Sapienza
Università di Roma

IDK something about proofs, search problems, circuits, protocols and P $\neq$ NP?

Faculty of Information Engineering, Computer Science and Statistics
Bachelor's Degree in Computer Science

Simone Bianco
ID number 1986936

Advisor
Prof. Nicola Galesi
Prof. Massimo Lauria

Academic Year 2023/2024

Thesis not yet defended

IDK something about proofs, search problems, circuits, protocols and $\mathbf{P} \neq \mathbf{NP}$?
Bachelor's Thesis. Sapienza University of Rome

This thesis has been typeset by LaTeX and the Sapthesis class.

Author's email: bianco.simone@outlook.it

Please help me.

Abstract

Uhhh, idk

Contents

Chapter 1

Introduction

For many years, the study of **decision problems** has been the main focus of computability theory. These types of problems include any problem that can be described as a simple question with a yes-or-no answer, such as asking if some input object has got some kind of property or not. Decidability theory plays a core rule in math and computer science due to the subjects studied by both fields. However, even thought decision problem can be computed by an algorithm producing a solution for a given input, not all decidable problems can be solved "efficiently", meaning in a reasonable amount of time.

This very nature of decision problems has given birth to **complexity theory**, the field of computer science focused on solving the following fundamental question commonly referred to as the P vs. NP problem: «does every decision problem with an efficient way to *verify* a solution for an input also have an efficient way to *solve* the problem for that input?». The hardness of this question sparked into the establishment of many subsets of complexity theory, in particular proof complexity, communication complexity and circuit complexity. Each of these subfields revolve around solving this question for one single NP-Complete problem, that being problems for which finding an efficient algorithm would automatically imply that $\mathsf{P} = \mathsf{NP}$.

In recent years, the study of decision problems has been generalized to the study of **functional problems**, i.e. any problem where an output that is more complex than a yes-or-no answer is expected for a given input. By their very nature, functional problems are an "harder type" of problems respect to decision problems, describing any possible type of computation achievable through the concept of mathematical function and algorithm. In the same fashion of decision problems, the study of functional problems focuses on the FP vs. FNP question. In particular, solving this question for the functional case would also imply solving it for the decisional case and vice versa.

The study of functional problems has given many important results through its characterization both as a **black-box model** and a **white-box model**. These two models have been shown to be highly correlated to the previous subfields of decision problems, in particular proof complexity. These correlations give a way to study the latter through the lens of functional problems, which enables "less restrictive" methods of study. Moreover, it has been shown that so-called *natural proof systems* effectively correspond to black-box total functional problems.

Recent studies discuss if the already known relations between white-box functional problems, communication complexity and circuit complexity can be extended in order to establish a strong characterization as the one found for proof complexity. If this characterization is solid, the study of total functional problems would play an essential role in complexity theory, becoming an **unifying theory** between its subfields and thus implying that any result found in any subfield would also have impact in the others.

However, such results have not yet been found, even though a lot of process has been made. In particular, the concepts of **feasible interpolation** and **query-to-communication lifting theorems** play a very important role in finding such relations, which however are still not enough to ensure a solid "organizing theory". Nonetheless, such unifying characterizations are well-defined for highly studied proof systems and circuit models, such as Treelike Resolution and Monotone Formula Circuits.

The objective of this work is to study the relations found in proof, communication and circuit complexity, formalizing the concepts involved in each field and giving an in-depth view on how they are linked to the study of total functional problems.

Chapter 2

Preliminaries

2.1 Search Problems

As briefly discussed in the introduction, the concept of **functional problems** rose as a generalization of the concept of decision problems. Mathematically, each decision problem can be defined as a subset of possible inputs: an input object is part of the set if and only if it has the required property. For example, the decision problem «is this number prime?» can be described as the set $\text{PRIMES} = \{n \in \mathbb{N} \mid n \text{ is prime}\}$.

In a very similar way, functional problems can be described mathematically described through the concept of relation: given the set of inputs X and the set of outputs Y of the functional problem, the latter can be described as the relation $R \subseteq X \times Y$. An important thing to notice is that even though the name implies a correlation to mathematical functions, the given definition also includes partial and multi-valued functions, that being functions for which not all inputs have a corresponding output and functions for which one input can have more outputs.

For these reasons, the term *functional problem* is considered to be slightly abused. In recent years, this issue was solved by the introduction of the term **search problems**, which describes problems based on finding an output for the given input. It's easy to see that this informal definition of search problems better suits the previous definition given for functional problems. While decision problems focus on answering the question «does this object have the following property?», search problems focus on answering the question «what gives this object the following property?». Mathematically, this can be described as the difference between «is there an output?» and «what is the output?».For example, the search problem equivalent of the previous prime number problem would answer the question «what is the prime factorization of this number?».

We give a more detailed definition of each search problems through the use of a *sequence of relations* rather than a single relation in order to allow inputs of different length and different types of outputs based on the length of the inputs. This definition is a conjunction of the various definitions given in [LNN+95; BCE+98; RGR22; BFI23].

Definition 1. A search problem is a sequence $R = (R_n)_{n\in\mathbb{N}}$ of relations $R_n \subseteq \{0,1\}^n \times O_n$, one for each $n \in \mathbb{N}$, where each O_n is a finite set called "outcome set".

A search problem is said to be total if for each R_n in the sequence it holds that $\forall x \in \{0,1\}^n$ there is an $y \in O_n$ such that $(x, y) \in R_n$.

In particular, this work will focus on **total search problems**. Notice that this definition removes partial function from the context, while multi-valued functions are still allowed. Moreover, complexity theory focuses on the study of **decidable** decision and search problems, that being problems for which we know that there is always an computable answer.

2.2 The complexity classes FP, FNP and TFNP

In complexity theory, decidable decision problems are grouped in two major classes: problems that can be **solved** in a reasonable amount of time and problems that can be **verified** in a reasonable amount of time. These classes are respectively referred to as P, the class of problems solvable by a deterministic algorithm in polynomial time, and NP, the class of problems for which a solution can be verified by a a deterministic algorithm in polynomial time (or equivalently, the class of problems solvable by a non-deterministic algorithm). By the very definition of these classes, it's easy to see that $\mathsf{P} \subseteq \mathsf{NP}$.

Similarly, in the context of search problems we define the classes FP and FNP, standing for *functional P* and *functional NP*. An important remark to be made is that, since they are defined on two different types of problems, it doesn't hold that $\mathsf{P} \subseteq \mathsf{FP}$ or that $\mathsf{NP} \subseteq \mathsf{FNP}$. However, a decision problem can indeed be seen as a search problem with only two different outputs: *true* or *false*. In fact, as discussed in [BG94; BCE+98; DK14], an important result is that $\mathsf{P} = \mathsf{NP}$ if and only if $\mathsf{FP} = \mathsf{FNP}$, meaning that even though search problems are generally harder than decision problems, even if the latter are efficiently solvable then the other also is.

Moreover, by the very own nature of search problems, it's important to distinct between *total* and *partial* search problems. Thus, for search problems we also define the class TFNP, standing for *total functional NP*.

Definition 2. A search problem R is in FP if it is solvable by an algorithm in polynomial time. Likewise, as search problem R is in FNP if its solutions are verifiable by an algorithm in polynomial time. If the search problem is also total, it is in TFNP.

Additionally, we will assume that each problem in FP is also total: since problems in FP are *solvable* in polynomial time, when a solution doesn't exist for a given input we can consider the solution to be a pre-chosen «doesn't exist» value, making the problem total. Obviously, this assumption implies that $\mathsf{FP} \subseteq \mathsf{TFNP} \subseteq \mathsf{FNP}$.

Differently from decision problems, search problems are conjectured to not have any "normal" complete problem, that being problems for which an efficient solution would imply an efficient solution for any other search problem. The reason behind this conjecture is the nature itself of total search problems: in decision problems, any "yes" (or "no") answer can be reduced to a "yes" (or "no) answer of a complete decision problem, but total search problems imply that every input has a "yes" instance as output, meaning that there is no way for an instance to be reduced to another "no" instance.

For these reasons, for search problems we define the concept of completeness with respect to a **specific search problem**: given a search problem R, we define the subclass of all search problems reducible to R. Thus, the problem R is said to be "complete" for its own class of reducible problems. Unexpectedly, a lot of TFNP problems can be characterized with very few cases of such subclasses, giving birth to an actual hierarchy of search problems.

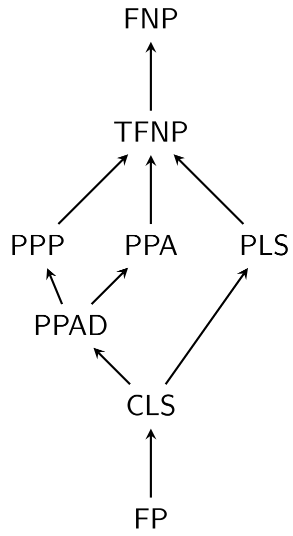

Figure 2.1. Hierarchy of the most commonly defined complete search problem classes. An arrow from class A to class B means that $A \subseteq B$.

Each of the subclasses shown in the previous hierarchy is characterized by a **complete search problem**:

- PPP (Polynomial Pigeonhole Principle): the class of problems whose solution is guaranteed by the Pigeonhole principle. It is defined as the class of problems that are polynomial-time reducible to the *Pigeon problem*

- PPA (Polynomial Parity Argument): is the class of problems whose solution is guaranteed by the handshaking lemma. It is defined as the class of problems that are polynomial-time reducible to the *Odd-degree Vertices problem.*

- PLS (Polynomial Local Search): the class of search problems designed to model the process of finding a local optimum of a function. It is defined as the class of problems that are polynomial-time reducible to the *Sink-of-DAG problem.*

- PPAD (Polynomial Parity Argument - Directed): is the class of problems whose solution is guaranteed by the directed version of the handshaking lemma. It is defined as the class of problems that are polynomial-time reducible to the *End-of-Line problem.*

- CLS (Continuous Local Search): the class of search problems designed to model the process of finding a local optimum of a continuous function over a continuous domain. It is defined as the class of problems that are polynomial-time reducible to the *Continuous Localpoint problem*.

Proving any separation between one of these inclusions would directly conclude that $\mathsf{FP} \neq \mathsf{FNP}$, giving an answer to the conjecture.

2.3 Proof Complexity

2.4 Communication Complexity

2.5 Circuit Complexity

Chapter 3

Black-box TFNP

3.1 The black-box model

3.2 Proof System Characterization

3.3 Natural Proof Systems

3.3.1 The Reflection Principle

3.3.2 Verification Procedures

3.4 The TFNP^{dt} hierarchy

3.5 An in-depth analysis: FP^{dt} = TreeRes

Chapter 4

White-box TFNP

4.1 The white-box model

4.2 Karchmer-Widgerson Games

4.2.1 Unsatisfiability Certificate

4.3 Circuit Characterization

4.4 The TFNP^{cc} hierarchy

4.5 An in-depth analysis: FP^{cc} = MonotoneFormulas

Chapter 5

Notes

The following definitions and proofs are a reformulation of the results shown in [BFI23; GHJ+22; RGR22]

Definition 3. A total (query) search problem R is a sequence of relations $R = \{R_n : R_n \subseteq \{0,1\}^n \times O_n\}$, one for each $n \in \mathbb{N}$, where each O_n is a finite set called outcome set, such that $\forall x \in \{0,1\}^n$ there is an $o \in O_n$ for which $(x, o) \in R_n$.

A total search problem R is in TFNP^{dt} if its solutions are verifiable through decision trees: for each $i \in O$ there is a decision tree $T_j : \{0,1\}^n \to \{0,1\}$ with poly(log n)-depth such that $T_j(x) = 1 \iff (x, j) \in R_n$.

While total search problems are formally defined as sequences $R = \{R_1, \ldots, R_n\}$, it will often make sense to speak of an individual search problem R_i in the sequence. Therefore, we will slightly abuse the notation and also call R_i a total search problem.

Definition 4. Given $R \subseteq \{0,1\}^n \times O$ and $S \subseteq \{0,1\}^m \times O'$, a decision tree reduction from R to S is defined by two sets of decision trees $\{T_i \mid T_i : \{0,1\}^n \to \{0,1\}\}$ and $\{T_j^o \mid T_j^o : \{0,1\}^n \to O\}$, for each $i \in [m]$ and each $j \in O'$, such that

$$\forall x \in \{0,1\}^n \;\; ((T_1(x), \ldots, T_m(x)), j) \in S \implies (x, T_o'(x)) \in R$$

<u>Note</u>: the o in the decision trees T_j^o is purely a notation.

To give an easier intuition of a decision tree reduction, the decision trees T_i map inputs from Q to R, while the decision trees T_o' map solutions to R back into solutions of Q. The *size* s of the reduction is the number of input bits to S, meaning that $s = m$, while the *depth* d of the reduction is the maximum depth of any tree involved in the reduction

$$d := \max(\{D(T_i) : i \in [m]\} \cup \{D(T_o') : o \in O_m\})$$

Finally, we define the *complexity* of the reduction as $\log s + d$. Moreover, we denote as $R^{dt}(S)$ the minimum complexity of any decision tree reduction from R to S. Using this definition, we can define complexity classes of total query search problems via decision tree reductions. Given a total query search problem $S = (S_n)$, we define the subclass of problems reducible to S as:

$$S^{dt} := \{R : S^{dt}(R) = \text{poly}(\log n)\}$$

where $R = (R_n)$.

Any total query search problem with solution verifiers T_o for each $o \in O$ can be *encoded* into a canonical unsatisfiable CNF formula.

Proposition 1. *Given a total query search problem $R \subseteq \{0,1\}^n \times O$, there exists an unsatisfiable* CNF *formula F defined on $|O|$-many variables such that $R = \mathsf{Search}(F)$. This formula is called the canonical* CNF *encoding of R.*

Proof. Since $R \in \mathsf{TFNP}^{dt}$, for each $o \in O$ there is a $\mathrm{poly}(\log n)$-depth decision tree T_o that verifies R. Then, for each T_o, let C_o be the clause obtained by taking the disjunction over the conjunction of the literals along each of the accepting paths in T_o, meaning that C_o is a DNF and, by De Morgan's theorem, that $\overline{C_o}$ is a CNF.

Let $F := \bigwedge_{o \in O} \overline{C_o}$. Since each R is a total search problem, for each input there is a valid output, implying that at least one tree T_o will have an accepting path. Hence, by definition of C_o, we get that $\overline{C_o} = 0$, implying that there will always be a false clause in F and thus that F is an unsatisfiable CNF.

concluding that:

$$(x, o) \in R \iff T_o(x) = 1 \iff \overline{C_o} = 0 \iff (x, o) \in \mathsf{Search}(F)$$

$\square$

This result implies that black-box TFNP is *exactly* the study of the false clause search problem. Then, instead of studying a total search problem R, it's sufficient to study the search problem $\mathsf{Search}(F)$ associated with the canonical CNF encoding F of R.

Given a proof system P and an unsatisfiable CNF formula F, we define the *complexity required by P to prove F*, denoted with $P(F)$, as:

$$P(F) := \min_{\Pi \ P\text{-proof of } F} (\deg(\Pi) + \log \mathrm{size}(\Pi))$$

where deg is the *degree* of the proof, which is a measure defined by the proof system itself. For example, for the Resolution proof system the degree is defined as the *width* of the proof, which is the maximum number of literals in any clause in Π.

Definition 5. Given $R \in \mathsf{TFNP}^{dt}$, we say that R *characterizes* and a proof system P (and that P *characterizes* R) if it holds that $R^{dt} = \{\mathsf{Search}(F) : P(F) = \mathrm{poly}(\log n)\}$.

Many of such characterizations hold in the following stronger sense. In particular, for any of the common "natural" proof systems P, if R is the problem that characterizes P then for any unsatisfiable CNF F it holds that $P(F) = \theta(R^{dt}(\mathsf{Search}(F)))$.

Definition 6. Given a proof system P, the reflection principle Ref_P states that P-proofs are sound: if Π is a P-proof of a CNF formula H then H must be unsatisfiable for any assignment α. Formally, we sat that:

$$\mathrm{Proof}_P(H, \Pi) \implies \mathrm{Unsat}(H, \alpha)$$

Tree-like resolutions for an unsatisfiable CNF formula are strictly connected to the decision trees that solve its associated search problem. In particular, it can be proven that the smallest tree-like refutation has the exact same structure of the smallest decision tree.

Lemma 1. *[BGL13] Let F be an unsatisfiable* CNF *formula. If there is a tree-like refutation of F with structure T, there also exists a decision tree with structure T that solves* $\mathsf{Search}(F)$

Proof. We procede by induction on the size s of the refutation of F.

Let $F = C_1 \wedge \ldots \wedge C_m$. If $s = 1$, then the refutation is made up of only one step that ends with the empty clause, implying that $\exists i \in [m]$ such that $F = C_i = \bot$. Hence, $\mathsf{Search}(F)$ can be solved by the decision tree made of only one vertex labeled with i.

We now assume that every formula with a tree-like refutation with a structure of size s there exists a decision tree with the same structure that solves the search problem associated with the formula.

Suppose now that the size s of the refutation is bigger than 1. Let x be the last variable resolved by the refutation and let T_0 and T_1 be the subtrees of T such that x is the root of T_0 and $\overline{x}$ is the root of T_1.

Consider now the formulas $F\restriction_{x=0}$ and $F\restriction_{x=1}$, respectively corresponding the formula F with the value 0 or 1 assigned to x. It's easy to see that the subtrees T_0 and T_1 are valid refutations of the formulas $F\restriction_{x=0}$ and $F\restriction_{x=1}$: if $b = 0$, then x evaluates to 0, otherwise if $b = 1$ then $\overline{x}$ evaluates to 0.

Since T_0 and T_1 have size $s - 1$, by inductive hypothesis there exist two decision tree with structure T_0 and T_1 that solve $\mathsf{Search}(F\restriction_{x=0})$ and $\mathsf{Search}(F\restriction_{x=1})$.

Finally, the search problem $\mathsf{Search}(F)$ can be solved by the decision tree that queries x and proceeds with the decision tree T_b based on the value $b \in \{0, 1\}$ such that $x = b$.

□

Definition 7. Given two rooted trees T and T', we say that T is embeddable in T' if there exists a mapping $f : V(T) \to V(T')$ such that, for any vertices $u, v \in V(T)$, if u is a parent of v in T then $f(u)$ is an ancestor of $f(v)$ in T'.

Lemma 2. *[BGL13; LNN+95] Let F be an unsatisfiable* CNF *formula. If there is a decision tree with structure T that solves* $\mathsf{Search}(F)$*, there also exists a tree-like refutation of F with structure T' such that T' is embeddable in T.*

Proof. The main idea is to associate inductively, starting from the leaves, a clause to each vertex of T in order to transform T in a tree-like refutation of F. In particular, each vertex v gets associated to a clause $C(v)$ such that every input of the decision tree that reaches v falsifies $C(v)$.

Let $F = C_1 \wedge \ldots \wedge C_m$. For all $i \in [m]$, we associate the clause C_i to the leaf of T labeled with i. This constitutes our base case.

Consider now a vertex v that isn't a leaf. Let x be the variable that labels v and let u_0, u_1 be the vertices such that the edge (v, u_0) is taken if $x = 0$ and the edge (v, u_1) is taken if $x = 1$. By induction, assume that u_0 and u_1 have already been associated with the clauses C_0 and C_1.

By way of contradiction, suppose that C_0 contains the literal $\overline{x}$. Then, since in a decision tree each variable can be queried only once in every path, there will always be an input with $x = 0$ that reaches v. Since $x = 0$ and since C_0 contains $\overline{x}$, this input would satisfy C_0, contradicting the fact that C_0 was associated to u_0 in a way that it is falsified by every input.

Thus, the only possibility is that C_0 can't contain the literal $\overline{x}$. Similarly, we can show that C_1 can't contain the literal x. This leaves us with only two possibilities: either $C_0 = x \vee \alpha$ and $C_1 = \overline{x} \vee \beta$ or one of C_0, C_1 doesn't contain $x, \overline{x}$.

In the first case, we can simply associate to v the clause $C = \alpha \vee \beta$. In the second case, we associate to v the clause that doesn't contain $x, \overline{x}$ (chose any of them if both clauses do not contain $x, \overline{x}$).

In particular, we notice that the first case directly emulates the resolution rule, while the second case essentially represent "redundant steps". By "skipping" these redundant steps, we can obtain a tree T' that is embeddable in T and that contains only nodes on which the first case was applied. Finally, it's easy to deduce that the root node of T' will always be associated with the empty clause $\perp$, concluding that T' is the structure of a tree-like refutation of F.

$\square$

Theorem 1. *Let F be an unsatisfiable* CNF *formula. The smallest tree-like refutation of F has size s and depth d if and only if the smallest decision tree solving* Search(F) *has size s and depth d.*

Proof. Let s and d be the size and depth of the smallest tree-like refutation of F. Likewise, let x and y be the size and depth of the smallest decision tree solving Search(F).

Then, by Lemma 1, we know that there exists a decision tree that solved Search(F) with the same structure of the smallest refutation. Let α and β be the size and depth of this decision tree. It's easy to see that $s = \alpha \geq x$ and $d = \beta \geq y$.

Viceversa, by Lemma 2, we know that there exists a tree-like refutation of F such that its structure is embeddable in the one of the smallest decision tree. Let γ and β be the size and depth of this tree-like refutation. Since the latter is embedded in the smallest decision tree, it's structure must be smaller or equal. Hence, it's easy to see that $x \geq \gamma \geq s$ and $y \geq \delta \geq d$. Thus, we can conclude that $s = x$ and $d = y$. $\square$

Note: [RGR22] says that this theorem should be generalizable to each tree and not only for the smallest trees (doubt this is true)

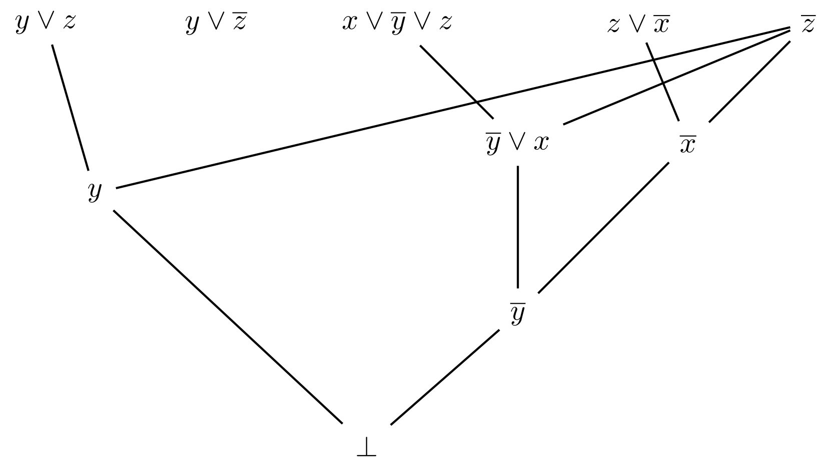

Figure 5.1. Dag-like refutation of the previous formula

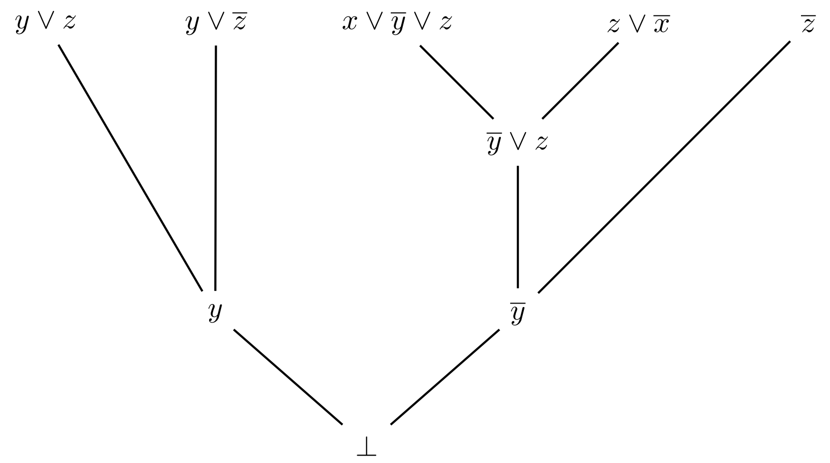

Figure 5.2. Tree-like refutation of the previous formula

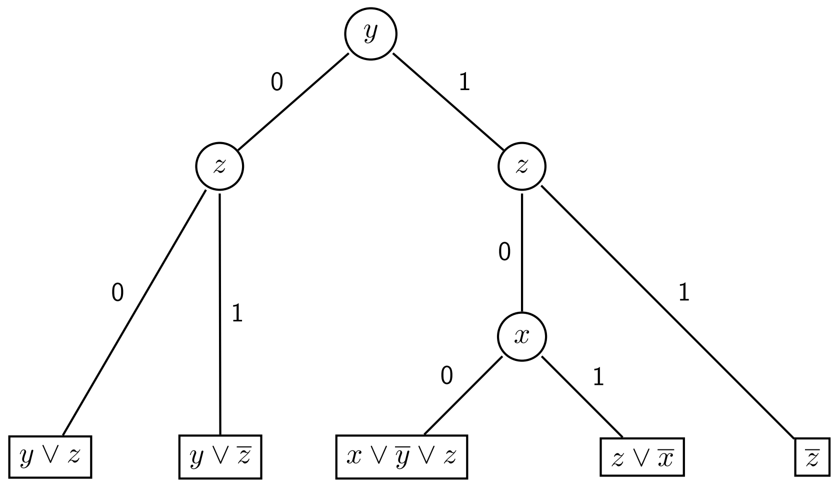

Figure 5.3. Decision tree for the previous formula

5.1 The $\frac{1}{3}, \frac{2}{3}$ lemma

Definition 8. Given a tree T and a node v, we denote as T_v the subtree of T having v as its radix.

Lemma 3 (Lewis' $\frac{1}{3}, \frac{2}{3}$ lemma [**1-3_2-3**])**.** *If T is a binary tree of size $s > 1$ then there is a node v such that the subtree T_v has size between $\left\lfloor \frac{1}{3}s \right\rfloor$ and $\left\lceil \frac{2}{3}s \right\rceil$.*

Proof. Let r be the radix of T and let ℓ be a leaf of T with the longest possible path $r \to \ell$. Let $v_1, \dots, v_k$ be the nodes of such path, where $r = v_1$ and $\ell = v_k$. For each index i such that $1 \leq i \leq k$, let $a_i b_i$ be the two children of v_i.

Claim 3.1. For any index i, if T_{v_i} has size at least $\left\lfloor \frac{1}{3}s \right\rfloor$ then for some index j, where $i \leq j \leq k$, it holds that T_{v_j} has size between $\left\lfloor \frac{1}{3}s \right\rfloor$ and $\left\lceil \frac{2}{3}s \right\rceil$.

Proof of the claim. If T_{v_i} has also size less than $\left\lceil \frac{2}{3}s \right\rceil$ then we are done. Otherwise, since $T_{v_i} = \{v_i\} \cup T_{a_i} \cup T_{b_i}$, one between the subtrees T_{a_i}, T_{b_i} must have size at least $\frac{1}{2} \lceil 2 \rceil 3s - 1$, meaning that it has size at least $\left\lfloor \frac{1}{3}s \right\rfloor$. If this subtree has also a size at most $\left\lceil \frac{2}{3}s \right\rceil$ then we are done. Instead, if this doesn't hold for both subtrees, we can repeat the process (assuming that $v_{i+1} := a_i$ without loss of generality) since we know that $T_{v_{i+1}}$ has size greater than $\left\lfloor \frac{1}{3}s \right\rfloor$.

By way of contradiction, suppose that this process never finds a subtree with size at most $\left\lceil \frac{2}{3}s \right\rceil$. Then, this would mean that it also holds for $v_k = \ell$. However, since ℓ is a leaf, we know that T_{v_ℓ} must have size 1, which is definitely at most $\left\lceil \frac{2}{3}s \right\rceil$ for any value of s, giving a contradiction. Thus, there must be a node that terminates the process.

□

Since $T_{v_1} = \{r\} \cup T_{a_1} \cup T_{b_1}$, we know that for both of these subtrees must have at least $\left\lfloor \frac{1}{3}s \right\rfloor$. Thus, assuming that $a_1 = v_2$, the claim directly concludes the proof.

□

5.2 Nullstellensatz

Definitions taken from [**Nullstellensatz**]

Definition 9 (Hilbert's Nullstellensatz)**.** Given the polynomials $p_1, \dots, p_m \in \mathbb{F}[x_1, \dots, x_n]$, the equation $p_1 = \ldots = p_m = 0$ is unsolvable if and only if $\exists g_1, \dots, g_m \in \mathbb{F}[x_1, \dots, x_n]$ such that $\sum\limits_{i=1}^{m} g_i p_i = 1$.

Hilbert's Nullstellensatz can be used to define the following proof system:

Definition 10 (Nullstellensatz Refutation)**.** Given the set of polynomial equations $P = \{p_1 = 0, \dots, p_m = 0\}$ over $\mathbb{F}[x_1, \dots, x_n]$, where $\mathbb{F}$ is any field, a Nullstellensatz refutation is a set of polynomials $\pi = \{g_1, \dots, g_n\} \subseteq \mathbb{F}[x_1, \dots, x_n]$ such that $\sum\limits_{i=1}^{m} g_i p_i = 1$.

The set of polynomials $P = \{p_1, \ldots, p_n\}$ is called the axiom set and the set $\pi = \{g_1, \ldots, g_n, h_1, \ldots, h_m\}$ is called proof of P.

By also adding the polynomial equations $x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0$ to the set of axioms, the NS proof system is sound and complete for the set of unsatisfiable CNF formulas. Thus, in general, given the set of axioms $P = \{p_1 = 0, \ldots, p_m = 0, x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0\}$, we say that $\pi = \{g_1, \ldots, g_m, h_1, \ldots, h_n\}$ is a CNF proof of P if:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = 1$$

For any proof $\pi = \{g_1, \ldots, g_n, h_1, \ldots, h_m\}$ of the axioms $P = \{p_1, \ldots, p_n\}$, we define the *degree of* π as:

$$\deg(\pi) = \max\{\deg(g_i p_i), \deg(h_j) + 2 \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

If P has a proof π of degree $\deg(\pi) = d$ then we say that $P \vdash_d^{\mathsf{NS}} 1$.

Proposition 2. *Given a set of axioms P, if $P \vdash_d^{\mathsf{NS}} q$ then $P, 1 - q \vdash_d^{\mathsf{NS}} 1$*

Proof. Since $P \vdash_d^{\mathsf{NS}} q$, we know that $\exists g_1, \ldots, g_m, h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = q$$

where $\deg(q) = d$.

Let $p_{m+1} := 1 - q$ and $P' = P \cup \{p_{m+1} = 0\}$. We define $g'_1, \ldots, g'_m, g'_{m+1}$ as:

$$g'_i = \begin{cases} 1 & \text{if } i = m+1 \\ g_i & \text{otherwise} \end{cases}$$

With simple algebra we get that:

$$\sum_{i=1}^{m+1} g'_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = g'_{m+1} p_{m+1} + \sum_{i=1}^{m} g'_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = (1 - q) + q = 1$$

thus $\pi = \{g'_1, \ldots, g'_{m+1}, h_1, \ldots, h_n\}$ is a proof of P. Moreover, since $\deg(q) = d$ implies that $\deg(g'_{m+1} p_{m+1}) = d$, it's easy to see that $\deg(\pi) = d$ holds, concluding that $P, 1 - q \vdash_d^{\mathsf{NS}} 1$

□

Lemma 4. *Given two disjoint axiom sets P_1, P_2, if $P_1, p \vdash_{d_1}^{\mathsf{NS}} 1$ and $P_2, 1 - p \vdash_{d_2}^{\mathsf{NS}} 1$ then $P_1, P_2 \vdash_{d_1 + d_2}^{\mathsf{NS}} 1$.*

Proof. Suppose that $P_1 = \{p_1, \ldots, p_m\}$ and $P_2 = \{q_1, \ldots, q_k\}$. Let $p_{m+1} = p$ and let $q_{k+1} = 1 - p$. By hypothesis, we know that

$$\sum_{i=1}^{m+1} g_i p_i + \sum_{j=1}^{n} a_j (x_j^2 - x_j) = 1$$

for some $g_1, \dots, g_{m+1}, a_1, \dots, a_n$, implying that:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j) = 1 - g_{m+1}p_{m+1} = 1 - g_{m+1}p$$

Likewise, we know that:

$$\sum_{i=1}^{k+1} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j) = 1$$

for some $r_1, \dots, r_{k+1}, b_1, \dots, b_n$, implying that:

$$\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j) = 1 - r_{k+1}q_{k+1} = 1 - r_{k+1}(1-p)$$

We notice that:

$$\begin{aligned}(1-p)\left(\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j)\right) &= (1-p)(1-g_{m+1}p) \\ &= 1 - g_{m+1}p - p + g_{m+1}p^2 \\ &= 1 - p\end{aligned}$$

In the last step, we used the fact that, due to multilinearity, it holds that $p^2 = p$. Proceeding the same way, we find that:

$$\begin{aligned}p\left(\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j)\right) &= p\,(1 - r_{k+1}(1-p)) \\ &= p\,(1 - r_{k+1} + r_{k+1}p) \\ &= p - r_{k+1}p + r_{k+1}p^2 \\ &= p\end{aligned}$$

Now, we define $s_1, \dots, s_{m+k}$

$$s_i = \begin{cases} g_i \cdot (1-p) & \text{if } 1 \le i \le m \\ r_i \cdot p & \text{if } m+1 \le i \le k \end{cases}$$

and $h_1, \dots, h_n$ as $h_j = a_j \cdot (1-p) + b_j \cdot p$.
At this point, through simple algebra we get that:

$$\sum_{i=1}^{m+k} s_i p_i + \sum_{j=1}^{n} h_j(x_j^2 - x_j) =$$

$$(1-p)\left(\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j)\right) + p\left(\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j)\right) =$$

$$(1-p)(1-g_{m+1}p) + p\,(1 - r_{k+1}(1-p)) = p + 1 - p = 1$$

concluding that $\pi_3 = \{s_1, \ldots, s_{m+k}, h_1, \ldots, h_n\}$ is a proof of $P_1 \cup P_2$. Furthermore, we notice that:

$$\deg((1-p)(1-g_{m+1}p)) = \deg(1-p) + \deg(1-g_{m+1}p) = d_1 + d_2$$

and that:

$$\deg(p\,(1-r_{k+1}(1-p))) = \deg(p) + \deg(1-r_{k+1}(1-p)) = d_2 + d_1$$

Finally, we get that:

$$\deg(\pi_3) = \max(\deg((1-p)(1-g_{m+1}p)), \deg(p\,(1-r_{k+1}(1-p)))) = d_1 + d_2$$

concluding that $P_1, P_2 \vdash^{\mathsf{NS}}_{d_1+d_2} 1$.

$\square$

5.3 Treelike Res and Nullstellensatz

Definition 11 ($\mathbb{F}_2$-NS encoding of Res)**.** Given a Res linear clause $C = \bigvee_{i=0}^{k_1} x_i \vee \bigvee_{j=0}^{k_2} \overline{x_j}$, the $\mathbb{F}_2$-NS encoding of C is defined as $\mathrm{enc}(C) := \prod_{i=0}^{k_1} x_i \cdot \prod_{j=0}^{k_2} (1 - x_j)$.

In general, a Res($\oplus$) formula $F = C_1 \wedge \ldots \wedge C_m$ defined on the variables $x_1, \ldots, x_n$ gets encoded in $\mathbb{F}_2$-NS as the set of axioms $P_F = \{\mathrm{enc}(C_i) = 0 \mid 1 \leq i \leq m\} \cup \{x_j^2 - x_j = 0 \mid 1 \leq j \leq n\}$.

Theorem 2. *Let F be an unsatisfiable* CNF*. If T is* Res($\oplus$) *refutation of F of size s then there is* NS *refutation of F of degree $O(\log(s))$.*

Proof. Let $F = C_1 \wedge \cdots \wedge C_n$. We proceed by strong induction on the size s.

If $s = 1$ then the T contains only the empty clause $\perp$, meaning that it also is one of the starting clauses and thus one of the axioms. We notice that $\mathrm{enc}(\perp) = 1$, which easily concludes that $\perp \vdash_0^{\mathsf{NS}} 1$.

Suppose now that $s > 1$. Let $\mathcal{L}$ be axioms of T. Since T is a binary tree, by Lemma 3 we know that there is a clause C_k, i.e. a node, of T such that T_{C_k} has size between $\left\lfloor \frac{1}{3} s \right\rfloor$ and $\left\lceil \frac{2}{3} s \right\rceil$.

Let $T' = (T - T_{C_k}) \cup \{C_k\}$. Due to the size of T_{C_k}, we get that T' has size between $\left\lfloor \frac{1}{3} s \right\rfloor + 1$ and $\left\lceil \frac{2}{3} s \right\rceil + 1$. Moreover, we notice that since T is a treelike refutation it holds that T_{C_k} and T' work with different clauses (except C_k), thus their axioms are disjoint. Let $\mathcal{L}_1, \mathcal{L}_2$ be the two sets of axioms respectively used by T_{C_k} and T'.

By construction, we notice that T_{C_k} derives the clause C_k using the axioms $\mathcal{L}_1$, while T_{C_k} derives the clause $\perp$ using the axioms $\mathcal{L}_2, C_k$. Thus, since T_{C_k} and T' have size lower than s, by induction hypothesis we get that $\mathrm{enc}(\mathcal{L}_1) \vdash_{c_1 \cdot \log s}^{\mathsf{NS}} \mathrm{enc}(C_k)$ and $\mathrm{enc}(\mathcal{L}_2), \mathrm{enc}(C_k) \vdash_{c_2 \cdot \log s}^{\mathsf{NS}} 1$ for some constants c_1, c_2. By Proposition 2 we easily conclude that $\mathrm{enc}(\mathcal{L}_1), (1 - \mathrm{enc}(C_k)) \vdash_{c_1 \cdot \log s}^{\mathsf{NS}} 1$ and, by Lemma 4, that $\mathrm{enc}(\mathcal{L}_1), \mathrm{enc}(\mathcal{L}_2) \vdash_{(c_1+c_2) \cdot \log s}^{\mathsf{NS}} 1$. Finally, since $\mathcal{L}_1 \cup \mathcal{L}_2 = \mathcal{L}$, we get that $\mathrm{enc}(\mathcal{L}) \vdash_{(c_1+c_2) \cdot \log s}^{\mathsf{NS}} 1$, meaning that $\mathcal{L}$ has a NS refutation of degree $O(\log s)$.

$\square$

5.4 Treelike $\mathsf{Res}(\oplus)$ and Nullstellensatz

Definition 12 ($\mathbb{F}_2$-NS encoding of Res)**.** Given a $\mathsf{Res}(\oplus)$ linear clause $C = \bigvee_{i=0}^{k}(\ell_i = \alpha_i)$, the $\mathbb{F}_2$-NS encoding of C is defined as $\mathrm{enc}_{\oplus}(C) := \prod_{i=0}^{k}(\alpha - \ell_i)$.

In general, a $\mathsf{Res}(\oplus)$ formula $F = C_1 \wedge \ldots \wedge C_m$ defined on the variables $x_1, \ldots, x_n$ gets encoded in $\mathbb{F}_2$-NS as the set of axioms $P_F = \{\mathrm{enc}_{\oplus}(C_i) = 0 \mid 1 \leq i \leq m\} \cup \{x_j^2 - x_j = 0 \mid 1 \leq j \leq n\}$.

Theorem 3 ([**res_parity**])**.**

1. *Every tree-like* $\mathsf{Res}(\oplus)$ *proof of an unsatisfiable formula* F *may be translated to a parity decision tree for* F *without increasing the size of the tree.*

2. *Every parity decision tree for an unsatisfiable linear CNF may be translated into a tree-like* $\mathsf{Res}(\oplus)$ *proof and the size of the resulting proof is at most twice the size of the parity decision tree (and where the weakening is applied only to the axioms).*

Corollary 1. *Every tree-like* $\mathsf{Res}(\oplus)$ *proof of an unsatisfiable formula* F *can be converted to a tree-like* $\mathsf{Res}(\oplus)$ *proof of at most double the size and with weakening applied only to the axioms.*

Acknowledgements

this is sad, alexa play despacito

Bibliography

[BCE+98] Paul Beame, Stephen Cook, Jeff Edmonds, et al. "The Relative Complexity of NP Search Problems". In: *Journal of Computer and System Sciences* 57.1 (1998), pp. 3–19. ISSN: 0022-0000. DOI: https://doi.org/10.1006/jcss.1998.1575. URL: https://www.sciencedirect.com/science/article/pii/S0022000098915756.

[BFI23] Sam Buss, Noah Fleming, and Russell Impagliazzo. "TFNP Characterizations of Proof Systems and Monotone Circuits". In: *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*. Ed. by Yael Tauman Kalai. Vol. 251. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 30:1–30:40. ISBN: 978-3-95977-263-1. DOI: 10.4230/LIPIcs.ITCS.2023.30. URL: https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2023.30.

[BG94] Mihir Bellare and Shafi Goldwasser. "The Complexity of Decision Versus Search". In: *SIAM Journal on Computing* 23.1 (1994), pp. 97–119. DOI: 10.1137/S0097539792228289. URL: https://doi.org/10.1137/S0097539792228289.

[BGL13] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. "A characterization of tree-like Resolution size". In: *Information Processing Letters* 113.18 (2013), pp. 666–671. ISSN: 0020-0190. DOI: https://doi.org/10.1016/j.ipl.2013.06.002. URL: https://www.sciencedirect.com/science/article/pii/S0020019013001592.

[DK14] Ding-Zhu Du and Ker-I Ko. "Models of Computation and Complexity Classes". In: *Theory of Computational Complexity*. 2014. Chap. 1, pp. 1–44. ISBN: 9781118595091. DOI: https://doi.org/10.1002/9781118595091.ch1. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118595091.ch1. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118595091.ch1.

[GHJ+22] Mika Göös, Alexandros Hollender, Siddhartha Jain, et al. "Separations in Proof Complexity and TFNP". In: *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*. 2022, pp. 1150–1161. DOI: 10.1109/FOCS54457.2022.00111.

[LNN+95] László Lovász, Moni Naor, Ilan Newman, et al. "Search Problems in the Decision Tree Model". In: *SIAM J. Discret. Math.* 8.1 (Feb. 1995), pp. 119–132. ISSN: 0895-4801. DOI: 10.1137/S0895480192233867. URL: https://doi.org/10.1137/S0895480192233867.

[RGR22] Susanna F. de Rezende, Mika Göös, and Robert Robere. “Proofs, Circuits, and Communication”. In: *ArXiv* abs/2202.08909 (2022). URL: https://api.semanticscholar.org/CorpusID:246996726.