constant-depth Whereas it is clear how to define a 0/1 restriction of a decision tree and this definition guarantees several nice properties, doing so with substitutions requires more care.

Given a mapping on literals, we will extend it in the natural way to a mapping on formulas and a mapping on sets of literals.

Definition VI.F.1 *Let $\mathcal{U}$ and $\mathcal{V}$ be universes. A* **simplification** *is a mapping Σ which maps $Lits(\mathcal{U})$ to $Lits(\mathcal{V}) \cup \{0,1\}$ and $\mathcal{Q}(\mathcal{U}) \cup \{null\}$ to $\mathcal{Q}(\mathcal{V}) \cup \{null\}$ with the following properties:*

1. *If $l_1, l_2 \in Lits(\mathcal{U})$ are inconsistent, then $\Sigma(l_1)$ and $\Sigma(l_2)$ are inconsistent.*
2. *For all queries $Q \in \mathcal{Q}(\mathcal{U})$, if $\Sigma(Q) \neq null$, then $\Sigma(\mathcal{ANS}^{\mathcal{U}}(Q)) = \mathcal{ANS}^{\mathcal{V}}(\Sigma(Q))$*

3. *For each* $v \in Vars(\mathcal{U})$, *if* $\Sigma(Q_v) \neq null$, *then* $\Sigma(Q_v) = Q_{\Sigma(v)}$.

4. *For every hypothesis* $H \in MIS_m(\mathcal{U})$, $\Sigma_\rho(H) = 1$, $\Sigma_\rho(H) = w \vee \neg w$ *(for some variable* w*), or* $\Sigma_\rho(H) \in MIS_m(\mathcal{V})$.

5. $\Sigma(null) = null$

Property (1) allows us to strengthen property (2). Because distinct answers to a query are inconsistent, at most one answer to Q can simplify to an answer of $\Sigma(Q)$.

Lemma 72 *Let* Σ *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$, *and let* Q *be a query of* $\mathcal{U}$ *so that* $\Sigma(Q) \neq null$. *For each* $B \in \mathcal{ANS}^{\mathcal{V}}(\Sigma_\rho(Q))$, *there is exactly one* $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$ *so that* $\Sigma_\rho(A) = B$.

Lemma 73 *Let* Σ *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$, *and let* A *be a closed, consistent set of literals from* $BLits(\mathcal{U})$. Σ *is also a simplification from* $\mathcal{U} \restriction_A$ *to* $\mathcal{V} \restriction_{\Sigma(A)}$.

Lemma 74 *Let* Σ_1 *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$, *and let* Σ_2 *be a simplification from* $\mathcal{V}$ *to* $\mathcal{W}$. *Then* $\Sigma_2 \circ \Sigma_1$ *is a simplification from* $\mathcal{U}$ *to* $\mathcal{W}$.

Definition VI.F.2 *Let* Σ *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$. *Let* T *be a decision tree over* $\mathcal{U}$. *The* **simplification of T by Σ**, $\mathbf{\Sigma(T)}$, *is defined recursively as follows:*

If T *is a single node, then* $\Sigma(T) = T$.
If T *has multiple nodes, then* $\Sigma(T)$ *is the tree constructed as follows:*
Let Q *be the label on the root of* T, *and for each* $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$,
let T_A *denote the subtree of* T *immediately underneath the root,*
underneath the edge labeled A
If there exists $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$ *so that* $\Sigma(A) = 1$
then $\Sigma(T) = \Sigma(T_A)$
Otherwise,
the root of $\Sigma(T)$ *is labeled with* $\Sigma(Q)$

For each $A \in \Sigma(\mathcal{ANS}^{\mathcal{U}}(Q))$

place an arc labeled $\Sigma(A)$ *underneath the root*

and underneath this arc, place a copy of $\Sigma(T_A)$

Lemma 75 *Let* $\mathcal{U}$ *and* $\mathcal{V}$ *be universes, and let* Σ *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$. *Let* T *be a decision tree over* $\mathcal{U}$. *If* T *is a decision tree of height* h *over* $\mathcal{U}$ *then* $\Sigma(T)$ *is a decision tree of height* $\leq h$ *over* $\mathcal{V}$.

Proof: We prove this by induction on h. If $h = 0$, then T is a single node labeled with a value, and $\Sigma(T)$ is that same node. This is a decision tree over $\mathcal{V}$.

Assume that the lemma holds for all trees of height $\leq h$. Let T be a decision tree of height $h+1$ over $\mathcal{U}$. Let Q be the query on the root of T. There are two cases: the case that there exists $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$ so that $\Sigma(A) = 1$, and the case that for all $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$, $\Sigma(A) \neq 1$.

Consider the case when there exists $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$ so that $\Sigma(A) = 1$. Let A be the unique such element of $\mathcal{ANS}^{\mathcal{U}}(Q)$. By definition, $\Sigma(T) = \Sigma(T_A)$. By definition, T_A is a decision tree over $\mathcal{U} \restriction_A$ and by lemma 73, Σ is a simplification from $\mathcal{U} \restriction_A$ to $\mathcal{V} \restriction_{\Sigma(A)} = \mathcal{V}$. Therefore, by the induction hypothesis, $\Sigma(T_A)$ is a decision tree over $\mathcal{V}$.

In the case when for all $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$, $\Sigma(A) \neq 1$, we have that $\Sigma(Q) \neq$ null. By definition, the label on the root of $\Sigma(T)$ is $\Sigma(Q)$, and for each $A \in \mathcal{ANS}^{\mathcal{Q}}(\mathcal{U})$ so that $\Sigma(A) \neq 0$, there is an arc labeled $\Sigma(A)$ leading to $\Sigma(T_A)$. For each such A, because Σ is a simplification from $\mathcal{U} \restriction_A$ to $\mathcal{V} \restriction_{\Sigma(A)}$, by the induction, $\Sigma(T_A)$ is a decision tree over $\mathcal{V} \restriction_{\Sigma(A)}$. Because $\Sigma(\mathcal{ANS}^{\mathcal{U}}(Q)) = \mathcal{ANS}^{\mathcal{V}}(\Sigma(Q))$, we have that $\Sigma(T)$ is a decision tree over $\mathcal{V}$. ∎

Lemma 76 *Let* Σ *be a simplification from* $\mathcal{U}$ *to* $\mathcal{V}$. *Let* T *be a decision tree over* $\mathcal{U}$ *with leaf labels from some set* V, $\Sigma(Br_v(T)) = Br_v(\Sigma(T))$.

Proof: The proof is by induction on the height of T. If T is a single node, then the lemma trivially holds. Suppose that the lemma holds for all trees of height $\leq h$. Let T be a decision tree of height $h+1$ over $\mathcal{U}$. Let Q be the query on the root of T. By the induction hypothesis and lemma 73, for each $A \in \mathcal{ANS}_Q$, $\Sigma(\mathrm{Br}_v(T_A)) = \mathrm{Br}_v(\Sigma(T_A))$. There are two cases: that that there exists $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$ so that $\Sigma(A) = 1$, and the case that for all $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$, $\Sigma(A) \neq 1$.

Consider the case when there exists $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$, so that $\Sigma(A) = 1$. In this case, $\Sigma(T) = \Sigma(T_A)$. Because distinct answers to a query are inconsistent, for every $A' \in \mathcal{ANS}^{\mathcal{U}}(Q) \restriction_\pi$, if $A' \neq A$, then $\Sigma(A) = 0$. Therefore, $\Sigma(\mathrm{Br}_v(T)) = \Sigma(\mathrm{Br}_v(T_A))$ and thus $\mathrm{Br}_v(\Sigma(T)) = \mathrm{Br}_v(\Sigma(T_A)) = \Sigma(\mathrm{Br}_v(T_A)) = \Sigma(\mathrm{Br}_v(T))$.

Now consider the case when for all $A \in \mathcal{ANS}^{\mathcal{U}}(Q)$, $\Sigma(A) \neq 1$.

$$\begin{aligned}
\Sigma(\mathrm{Br}_v(T)) &= \{\Sigma(A \cup B) \mid A \in \mathcal{ANS}^{\mathcal{U}}(Q),\ \Sigma(A) \neq 0,\ B \in \mathrm{Br}_v(T_A)\} \\
&= \{\Sigma(A) \cup B' \mid A \in \mathcal{ANS}^{\mathcal{U}}(Q),\ \Sigma(A) \neq 0, B' \in \Sigma(\mathrm{Br}_v(T_A))\} \\
&= \{\Sigma(A) \cup B' \mid A \in \mathcal{ANS}^{\mathcal{U}}(Q),\ \Sigma(A) \neq 0, B' \in \mathrm{Br}_v(\Sigma(T_A))\} \\
&= \mathrm{Br}_v(\Sigma(T))
\end{aligned}$$

■

Corollary 77 *Let Σ be a simplification from $\mathcal{U}$ to $\mathcal{V}$. Let T be a decision tree in $\mathcal{U}$ with leaf labels from $\{0,1\}$. Let T^c denote the tree obtained by inverting the leaf labels of T.*

1. *If $Br(T) = Br_0(T)$ then $Br(\Sigma(T)) = Br_0(\Sigma(T))$.*
2. *If $Br(T) = Br_1(T)$ then $Br(\Sigma(T)) = Br_1(\Sigma(T))$.*
3. *$\Sigma(T^c) = (\Sigma(T))^c$*
4. *$\Sigma(\bigvee Br_1(T)) = \bigvee Br_1(\Sigma(T))$*

Lemma 78 *Let T be a decision tree which strongly represents a DNF F. Then $\Sigma(T)$ strongly represents $\Sigma(F)$.*

Proof: It is easily checked that if $\Sigma(F) = 0$ is constant, then $\Sigma(T)$ is a single node labeled with 0 and if $\Sigma(F) = 1$ then $\Sigma(T)$ is a single node labeled with 1.

By lemma 76, for any leaf label value v, and for each $\sigma \in \mathrm{Br}_v(\Sigma(T))$, there exists $\tau \in \mathrm{Br}_v(T)$ so that $\Sigma(\tau)$ is non-constant and $\Sigma(\tau) = \sigma$.

Let $\sigma \in \mathrm{Br}_1(T)$ be given. Choose $\tau \in \mathrm{Br}_1(T)$ so that $\Sigma(\tau) = \sigma$ and choose a term C of F so that $C \subseteq \tau$. We have $\Sigma(C) \subseteq \Sigma(\tau) = \sigma$ as needed.

Let $\sigma \in \mathrm{Br}_0(T)$ be given. Choose $\tau \in \mathrm{Br}_0(T)$ so that $\Sigma(\tau) = \sigma$. Let C be a term of F. Because T strongly represents F, $C \restriction_\tau = 0$. Because Σ is a simplification, $\Sigma(C) \restriction_{\Sigma(\tau)} = 0$, and therefore $\Sigma(C) \restriction_\sigma = 0$. ∎

VI.G The Switching Lemma

Theorem 79 *Let r, c be positive constants. There exist constants $\epsilon > 0$ and h so that for all M, and all N sufficiently large, for every (M, N) universe $\mathcal{U}$ and every collection $\mathcal{R}$ of at most N^c many r-DNFs, there exists an (M, N^ϵ) universe $\mathcal{U}'$ and simplification $\Sigma : \mathcal{U} \to \mathcal{U}'$ so that for every $F \in \mathcal{R}$, $\Sigma(F)$ is strongly represented by a decision tree of height at most h.*

The standard tool for proving lower bounds for constant-depth circuits and constant-depth Frege systems is to apply random restrictions to the formulas which collapse them into short decision trees. This approach does not suffice to prove size lower bounds for refutations the MIS_m principles. We require a process which we call "random simplification" that first applies a random restriction and then substitutes some literals for other variables.

In subsection VI.G.1 we show why random restrictions alone do not suffice to prove lower bounds for our tautologies. The random simplifications are described

in subsection VI.G.2. The crucial result of this section is that the simplification process is indeed a simplification as described in section VI.F, lemma 82.

Subsection VI.G.3 contains the proof of our switching lemma, in the guise of theorem 83. We combine theorem 82 and theorem 83 to prove theorem 79.

VI.G.1 The Inadequacy of Restrictions Alone

Restrictions alone do not seem sufficient to collapse DNFs to short decision trees with respect to the $\mathrm{MIS}_m(\mathcal{U})$ principles. This is because for a monomial X_iX_j with $i \in R_r,\ j \in R_{r+1}$, it is possible that X_i is set to 1 and X_j is left unset. Because the monomial may in the future be set to 0 or 1, depending on how X_j is set, we can neither match with some extra points nor say that it is unmatched. If the random restriction sets a reasonable numbers one and leaves a reasonable number of variables unset in each row, this event happens with significant probability.

We now give an example of a DNF that cannot be represented by a short decision tree after the application of any 0/1 restriction that does not set every variable in each row. Fix $i \in R_r$ and consider a disjunction $\bigvee_{\substack{j \in R_{r+1} \\ e \ni \{i,j\}}} Y_e$, for a fixed $i \in R_r$. In the event that X_i is left unset, none of the matching variables in the disjunction are set to 1. A matching query must be made for each $\{i,j\}$ with X_j not set to zero, so any decision tree to representing the restriction of this DNF requires height proportional to the number of $j \in R_{r+1}$ so that X_j is not set to zero. This is too large for our purposes.

VI.G.2 Presimplifications

To avoid the difficulties described in the preceding section, we apply a random restriction and then substitute one variable for another. In particular, for monomials $\{i,j\}$ with X_i set to 1 and X_j set to $*$, we reserve a particular $e \in E_r$ with $\{i,j\} \in e$ and substitute X_j for the variable Y_e and 0 for every other Y_f with $\{i,j\} \in f$. Notice that this reduces the troublesome disjunction of subsection

VI.G.1 to the single variable X_j which is strongly represented by a decision tree of height 1.

Definition VI.G.1 *Let $\mathcal{U}$ be an (M, N) universe, and let ρ be a partial assignment to Vars($\mathcal{U}$). Let $r \in \{1, \ldots, M-1\}$, $i \in R_r, j \in R_{r+1}$ be given. We say that the monomial $\{i, j\}$* **is a half-star of** *ρ if $\rho(X_i) = 1$ and $\rho(X_j) = *$, or, $\rho(X_i) = *$ and $\rho(X_j) = 1$.*

For each half-star $I = \{i, j\}$, some $e \ni I$ is reserved to cover $\{i, j\}$ should X_i and X_j both be set to 1. The monomial can be covered by no other edge. Of course, if the monomial X_I later becomes a 0, then something must be done with the extra points in the reserved edge. Notice that the monomial $\{i, j\}$ becomes 0 only when X_j is set to 0. In this case, all the other half-stars dependent on j, $\{i', j\}$, become 0 and the extra points of the edges for these half-stars become free as well. We place a predetermined partition on all of these extra-points and use it when X_j is set to 0: for f belonging to this partition, $\neg X_j$ is substituted for Y_f.

Definition VI.G.2 *Let $\mathcal{U}$ be an (M, N) universe. Let $L \leq N$ be given so that $K = \frac{N-L}{2}$ is an integer divisible by m. An* **L-presimplification for** *$\mathcal{U}$ is a consistent, closed partial assignment ρ satisfying the following properties:*

1. *In each row, ρ sets K ones: $\forall r \in \{1, \ldots, M\}$, $|\{i \in R_r \mid X_i \in \rho\}| = K$.*
2. *In each row, ρ sets K zeroes: $\forall r \in \{1, \ldots, M\}$, $|\{i \in R_r \mid \neg X_i \in \rho\}| = K$.*
3. *In equations 1 through $M-1$, $2mKN - mK^2 + m(m-1)K$ many extra points are covered: $\forall r \in \{1, \ldots, M-1\}$, $|\{p \in V_r \mid \exists e \in [V_r]^m, p \in e,\ Y_e \in \rho\}| = 2mKN - mK^2 + m(m-1)K$.*
4. *In equations 0 and M, $(m+1)K$ extra points are covered: $\forall r \in \{0, M\}$, $|\{p \in V_r \mid \exists e \in [V_r]^2, p \in e,\ Y_e \in \rho\}| = K$.*
5. *In equations 0 through $M-1$, every satisfied monomial is matched.*

   $\forall r \in \{0, \ldots, M-1\}$, $\forall I \in U_r$, $(\forall i \in I,\ X_i \in \rho) \Rightarrow \exists e \ni I,\ Y_e \in \rho$

6. *In equation M, all satisfied monomials but $m-1$ are matched.* $|\{I \in U_M \mid \exists e \ni I,\ Y_e \in \rho\}| = K$

7. *Potential matches are reserved for the half-stars:*

   For each $r \in \{1,\ldots,M-1\}, i \in R_r, j \in R_{r+1}$ so that $\rho(X_i) = 1$ and $\rho(X_j) = *$, there is $e_\rho^{i,j} \in E_r$ with $\{i,j\} \in e_\rho^{i,j}$ so that

   - $\forall f,\ \{i,j\} \in f,\ f \neq e_\rho^{i,j},\ \rho(Y_f) = 0$
   - $\rho(Y_{e_\rho^{i,j}}) = *$

   For each $r \in \{1,\ldots,M-1\}$, $j \in R_{r+1}$ so that $\rho(X_j) = *$, let $S_\rho^j = \bigcup_{\substack{i \in R_r \\ \rho(X_i)=1}} e_\rho^{i,j}$. Let $\mathcal{E}_\rho^j$ be a fixed m-partition on the points of S_ρ^j.

   - *If $e \in \mathcal{E}_\rho^j$ then $\rho(Y_e) = *$.*
   - *$\forall e$, if $e \cap S_\rho^j \neq \emptyset$ and $e \notin \mathcal{E}_\rho^j$ then $\rho(Y_e) = 0$.*

   For each $r \in \{1,\ldots,M-1\}, i \in R_r, j \in R_{r+1}$ so that $\rho(X_i) = *$ and $\rho(X_j) = 1$, there is $f_\rho^{i,j} \in V_r$ so that

   - *$\forall e,\ \{i,j\} \in e,\ e \neq f_\rho^{i,j}$, $rho(Y_e) = 0$.*
   - *$\rho(Y_{f_\rho^{i,j}}) = *$*

   For each $r \in \{1,\ldots,M-1\}$, $i \in R_r$ so that $\rho(X_i) = *$, let $T_\rho^i = \bigcup_{\substack{j \in R_{r+1} \\ \rho(X_j)=1}} f_\rho^{i,j}$. Let $\mathcal{F}_\rho^i$ be a fixed m-partition on the points of T_ρ^i.

   - *If $f \in \mathcal{F}_\rho^i$, then $\rho(Y_f) = *$.*
   - *$\forall f$, if $f \cap T_\rho^i \neq \emptyset$ and $f \notin \mathcal{F}_\rho^i$ then $\rho(Y_f) = 0$.*

8. *If l is a literal inconsistent with a variable v and $v \in \rho$ then $\neg l \in \rho$.*

9. *No other literals belong to ρ.*

Lemma 80 *Let $\mathcal{U}$ be an (M,N) universe, and let π be a consistent, closed set of literals with $|\pi| < N$. There exists a $(N - |\pi|)$-simplification ρ so that $\pi \subseteq \rho$.*

Definition VI.G.3 *Let $\mathcal{U}$ be an (M,N) universe, and let ρ be an L-presimplification for $\mathcal{U}$. An* **e-extension of** *ρ is an $(L-2e)$-presimplification κ so that $\rho \subseteq \kappa$.*

We call this an e-extension rather than a $2e$-extension because it adds e ones in each row and e zeroes in each row.

Definition VI.G.4 *Let M and N be positive integers.*

Let $\mathcal{U} = (R_1, \ldots, R_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ be an (M,N) universe. For each r, $1 \leq r \leq M$, we define $\Sigma_\rho(R_r) := \{i \in R_r \mid \rho(X_i) = *\}$. For each r, $0 \leq r \leq M$, we define

$$\begin{aligned}
\Sigma_\rho(U_r) &:= \{I \in U_r \mid \forall i \in I,\ \rho(X_i) = *\} \\
\Sigma_\rho(V_r) &:= \{p \in V_r \mid \forall i \in R_r, \forall j \in R_{r+1}, p \notin e_\rho^{i,j},\ p \notin f_\rho^{i,j}, \forall e \ni p,\ \rho(Y_e) \neq 1\} \\
\Sigma_\rho(\mathcal{U}) &:= (\Sigma_\rho(R_1), \ldots, \Sigma_\rho(R_M), \Sigma_\rho(U_0), \ldots, \Sigma_\rho(U_M), \Sigma_\rho(V_0), \ldots, \Sigma_\rho(V_M))
\end{aligned}$$

Lemma 81 *Let $\mathcal{U} = (R_1, \ldots, R_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ be an (M,N) universe and let ρ be an L-presimplification for $\mathcal{U}$. $\Sigma_\rho(\mathcal{U})$ is an (M,L) universe.*

Definition VI.G.5 *Let $\mathcal{U}$ be an (M,N) universe, and let ρ be a presimplification for $\mathcal{U}$. For each query $Q \in \mathcal{Q}(\mathcal{U})$, we define* **the simplification of Q by** *ρ, $\boldsymbol{\Sigma}_\rho(\mathbf{Q})$, as follows:*

If $Q = Value(i)$ then
  if $\Sigma_\rho(X_i) = X_i$ then $\Sigma_\rho(Q) = Value(i)$
  otherwise $\Sigma_\rho(Q) = null$
if $Q = Match(\{i\})$ then
  if $\Sigma_\rho(X_i) = X_i$ then $\Sigma_\rho(Q) = Match(i)$
  otherwise $\Sigma_\rho(Q) = null$
If $Q = Match(\{i,j\})$, then
  if $\Sigma_\rho(X_i) = X_i$ and $\Sigma_\rho(X_j) = X_j$ then $\Sigma_\rho(Q) = Match(\{i,j\})$
  if $\Sigma_\rho(X_i) = 1$ and $\Sigma_\rho(X_j) = X_j$ then $\Sigma_\rho(Q) = Value(j)$
  otherwise, $\Sigma_\rho(Q) = null$

If $Q = Match(p)$, *then*

if $p \in e_\rho^{i,j}$ *then* $\Sigma_\rho(Q) = Value(j)$

if $p \in f_\rho^{i,j}$ *then* $\Sigma_\rho(Q) = Value(i)$

if $p \in \Sigma_\rho(V_r)$ *for some* r, *then* $\Sigma_\rho(Q) = Match(p)$

otherwise $\Sigma_\rho(Q) = null$

Lemma 82 *Let* $\mathcal{U}$ *be an* (M, N) *universe and let* ρ *be a presimplification for* $\mathcal{U}$. Σ_ρ *is a simplification from* $\mathcal{U}$ *to* $\Sigma_\rho(\mathcal{U})$.

Proof: We show that the three criteria of the definition of simplification are met:

1. If $l_1, l_2 \in \text{Vars}(\mathcal{U})$ are inconsistent, then either (i) $\Sigma_\rho(l_1) = 0$ or $\Sigma_\rho(l_2) = 0$, or (ii) $\Sigma_\rho(l_1)$ and $\Sigma_\rho(l_2)$ are inconsistent.

   This is non-trivial only when $\Sigma_\rho(l_1) \neq l_1$ or $\Sigma_\rho(l_2) \neq l_2$. Without loss of generality, there are two cases to consider, $l_1 = M_{I,p}$, with $\Sigma_\rho(M_{I,p}) = X_i$, and $l_1 = Y_e$, with $\Sigma_\rho(l_1) = \neg X_i$.

   Consider the case when $l_1 = Y_e$ and $\Sigma_\rho(Y_e) = X_i$ with $i \in I \in e$. This happens when e is the edge reserved for the monomial $\{i, j\}$ with $\rho(X_i) = *$ and $\rho(X_j) = 1$. There are three possibilities for what l_2 can be: $\neg X_i$, $\neg X_j$, and Y_f with $f \perp e$. If $l_2 = \neg X_i$, then $\Sigma_\rho(l_2) = \neg X_i$. If $l_2 = \neg X_j$ then $\Sigma_\rho(l_2) = 0$. If $l_2 = Y_f$ with $f \perp e$, then either $\Sigma_\rho(l_2) = 0$ or $\Sigma_\rho(l_2) = \neg X_i$.

   Consider the case when $l_1 = Y_e$ and $\Sigma_\rho(Y_e) = \neg X_i$. This happens when $e \in \mathcal{E}_\rho^i$ or $e \in \mathcal{F}_\rho^i$, and $e \ni \{i, j\}$ with $\rho(X_j) = 1$. The possibilities for what l_2 can be are $\neg X_i$, $\neg X_j$, and Y_f with $f \perp e$. If $l_2 = \neg X_i$ then $\Sigma_\rho(l_2) = \neg X_i$. If $l_2 = \neg X_j$ then $\Sigma_\rho(l_2) = 0$. If $l_2 = Y_f$ with $e \perp f$ then either $\Sigma_\rho(Y_f) = X_i$ or $\Sigma_\rho(Y_f) = 0$.

2. For all queries $Q \in \mathcal{Q}(\mathcal{U})$, if $\Sigma_\rho(Q) \neq \text{null}$, then
   $\Sigma(\mathcal{ANS}^{\mathcal{U}}(Q)) = \mathcal{ANS}^{\Sigma_\rho(\mathcal{U})}(\Sigma_\rho(Q))$.

   Consider a query of the form $Q = \text{Match}(\{i, j\})$. The other queries are handled with similar case analyses and we omit them to save space.

Recall that

$$\begin{aligned}\mathcal{ANS}^{\mathcal{U}}(\text{Match}(\{i,j\})) &= \{\{\neg X_i, \neg X_j\}, \{\neg X_i, X_j\}, \{X_i, \neg X_j\}\} \\ &\quad \cup \{\{Y_e, X_i, X_j\} \mid e \ni I\}\end{aligned}$$

Consider the case when $\Sigma_\rho(X_i) = X_i$ and $\Sigma_\rho(X_j) = X_j$. In this case $\Sigma_\rho(Q) = \text{Match}(\{i,j\})$. Clearly, for each $e \in [\Sigma_\rho(U_r) \cup \Sigma_\rho(V_r)]^m$, with $\{i,j\} \in e$, $\Sigma_\rho(\{Y_e, X_i, X_j\}) = \{Y_e, X_i, X_j\}$, and for each $e \notin [\Sigma_\rho(U_r) \cup \Sigma_\rho(V_r)]^m$, $\{i,j\} \in e$, $\Sigma_\rho(Y_e, X_i, X_j\}) = 0$. Also, for $A = \{\neg X_i, \neg X_j\}$, $\{\neg X_i, X_j\}$, or $\{X_i, \neg X_j\}$, we trivially have that $\Sigma_\rho(A) = A$. Therefore, $\Sigma(\mathcal{ANS}^{\mathcal{U}}(Q)) = \mathcal{ANS}^{\Sigma_\rho(\mathcal{U})}(\Sigma_\rho(Q))$.

Consider the case when $\Sigma_\rho(X_i) = 1$ and $\Sigma_\rho(X_j) = *$. In this case $\Sigma_\rho(\{\neg X_i, \neg X_j\}) = 0$, $\Sigma_\rho(\{\neg X_i, X_j\}) = 0$, and $\Sigma_\rho(\{X_i, \neg X_j\}) = \{\neg X_j\}$. For each $e \ni I$, $\Sigma_\rho(Y_e) = 0$ if e is not the edge reserved for $\{i,j\}$ and $\Sigma_\rho(Y_e) = X_j$ if it is. Therefore,

$$\Sigma_\rho(\mathcal{ANS}^{\mathcal{U}}(Q)) = \{\{X_j\}, \{\neg X_j\}\} = \mathcal{ANS}^{\Sigma_\rho(\mathcal{U})}(\text{Value}(j))$$

3. For each $v \in \text{Vars}(\mathcal{U})$, if $\Sigma_\rho(Q_v) \neq \text{null}$, then $\Sigma_\rho(Q_v) = Q_{\Sigma_\rho(v)}$.

   This is trivial whenever $\Sigma_\rho(v) = v$. The only other cases are when $\Sigma_\rho(Y_e) = X_i$ and $\Sigma_\rho(Y_f) = \neg X_i$. In the former case, $\Sigma_\rho(\text{Match}(I)) = \text{Value}(i) = Q_{X_i}$ and in the latter case $\Sigma_\rho(\text{Match}(p)) = \text{Value}(i) = Q_{X_i}$.

4. For every hypothesis $H \in \text{MIS}_m(\mathcal{U})$, $\Sigma_\rho(H) = 1$, $\Sigma_\rho(H) = w \vee \neg w$ (for some variable w), or $\Sigma_\rho(H) \in \text{MIS}_m(\Sigma_\rho(\mathcal{U}))$.

   The proof is a case analysis for each type of clause in $\text{MIS}_m(\mathcal{U})$. To save space, we give the proof only for axioms of the form $\bigvee_{e \ni p} Y_e$, for some $p \in V_r$, $0 \leq r \leq M$. The other axioms are handled similarly.

   In the case that there exists $e \ni I$ so that $\Sigma_\rho(Y_e) = 1$, $\Sigma_\rho(A) = 1$.

   In the case when p is belongs to an edge e reserved for some half-star, $\{i,j\}$ with $\Sigma_\rho(X_j) = X_j$ and $\Sigma_\rho(X_i) = 1$, we have that $\Sigma_\rho(Y_e) = X_j$. Also, there is

exactly one edge $f \ni p$ with $\Sigma_\rho(Y_f) = \neg X_j$; for all other $g \ni p$, $\Sigma_\rho(Y_g) = 0$. Therefore, $\Sigma_\rho(\bigvee_{e \ni p} = X_j \vee \neg X_j$.

The remaining case is when $p \in \Sigma_\rho(V_r)$. In this case, for $e \in [\Sigma_\rho(U_r) \cup \Sigma_\rho(V_r)]^m$, $|e \cup \Sigma_\rho(U_r)| \leq 1$, $\Sigma_\rho(Y_e) = Y_e$. For $e \in [\Sigma_\rho(U_r) \cup \Sigma_\rho(V_r)]^m$ with $e \cap (V_r \setminus \Sigma_\rho(V_r)) \neq \emptyset$, we have that $\Sigma_\rho(Y_e) = 0$. Similarly, e contains a half-star or a satisfied monomial, then $\Sigma_\rho(Y_e) = 0$. Therefore, $\Sigma_\rho(\bigvee_{e \ni p} Y_e) = \bigvee_{e \ni p} Y_e$.

■

VI.G.3 An Independent Set Style Switching Lemma

Definition VI.G.6 *Let $\mathcal{U}$ be an (M, N) universe, and let ρ a presimplification for $\mathcal{U}$. The minimum height of a decision tree strongly representing $\Sigma_\rho(F)$ is denoted as $\mathbf{h}_\rho(\mathbf{F})$.*

Theorem 83 *Let r, c be positive constants. There exist constants $\epsilon > 0$ and h so that for all M, and all N sufficiently large, for every (M, N) universe $\mathcal{U}$, for a randomly chosen N^ϵ-presimplification for $\mathcal{U}$, ρ,*

$$Pr_\rho[h_\rho(F) \geq h] \leq N^{-c}$$

Lemma 84 *Let $\mathcal{U}$ be an (M, N) universe. Let $L \leq N$ be given, and let $K = \frac{1}{2}(N - L)$. Let F be an r-DNF in Vars($\mathcal{U}$), and let ρ be an L-presimplification for $\mathcal{U}$. If ρ is selected uniformly among L-presimplifications, then*

$$Pr_\rho[h_\rho(F) \geq 4m^2r^4s^2)] \leq \left(\frac{4r^2sL^{Cr}}{K}\right)^s$$

Proof:(of theorem 83 from lemma 84) Simply set $\epsilon = 1/2cr$ and $s = 4c$. For N large enough so that $N - N^\epsilon \geq (4/5)N$ and $(10r^s)^s \leq N^c$,

$$\begin{aligned} Pr_\rho[h_\rho(F) \geq 4m^2r^4s^2)] &\leq \left(\tfrac{4r^2sL^{Cr}}{K}\right)^s \leq \left(\tfrac{4r^2s(N)^{\epsilon Cr}}{\frac{1}{2}(N-N^\epsilon)}\right)^s \leq \left(\tfrac{8r^2sN^{1/2}}{N-N^\epsilon}\right)^s \\ &\leq \left(\tfrac{10r^2s}{N^{1/2}}\right)^s \leq \tfrac{\left(10r^2s\right)^s}{N^{2c}} \leq N^{-c} \end{aligned}$$

■

The proof of theorem 84 is the direct combination of theorems 88 and 93, which are proved in subsubsection VI.G.3 and VI.G.3, respectively.

Definition VI.G.7 *We define the* **skeleton of a literal** *as follows:* $\widetilde{X_i} = X_i$, $\widetilde{\neg X_i} = \neg X_i$, *for* $e \in [V_r]^m$, $\widetilde{Y_e} = Y_e$, *and for* $e \ni I$, $I \in U_r$, $\widetilde{Y_e} = \{X_i \mid i \in I\}$. *The* **skeleton of a set of literals** *is defined as follows:*

$$\widetilde{\mathbf{S}} = \bigcup_{l \in S} \tilde{l}$$

Definition VI.G.8 *Let* $\mathcal{U}$ *be an* (M, N) *universe, and let* ρ *be a presimplification for* $\mathcal{U}$. *Let* B *be a consistent, closed set of literals from* $BLits(\Sigma_\rho(\mathcal{U}))$. *We define* $\mathbf{B}^\rho$, **the pullback of B along** ρ *as follows:* $B^\rho = \{l \mid \Sigma_\rho(l) = 1 \text{ or } \Sigma_\rho(l) \in B\}$

Definition VI.G.9 *Let* $\mathcal{U} = (R_1, \ldots, R_M, S_1, \ldots, S_M, U_0, \ldots, U_M, V_0, \ldots, V_M)$ *be a universe. Let* B *be a set of literals in* $Vars(\mathcal{U})$. *We say that* B **matches its ones** *if for every* $r \in \{0, \ldots M\}$, *and every* $I \in U_r$, *if* $\{X_i \mid i \in I\} \subseteq B$ *then there exists* $Y_e \in B$ *with* $I \in e$.

Definition VI.G.10 *Let* $\mathcal{U}$ *be an* (M, N) *universe. Let* F *be a DNF in the literals* $BLits(U)$. *Let* ρ *be a presimplification for* $\mathcal{U}$. *Let* $T_1, \ldots, T_s$ *be terms from* F. *We say that* $T_1, \ldots, T_s$ *are* ρ**-consistent** *if there exists* κ, *so that* $\rho \cup T_1 \cup \ldots \cup T_s \subseteq \kappa$. *Let* B *be a consistent, closed partial assignment in the variables* $BLits(\Sigma_\rho(\mathcal{U}))$ *that matches its ones. We say that* $T_1, \ldots, T_s$ *are* **B-independent** *if for all* $1 \leq i < j \leq s$, $\widetilde{T_i} \cap \tilde{T_j} \subseteq B^\rho$. *We say that that* $T_1, \ldots, T_s$ *form a* **B-independent-set for F with respect to** ρ *if* $T_1, \ldots, T_s$ *are* B*-independent,* $T_1, \ldots, T_s$ *are* ρ*-consistent and* $\Sigma_\rho(F) \restriction_B$ *is non-constant. We will say that* $T_1, \ldots, T_s$ *form an* **independent set for F with respect to** ρ *is there exists a* B *so that* $T_1, \ldots, T_s$ *is a* B*-independent-set for* F *with respect to* ρ. *We say that that* $T_1, \ldots, T_s$ *is a* **maximal B-independent-set for F with respect to** ρ *if for every term* T' *in* F *that is not one of* $T_1, \ldots, T_s$, *the set* $T, T_1, \ldots, T_s$ *is not a* B*-independent-set for* F *with respect to* ρ.

Definition VI.G.11 *Let $\mathcal{U}$ be an (M, N) universe, and let ρ be an L-presimplification for $\mathcal{U}$. Let F be a DNF in BLits($\mathcal{U}$). We say that* ρ **is s-bad for F** *if there is an independent set for F with respect to ρ of size s. Let κ be an e-extension of ρ. We say that κ* **is an s-encoding for ρ with respect to F** *if there exists an independent set for F with respect to ρ, $T_1, \ldots, T_s$, so that κ satisfies $T_1 \cup \ldots \cup T_s$.*

Lemma 85 *If ρ is not s-bad for F, then for any consistent, closed set of literals B that matches its ones so that $\Sigma_\rho(F) \restriction_B$ is non-constant, there exists a maximal B-independent set of size at most s.*

Proof: A single, non-constant, term is trivially B-independent, and by repeatedly adding terms, we can construct a maximal B-independent set for F with respect to ρ. ∎

Needed Facts About Simplifications and Restrictions

Lemma 86 *If $F \restriction_{B^\rho}$ is constant then $\Sigma_\rho(F) \restriction_B$ is constant and $F \restriction_{B^\rho} = \Sigma_\rho(F) \restriction_B$.*

Proof: Suppose that $F \restriction_{B^\rho} = 1$. For each $l \in F$, $l \in B^\rho$ so $\Sigma_\rho(l) = 1$ or $\Sigma_\rho(l) \in B$. Therefore, $\Sigma_\rho(F) \restriction_B = 1$. Suppose that $F \restriction_{B^\rho} = 0$. Choose $l_1 \in F$ and $l_2 \in B^\rho$ that are inconsistent. By definition, $\Sigma_\rho(l_2) = 1$ or $\Sigma_\rho(l_2) \in B$. Because Σ_ρ maps inconsistent literals to inconsistent literals, $\Sigma_\rho(F) \restriction_B = 0$. ∎

Lemma 87 *Let $\mathcal{U}$ be a universe, let ρ be a restriction, and let $\mathcal{V} = \Sigma_\rho(\mathcal{U})$. Let B be a consistent, closed partial assignment to Vars($\mathcal{V}$) and let T_1, T_2 be terms in Vars($\mathcal{U}$) so that $\Sigma_\rho(T_1) \neq 0$ and $\Sigma_\rho(T_2) \neq 0$. If $\widetilde{T_1} \cap \widetilde{T_2} \not\subseteq B^\rho$, then $\widetilde{\Sigma_\rho(T_1)} \cap \widetilde{\Sigma_\rho(T_2)} \not\subseteq B$.*

Proof: Choose $l \in \widetilde{T_1} \cap \widetilde{T_2} \setminus B^\rho$. By definition of Σ_ρ, $\Sigma_\rho(l)$ is *not* a matching literal $M_{I,p}$, so $\Sigma_\rho(l) \in \widetilde{\Sigma_\rho(T_1)} \cap \widetilde{\Sigma_\rho(T_2)}$. Moreover, because $l \notin B^\rho$, $\Sigma_\rho(l) \notin B$ and $\Sigma_\rho(l) \neq 1$. Finally, $\Sigma_\rho(l) \neq 0$ because $\Sigma_\rho(T_1) \neq 0$ and B is closed. ∎

With High Probability, a Random Presimplification is Not Bad

Theorem 88 *Let M, N, L, r and s be positive integers, so that $2rs < L \leq N$. Set $K = \frac{1}{2}(N - L)$. For any (M, N) universe, $\mathcal{U}$, for any r-DNF F in the literals BLits($\mathcal{U}$), with ρ a uniformly drawn L-presimplification for $\mathcal{U}$,*

$$Pr_{\rho}[\rho \text{ is } s\text{-bad for } F] \leq \left(\frac{4r^2 s L^{Cr}}{K}\right)^s$$

Theorem 88 is proved through a sequence of three lemmas. It shown that it is very unlikely that any adversary can recover much of an L-presimplification from a randomly chosen extension, lemma 89, then it is shown that if a presimplification is bad for F then an extension probably encodes the independent set, lemma 90, and an encoding for a bad presimplification can be exploited to guess a substantial part of the extension, lemma 91. Therefore, the probability of the original extension being bad is small. We first prove the three lemmas and then we combine them to prove theorem 88.

Lemma 89 *Let $\mathcal{U}$ be an (M, N) universe, and let L and e be integers so that $e \leq L \leq N$. Set $K = \frac{N-L}{2}$. If ρ is a uniformly drawn L-presimplification for $\mathcal{U}$. and κ is a uniformly drawn e-extension of ρ, then for any adversary A that returns a set of s literals:*

$$Pr_{\rho,\kappa}[A(\kappa) \subseteq \tilde{\kappa} \setminus \rho] \leq \left(\frac{e}{K}\right)^s$$

Proof: Notice that the distribution on pairs (ρ, κ) so that ρ is a random L-presimplification and κ is a random e-extension of ρ is the same distribution on pairs (ρ, κ) where κ is a randomly chosen $(L - e)$-presimplification and ρ is a randomly selected sub-presimplification of κ. This is simply because both choose uniformly among such pairs, which in turn holds because the number of e-extensions of an L-presimplification depends only on L and the number of L-presimplifications which are extended by a given $(L - e)$-presimplification depends only on L and e.

Fix an $(L - e)$-presimplification κ and let $S = A(\kappa)$. Without loss of generality, there are no literals of the form $M_{I,p}$ in S because the adversary knows

that such literals do not belong to $\tilde{\kappa}$. We now show that a randomly selected $\rho \subseteq \kappa$ is disjoint from S with less than the stated probability. By the principle of deferred decisions, this proves the lemma.

For each r, $1 \leq r \leq M$, let $a_r = |\{i \in R_r \mid X_i \in S\}|$, $b_r = |\{i \in R_r \mid \neg X_i \in S\}|$, and for r, $0 \leq r \leq M$, let $c_r = |\{e \in [V_r]^m \mid Y_e \in S\}|$.

In row r, we choose K ones. The probability that positions set are not specified by S is

$$\frac{\binom{K+e-a_r}{K}}{\binom{K+e}{K}} = \frac{(K+e-a_r)!K!e!}{(K+e)!K!(e-a_r)!} \leq \left(\frac{e}{K+e-a_r+1}\right)^{a_r} \leq \left(\frac{e}{K}\right)^{a_r}$$

Similarly, we must choose K zeroes in row r, and the probability that this is done without meeting S is at most $\left(\frac{e}{K}\right)^{b_r}$. For the extra points in equation 0, an assignment that does meet S chooses $K/2$ pairs from $(K+e)/2 - c_0$, and for the extra points in equation M, it chooses $K/2$ pairs from $(K+e)/2 - c_M$. The probabilities of these events are at most $(e/K)^{c_0}$ and $(e/K)^{c_M}$, respectively. In equation r, $1 \leq r \leq M-1$, we choose $\frac{1}{2}(2KN + K^2 + K)$ pairs $e \in [V_r]^2$ from $\rho\kappa$ that are disjoint from S. Let P denote the number of vertices of V_r covered by an edge $Y_e \in \rho$ with $e \in [V_r]^m$, and let P' denote the number of vertices of V_r covered by an edge $Y_e \in \rho$ with $e \in [V_r]^m$. Note that $P = 2mKN - mK^2 + m(m-1)K$ and $P' = 2m(K+e)N - m(K+e)^2 + m(m-1)(K+e)$, and therefore $P' - P = 2meN - 2meK - me^2 + m(m-1)e$.

The probability of this happening is:

$$\frac{\binom{P'-c_r}{P}}{\binom{P'}{P}} = \frac{\binom{P+(P'-P)-c_r}{P}}{\binom{P+(P'-P)}{P}} \leq \left(\frac{P'-P}{P}\right)^{c_r}$$

$$= \left(\frac{2meN - 2meK - me^2 + m(m-1)e}{2mKN - mK^2 + m(m-1)K}\right)^{c_r}$$

$$\leq \left(\frac{2meN - meK + m(m-1)e}{2mKN - mK^2 + m(m-1)K}\right)^{c_r} = \left(\frac{e}{K}\right)^{c_r}$$

Therefore, the probability that a randomly selected presimplification will have its skeleton disjoint from S is at most $(e/K)^{a+b+c} = (e/K)^s$.

■

Lemma 90 *There exists a positive constant C so that for any positive integers M and N, any (M,N) universe $\mathcal{U}$, all e and L so that $2rs \leq e \leq L \leq N$, and all L-presimplifications for $\mathcal{U}$, ρ, and when κ is a uniformly selected e-extension of ρ:*

$$Pr_{\kappa}[\kappa \text{ is an } s\text{-encoding for } \rho \text{ wrt } F \mid \rho \text{ is } s\text{-bad for } F] \geq \frac{1}{L^{Crs}}$$

Proof: Let ρ be an L-presimplification for $\mathcal{U}$ so that there is a family of terms from F, $T_1, \ldots, T_s$, that form an s independent set for F with respect to ρ. Notice that κ satisfies $T_1 \cup \ldots \cup T_s$ if and only if κ satisfies $\Sigma_\rho(T_1 \cup \ldots \cup T_s)$. Let $\kappa_0 = \Sigma_\rho(T_1 \cup \ldots \cup T_s)$.

For each r, $1 \leq r \leq M$, let $a_r = |\{i \mid i \in R_r,\ X_i \in \kappa_0\}|$. For each r, $1 \leq r \leq M$, let $b_r = |\{i \mid i \in R_r,\ \neg X_i \in \kappa_0\}|$. For each r, $0 \leq r \leq M$, let $c_r = |\{p \mid \exists e \in [V_r]^m,\ Y_e \in \kappa_0\}|$. For each r, $0 \leq r \leq M$, let $d_r = |\{I \mid \exists Y_e \kappa_0,\ I \in e\}|$.

Probability of getting the ones correct, in row r: $\binom{L-a_r}{e-a_r}/\binom{L}{e} = (L-a_r)!e!(L-e)!/(e-a_r)!(L-e)!L! \geq 1/L^{a_r}$. Probability of getting the zeroes correct (conditioned upon getting the ones correct), in row r: $\binom{L-e-b_r}{e-b_r}/\binom{L-e}{e} \geq 1/(L-e)^{b_r}$.

To bound the probability of getting the partition edges that are contained within V_r correct, we note that there are $mL^2 + m(m-1)L$ many points in V_r, for $1 \leq r \leq M-1$, ($mL$and $mL+m$ for equations 0 and M, respectively), and $\binom{mL^2+m(m-1)L}{m}$ many edges. Therefore, the chance of the extension including the c_r specified edges is clearly $\geq \frac{1}{L^{O(mc_r)}}$.

Similarly, the probability of getting the edges containing the satisfied monomials is clearly $\geq 1/L^{O(md_r)}$.

Let $a = \sum_{r=1}^{M} a_r$, $b = \sum_{r=1}^{M} b_r$, $c = \sum_{r=0}^{M} c_r$ and $d = \sum_{r=0}^{M} d_r$. Therefore, the probability of κ satisfying κ_0 is at least:

$$\prod_{r=1}^{M} \frac{1}{L^{a_r}} \prod_{r=1}^{M} \frac{1}{L^{b_r}} \prod_{r=0}^{M} \frac{1}{L^{O(c_r+d_r)}} \geq L^{O(a+b+c+d)}$$

Because $a+b+c+d \leq 3rs$, for L sufficiently large, this probability is at least $1/L^{Crs}$ for some constant C. ∎

Definition VI.G.12 *Let $\mathcal{U}$ be a universe, let F be an r-DNF in BLits($\mathcal{U}$) and let s be an integer. Let $\mathbf{A_{F,s}}(\kappa)$ be the following algorithm:*

Let $\kappa_1 = \kappa$

For $i = 1$ *to* s *:*

Find the lexicographically first term of F which is satisfied by κ_i, call it T_i.

If there is no such term, abort with output "error".

Randomly choose $l_i \in \widetilde{T}_i$

$\kappa_{i+1} \leftarrow \kappa_{i-1} \setminus \{l\}$

if $l = X_j$ *then* $\kappa_{i+1} \leftarrow \kappa_{i+1} \setminus \{Y_e \mid j \in I,\ I \in e\}$

Output $\{l_1, \ldots, l_s\}$

Lemma 91 *Let $\mathcal{U}$ be an (M, N) universe, let F be an r-DNF in BLits($\mathcal{U}$), and let s, e and L be integers with $e \leq L \leq N$. Let ρ be an L-presimplification for $\mathcal{U}$. and let κ be an e-extension of ρ.*

$$Pr[A_{F,s}(\kappa) \subseteq \tilde{\kappa} \setminus \rho \mid \kappa \text{ is an } s\text{-encoding of } \rho] \geq \left(\frac{1}{2r}\right)^s$$

Proof: Fix ρ and κ so that F contains an independent set of size s with respect to ρ, and κ satisfies every term of this independent set. Let $B \subseteq \text{BLits}(\mathcal{V})$ be the core of the independent set. For each t, $0 \leq t < s$, let E_t denote the event that for all i, $1 \leq i \leq t$, $l_i \in \widetilde{\kappa} \setminus B^\rho$. We will show that for each $t < s$, $Pr\left[l_{t+1} \in \widetilde{\kappa} \setminus B^\rho \mid E_t\right] \geq 1/2r$.

Let $t < s$ be given and assume that event E_t holds, that is, for all i, $1 \leq i \leq t$, $l_i \in \widetilde{\kappa} \setminus B^\rho$. Notice that each $\{l_i\} \cup \{Y_e \mid l_i \in \widetilde{Y}_e\}$ can meet at most one term of the independent set because for terms T, T' of the independent set, $\widetilde{T} \cap \widetilde{T'} \subseteq B^\rho$ and $l_i \notin B^\rho$. Therefore, there is some term of the independent set which is satisfied by κ_{t+1}.

Let T_{t+1} be the term found at the $t+1$'th iteration of $A_{F,s}(\kappa)$, with $T_{t+1} \restriction_{\kappa_{t+1}} = 1$. Because $\Sigma_\rho(F) \restriction_B$ is non-constant, $F \restriction_{B^\rho}$ is nonconstant, therefore there is a literal of T_{t+1} not set by B^ρ. However, $T_{t+1} \restriction_{\kappa_t} = 1$ and thus there exists

$l \in T_{t+1} \setminus B^\rho$. Because B^ρ matches its ones, there exists $l \in \widetilde{T_{t+1}} \setminus B^\rho$. Because T_{t+1} is a term of size at most r, $\widetilde{T_{t+1}}$ has size at most $2r$. Therefore, $l_{t+1} \in \widetilde{T_{t+1}} \setminus B^\rho$ with probability at least $1/2r$. ∎

Now we can show that a random L-presimplification is unlikely to be s-bad for F.

Proof: (of theorem 88) Let M, N, r, s, L be given with $L > 2rs$. Let ρ be a randomly selected L-presimplification and let κ be a randomly selected $2rs$-extension of ρ. Lemmas 90 and 91 tell us that

$$\begin{aligned} \Pr_{\rho,\kappa}[\kappa \text{ is an } s\text{-encoding of } F \text{ wrt } \rho \mid \rho \text{ is } s\text{-bad for } F] &\geq \tfrac{1}{L^{Crs}} \\ \Pr_{\rho,\kappa}[A_{F,s}(\kappa) \subseteq \tilde{\kappa} \setminus \rho \mid \kappa \text{ is an } s\text{-encoding of } F \text{ wrt } \rho] &\geq \left(\tfrac{1}{2r}\right)^s \end{aligned}$$

Combining these two inequalities gives us

$$\Pr_{\rho,\kappa}[A_{F,s}(\kappa) \subseteq \tilde{\kappa} \setminus \rho \mid \rho \text{ is } s\text{-bad for } F] \geq \left(\tfrac{1}{2r}\right)^s \tfrac{1}{L^{Crs}}$$

By lemma 89, we have that

$$\begin{aligned} \left(\tfrac{2rs}{K}\right)^s &\geq \Pr_{\rho,\kappa}[\mathrm{DECODE}(\kappa) \subseteq \tilde{\kappa} \setminus \rho] \\ &\geq \Pr_{\rho,\kappa}[\mathrm{DECODE}(\kappa) \subseteq \tilde{\kappa} \setminus \rho \mid \rho \text{ is } s\text{-bad for } F] \Pr_\rho[\rho \text{ is } s\text{-bad for } F] \\ &\geq \left(\tfrac{1}{L^{Cr}}\right)^s \left(\tfrac{1}{2r}\right)^s \Pr_\rho[\rho \text{ is } s\text{-bad for } F] \end{aligned}$$

Therefore,

$$\left(\frac{4r^2 s L^{Cr}}{K}\right)^s \geq \Pr_\rho[\rho \text{ is } s\text{-bad for } F]$$

∎

Building Decision Trees Using Maximal Independent Sets

The construction works by making a small set of queries for each variable that appears in the independent set. Maximality guarantees that each term outside of the independent set is either falsified or shortened by the answers to these queries. First, we define the queries associated with each literal.

Definition VI.G.13 *The* **query for $\mathbf{X_i}$** *is Value(i). The* **query for $\neg\mathbf{X_i}$** *is Value(i). The* **queries for $\mathbf{Y_e}$**, *are Match(p), for each $p \in e \cap V_r$, and Match(I), for each $I \in e \cap U_r$.*

Lemma 92 *Let $\mathcal{V}$ be a universe, let B be a consistent, closed subset of BLits($\mathcal{U}$) that matches its ones and let $l_1, l_2 \in$ BLits($\mathcal{V}$) be inconsistent literals, both of which are consistent with B. There is a query Q of l_1, so that for every answer $A \in \mathcal{ANS}^{\mathcal{V}}(Q)$, either A falsifies l_2 or A satisfies some $l' \in \widetilde{l_2} \setminus B$.*

The proof of lemma 92 is a straightforward case analysis on l_1 and l_2.

Theorem 93 *Let $\mathcal{U}$ be an (M, N) universe, let F be an r-DNF in the literals BLits($\mathcal{U}$), and let ρ be a presimplification for $\mathcal{U}$ that is not s-bad for F. Then $\Sigma_\rho(F)$ has decision tree of height at most $4m^2r^4s^2$. Moreover, this decision tree strongly represents F.*

Proof: For a presimplification ρ which is not s-bad for F, and a closed partial assignment to Vars($\mathcal{U}$) which matches its ones, B, we build a decision tree strongly representing $\Sigma_\rho(F) \restriction_B$ recursively as follows. The decision tree for $\Sigma_\rho(F)$, $T_{\Sigma_\rho(F),B}$, is constructed as follows:

If for some term C of F, $\Sigma_\rho(C) \restriction_B = 1$, then $T_{\Sigma_\rho(F),B}$ is a leaf labeled with 1.
If for all terms C of F, $\Sigma_\rho(C) \restriction_B = 0$, then $T_{\Sigma_\rho(F),B}$ is a leaf labeled with 0.
Otherwise

Choose $C_1, \ldots, C_t$ to be a maximal B-independent set for F w.r.t. ρ

Let T_0 be the decision tree which, makes the queries for $\bigcup_{i=1}^{t} \Sigma_\rho(C_i) \restriction_B$, and underneath each branch, makes a matching query for every monomial satisfied by that branch.

$T_{\Sigma_\rho(F),B}$ is the tree obtained by taking a copy of T_0, and underneath each branch $B' \in \mathrm{Br}(T_0)$, placing a copy of $T_{\Sigma_\rho(F),B\cup B'}$

This construction can proceed for at most $2r$ iterations. We will show that for each term C of F that does not belong to the maximal independent set,

either $\Sigma_\rho(C)$ is falsified or the size of $\widetilde{\Sigma_\rho(C)}$ decreases by one after the query phase. Because B matches its ones, whenever $\widetilde{\Sigma_\rho(C)} \restriction_B$ is constant, $\Sigma_\rho(C) \restriction_B$ is constant. Therefore, because terms have skeletons of size at most $2r$, there are at most $2r$ iterations.

Let C be a term of F so that $\Sigma_\rho(C) \restriction_B$ is non-constant and C does not belong to the maximal B-independent set. In the case that there is a term C_i in the maximal independent set so that $\widetilde{C} \cap \widetilde{C_i} \not\subseteq B^\rho$. By lemma 87, $\widetilde{\Sigma_\rho(C)} \cap \widetilde{\Sigma_\rho(C_i)} \not\subseteq B$. Choose $l \in \widetilde{\Sigma_\rho(C)} \cap \widetilde{\Sigma_\rho(C_i)} \setminus B$. When the l is queried, $\Sigma_\rho(C)$ is falsified or the size of $\widetilde{\Sigma_\rho(C)}$ decreases. Consider the case when there is no extension of ρ that satisfies $C_1 \cup \ldots \cup C_t \cup C$. Because each term has size at most r, and $r(s+1) << L$, there is some C_i which is inconsistent with C. Because Σ_ρ maps inconsistent literals to inconsistent literals, $\Sigma_\rho(C)$ and $\Sigma_\rho(C_i)$ are inconsistent. Choose $l_1 \in \Sigma_\rho(C_i)$ and $l_2 \in \Sigma_\rho(C)$ so that l_1 and l_2 are inconsistent. Because $\Sigma_\rho(C) \restriction_B$ and $\Sigma_\rho(C_i) \restriction_B$ are both non-constant, l_1 and l_2 are both consistent with, but unset by, B. By lemma 92, there is $l' \in \widetilde{l_2} \setminus B$ so that for each answer to the queries for l, either l' is satisfied or l_2 is falsified. Therefore, $\Sigma_\rho(C)$ becomes falsified or the size of $\widetilde{\Sigma_\rho(C)}$ decreases.

Each independent set has size at most s because ρ is not s-bad for F, and because F is an r-DNF, each independent set contains at most rs literals. Therefore, each iteration makes at most mrs many queries. Excluding the matching queries made at the end of each phases, at most $2mr^2s$ queries are made. Because the non-matching phases can create at most $(2mr^2s)^2$ many satisfied monomials, the matching phases make at most $4m^2r^4s^2$ queries. ∎

Proof:(of lemma 92) If $l_2 = X_i$, then the only possibility is that $l_1 = \neg X_i$ and the claim clearly holds.

If $l_2 = \neg X_i$, then either $l_1 = X_i$ or $l_1 = Y_e$ with $i \in I,\ I \in e$. The former case is trivial, and in the latter case, the answers to the query Match(I) will set X_i to 0 or 1.

If $l_2 = Y_e$ then either $l_1 = \neg X_i$, with $i \in I$, $I \in e$, or $l_1 = Y_f$, with $e \perp f$. In the former case, there is a half-star $\{i, j\} \in e$; let $I = \{i, j\}$. Because both X_i and $\neg X_i$ are consistent with B, neither is set by B, and the query Value(i) will either falsify l_2 or satisfy the literal $X_i \in \widetilde{l_2} \setminus B$. Finally, consider the case of $l_2 = Y_e$ and $l_1 = Y_f$ with $e \perp f$. If there exists $I \in e \cap f \cap U_r$, then because B matches its ones, we must have that there exists $i \in I$, X_i is unset by B. The query Match(I) will set X_i. If $e \cap f \subseteq V_r$, then choose $p \in e \cap f$. The query Match(p) will satisfy or falsify l_2, and in either case, $\widetilde{l_2} = \{l_2\} = \{Y_e\}$.

■

VI.H k-Evaluations

A k-evaluation of a proof is a mapping associating a height $\leq k$ decision tree to each subformula of the refutation.

Definition VI.H.1 *Let $\mathcal{U}$ and $\mathcal{V}$ be universes. Let Γ be a set of formulas in Vars($\mathcal{U}$) which is closed under subformulas. A* **k-evaluation for Γ in $\mathcal{V}$** *is a mapping $\mathbb{T}$ from Γ to $\mathcal{T}(\mathcal{V}, k)$, $A \mapsto \mathbb{T}_A$, with the following properties:*

$Br(\mathbb{T}_0) = Br_0(\mathbb{T}_0)$
for each clause $H \in MIS_m(\mathcal{U})$, $Br(\mathbb{T}_H) = Br_1(\mathbb{T}_H)$
for $A = \neg B$, $\mathbb{T}_A = (\mathbb{T}_B)^c$
for $A = \bigvee_{i=1}^{W} B_i$, $\mathbb{T}_A$ *strongly represents* $\bigvee_{i=1}^{W} \bigvee_i Br_1(\mathbb{T}_{B_i})$

Definition VI.H.2 *Let $\mathbb{T}$ be a k-evaluation for Γ in $\mathcal{V}$. For $A \in \Gamma$, we say that* **A $\mathbb{T}$-evaluates to 1** *if every leaf of $\mathbb{T}_A$ is labeled with 1, and that* **A $\mathbb{T}$-evaluates to 0** *if every leaf of $\mathbb{T}_A$ is labeled with 0.*

Therefore we say, for every k-evaluation $\mathbb{T}$, the constant 0 $\mathbb{T}$-evaluates to 0, and each $H \in \mathrm{MIS}_m(\mathcal{U})$ $\mathbb{T}$-evaluates to 1.

In subsection VI.H.1 we construct a k-evaluation from a small proof, using the switching lemma proved in section VI.G. In subsection VI.H.2, we prove some proof theoretical properties of k-evaluations that will be needed in section VI.I.

VI.H.1 Building a k-Evaluation

Theorem 94 *Let c be a positive integer. There exist constants k and ϵ so that for N sufficiently large, for any (M, N) universe $\mathcal{U}$ if there exists a refutation $\mathcal{R}$ of GIS($\mathcal{U}$) of size N^c, then there is a k-evaluation for $\mathcal{R}$ in $\mathcal{V}$ where $\mathcal{V}$ is an (M, N^ϵ) universe.*

Iterated application of the switching lemma can be used to create a k-evaluation of a refutation, in substantially smaller universe. The method of this construction is similar to that in [59].

We begin by constructing a k-evaluation for the formulas of depth ≤ 1 that appear in the proof, and then we repeatedly apply the switching lemma to obtain a k-evaluation for the entire proof.

Definition VI.H.3 *The* **tree for 0, $\mathbf{T_0}$,** *is a single node labeled* 0. *The* **tree for 1, $\mathbf{T_1}$,** *is a single node labeled* 1.

Definition VI.H.4 *Let $\mathcal{U}$ be a universe. For variables $v \in Vars(\mathcal{U})$ we define* **the tree for v over $\mathcal{U}$, $\mathbf{T}^{\mathcal{U}}_{\mathbf{v}}$,** *as follows: The root is labeled with Q_v, and underneath each arc L, the leaf is labeled with* 1 *if and only if $v \in L$, otherwise the leaf is labeled with* 0.

Definition VI.H.5 *Let $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$ be universes, let Γ be a subformula-closed set of formulas in Vars($\mathcal{U}$) and let $\mathbb{T}$ be a k-evaluation of Γ in $\mathcal{V}$. For a simplification $\Sigma : \mathcal{V} \to \mathcal{W}$, we define* **the simplification of $\mathbb{T}$ by Σ, $\Sigma(\mathbb{T})$,** *to be the mapping from Γ to $\mathcal{T}(k, \mathcal{W})$ defined by $(\Sigma(\mathbb{T}))_A = \Sigma(\mathbb{T}_A)$.*

Lemma 95 *Let $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$ be universes, let Γ be a subformula-closed set of formulas in Vars($\mathcal{U}$) let $\mathbb{T}$ be a k-evaluation of Γ in $\mathcal{V}$, and let Σ be a simplification from $\mathcal{V}$ to $\mathcal{W}$. $\Sigma(\mathbb{T})$ is a k-evaluation of Γ in $\mathcal{W}$.*

Proof:By lemma 75, $\Sigma(\mathbb{T})$ maps Γ to decision trees of height $\leq k$ over $\mathcal{W}$. Because $\mathbb{T}$ is a k-evaluation, $\mathrm{Br}(\mathbb{T}_0) = \mathrm{Br}_0(\mathbb{T})$ and therefore, by corollary 77, $\mathrm{Br}(\Sigma(\mathbb{T}_0)) = \mathrm{Br}_0(\Sigma(\mathbb{T}_0))$. For each $H \in \mathrm{MIS}_m(\mathcal{U})$, $\mathrm{Br}(\mathbb{T}_H) = \mathrm{Br}_1(\mathbb{T}_H)$ and thus by corollary 77, $\mathrm{Br}(\Sigma(\mathbb{T}_H)) = \mathrm{Br}_1(\Sigma(\mathbb{T}_H))$. If $A = \neg B$, then by corollary 77, $(\Sigma(\mathbb{T}))_{\neg B} = \Sigma(\mathbb{T}_{\neg B}) = \Sigma((\mathbb{T}_B)^c) = (\Sigma(\mathbb{T}_B))^c$. If $A = \bigvee B_i$, then $\mathbb{T}_A$ strongly represents $\bigvee_i \mathrm{Br}_1(\mathbb{T}_{B_i})$. By lemma 78 and corollary 77, $\Sigma(\mathbb{T}_A)$ strongly represents $\Sigma(\bigvee_i \mathrm{Br}_1(\mathbb{T}_{B_i})) = \bigvee_i \mathrm{Br}_1(\Sigma(\mathbb{T}_{B_i}))$. ∎

Lemma 96 *Let $\mathcal{U}$, $\mathcal{V}$ be universes and let Σ be a simplification from $\mathcal{U}$ to $\mathcal{V}$. For every $v \in Vars(\mathcal{U})$, $\Sigma(T_v^{\mathcal{U}}) = T^{\mathcal{V}}_{\Sigma(v)}$.*

Proof: It easy to check that when $\Sigma(v)$ is a constant, $\Sigma(T_v^{\mathcal{U}})$ is a single node labeled with $\Sigma(v)$. Consider the case when $\Sigma(v)$ is non-constant. The root of $\Sigma(T_v^{\mathcal{U}})$ is labeled by $\Sigma(Q_v) = Q_{\Sigma(v)}$. By lemma 72, $\Sigma(\mathcal{ANS}^{\mathcal{U}}(Q_v)) = \mathcal{ANS}^{\mathcal{V}}(\Sigma(Q_v))$, so the labels on the arcs are correct. In the tree in $T_v^{\mathcal{U}}$, under the edge labeled L there is a one if and only if $v \in L$, and there is a zero underneath L if and only if L is inconsistent with v. Because Σ maps inconsistent literals to inconsistent literals, if L leads to 0 then either $\Sigma(L) = 0$ or $\Sigma(v) \notin \Sigma(L)$. Therefore, there is a zero underneath the edge labeled $\Sigma(L)$ (in $T^{\mathcal{V}}_{\Sigma(v)}$) only if $\Sigma(v) \in L$. Therefore, $\Sigma(T_v^{\mathcal{U}}) = T^{\mathcal{V}}_{\Sigma(v)}$. ∎

Definition VI.H.6 *Let $\mathcal{R}$ be a set of formulas and let d be a positive integer. The set of formulas in $\mathcal{R}$ of depth $\leq d$ is denoted by $\mathcal{R}_d$.*

Lemma 97 *Let c be a positive integer. There exist constants k and ϵ so that for N sufficiently large, for any (M, N) universe $\mathcal{U}$ if there exists a refutation $\mathcal{R}$ of GIS($\mathcal{U}$) of size N^c, then there is a k-evaluation for $\mathcal{R}$ in $\mathcal{V}$ where $\mathcal{V}$ is an (M, N^ϵ) universe.*

Proof: Let c, d be given. Let M, N be "sufficiently large" (defined later). Let $\mathcal{U}$ be a universe with $w(\mathcal{U}) = N$, and let $\mathcal{R}$ be a refutation of GIS($\mathcal{U}$) .

For each $v \in \mathrm{Vars}(\mathcal{U})$ $\mathbb{T}^0$ maps v and $\neg v$ to $\mathbb{T}_v^{\mathcal{U}}$ and $(\mathbb{T}_v^{\mathcal{U}})^c$, respectively. $\mathbb{T}^0$ also maps 0 to T_0 and 1 to T_1. Clearly $\mathbb{T}^0$ is a 1-evaluation of $\mathcal{R}_0$ in $\mathcal{U}$.

Notice that for any $A \in \mathcal{R}_1 \setminus \mathcal{R}_0$, if $A = \bigvee B_j$ then $\bigvee_j \mathrm{Br}_1\left(\mathbb{T}_{B_j}\right)$ is a DNF of width at most 5. Apply theorem 79 with $5k$ and c to obtain ϵ and k. Let N be large enough to meet the conditions of the switching lemma, moreover, large enough that $2k + 2 \leq N^{\epsilon}$. Because there are at most N^c formulas in $\mathcal{R}_1$, there exists a simplification Σ of $\mathcal{U}$ into some (M, N^{ϵ}) universe $\mathcal{V}$.

We define the mapping $\mathbb{T}$ from $\mathcal{R}_1$ into $\mathcal{T}(k, \mathcal{V})$ as follows: for $A \in \mathcal{R}_0$, let $\mathbb{T}_A$ be $\Sigma\left(\mathbb{T}_A^0\right)$, for $\neg B \in \mathcal{R}_1 \setminus \mathcal{R}_0$, let $\mathbb{T}_{\neg B} = (\Sigma(\mathbb{T}_B^0))^c$, and for $A = \bigvee B_j \in \mathcal{R}_1 \setminus \mathcal{R}_0$, let $\mathbb{T}_A$ be the lexicographically first decision tree of height $\leq k$ strongly representing $\Sigma(\bigvee_j \mathrm{Br}_1(\mathbb{T}_{B_j}^0))$

The condition $\mathrm{Br}(\mathbb{T}_0) = \mathrm{Br}_0(\mathbb{T}_0)$ is met because $\mathbb{T}_0 = \Sigma(\mathbb{T}_0^0)$ and $\mathrm{Br}(\mathbb{T}_0^0) = \mathrm{Br}_0(\mathbb{T}_0^0)$. For $A = \neg B$, $\mathbb{T}_A = (\mathbb{T}_B)^c$. If $A = \bigvee B_j$, by construction $\mathbb{T}_A$ strongly represents $\Sigma(\bigvee_j \mathrm{Br}_1\left(\mathbb{T}_{B_j}^0\right))$, which by lemma 78 , equals $\bigvee_j \mathrm{Br}_1\left(\Sigma\left(\mathbb{T}_{B_j}^0\right)\right) = \bigvee_j \mathrm{Br}_1\left(\mathbb{T}_{B_j}\right)$.

We now show that for all $H \in \mathrm{MIS}_m(\mathcal{U})$, H $\mathbb{T}$-evaluates to 1. Let $H \in \mathrm{MIS}_m(\mathcal{U})$ be given. Recall that H is a clause, $\bigvee_i l_i$, and because Σ is a simplification, $\Sigma(H)$ is either 1, $X_i \vee \neg X_i$ or an element of $\mathrm{MIS}_m(\mathcal{V})$.

If $\Sigma(H) = 1$, then for some l_i, $\Sigma(l_i) = 1$ so $\Sigma(\mathbb{T}_{l_i}^0) = \Sigma(T_{l_i}^{\mathcal{U}}) = 1$. Let $\beta \in \mathrm{Br}(\mathbb{T}_H)$ be given. Because $\mathbb{T}_H$ strongly represents $\bigvee_i \Sigma(\mathrm{Br}_1(\mathbb{T}_{l_i}^0))$, if β leads to a 0 then β is inconsistent with the empty assignment. Therefore, $\mathrm{Br}(\mathbb{T}_H) = \mathrm{Br}_1(\mathbb{T}_H)$.

If $\Sigma(H) = w \vee \neg w$, then we may choose literals l_k, l_j of H so that $\Sigma(l_k) = w$ and $\Sigma(l_j) = \neg w$. Let $\beta \in \mathrm{Br}(\mathbb{T}_H)$ be given. If β leads to a 0, then because $\mathbb{T}_H$ strongly represents $\bigvee_i \mathrm{Br}_1(\Sigma(\mathbb{T}_{l_i}^0))$, β must be inconsistent with all branches in $\mathrm{Br}_1\Sigma(T_{l_k}^{\mathcal{U}}) \cup \mathrm{Br}_1\Sigma(T_{l_j}^{\mathcal{U}}) = \mathrm{Br}_1 T_w^{\mathcal{U}_1}) \cup \mathrm{Br}_1\Sigma(T_{\neg w}^{\mathcal{U}_1}) = \mathrm{Br}(T_w^{\mathcal{U}_1})$. However, because $||\beta|| + 2k < N^{\epsilon}$, by lemma 71, this impossible and therefore, $\mathrm{Br}(\mathbb{T}_H) = \mathrm{Br}_1(\mathbb{T}_H)$.

Consider the case when $\Sigma(H) \in \mathrm{MIS}_m(\mathcal{V})$. Let $\pi \in \mathrm{Br}(\mathbb{T}_H)$ be given, and suppose for the sake of contradiction that $\pi \in \mathrm{Br}_0(\mathbb{T}_H)$. Because $\mathbb{T}_H$ is a height k-decision tree, π is closed and $||\pi|| \leq 2k \leq w(\mathcal{V}) - 2$, there exists a consistent,

closed extension σ of π so that σ satisfies l and $||\sigma|| \leq 2k+2$. Choose a literal l_j of H so that $\Sigma(l_j) = l$. Note that $\mathbb{T}_{l_j} = T_l^{\mathcal{U}_1}$. Because $||\sigma|| \leq 2k+2 \leq w(\mathcal{V}) - 2$, we may choose $\beta \in \mathrm{Br}_1(T_l)$ that is consistent with σ. However, $\mathbb{T}_H$ strongly represents $\bigvee_i \mathrm{Br}_1(\Sigma(\mathbb{T}_{l_i}))$, π must be inconsistent with β, contradiction. Therefore, $\pi \in \mathrm{Br}_1(\mathbb{T}_H)$ and H $\mathbb{T}$-evaluates to 1. ∎

Lemma 98 *Let c, d, k, ϵ be positive integers. There exist constants k' and ϵ' so that for N sufficiently large, for any (M, N) universe $\mathcal{U}$ if there exists a refutation $\mathcal{R}$ of GIS($\mathcal{U}$) of size N^c and a k-evaluation of $\mathcal{R}_d$ over an (M, N^ϵ) universe $\mathcal{V}$, then there exists a k'-evaluation $\mathbb{T}'$ for $\mathcal{R}_{d+1}$ over $\mathcal{V}'$ where $\mathcal{V}'$ is an $(M, N^{\epsilon\cdot\epsilon'})$ universe.*

Proof: Let c, d, k, ϵ be given with $d \geq 1$. Let M, N be "sufficiently large" (defined later). Let $\mathcal{U}$ be an (M, N) universe, let $\mathcal{R}$ be a refutation of GIS($\mathcal{U}$), and let a k-evaluation of $\mathcal{R}_d$ over an (M, N^ϵ) universe $\mathcal{V}$.

Notice that for any $A \in \mathcal{R}_{d+1} \setminus \mathcal{R}_d$, if $A = \bigvee B_j$ then $\bigvee \mathrm{Br}_1\left(\mathbb{T}_{B_j}\right)$ is a DNF of width at most $5k$ in the variables BLits($\mathcal{V}$).

Let N be large enough so that N^ϵ meets the hypotheses of the switching lemma 79 (with c and DNF width $5k$) and choose ϵ', k' as guaranteed. Because there are at most N^c formulas in $\mathcal{R}_{d+1}$, there exists a simplification Σ from $\mathcal{U}$ to some $(M, N^{\epsilon\cdot\epsilon'})$ universe $\mathcal{V}'$.

We define the mapping $\mathbb{T}'$ from $\mathcal{R}_{d+1}$ into $\mathcal{T}(k', \mathcal{V}'$ as follows: for $A \in \mathcal{R}_d$, let $\mathbb{T}'_A$ be $\Sigma\left(\mathbb{T}_A\right)$, for $\neg B \in \mathcal{R}_{d+1} \setminus \mathcal{R}_d$, let $\mathbb{T}'_{\neg B} = (\Sigma(\mathbb{T}_B))^c$, and for $A = \bigvee B_j \in \mathcal{R}_{d+1} \setminus \mathcal{R}_i$, let $\mathbb{T}'_A$ be lexicographically first decision tree of height $\leq k'$ strongly representing $\Sigma(\bigvee_j \mathrm{Br}_1(\mathbb{T}_{B_j}))$

We now show that $\mathbb{T}'$ is a k' evaluation for $\mathcal{R}_{d+1}$ over $\mathcal{V}_{d+1}$. Lemma 95 shows that $\mathbb{T}'$ is a k'-evaluation for $\mathcal{R}_d$. Consider $A \in \mathcal{R}_{d+1} \setminus \mathcal{R}_d$. If $A = \neg B$, then $\mathbb{T}_A^{d+1} = \left(\mathbb{T}_B^d\right)^c$. If $A = \bigvee B_j$, by construction $\mathbb{T}_A^{d+1}$ strongly represents $\Sigma(\bigvee_j \mathrm{Br}_1\left(\mathbb{T}_{B_j}^d\right))$, which by lemma 78, equals $\bigvee_j \mathrm{Br}_1\left(\Sigma\left(\mathbb{T}_{B_j}^d\right)\right) = \bigvee_j \mathrm{Br}_1\left(\mathbb{T}_{B_j}^{d+1}\right)$. ∎

Combining lemmas 97 and 98 gives us theorem 94.

VI.H.2 k-Evaluations and Refutations

Lemma 99 *Let $\mathbb{T}$ be a k-evaluation for Γ in $\mathcal{V}$. If $4k < w(\mathcal{V})$ then every instance of an axiom $A \vee \neg A$ in Γ $\mathbb{T}$-evaluates to 1.*

Proof: Let $A \vee \neg A$ be some axiom instance in Γ. Suppose, for the sake of contradiction that there is some $\pi \in \mathrm{Br}_0(\mathbb{T}_{A \vee \neg A})$. Because $\mathbb{T}_{A \vee \neg A}$ strongly represents $\mathrm{Br}_1(\mathbb{T}_A) \vee \mathrm{Br}_1(\mathbb{T}_{\neg A}) = \mathrm{Br}_1(\mathbb{T}_A) \vee \mathrm{Br}_0(\mathbb{T}_A) = \mathrm{Br}(\mathbb{T}_A)$, π is inconsistent with every branch of $\mathbb{T}_A$. On the other hand, because $2Ht(\mathbb{T}_A) + |\pi| \leq 4k < w(\mathcal{V})$, by lemma 71, there exists $\sigma \in \mathrm{Br}(\mathbb{T}_A)$ consistent with π; contradiction. ∎

Theorem 100 *Let $\mathcal{R}$ be a refutation of GIS($\mathcal{U}$) in the system $\mathcal{F}_p$. Let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ in $\mathcal{V}$ where k be a positive integer so that $4k < w(\mathcal{V})$. There exists an instance of a counting axiom in $\mathcal{R}$ that does not $\mathbb{T}$-evaluate to 1.*

Proof: Suppose for the sake of contradiction that every instance of a counting axiom $\mathbb{T}$-evaluates to 1. We will show by induction that every line of the refutation must $\mathbb{T}$-evaluate to 1, which contradicts the fact that the final line of the refutation (the constant 0) must $\mathbb{T}$-evaluate to 0.

For the base cases, every clause from $\mathrm{MIS}_m(\mathcal{U})$ $\mathbb{T}$-evaluates to 1 by definition, and by lemma 99, every instance of an axiom schema, $A \vee \neg A$ $\mathbb{T}$-evaluates to 1.

For the induction step, consider an inference in $\mathcal{R}$.

$$\frac{A_1(B_1/p_1,\ \ldots,\ B_m/p_m), \ldots, A_l(B_1/p_1, \ldots, B_m/p_m)}{A_0(B_1/p_1, \ldots, B_m/p_m)}$$

and assume that for all $i \in [l]$, $A_i(B_1/p_1, \ldots,\ B_m/p_m)$, $\mathbb{T}$-evaluates to 1. Note that $l \leq 2$ because all the rules in our Frege system have fan-in two.

Let $\Gamma_0 = \{G_0, \ldots, G_t\}$ be the set of distinct subformulas of $A_0(p_1, \ldots, p_m), \ldots, A_l(p_1, \ldots, p_m)$. Furthermore, let $G_i = A_i$ for $i \leq l$, and for each $0 \leq i \leq t$, let $F_i = G_i\,[B_1/p_1, \ldots, B_m/p_m]$. Note that $F_0 = A_0\,[B_1/p_1, \ldots, B_m/p_m]$.

Let $\pi_0 \in \mathrm{Br}(T_{F_0})$ be given. Because $4k < w(\mathcal{U})$, we can repeatedly apply lemma 71 to find $\pi_i \in \mathrm{Br}(\mathbb{T}_{F_i})$ consistent with $\bigcup_{j=0}^{i-1} \pi_j$. Let $\pi = \bigcup_{j=0}^{s} \pi_j$.

Clearly, for all G_i, $\bigvee \mathrm{Br}_1(\mathbb{T}_{G_i}) \restriction_\pi$ is the constant 0 or 1. Define $V : \Gamma_0 \to \{0,1\}$ by $V(F_i) = \mathrm{Br}_1(\mathbb{T}_A) \restriction_\pi$. By the definition of k-evaluations, V is a consistent truth assignment to Γ, and by assumption, $V(A_1) = \ldots = V(A_m) = 1$. Because the rules of inference are sound, $V(A_0) = 1$. Therefore, $\mathbb{T}_{A_0} \restriction_{\pi_0} = \mathbb{T}_{A_0} \restriction_\pi = 1$. Because π_0 was an arbitrary branch of $\mathbb{T}_{A_0}$, the tree has every branch labeled with 1.

■

VI.I Nullstellensatz Refutation from k-Evaluation

Theorem 101 *Let $\mathcal{U}$ and $\mathcal{V}$ be universes, let $\mathcal{R}$ be a refutation of $MIS_m(\mathcal{U})$, and let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ in $\mathcal{V}$. If $8k+2 \leq w(\mathcal{V})$ then there is a degree $\leq 3mk$ Nullstellensatz refutation of $AMIS_m(\mathcal{W})$, where $\mathcal{W}$ is an $(M, N-2k)$ universe.*

The proof of theorem 101 follows from a sequence of lemmas in which we first use the k-evaluation to construct a family of highly symmetric decision trees called a generic system, and then we use the generic system to construct a Nullstellensatz refutation of $\mathrm{AMIS}_m(\mathcal{V})$.

Definition VI.I.1 *A* **generic system of height h over $\mathcal{U}$** *is a collection of K decision trees in $\mathcal{U}$, $\{T_i \mid i \in [K]\}$, with leaf labels that are m-subsets of $[K]$ so that:*

1. *Each tree has height at most h.*
2. *Each branch in T_i has a leaf label e with $i \in e$.*
3. *For all $e \in [K]^m$, and all $i, j \in e$, $Br_e(T_i) = Br_e(T_j)$.*

Observation: Let T_i, $i \in [K]$, be a generic system. For each partial assignment β, $|\{i \in [K] \mid \beta \in \mathrm{Br}(T_i)\}|$ is divisible by m.

In subsection VI.I.1, we use a k-evaluation to construct a generic system, lemma 106. In subsection VI.I.2, we a generic system to construct a Nullstellensatz refutation, lemma 109. Finally, in subsection VI.I.3 we combine these results to prove theorem 101.

VI.I.1 From k-Evaluation to Generic System

Lemma 102 *Let $\mathcal{U}$ and $\mathcal{V}$ be universes, let $\mathcal{R}$ be a refutation of $MIS_m(\mathcal{U})$, and let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ of $\mathcal{V}$. If $4k+2 \leq w(\mathcal{V})$ then there exists an instance of a counting axiom A in $\mathcal{R}$, and k-evaluation $\mathbb{T}'$ so that A $\mathbb{T}'$-evaluates to 0, where $\mathbb{T}'$ is a k-evaluation over an $(M, N-2k)$ universe $\mathcal{W}$.*

Proof: By lemma 100, we may choose an instance of a counting axiom $A \in \mathcal{R}$ so that A does not $\mathbb{T}$-evaluate to 1. Choose $\pi \in \mathrm{Br}_0(T_A)$. Apply lemma 80 and choose a $2k$-simplification ρ so that $\pi \subseteq \rho$. Let $\mathcal{W} = \Sigma_\rho(\mathcal{V})$, and let $\mathbb{T}' = \Sigma_\rho(\mathbb{T})$. ■

Lemma 103 *Let $\mathbb{T}$ be a k-evaluation over Σ where Σ is a simplification from $\mathcal{U}$ to $\mathcal{W}$ and $4k < w(\mathcal{W})$. If $A = \bigvee_i F_i$ $\mathbb{T}$-evaluates to 0, then for each i, F_i $\mathbb{T}$-evaluates to 0.*

Proof: Suppose for the sake of contradiction that there exists $\beta \in \mathrm{Br}_1(T_{F_i})$. Because $2\mathrm{Ht}(\mathbb{T}_A) + ||\beta|| \leq 4k < w(\mathcal{W})$, by lemma 71 we may choose $\tau \in \mathrm{Br}(\mathbb{T}_A)$ consistent with β. Because $\mathbb{T}_A$ strongly represents $\bigvee_i \mathrm{Br}_1(\mathbb{T}_{F_i})$, $\tau \in \mathrm{Br}_1(\mathbb{T}_A)$, contradiction to the assumption that A $\mathbb{T}$ evaluates to 0. ■

Lemma 104 *Let $\mathcal{U}$ and $\mathcal{W}$ be universes, let $\mathcal{R}$ be a refutation of $MIS_m(\mathcal{U})$, and let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ in $\mathcal{W}$ with $w(\mathcal{W}) > 6k$. If $A = \bigvee_{i\in[K]} \neg \left(\bigvee_{e \ni i} F_e\right) \vee \bigvee_{e \perp f} \neg (\neg F_e \vee \neg F_f)$ is an instance of a counting axiom in $\mathcal{R}$ that $\mathbb{T}$-evaluates to 0, then for each $i \in [K]$ and $\pi \in Br_1(\mathbb{T}_{\bigvee F_i})$ there is exactly one $e \ni i$ so that there exists $\sigma \in Br_1(\mathbb{T}_{F_e})$ with $\pi \supseteq \sigma$.*

Proof: For each $e \in [K]^m$, let $T_e = \mathbb{T}_{F_e}$, and for each $i \in [K]$, let $T_i = \mathbb{T}_{\bigvee_{e \ni i} F_e}$. By lemma 103, each $\bigvee_{e \ni i} F_e$ $\mathbb{T}$-evaluates to 1, and each $\neg F_e \vee \neg F_f$ $\mathbb{T}$-evaluates to 1.

We show that if $e, f \in [K]^m$ with $e \perp f$ then there are no mutually consistent branches in $\mathrm{Br}_1(T_e)$ and $\mathrm{Br}_1(T_f)$. Suppose that $\sigma_1 \in \mathrm{Br}_1(T_e)$ and $\sigma_2 \in \mathrm{Br}_1(T_f)$ were consistent. Because $2\mathrm{Ht}(\mathbb{T}_{\neg F_e \vee \neg F_f}) + ||\sigma_1 \cup \sigma_2|| \leq 6k < w(\mathcal{W})$, by lemma 71, there must exist $\tau \in \mathrm{Br}\left(\mathbb{T}_{\neg F_e \vee \neg F_f}\right)$ consistent with $\sigma_1 \cup \sigma_2$. Because $\neg F_e \vee \neg F_f$ $\mathbb{T}$-evaluates to 1, $\tau \in \mathrm{Br}_1\left(\mathbb{T}_{\neg F_e \vee \neg F_f}\right)$. Because $\mathbb{T}_{\neg F_e \vee \neg F_f}$ strongly represents $\mathrm{Br}_1(\mathbb{T}_{\neg F_e}) \cup \mathrm{Br}_1(\mathbb{T}_{\neg F_f})$, τ is extends some $\beta \in \mathrm{Br}_0(\mathbb{T}_{F_e}) \cup \mathrm{Br}_0(\mathbb{T}_{F_f})$. This is impossible because $\sigma_1 \in \mathrm{Br}_1(T_e)$ and $\sigma_2 \in \mathrm{Br}_1(T_f)$ and $\sigma_1 \cup \sigma_2$ is consistent with τ.

Now we show that for each $i \in [K]$ and $\pi \in \mathrm{Br}(T_i)$ there is exactly one $e \ni i$ so that there exists $\sigma \in \mathrm{Br}_1(T_e)$ with $\pi \supseteq \sigma$. Let $i \in [K]$ and $\pi \in \mathrm{Br}(T_i)$ be given. Because $\mathrm{Br}(T_i) = \mathrm{Br}_1(T_i)$, and T_i strongly represents $\bigcup_{e \ni i} \mathrm{Br}_1(T_e)$, there exists $e \ni i$ and $\sigma \in \mathrm{Br}_1(T_e)$ so that $\pi \supseteq \sigma$. By the preceding paragraph, there cannot be another $f \ni i$ with $\sigma' \in \mathrm{Br}_1(T_f)$ so that $\pi \supseteq \sigma'$ because that σ and σ' would be consistent. Therefore, for each $\pi \in \mathrm{Br}(T_i)$, there exists exactly one $e \ni i$ so that there exists $\sigma \in \mathrm{Br}_1(T_e)$ with $\pi \supseteq \sigma$. ∎

Lemma 105 *Let $\mathcal{U}$ and $\mathcal{W}$ be universes, let $\mathcal{R}$ be a refutation of $MIS_m(\mathcal{U})$, and let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ in $\mathcal{W}$ with $w(\mathcal{W}) \geq 6k+2$. If there exists an instance of a counting axiom in $\mathcal{R}$ that $\mathbb{T}$-evaluates to 0, then there exists is a generic system $\{G_i \mid i \in [K]\}$ of height at most mk over $\mathcal{W}$.*

Proof: Suppose that A is an instance of a counting axiom in $\mathcal{R}$ so that A $\mathbb{T}$-evaluates to 0. Say that $A = \bigvee_{i \in [K]} \neg \left(\bigvee_{e \ni i} F_e\right) \vee \bigvee_{e \perp f} \neg (\neg F_e \vee \neg F_f)$. For each $e \in [K]^m$, let $T_e = \mathbb{T}_{F_e}$, and for each $i \in [K]$, let $T_i = \mathbb{T}_{\bigvee_{e \ni i} F_e}$.

For each $i \in [K]$, let S_i be the tree obtained by relabeling each leaf l of T_i with the unique $e \ni i$ so that there is a $\sigma \in \mathrm{Br}_1(T_e)$ consistent with the branch to that leaf.

We now show that for $i, j \in [K]$ and each $\beta_1 \in \mathrm{Br}(S_i)$, $\beta_2 \in \mathrm{Br}(S_j)$, if β_1 and β_2 are consistent then their leaf labels are the same. Suppose that $\beta_1 \in \mathrm{Br}(S_i)$, $\beta_2 \in \mathrm{Br}(S_j)$ and $\beta_1 \cup \beta_2$ is consistent. Let e_1 be the leaf label for β_1 and let e_2 be the leaf label for β_2 and suppose for the sake of contradiction that $e_1 \neq e_2$. Apply lemma 104 and choose $\sigma_1 \in \mathrm{Br}_1(T_{e_1})$ with $\sigma_1 \subseteq \beta_1$, $\sigma_2 \in \mathrm{Br}_1(T_{e_2})$ with $\sigma_2 \subseteq \beta_2$. Because $\beta_1 \cup \beta_2$ is consistent, $\sigma_1 \cup \sigma_2$ are consistent. Choose $\pi \in \mathrm{Br}(\mathbb{T}_{\neg(\neg F_{e_1} \vee \neg F_{e_2})})$ that is consistent with $\beta_1 \cup \beta_2$. Because $\neg(\neg F_{e_1} \vee \neg F_{e_2})$ $\mathbb{T}$-evaluates to 0, $\pi \in \mathrm{Br}_1(\mathbb{T}_{\neg F_{e_1} \vee \neg F_{e_2}})$. By definition, π satisfies some $\delta \in \mathrm{Br}_1(\mathbb{T}_{\neg F_{e_1}}) \cup \mathrm{Br}_1(\mathbb{T}_{\neg F_{e_2}})$. However, such a δ is inconsistent with $\sigma_1 \cup \sigma_2$ and therefore π is inconsistent with $\sigma_1 \cup \sigma_2$; contradiction.

For each $i \in [K]$, let G_i be the tree obtained as follows: Start with the tree S_i, and underneath each branch σ that leads to a leaf labeled $e = \{i, i_1, \ldots, i_{m-1}\}$, replace the leaf with a copy of $S_{i_1} \restriction_\sigma$. Underneath each branch of this tree, replace a restricted copy of i_3, and so forth. Notice that every leaf of G_i that is underneath this leaf of S_i will lead to a leaf labeled e.

Clearly, the G_i's are decision trees of height $\leq mk$, and each leaf of G_i is labeled with some edge $e \ni i$. Finally, we have that for all $e = \{i_1, \ldots, i_m\}$, all any $i_j, i_k \in e$,

$$\begin{aligned}
\mathrm{Br}_e(G_{i_j}) &= \{\sigma_j \cup \bigcup_{\substack{l \in [1,m] \\ l \neq j}} \left(\sigma_l \restriction_{\sigma_j \ldots \sigma_{i-1}}\right) \mid \sigma_l \in \mathrm{Br}_e(S_{i_l}),\ 1 \leq l \leq m\} \\
&= \{\bigcup_{l=1}^{m} \sigma_l \mid \sigma_l \in \mathrm{Br}_e(S_{i_l}),\ 1 \leq l \leq m\} \\
&= \{\sigma_k \cup \bigcup_{\substack{l \in [1,m] \\ l \neq k}} \left(\sigma_l \restriction_{\sigma_k \ldots \sigma_{i-1}}\right) \mid \sigma_l \in \mathrm{Br}_e(S_{i_l}),\ 1 \leq l \leq m\} \\
&= \mathrm{Br}_e(G_{i_k})
\end{aligned}$$

■

Lemma 106 *Let $\mathcal{U}$ and $\mathcal{V}$ be universes, let $\mathcal{R}$ be a refutation of $MIS_m(\mathcal{U})$, and let $\mathbb{T}$ be a k-evaluation of $\mathcal{R}$ of $\mathcal{V}$. If $8k + 2 \leq w(\mathcal{V})$ then there exists an $(M, N - 2k)$ universe $\mathcal{W}$ and a generic system of height at most mk in $\mathcal{W}$.*

Proof: By lemma 102, we may choose an $(M, N - 2k)$ universe $\mathcal{W}$ with and a k-evaluation $\mathbb{T}'$ of $\mathcal{R}$ in $\mathcal{W}$ so that there exists some instance of a counting axiom

A in $\mathcal{R}$ so that A $\mathbb{T}'$-evaluates to 0. By lemma 105, this guarantees the existence of a generic system of height at most mk in $\mathcal{W}$.

■

VI.I.2 From Generic System to Nullstellensatz Refutation

Definition VI.I.2 *Let S be a subset of $BLits(\mathcal{W})$. The* **monomial of S**, $\mathbf{p_S}$, *is defined as follows.*

$$p_S = \prod_{\neg X_i \in S} (1 - X_i) \prod_{X_i \in S} X_i \prod_{Y_e \in S} Y_e$$

Let T be a decision tree. The **polynomial of T**, $\mathbf{p_T}$, *is the sum of the monomials of its branches.*

$$p_T = \sum_{\pi \in Br(T)} p_\pi$$

Lemma 107 *Let $Q \in \mathcal{Q}(\mathcal{U})$ be given. From $AMIS_m(\mathcal{W})$ there is a Nullstellensatz derivation of $\sum_{A \in \mathcal{ANS}^{\mathcal{W}}(Q)} p_A = 1$ of degree at most 3.*

Proof: The proof is done by case analysis on the query Q. When $Q = \text{Value}(i)$, $\mathcal{ANS}^{\mathcal{W}}(\text{Value}(i)) = \{\{X_i\}, \{\neg X_i\}\}$. Trivially, $\sum_{A \in \mathcal{ANS}^{\mathcal{W}}(Q)} p_A = X_i + 1 - X_i = 1$.

When $Q = \text{Match}(p)$, with $p \in V_r$, $\mathcal{ANS}^{\mathcal{W}}(p) = \{\{Y_e\} \cup \{X_k \mid k \in I \cap R,\ I \in e \cap U_r\} \mid e \in E_r,\ p \in e\}$. Notice that for each $I \in U_r$, $e \ni I$, there is a family of degree ≤ 1 polynomials $c_q^{I,e}$, $q \in \text{AMIS}_m(\mathcal{W})$, so that $Y_e - Y_e \prod_{i \in I \cap R} X_i = \sum_{q \in \text{AMIS}_m(\mathcal{W})} c_q^{I,e} q$. Therefore, (using the fact that for all e, $|e \cap U_r| \leq 1$ to reduce the second expression to 1),

$$\begin{aligned}
&\textstyle\sum_{A \in \mathcal{ANS}^{\mathcal{W}}(Q)} p_A + \sum_{e \ni p} \sum_{I \in e \cap U_r} \sum_{q \in \text{AMIS}_m(\mathcal{W})} c_q^{I,e} q - \left(\sum_{e \ni p} Y_e - 1\right) \\
&= \textstyle\sum_{A \in \mathcal{ANS}^{\mathcal{W}}(Q)} Y_e \prod_{i \in I \cap R} X_i + \sum_{e \ni p} \sum_{I \in e \cap U_r} \left(Y_e - Y_e \prod_{i \in I \cap R} X_i\right) - \sum_{e \ni p} Y_e - 1 \\
&= 1
\end{aligned}$$

When $Q = \text{Match}(I)$, with $I \in U_r$, $\mathcal{ANS}^{\mathcal{W}}(\text{Match}(I)) = \{\{X_i^{\epsilon_i} \mid i \in I \cap R\} \mid \epsilon \in \{-1, 1\}^{I \cap R},\ \exists j \in I \cap R, \epsilon_j = -1\} \cup \{\{Y_e\} \cup \{X_k \mid k \in I \cap R\} \mid e \in E_r,\ I \in e\}$

Let $\mathcal{A}_0 = \{\{X_i^{\epsilon_i} \mid i \in I \cap R\} \mid \epsilon \in \{-1,1\}^{I \cap R},\ \exists j \in I \cap R, \epsilon_j = -1\}$ and $\mathcal{A}_1 = \{\{Y_e\} \cup \{X_k \mid k \in I \cap R\} \mid e \in E_r,\ I \in e\}$ It is easily shown by induction on $|I \cap R|$ that $\sum_{A \in \mathcal{A}_0} p_A = 1 - \prod_{i \in I \cap R} X_i$. Moreover, $\sum_{A \in \mathcal{A}_1} p_A - \prod_{i \in I \cap R} X_i$ is one of the hypotheses of $\mathrm{AMIS}_m(\mathcal{W})$. ; this immediately implies that there is a degree ≤ 3 derivation of 1 from $\sum_{A \in \mathcal{ANS}^{\mathcal{W}}(\mathcal{Q})} p_A$ and $\mathrm{AMIS}_m(\mathcal{W})$.

$$\prod_{i \in I \cap R} X_i \left(\sum_{e \ni I} Y_e - 1\right) = \sum_{e \ni I} \prod_{i \in I \cap R} X_i Y_e - \prod_{i \in I} X_i = \sum_{A \in \mathcal{A}_1} p_A - \prod_{i \in I} X_i$$

■

Lemma 108 *Let $\mathcal{W}$ be a universe, and let T be a decision tree in $\mathcal{W}$. There exists a family of polynomials, c_q, for $q \in AMIS_m(\mathcal{W})$, each of degree $< 3Ht(T)$ so that $P_T = 1 + \sum_{q \in AMIS_{m(\mathcal{W})}} c_q q$.*

Proof: We prove this by induction on the height of T. The base case is when $h = 0$ and T has a single node. By definition, $p_T = 1$. For the induction step, assume that the lemma works for all decision trees of height h. Let T be a decision tree of height $h+1$ vertices. Choose v to be a an internal vertex in T of depth h. Let T_v denote the decision tree obtained by deleting the children of v. Let π_v be the branch of T leading to v. Let Q be the query of node v.

Let $\mathcal{A}_0 = \{A \in \mathcal{ANS}(Q) \mid A \restriction_{\pi_v} = 0\}$ and $\mathcal{A}_1 = \{A \in \mathcal{ANS}(Q) \mid A \restriction_{\pi_v} \neq 0\}$. By lemma 70, $\mathcal{ANS}^{\mathcal{W}\restriction_{\pi_v}}(Q) = \mathcal{A}_1$.

$$p_T = p_{T_v} - p_{\pi_v} + \sum_{A \in \mathcal{ANS}^{\mathcal{W}\restriction_{\pi_v}}(Q)} p_A p_{\pi_v} = p_{T_v} + p_{\pi_v}\left(\sum_{A \in \mathcal{A}_1} p_A - 1\right)$$

By lemma 107, we may choose a family of polynomials r_q, for $q \in \mathrm{AMIS}_m(\mathcal{W})$, each of degree ≤ 3 so that

$$\sum_{A \in \mathcal{A}_1} p_A - 1 = \sum_{A \in \mathcal{A}_0} p_A + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} r_q q$$

Therefore,

$$p_T = p_{T_v} + p_{\pi_v}\left(\sum_{A \in \mathcal{A}_0} p_A + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} r_q q\right)$$

Because each $A \in \mathcal{A}$ is inconsistent with π_v, there is some $q \in \mathrm{AMIS}_m(\mathcal{W})$ a degree $\deg(p_{\pi_v} p_A) - 2$ monomial $s_{A,q}$ so that $p_{\pi_v} p_A = s_{A,q} q$. Therefore,

$$p_T = p_{T_v} + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} \left(\left(\sum_{A \in \mathcal{A}_0} s_{A,q} \right) + r_q \right) q$$

For each polynomial $s_{A,q}$, $\deg(r_{A,q}) \leq \deg(p_{\pi_v} p_A) - 2 \leq 3h + 3 - 2 = 3h + 1 < 3(h+1)$. By the induction hypothesis, there exists family of degree $< 3h$ polynomials t_q, $q \in \mathrm{AMIS}_m(\mathcal{W})$, so that $p_{T_v} = 1 + \sum t_q q$. Therefore,

$$\begin{aligned} p_T &= 1 + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} t_q q + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} \left(\left(\sum_{A \in \mathcal{A}_0} s_{A,q} \right) + r_q \right) q \\ &= 1 + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} \left(\left(\sum_{A \in \mathcal{A}_0} s_{A,q} \right) + r_q + t_q \right) q \end{aligned}$$

For $q \in \mathrm{AMIS}_m(\mathcal{W})$, let $c_q = \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} \left(\left(\sum_{A \in \mathcal{A}_0} s_{A,q} \right) + r_q + t_q \right)$. Each such c_q is clearly of degree $< 3(h+1)$. ∎

Lemma 109 *Let $\mathcal{W}$ be a universe, K be an odd integer. If there exists a generic system $\{T_i \mid i \in [K]\}$ height $\leq h$ over $\mathcal{W}$ then $AMIS_m(\mathcal{W})$ has a Nullstellensatz refutation of degree $< 3h$.*

Proof: For each $i \in [K]$, an application of lemma 108 shows that there is a family of polynomials c_q^i, for $q \in \mathrm{AMIS}_m(\mathcal{W})$, each of degree less than $3h$, so that $p_{T_i} = 1 + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} c_q^i q$. Therefore, summing over $i \in [K]$ yields $\sum_{i \in [K]} p_{T_i} = \sum_{i \in [K]} (1 + \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} c_q^i q) = 1 + \sum_{i \in [K]} \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} c_q^i q$. Because the T_i's form a generic system, every branch and therefore every monomial, appears an even number of times. Therefore, $\sum_{i=1}^{K} p_{T_i} = 0$ and hence $1 + \sum_{i \in [K]} \sum_{q \in \mathrm{AMIS}_m(\mathcal{W})} c_q^i q$.

∎

VI.I.3 The Proof of Theorem 101

Proof:(of theorem 101) By lemma 106, there is an $(M, N - 2k)$ universe $\mathcal{W}$ and a generic system of height at most mk in $\mathcal{W}$. By lemma 109, this guarantees the

existence of a degree $< 3mk$ Nullstellensatz refutation of $\text{AMIS}_m(\mathcal{W})$. ∎

VI.J A Degree Lower Bound for Nullstellensatz Refutations of AMIS_m

Theorem 110 *Let M be an integer, and let $\mathcal{W}$ be a universe of length M and width ≥ 1. All Nullstellensatz refutations of $AMIS_m(\mathcal{W})$ have degree $\Omega(\log M)$.*

The proof is a reduction to the linear induction principles of length M, which are known to require degree $\Omega(\log M)$ Nullstellensatz refutations.

Definition VI.J.1 *Let M be a positive integer. The* **linear induction principle of length M, IND(M)**, *is a system of polynomials in the variables $t_1, \ldots, t_M$ with coefficients from $\mathbb{Z}_2$. It contains exactly the polynomials t_1, $t_M - 1$ and, for each $i < M$, $t_i t_{i+1} - t_{i+1}$*

Theorem 111 *[61, 60] The IND(M) system has Nullstellensatz refutations of degree $O(\log M)$ over any field. Moreover, over any field the system requires degree $\Omega(\log M)$ Nullstellensatz refutations.*

The following definition is almost verbatim from [73], although we are concerned with Nullstellensatz derivations whereas they were interested in polynomial calculus derivations.

Definition VI.J.2 *Let $P(\vec{x})$ and $Q(\vec{y})$ be two sets of polynomials over a field $\mathbb{F}$. We say that P is* **$(\mathbf{d_1}, \mathbf{d_2})$-reducible to Q** *if: (1) for every y_i, there is a degree d_1 definition of y_i in terms of $\vec{x}$. That is, for every i, there exists a degree d_1 polynomial r_i where y_i will be viewed as being defined by $r_i(\vec{x})$; (2) there exists a degree d_2 Nullstellensatz derivation of the polynomials $Q(\vec{r}(\vec{x}))$ from the polynomials $P(\vec{x})$; (3) there exists a degree d_2 Nullstellensatz derivation of the polynomials $r_i^2(\vec{x}) - r_i(\vec{x})$ from the polynomials of $P(\vec{x})$.*

Lemma 112 *Suppose that $P(\vec{x})$ is (d_1, d_2)-reducible to $Q(\vec{y})$. Then if there is a degree d_3 Nullstellensatz refutation of $Q(\vec{y})$ then there is a degree $d_1 d_3 + d_2$ Nullstellensatz refutation of $P(x)$.*

We omit the proof of the following lemma; the reduction is simply an application an $(N-1)$-simplification.

Lemma 113 *Let $\mathcal{W}$ be an (M, N) universe with $N \geq 1$. $AMIS_m(M, 1)$ is $(1, 1)$-reducible to $AMIS_m(\mathcal{W})$*

Lemma 114 *$IND(M)$ is $(1, 1)$-reducible to $AIS(M, 1)$.*

Proof: Observe that when $\mathcal{U}$ is an $(M, 1)$ universe, we may rename the underlying indices so that $R_r = \{r\}$.

Notice that $|U_0| = 1$ and $|V_0| = m$, and for r, $1 \leq r \leq M$, $|U_r| = m$ and $|V_r| = m^2$. For each r, $1 \leq r \leq M$, let $\mathcal{E}_r \subset E_r$ be an m-partition on $U_r \cup V_r$, and let $\mathcal{F}_r \subseteq E_r$ be an m-partition on V_r. Let $e_0 = V_0$.

We will use the following definitions for the variables of $\mathrm{IS}_m(M, 1)$. Let $Y_{e_0} := 1 - t_1$, for each r, $1 \leq r \leq M$, $X_r := t_r$, for equation r, $1 \leq r \leq M - 1$, for $e \in \mathcal{E}_r$, $Y_e := t_{r+1}$, for $f \in \mathcal{F}_r$, $Y_f := 1 - t_{r+1}$, for all other e, $Y_e := 0$, and for equation M, for $e \in \mathcal{E}_M$, $Y_e := t_M$, for $f \in \mathcal{F}_M$, $Y_f := 1 - t_M$.

Recall that $\mathrm{AMIS}_m(M, 1)$ is the following system of polynomials.

For each r, $0 \leq r \leq M$,

For each $I \in U_r$,	$\prod_{i \in I \cap R} X_i \left(\sum_{e \ni I} Y_e - 1\right)$
for each e, $I \in e \cap U_r$, $i \in I \cap R$,	$Y_e(1 - X_i)$
For $p \in V_r$,	$\sum_{e \ni p} Y_e - 1$
For each $e \perp f$,	$Y_e Y_f$

The polynomials for equation 0:

$$\begin{array}{lcll} X_1 \left(\sum_{e \ni I} Y_e - 1\right) & = & t_1 (0 - 1) & = & -t_1 \\ Y_f (1 - X_1) & = & 0(1 - t_1) & = & 0 \\ \sum_{e \ni p} Y_e - 1 & = & (1 - t_1) - 1 & = & -t_1 \end{array}$$

The polynomials for equation r, with $1 \leq r \leq M-1$ (we omit equations that are identically 0 because a factor Y_e is identically 0):

$$\begin{array}{lcll}
X_{r+1}\left(\sum_{e\ni\{r+1\}} Y_e - 1\right) & = & t_{r+1}\left(t_{r+1}-1\right) & = & t_{r+1}^2 - t_{r+1} \\
X_r X_{r+1}\left(\sum_{e\ni\{r,r+1\}} Y_e - 1\right) & = & t_r t_{r+1}\left(t_{r+1}-1\right) & = & t_r\left(t_{r+1}^2 - t_{r+1}\right) \\
Y_e(1-X_{r+1}) & = & t_{r+1}(1-t_{r+1}) & = & -(t_{r+1}^2 - t_{r+1}) \\
Y_e(1-X_r) & = & t_{r+1}(1-t_r) & = & -(t_{r+1}t_r - t_{r+1}) \\
\sum_{e\ni p} Y_e - 1 & = & t_{r+1} + 1 - t_{r+1} & = & 0 \\
Y_e Y_f & = & t_{r+1}(1-t_{r+1}) & = & -(t_{r+1}^2 - t_{r+1})
\end{array}$$

The polynomials for equation M (we omit equations that are identically 0 because a factor Y_e is identically 0):

$$\begin{array}{lcll}
\left(\sum_{e\ni\emptyset} Y_e - 1\right) & = & \left(t_M - 1\right) & = & t_M - 1 \\
X_M\left(\sum_{e\ni\{M\}} Y_e - 1\right) & = & t_M\left(t_M-1\right) & = & t_M^2 - t_M \\
Y_e(1-X_M) & = & t_M(1-t_M) & = & -(t_M^2 - t_M) \\
\sum_{e\ni p} Y_e - 1 & = & t_M + 1 - t_M - 1 & = & 0 \\
Y_e Y_f & = & t_M(1-t_M) & = & -(t_M^2 - t_M)
\end{array}$$

■

We now combine these elements to prove theorem 110.

Proof:(of theorem 110) Let d be the minimum degree of a Nullstellensatz refutation of $\mathrm{AMIS}_m(\mathcal{W})$. By lemmas 113 and 112, there is a degree $d+1$ Nullstellensatz refutation of $\mathrm{AMIS}_m(M,1)$. By lemmas 114 and 112, there is a degree $d+2$ refutation of $\mathrm{IND}(M)$. By theorem 111, we must have that $d = \Omega(\log M)$. ■

VI.K Putting It All Together

Theorem 115 *Let c, d be positive constants. For sufficiently large values of N, there is no depth d refutation of $MIS_m(N,N)$ of size $\leq N^c$.*

Proof: Let c, d be given and suppose that for every N and (N, N) universe $\mathcal{U}$ there is a refutation of $\mathrm{IS}(\mathcal{U})$ of size $\leq N^c$. Apply theorem 94 to get constants k and ϵ so that for sufficiently large N there is an a k-evaluation $\mathbb{T}$ for $\mathcal{R}$ over an (N, N^ϵ) universe $\mathcal{V}$

Take N large enough that $N^\epsilon > 8k+2$, and apply theorem 101, so we have a degree $3mk$ Nullstellensatz refutation of $\mathrm{AIS}_m(\mathcal{W})$ for an $(N, N^\epsilon - 2k)$ universe $\mathcal{W}$. By theorem 110, $\mathrm{AIS}_m(\mathcal{W})$ requires degree $\Omega(\log N)$ to refute; contradiction. ■

VI.K.1 Induction on Sums Principles

Using our reduction and simulation technique, we show that the induction on sums principles have quasipolynomial size constant-depth Frege with counting axioms refutations. The same reduction shows that there can be no small Nullstellensatz refutations of the induction on sums formulation as polynomials. This gives a superpolynomial *size* separation between Nullstellensatz and polynomial calculus refutations.

Lemma 116 *Fix a constant modulus m. For each M, N, $IS_m(M, N)$ reduces to $AIS_m(M, N)$ in depth $O(1)$ and size polynomial in M and N.*

Proof: To define an m-partition on the satisfied monomials of $\sum_{e \ni I} Y_e \prod_{i \in I} X_i - \prod_{i \in I} X_i$, we use the formula $Y_e \wedge \bigwedge_{i \in I} X_i$ for the edge which groups $\prod_{i \in I} X_i Y_e$ and with the $m-1$ copies of $\prod_{i \in I} X_i$. From the hypotheses $\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$ and $\neg Y_e \vee \neg Y_f$ (for all $e \perp f$), there is a proof that these formulas define an m-partition on the satisfied monomials of $\prod_{i \in I} X_i \left(\sum_{e \ni I} Y_e - 1\right)$.

To define an m-partition on the satisfied monomials of an equation $Y_e X_i - Y_e$, we simply group the monomials if and only if Y_e is satisfied. The hypothesis $\neg Y_e \vee X_i$ shows that this is a m-partition of the satisfied monomials.

For the polynomials $Y_e Y_f$, the hypothesis $\neg Y_e \vee \neg Y_f$ ensures that the monomial is never satisfied, so the empty partition is an m-partition of satisfied

monomials of this polynomial. ∎

The Lower Bound

In the course of proving a size lower bound for constant-depth Frege with counting axioms refutations of $\mathrm{IS}_m(M,N)$, it is shown that there are no low degree Nullstellensatz refutations for $\mathrm{AIS}_m(M,N)$. It had been conceivable that there are Nullstellensatz refutations for this system of high-degree but small size. Our simulation shows that this is not the case. By the reduction of lemma 116 and the simulation of theorem 55, if there were a polynomial size Nullstellensatz refutation of $\mathrm{AIS}_m(M,N)$, then there would be a polynomial size, constant-depth Frege refutation of $\mathrm{IS}_m(M,N)$. However, no such refutations exist.

Theorem 117 *[68] Let m be a fixed modulus. Let c,d be positive constants. For sufficiently large values of M and N, there is no depth d Frege with counting axioms modulo m refutation of $IS_m(M,N)$ of size less than N^c.*

Corollary 118 *Fix a modulus m. Let c be a positive constant. For sufficiently large values of M and N, there is no Nullstellensatz refutation of $AIS_m(M,N)$ of size less than N^c.*

On the other hand, the polynomial calculus modulo m has constant degree, polynomial size refutations of $\mathrm{AIS}_m(M,N)$:

Theorem 119 *[68] Let M,N be given, $AIS_m(M,N)$ system of polynomials has degree 3, size $O(MN^3)$ polynomial calculus modulo m refutation.*

Corollary 120 *The Nullstellensatz refutation system modulo m does not polynomially simulate the polynomial calculus modulo m.*

VI.L An Upper Bound for the $\mathrm{IS}_m(M,N)$ Principles

In this section, we show that constant-depth Frege systems with counting axioms have quasi-polynomial size refutations of the $\mathrm{IS}_m(M,N)$ principles. This

is a constant-degree reduction to the induction principles, which have logarithmic degree Nullstellensatz refutations [61, 60] over any field, combined with an application of

Theorem 121 *Fix a constant, prime modulus m. There exists a c (dependent on m) so that for all M, N, so the system $AIS_m(M, N)$ has a Nullstellensatz modulo m refutation of degree at most $c \log M$.*

The system $\mathrm{AIS}_m(M, N)$ uses $O(MN^{2m})$ many variables, therefore there are fewer than $(MN)^{2mc \log M}$ monomials of degree at most $c \log M$. For this reason, each polynomial of the Nullstellensatz refutation has size at most $(MN)^{2mc \log M}$. Therefore, the size of the refutation is quasipolynomial in the size of $\mathrm{AIS}_m(M, N)$.

Lemma 122 *Fix a constant, prime modulus m. There exists a constant C (dependent on m) so that for all M,N, the system $AIS_m(M, N)$ has a Nullstellensatz modulo m refutation of size at most $(MN)^{C \log M}$.*

Combining this refutation with the reduction of lemma 116 and the simulation of theorem 55, there are quasi-polynomial size constant-depth Frege refutations of $\mathrm{IS}_m(M, N)$.

Lemma 123 *Fix a constant, prime modulus m. There exists a constant C so that for all M and N, $IS_m(M, N)$ has a constant-depth Frege refutation of size at most $(MN)^{C \log M}$*

Lemma 124 *From the principle $AIS_m(M, N)$ there are degree $O(1)$ Nullstellensatz derivations of $IND[y_r \leftarrow \sum_{j \in R_r}^{N} X_j]$.*

Proof: First, we show that for each r from 0 to M there is a degree five Nullstellensatz derivation of $\sum_{I \in U_r} X_I$.

For each r and each $I \in U_r$, $e \in [U_r]^m$ with $e \ni I$, let $q_{I,e} = Y_e \prod_{i \in I} X_i - Y_e$. When $|I| = 1$, $q_{I,e} = X_i Y_e - Y_e$ belongs to $\mathrm{AIS}_m(M, N)$, and when $I = \{i, j\}$, there

is a degree Nullstellensatz 3 derivation of $q_{I,e}$ from $\mathrm{AIS}_m(M,N)$:

$$X_i(X_jY_e - Y_e) + X_iY_e - Y_e \;=\; X_iX_jY_e - Y_e \;=\; q_{I,e}$$

For each r and each $I \in U_r$, let $p_I = \sum_{e\ni I} Y_e - \prod_{i\in I} X_i$. These polynomials have degree ≤ 3 Nullstellensatz derivations from $\mathrm{AIS}_m(M,N)$ and the $q_{I,e}$'s:

$$\begin{aligned}\left(\textstyle\prod_{i\in I} X_i\right)\left(\textstyle\sum_{e\ni I} Y_e - 1\right) - \textstyle\sum_{e\ni I} q_{I,e} &= \textstyle\sum_{e\ni I}\left(Y_e \prod_{i\in I} X_i - q_{I,e}\right) - \prod_{i\in I} X_i \\ &= \textstyle\sum_{e\ni I} Y_e - \prod_{i\in I} X_i = p_I\end{aligned}$$

For each equation r, $0 \leq r \leq M$, when we negate the sum of all the p_I's, we obtain the desired polynomial $\sum_{I\in U_r}\prod_{i\in I} X_i$. The final identity $\sum_{I\in U_r}\sum_{e\ni I} Y_e = 0$ is true because each variable Y_e appears exactly m times in the sum.

$$\begin{aligned}-\textstyle\sum_{I\in U_r} p_I &= \textstyle\sum_{I\in U_r}\sum_{e\ni I}\left(\prod_{i\in I} X_i - \sum_{e\ni I} Y_e\right) \\ &= \textstyle\sum_{I\in U_r}\prod_{i\in I} X_i - \sum_{I\in U_r}\sum_{e\ni I} Y_e \\ &= \textstyle\sum_{I\in U_r}\prod_{i\in I} X_i\end{aligned}$$

Finally, we check that these are the hypotheses of $\mathrm{IND}(M)$ with $\sum_{i\in R_r} X_i$ substituted for y_r.

$$\begin{aligned}\textstyle\sum_{I\in U_0} X_I &= \textstyle\sum_{i\in R_1} X_i &&= y_1\left[y_r \leftarrow \textstyle\sum_{i\in R_r} X_i\right] \\ \textstyle\sum_{I\in U_M} X_I &= \textstyle\sum_{i\in R_M} X_i + (m-1) &&= (y_m - 1)\left[y_r \leftarrow \textstyle\sum_{i\in R_r} X_i\right]\end{aligned}$$

$$\begin{aligned}\textstyle\sum_{I\in U_r} X_I &= \textstyle\sum_{i\in R_r, j\in R_{r+1}} X_iX_j + (m-1)\sum_{j\in R_{r+1}} X_j \\ &= (y_{r+1}y_r - y_{r+1})\left[y_r \leftarrow \textstyle\sum_{i\in R_r} X_i\right]\end{aligned}$$

■

Combining this reduction with the $O(\log M)$ upper bounds of the $\mathrm{IND}(M)$ system of polynomials gives us upper bounds for the $\mathrm{AIS}_m(M,N)$ principles.

Corollary 125 *When m is a fixed prime, there is a degree $O(\log M)$ Nullstellensatz modulo m refutation of $AIS_m(M,N)$.*

VI.M Acknowledgements

Much of the text of this chapter was previously published as part of [68] in the proceedings of the Forty-second Annual IEEE Symposium on the Foundations of Computer Science. I was the primary researcher and author of this publication which forms the basis for this chapter.

Bibliography

[1] M. Alekhnovich, E. Ben-Sasson, A. Razborov and A. Wigderson. Pseudo-random generators in propositional proof complexity. In *Proceedings of the Forty-first Annual IEEE Symposium on Foundations of Computer Science*, pages 43–53, 2000.

[2] J. Krajíček. Tautologies from Pseudo-Random Generators. *The Bulletin of Symbolic Logic*, 7 (2): 197–212, 2001.

[3] T. Pitassi. Algebraic Propositional Proof Systems. In *Descriptive Complexity and Finite Models*. American Mathematical Society. 1997.

[4] J. Marques-Silva and K. Sakallah. Boolean Satisfiability in Electronic Design Automation. In *Proceedings of the IEEE/ACM Design Automation Conference*, 2000.

[5] T. Larrabee. Test Pattern Generation Using Boolean Satisfiability. In *IEEE Transactions on Computer-Aided Design*, 11 (1): 6–22. 1992.

[6] I. Gent and T. Walsh. Towards an Understanding of Hill-Climbing Procedures for SAT. In *National Conference on Artificial Intelligence*, pages 28–33, 1993.

[7] H. Kautz and B. Selman. Pushing the Envelope: Planning, Propositional Logic, and Stochastic Search. In *Proceedings of the Thirteenth National Conference on Artificial Intelligence and the Eighth Innovative Applications of Artificial Intelligence Conference*, pages 1194–1201, 1996.

[8] H. Kautz and B. Selman. Planning as Satisfiability. In *Proceedings of the Tenth European Conference on Artificial Intelligence*, pages 359–363, 1992.

[9] E. Ben-Sasson. Hard Examples for Bounded Depth Frege. In *Proceedings of the Thirty-fourth Annual ACM Symposium on Theory of Computing*, pages 563–572, 2002.

[10] M. Sipser. Borel Sets and Circuit Complexity. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, pages 61–69, 1983.

[11] M. Ajtai. Σ_1^1-formulae on finite structures. In *Annals of Pure and Applied Logic*, 24, 1–48, 1983.

[12] L. Cai, J. Chen, and J. Håstad. Circuit Bottom Fan-in and Computational Power. In *SIAM Journal on Computing*, 27 (2) : 341–355, 1998.

[13] R. Boppana and M. Sipser. The Complexity of Finite Functions. In *Handbook of Theoretical Computer Science volume A*. Elsevier and MIT Press. 1990.

[14] J. Håstad. Almost Optimal Lower Bounds for Small Depth Circuits. In *Advances in Computing Research*. JAI Press. 1989

[15] S. Dantchev and S. Riis. Tree Resolution Proofs of the Weak Pigeon-Hole Principle. In *Proceedings of the Sixteenth Annual IEEE Conference on Computational Complexity*, pages 69–75, 2001.

[16] T. Pitassi and R. Raz. Regular Resolution Lower Bounds for the Weak Pigeonhole Principle. In *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing*, pages 347–355, 2001.

[17] A. Urquhart. Hard Examples for Resolution. In *Journal of the ACM*, 34 (1) : 209–219, 1987.

[18] J. Esteban and J. Toran. Space Bounds for Resolution. In *Annual Symposium on Theoretical Aspects of Computer Science*, 1999.

[19] J. Esteban, N. Galesi, and J. Messner. On the Complexity of Resolution with Bounded Conjunctions. In *Proceedings of the Twenty-ninth International Colloquium on Automata, Languages and Programming*, pages 220–231, 2002.

[20] A. Razborov. Improved Resolution Lower Bounds for the Weak Functional Pigeonhole Principle. Manuscript to appear in *Theoretical Computer Science*. 2001.

[21] A. Razborov. Pseudorandom Generators Hard for k-DNF Resolution and Polynomial Calculus Resolution. Manuscript available at `http://genesis.mi.ras.ru/~razborov/` . 2003.

[22] A. Atserias and M. Bonet. On the Automatizability of Resolution and Related Propositional Proof Systems. In *Sixteenth International Workshop on Computer Science Logic, Lecture Notes in Computer Science volume 2471*. Pages 569–583. Springer. 2002.

[23] R. Raz. Resolution Lower Bounds for the Weak Pigeonhole Principle. In *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing*, pages 553–562, 2002.

[24] P. Beame, R. Karp, T. Pitassi, and M. Saks. The Efficiency of Resolution and Davis–Putnam Procedures. In *SIAM Journal on Computing*, 31 (4) : 1048–1075, 2002.

[25] P. Beame, R. Karp, T. Pitassi, and M. Saks. On the Complexity of Unsatisfiability Proofs for Random k-CNF Formulas. In *ACM Symposium on Theory of Computing*, 1998.

[26] A. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Space Complexity in Propositional Calculus. In *ACM Symposium on Theory of Computing*, 2000.

[27] V. Chvátal and E. Szemerédi. Many Hard Examples for Resolution. In *Journal of the ACM*, 35 (4) : 759–768, 1988.

[28] E. Ben-Sasson and N. Galesi. Space Complexity of Random Formulae in Resolution. In *Proceedings of the Sixteenth Annual Conference on Computational Complexity*, pages 42–51, 2000.

[29] G. Tseitin. On the Complexity of Proofs in Propositional Logics. In *Seminars in Mathematics*, volume 8, 1970.

[30] J. Alan Robinson. A Machine-Oriented Logic Based on the Resolution Principle. In *Journal of the ACM*, 12 (1) : 23–41, 1965.

[31] P. Erdös and R. Rado. Intersection Theorems for Finite Sets. In *Journal of the London Math Society*, 35 : 85–90, 1960.

[32] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press. 1995.

[33] V. Vazirani. *Approximation Algorithms*. Springer-Verlag. 2001.

[34] S. Buss, editor. *Handbook of Proof Theory*. Elsevier Science Publishers. 1998.

[35] P. Beame and T. Pitassi. Propositional Proof Complexity: Past, Present, and Future. In *Bulletin of the EATCS*, 65 : 66–89, 1998.

[36] A. Maciel, T. Pitassi, and A. Woods. A New Proof of the Weak Pigeonhole Principle. In *ACM Symposium on Theory of Computing*, 2000.

[37] A. Maciel, T. Pitassi, and A. Woods. A New Proof of the Weak Pigeonhole Principle. In *Journal of Computer and System Sciences*, 64 : 843–872, 2002.

[38] J. Paris, A. Wilkie, and A. Woods. Provability of the Pigeonhole Principle and the Existence of Infinitely Many Primes. In *Journal of Symbolic Logic*, 53, 1988.

[39] E. Ben-Sasson and A. Wigderson. Short proofs are narrow — resolution made simple. In *Journal of the ACM*, 48 (2) : 149–169, 2001.

[40] P. Beame and T. Pitassi. Simplified and Improved Resolution Lower Bounds. In *Proceedings of the Thirty-seventh Annual IEEE Symposium on Foundations of Computer Science*, pages 274–282, 1996.

[41] N. Segerlind, S. Buss, and R. Impagliazzo. A Switching Lemma for Small Restrictions and lower bounds for k-DNF Resolution. In *Forty-third Annual Symposium on Foundations of Computer Science*, pages 604–613, 2002.

[42] S. Buss and G. Turán. Resolution Proofs of Generalized Pigeonhole Principles. In *Theoretical Computer Science*, 62 (3) : 311–217, 1988.

[43] A. Goerdt. Unrestricted resolution versus N-resolution. In *Theoretical Computer Science*, 93 (1) : 159–167, 1992.

[44] M. Bonet and N. Galesi. A study of proof search algorithms for resolution and polynomial calculus. In *Proceedings of the Fortieth Annual IEEE Symposium on Foundations of Computer Science*, pages 422–431, 1999.

[45] J. Krajíček. On the Weak Pigeonhole Principle. In *Fudamenta Mathematicae*, 170 : 123–140, 2001.

[46] E. Palmer. *Graphical Evolution: An Introduction to the Theory of Random Graphs*. Wiley Interscience. 1985.

[47] A. Atserias, M. Bonet, and J. Esteban. Lower Bounds for the Weak Pigeonhole Principle and Random Formulas Beyond Resolution. In *Information and Computation*, 176 (2) : 136–152, 2002.

[48] M. Ajtai. The Complexity of the Pigeonhole Principle. In *Proceedings of the Twenty-Ninth Annual IEEE Symposium on the Foundations of Computer Science*, pages 346–355, 1988.

[49] S. Bellantoni, T. Pitassi, A. Urquhart. Approximation and Small Depth Frege Proofs. In *Proceedings of the Sixth Annual Conference on Structure in Complexity Theory*, pages 367–391, 1991.

[50] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential Lower Bounds for the Pigeonhole Principle. In *Computational Complexity*, 3 (2) : 97–140, 1993.

[51] J. Krajíček, P. Pudlák, and A. Woods. An Exponential Lower Bound to the Size of Bounded Depth Frege Proofs of the Pigeonhole Principle. In *Random Structures and Algorithms*, 1995.

[52] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press. 1995.

[53] M. Ajtai. Parity and the Pigeonhole Principle. In *Feasible Mathematics: A Mathematical Sciences Institute Workshop*. Birkhauser. 1990.

[54] M. Ajtai. The Independence of the Modulo p Counting Principles. In *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, pages 402–411, 1994.

[55] P. Beame and T. Pitassi. An exponential separation between the parity principle and the pigeonhole principle. In *Annals of Pure and Applied Logic*, 80 (3) : 195–228, 1996.

[56] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower Bound on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings of the Thirty-fifth Annual IEEE Symposium on Foundations of Computer Science*, pages 794–806, 1994.

[57] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, R. Razborov, and J. Sgall. Proof Complexity in Algebraic Systems and Bounded Depth Frege Systems with Modular Counting. In *Computational Complexity*, volume 6, 1997.

[58] S. Riis. Count(q) does not imply Count(p). In *Annals of Pure and Applied Logic*, 90(1–3) : 1–56, 1997.

[59] P. Beame and S. Riis. More one the Relative Strength of Counting Principles. In *Proof Complexity and Feasible Arithmetics*. American Mathematical Society. 1998.

[60] J. Buresh-Oppenheim, M. Clegg, R. Impagliazzo, and T. Pitassi. Homogenization and the Polynomial Calculus. In *Proceedings of the Twenty-seventh International Colloquium on Automata, Languages and Programming*, pages 926–937, 2000.

[61] S. Buss and T. Pitassi. Good degree bounds on Nullstellensatz refutations of the induction principle. In *Proceedings of the Eleventh Annual Conference on Computational Complexity*. 1996.

[62] J. Paris and A. Wilkie. Counting Problems in Bounded Arithmetic. In *Methods in Mathematical Logic: Lecture Notes in Mathematics number 1130*. Springer-Verlag. 1985.

[63] R. Impagliazzo, P. Pudlak, and J. Sgall. Lower Bounds for the Polynomial Calculus and the Groebner Basis Algorithm. In *Computational Complexity*, 8, 1999.

[64] P. Beame, R. Impagliazzo, and T. Pitassi. Improved Depth Lower Bounds for Small Distance Connectivity. In *Proceedings of the Thirty-Sixth Annual IEEE Symposium on the Foundations of Computer Science*, pages 692–703, 1995.

[65] P. Beame. A Switching Lemma Primer. Technical report. Department of Computer Science and Engineering, University of Washington. 1994.

[66] M. Furst, J. Saxe, and M. Sipser. Parity, Circuits, and the Polynomial-Time Hierarchy. In *Mathematical Systems Theory*, 17 (1) : 13–27, 1984.

[67] S. Jukna. *Extremal Combinatorics: with applications to computer science*. Springer-Verlag. 2001.

[68] R. Impagliazzo and N. Segerlind. Counting Axioms Do Not Polynomially Simulate Counting Gates (Extended Abstract). In *Proceedings of the Forty-Second Annual IEEE Symposium on Foundations of Computer Science*, pages 200–209, 2001.

[69] M. Alekhnovich and A. Razborov. Lower Bounds for the Polynomial Calculus: Non-Binomial Case. In *Proceedings of the Forty-Second Annual IEEE Symposium on Foundations of Computer Science*, pages 190–199, 2001.

[70] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 174–183, 1996.

[71] A. Razborov. Lower Bounds for the Polynomial Calculus. In *Computational Complexity*, 1998.

[72] E. Ben-Sasson and R. Impagliazzo. Random CNFs are hard for the polynomial calculus. In *Proceedings of the Fortieth Annual IEEE Symposium on Foundations of Computer Science*, pages 415–421, 1999.

[73] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi. Linear Gaps Between Degrees for the Polynomial Calculus Modulo Distinct Primes. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, 1999.

[74] S. Cook and R. Reckhow. The Relative Efficiency of Propositional Proof Systems. In *The Journal of Symbolic Logic*, 44 (1) : 36–50, 1979.

[75] A. Haken. The intractability of resolution. In *Theoretical Computer Science*, 39 (2–3) : 297–308, 1985.

[76] L. Cai, J. Chen, and J. Håstad. Circuit Bottom Fan-in and Computational Power. In *Proceedings, Twelfth Annual IEEE Conference on Computational Complexity*, pages 158–164, 1997.

[77] S. Cook. The Complexity of Theorem Proving Procedures. In *ACM Symposium on Theory of Computing*, 1971.

[78] U. Feige. Relations between Average Case Complexity and Approximation Complexity. In *Proceedings of the Thirty-fourth Annual ACM Symposium on Theory of Computing*, pages 534–543, 2002.

[79] E. Allender and U. Hertrampf. Depth Reduction for Circuits of Unbounded Fan-In. In *Information and Computation*, 112 (2) : 217–238, 1994.

[80] R. Impagliazzo and N. Segerlind. Bounded-depth Frege Systems with Counting Axioms Polynomially Simulate Nullstellensatz Refutations. In *Proceedings of the Twenty-Ninth Annual Colloquium on Automata, Languages and Programming*, pages 208–219, 2002.

[81] P. Beame, R. Impagliazzo, T. Pitassi, and N. Segerlind. On Formula Caching Proof Systems. To appear in Computational Complexity 2003.

[82] R. Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

[83] A. Razborov. On the Method of Approximations. In *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, pages 167–176, 1989.

[84] M. Garey and D. Johnson. Computers and Intractability, A Guide to the Theory of NP-Completeness. W.H. Freeman and Company. 1978.