Thesis Draft: Algebrization

A Thesis
Presented to
The Established Interdisciplinary Committee for
Mathematics and Computer Science
Reed College

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Arts

Patrick Norton

February 9, 2025

Approved for the Committee
(Mathematics and Computer Science)

Zajj Daugherty	Adam Groce

Contents

Introduction

The P vs NP problem is perhaps the most important open problem in complexity theory.

Chapter 1

Preliminaries

1.1 Turing machines

Central to our definitions of complexity is that of a Turing machine. This is the most common mathematical model of a computer, and is the jumping-off point for mant variants. There are many ways to think of a Turing machine, but the most common is that of a small machine that can read and write to an arbitrarily-long "tape" according to some finite set of rules. We give a more formal definition below, and then we will attempt to take this definition into a more manageable form.

Definition 1.1.1 ([23, Def. 3.1])**.** A *Turing machine* is a 7-tuple $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ where Q, Σ, and Γ are all finite sets and

1. Q is the set of *states*,
2. Σ is the *input alphabet*,
3. Γ is the *tape alphabet*,
4. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ is the *transition function*,
5. $q_0 \in Q$ is the *start state*,
6. $q_a \in Q$ is the *accept state*,
7. $q_r \in Q$ is the *reject state*, with $q_a \neq q_r$.

While we have this formalism here as a useful reference, even here we will most frequently refer to Turing machines in a more intuitionisitc form. There are several ways we will think about Turing machines.

The first way to think about a Turing machine is as a little computing box with a tape. We let the box read and write to the tape, and each step it can move the tape one space in either direction. At some point, the machine can decide it is done, in which case we say it "halts"; however it does not necessarily need to halt. For this paper, we will only think about machines that *do* halt, and in particular we will care about how many it takes us to get there. Further, we will use this informalism as a base from which we can define our Turing machine variants intuitively, without needing to deal with the (potentially extremely convoluted) formalism.

Another way we think about a Turing machine is as an algorithm. Perhaps the foundational paper of modern computer science theory, the *Church-Turing thesis* [25], states that any actually-computable algorithm has an equivalent Turing machine, and vice versa. We will use this fact liberally; in many cases we will simply describe an algorithm and not deal with putting it into the context of a Turing machine. If we have explained the algorithm well enough that a reader can execute it (as we endeavor to do), then we know a Turing machine must exist.

Definition 1.1.2. A *nondeterministic Turing machine* is

1.2 Complexity classes

Complexity classes are the main way we think about the hardness of problems in computer science. A complexity class is a collection of languages that all share a common level of difficulty.

We start with a relatively straightforward example of a complexity class: the class of languages that a Turing machine can recognize. First, we need to define what recognition is in order to make a complexity class out of it.

Definition 1.2.1 ([23, Def. 3.2])**.** A language L is *recognized* by a Turing machine M if for all strings $s \in L$, M halts in the accept state when given s as input.

Now, since our complexity classes are about *languages*, we naturally wish to extend our notion of recognition to a statistic on languages.

Definition 1.2.2. A language L is *Turing-recognizable* (frequently just *recognizable*) if it is recognized by some Turing machine.

Now that we have a property of languages, it is straightforward for us to turn it into a complexity class.

Definition 1.2.3. The class RE is the class of all Turing-recognizable languages.

For most other classes, we want our Turing machines to halt on *all* inputs, not just those in the class. From a practical perspective, this is useful because it tells us that we can be certain about whether any given string is in the given language. From here on, we will generally care about how much of some resource our machines take when making their decision, as opposed to whether or not they can.

1.2.1 Time complexity

The most intuitive (and most important) notion of complexity is that of time complexity. Time complexity is the answer of the question of how long it takes to solve a problem. We begin with an abstract base for our time classes, and will then introduce some specific ones that we care about.

Definition 1.2.4 ([2, Def. 1.19])**.** Let $f : \mathbb{N} \to \mathbb{N}$ be a function. The class $\mathsf{DTIME}(f(n))$ is the class of all problems computable by a deterministic Turing machine in $O(f(n))$ steps for some constant $c > 0$.

While DTIME is a useful base to start from, it is rare that we deal with DTIME classes directly.

Definition 1.2.5 ([2, Def. 1.20])**.** The complexity class P is the class

$$\mathsf{P} = \bigcup_{c>0} \mathsf{DTIME}(n^c).$$

The class P is perhaps the most important complexity class. Mathematically, we care about P because it is closed under composition: a polynomial-time algorithm iterated a polynomial number of times is still in P. Further, P turns out to generally be invariant under change of (deterministic) computation model, which allows us to reason about P problems easily without needing to resort to the formal definition of a Turing machine. More philosophically, P generally represents the set of "efficient" algorithms in the real world.[1]

Example 1.2.5.1. The language

$$\{(p, x, y) \mid p \text{ a polynomial and } p(x) = y\}$$

is in P. We can calculate whether a string is in this language by calculating $p(x)$ (which we can do efficiently), and then comparing it to y.

[1] It is worth mentioning that this is a *mathematical* efficiency—there are plenty of algorithms in P that a real-world computer scientist would never dare to call efficient.

As we have defined P in terms of DTIME, the question arises of whether there is an equivalent in terms of NTIME. Naturally, there is, and we call it NP.

Definition 1.2.6 ([23, Cor. 7.22])**.** The complexity class NP is the class

$$\mathsf{NP} = \bigcup_{c>0} \mathsf{NTIME}(n^c).$$

While this definition demonstrates how NP is similar to P, there are other equivalent ones that we can use. In particular, we very often like to think of NP in terms of deterministic *verifiers*. Since nondeterministic machines do not exist in real life, this definition gives a practical meaning to NP.

Example 1.2.6.1. The language SAT is the language of Boolean formulas with at least one solution. SAT is in NP: we can nondeterministically pick a potential solution and then evaluate our formula (which can be done efficiently); there will be an accepting path if and only if a solution to the formula exists.

Theorem 1.2.7 ([23, Def. 7.19])**.** NP *is exactly the class of all languages verifiable by a* P*-time Turing machine.*

Example 1.2.7.1. The language SAT we defined in Example 1.2.6.1 can be verified efficiently, where the certificate is an accepting set of variables. Since we can evaluate a Boolean formula efficiently, if we already have an accepting set of variables we can therefore verify it in P.

The next step up from polynomial complexities is that of exponential complexities. For these, instead of having the classes bounded above by a polynomial, we have the classes bounded above by 2 to the power of a polynomial. While we use 2 as the base, the value of the base turns out not to matter since for any $a, b > 1$,

$$a^{n^c} = b^{n^c \log_b(a)} \in O\left(b^{n^{c+1}}\right). \tag{1.1}$$

Definition 1.2.8 ([2, §2.6.2])**.** The complexity class EXP is the class

$$\mathsf{EXP} = \bigcup_{c>0} \mathsf{DTIME}\left(2^{n^k}\right).$$

Definition 1.2.9 ([2, §2.6.2])**.** The complexity class NEXP is the class

$$\mathsf{NEXP} = \bigcup_{c>0} \mathsf{NTIME}\left(2^{n^k}\right).$$

It is immediate that $\mathsf{P} \subseteq \mathsf{EXP}$ and $\mathsf{NP} \subseteq \mathsf{NEXP}$ (since the exponential classes allow the use of more of the same resource). Of slightly less-trivial interest is the relationship between NP and NEXP.

Theorem 1.2.10. $\mathsf{NP} \subseteq \mathsf{EXP}$.

Proof. If a nondeterministic machine solves a problem in $p(n)$ steps, it follows that the total number of branches is less than $a^{p(n)}$, where a is the maximum number of branches for a node within the machine. Hence, we can simulate the machine deterministically by simply enumerating every branch, giving us a total computation time of $p(n)a^{p(n)}$, which is in $O(2^{q(n)})$ for some other polynomial $q(n)$. Hence any NP problem is in EXP. □

It is perhaps illustrative to see an example of a problem in NEXP.

Definition 1.2.11 ([7, Def. 14.1])**.** The *oracle 3-satisfiability problem*, denoted O3SAT, is the language of all triplets (r, s, B), where $r, s \in \mathbb{N}^+$ and $B : \{0,1\}^{r+3s+3} \to \{0,1\}$ a boolean function, such that there exists a boolean function $A : \{0,1\}^s \to \{0,1\}$ having the property that for all $z \in \{0,1\}^r$ and $b_1, b_2, b_3 \in \{0,1\}^s$,

$$B(z, b_1, b_2, b_3, A(b_1), A(b_2), A(b_3)) = 1.$$

Theorem 1.2.12. O3SAT $\in$ NEXP.

Proof. We present the following non-deterministic algorithm to determine if $(r, s, B) \in$ O3SAT:

Input: A triplet (r, s, B)
Output: Whether or not $(r, s, B) \in$ O3SAT

```
1  Nondeterministically choose a function A : {0,1}^s → {0,1};
2  for z ∈ {0,1}^r do
3  |  for b_1, b_2, b_3 ∈ {0,1}^s do
4  |  |  Compute B(z, b_1, b_2, b_3, A(b_1), A(b_2), A(b_3));
5  |  |  if the above is not 1 then
6  |  |  |  return 0;
7  |  |  end
8  |  end
9  end
10 return 1;
```

Algorithm 1.1: A NEXP-time algorithm for determining O3SAT

□

1.2.2 Space complexity

In addition to time complexity, the an additional notion of complexity is that of space complexity. Space complexity is the question of how much space on its memory tape a machine needs in order to compute a problem. In many ways, our definitions of space complexity are analagous to those for time complexity that we have already defined. In particular, DSPACE will correspond nicely to DTIME, and NSPACE to NTIME.

Definition 1.2.13 ([2, Def. 4.1])**.** Let $f : \mathbb{N} \to \mathbb{N}$ be a function. A language L is in DSPACE$(f(n))$ if there exists a deterministic Turing machine M such that the number of locations on the tape that are non-blank at some point during the execution of M is in $O(f(n))$.

In the same way as we have defined DSPACE for deterministic machines, we now need to define NSPACE for nondeterministic machines.

Definition 1.2.14 ([2, Def. 4.1])**.** Let $f : \mathbb{N} \to \mathbb{N}$ be a function. A language L is in NSPACE$(f(n))$ if there exists a nondeterministic Turing machine M such that the number of locations on the tape that are non-blank at some point during the execution of M is in $O(f(n))$.

Analagously to P and NP, our two main classes of space complexity are PSPACE and NPSPACE.

Definition 1.2.15 ([2, Def. 4.5])**.** The complexity class PSPACE is the class

$$\mathsf{PSPACE} = \bigcup_{c>0} \mathsf{DSPACE}(n^c).$$

Definition 1.2.16 ([2, Def. 4.5])**.** The complexity class NPSPACE is the class

$$\mathsf{NPSPACE} = \bigcup_{c>0} \mathsf{NSPACE}(n^c).$$

Unlike with P and NP, the relationship between PSPACE and NPSPACE is well known. Due to the complexity of the proof of the theorem, we will not prove it here, as it is mostly not relevant to what we will be doing.

Theorem 1.2.17 (Savitch's theorem; [21])**.** PSPACE = NPSPACE.

Upon seeing this, one might ask why it is that we believe P $\neq$ NP if we know that PSPACE = NPSPACE, given they are defined analogously. The answer to this question boils down to the fact

that we are able to reuse space, while we are not able to reuse time. Space on the tape that is no longer needed can be overwritten, while time that is no longer needed is gone forever.

Since PSPACE and NPSPACE are equal classes, it is relatively rare to see NPSPACE referred to. Here, we will only refer to it when it makes a class relationship clearer; most frequently when comparing NPSPACE to some other nondeterministic class.

Example 1.2.17.1. The language

$$\{(x, y) \mid x, y \text{ regexes that accept the same set of strings}\}$$

is in PSPACE.

1.2.3 Completeness

Even within a complexity class, not all problems are created equal. The notion of *completeness* gives us a mathematically-rigorous way to talk about which problems in a class are the hardest. Since putting upper bounds on hard problems naturally puts those same bounds on any easier problems, complete problems can be useful in reasoning about the relationship between complexity classes.

Definition 1.2.18 ([23, Def. 7.29])**.** A language A is *polynomial-time reducible* to a language B if a polynomial-time computable function $f : \Sigma^* \to \Sigma^*$ exists such that for all $w \in \Sigma^*$, $w \in A$ if and only if $f(w) \in B$.

Polynomial-time reductions are important because they give us a way to say that A is *no harder* than B. In particular, if we have an algorithm M that determines B, we can construct the following algorithm that determines A with only a polynomial amount of additional work:

Input: A string $w \in \Sigma^*$
Output: Whether $w \in A$
1 Compute $f(w)$;
2 Use M to check whether $f(w) \in B$;
3 **return** *the result of* M;

Algorithm 1.2: An algorithm to reduce A to B

Definition 1.2.19 ([23, Def. 7.34])**.** A language L is NP-complete if $L \in \mathsf{NP}$ and every $A \in \mathsf{NP}$ is polynomial-time reducible to L.

This is a practical use of our polynomial-time reductions: since an NP-complete language has a reduction from every other language in NP, it follows that it is *at least as hard* as any other language in NP. Of particular interest to complexity theorists is the fact that $\mathsf{P} = \mathsf{NP}$ if and only if *any* NP-complete language is in P.

Example 1.2.19.1. A famous result of Cook [8], also proved around the same time by Levin and thus called the *Cook-Levin theorem*, is that the SAT problem we defined earlier in Example 1.2.6.1 is NP-complete.

The notion of completeness is very important to complexity theorists. Since these are the "hardest" problems in NP, this means that if we can do anything interesting to an NP-complete problem, we can leverage these reductions to do that interesting thing to *any* other problem in NP with only a little (i.e. polynomial) more effort. This will come in especially handy when we want to prove that complexity classes are equal or that NP is a subset of some other complexity class–since most complexity classes allow for things to change polynomially, we only need to prove that a single NP-complete element is in the other class for the subset relation to follow.

Along with completeness for NP, we have a notion of completeness for NEXP. While you might expect that the reducibility constraints might loosen (i.e. allow more complex reductions) since NEXP is more complex for NP, but this turns out not to be the case. In particular, while it might initially seem logical to allow for EXP-reductions, it turns out that NEXP is not closed under EXP-reductions, which makes a notion of completeness challenging. Despite this, we can still learn interesting things about NEXP by studing completeness under polynomial reductions.

Definition 1.2.20. A language L is NEXP-complete if $L \in \mathsf{NEXP}$ and every $A \in \mathsf{NEXP}$ is polynomial-time reducible to NEXP.

NEXP-completeness has many of the same nice properties of NP-completeness. Of particular interest to us will again be the ease with which NEXP-completeness allows us to determine subset relations, simply by proving the inclusion of a single complete language.

Theorem 1.2.21 ([4, Proposition 4.2])**.** *The language* O3SAT *(as defined in Definition 1.2.11) is* NEXP*-complete.*

Proof. We demonstrated in Theorem 1.2.12 that $\mathsf{O3SAT} \in \mathsf{NEXP}$, so all that remains is to prove that reductions exist for every NEXP language. Let $L \in \mathsf{NEXP}$, and let $x \in \{0,1\}^n$. We aim to construct an algorithm in $\mathsf{P}^{\mathsf{O3SAT}}$ that computes L. □

Just as we have NP-completeness and NEXP-completeness for time complexity, we also have notions of completeness for space complexity. Since PSPACE = NPSPACE, instead of calling the class NPSPACE-complete, we call it PSPACE-complete.

Definition 1.2.22 ([23, Def. 8.8])**.** A language L is PSPACE-complete if $L \in \mathsf{PSPACE}$ and every $A \in \mathsf{PSPACE}$ is polynomial-time reducible to NP.

While this definition is mostly analagous to that of NP-completeness, one might wonder why we use a time complexity for our reduction when PSPACE is a space-complexity class. This is because if we were to use space complexity, we would want to use PSPACE-reductions, but that would make every language in PSPACE trivially PSPACE-complete. Since that is not a useful definition, we instead restrict ourselves to polynomial-time reductions.

Example 1.2.22.1. A result of Stockmeyer and Meyer [24] is that the language we defined in Example 1.2.17.1 is PSPACE-complete.

1.2.4 Counting complexity

Definition 1.2.23. A *counting problem* is

Definition 1.2.24 ([2, Def. 9.2])**.** The class #P is the class of functions $f : \{0,1\}^* \to \mathbb{N}$ such that there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a polynomial-time Turing machine M such that for every $x \in \{0,1\}^*$,

$$f(x) = \left| \left\{ y \in \{0,1\}^{p(|x|)} \;\middle|\; M(x,y) = 1 \right\} \right|. \tag{1.2}$$

Definition 1.2.25. A language is #P-complete if

Definition 1.2.26. The function #SAT is the function that, given a Boolean formula ϕ, returns the number of distinct assignments such that ϕ is true.

Theorem 1.2.27. #SAT *is* #P*-complete.*

1.3 Polynomials

Definition 1.3.1 ([17])**.** Let P be a mathematical statement. The function $[P]$ is the the function

$$[P] = \begin{cases} 1 & P \text{ is true} \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

This is called the *Iverson bracket*, after its inventor Kenneth Iverson, who originally included it in the programming language APL[2] [12, p. 11].

[2]The original notation used parentheses, but square brackets are much less ambiguous, so that has become the standard and what we will use here.

Example 1.3.1.1. Using the Iverson bracket, the Kronecker delta function can be defined as

$$\delta_{ij} = [i = j].$$

Much of our work will deal with multivariate polynomials. For a given field $\mathbb{F}$, we will denote the set of m-variable polynomials over $\mathbb{F}$ with $\mathbb{F}[x_{1,\dots,m}]$.

Definition 1.3.2 ([1, p. 8])**.** The *multidegree* of a multivariate polynomial p, written $\operatorname{mdeg}(d)$, is the maximum degree of any variable x_i of p.

It is worth noting that for monovariate polynomials, multidegree and degree coincide. The difference between multidegree and degree is subtle, but important. We shall illustrate the difference with a simple example.

Example 1.3.2.1. Consider the polynomial $x_1^2 x_2 + x_2^2$. The multidegree of this polynomial is 2, while its degree is 3.

We denote by $\mathbb{F}[x_{1,\dots,m}^{\leq d}]$ the subset of $\mathbb{F}[x_{1,\dots,m}]$ of polynomials with multidegree at most d. We also need two special cases of these polynomials, which we will want to quickly be able to reference throughout the paper.

Definition 1.3.3 ([1, p. 8])**.** A polynomial is *multilinear* if it has multidegree at most 1. Similarly, a polynomial is *multiquadratic* if it has multidegree at most 2.

From here, we need to define the notion of an *extension polynomial*. This gives the ability to take an arbitrary multivariate function defined on a subset of a field and extend it to be a multivariate polynomial over the *whole* field.

Definition 1.3.4 ([1, p. 8])**.** Let $\mathbb{F}$ be a finite field, $H \subseteq \mathbb{F}$, $m \in \mathbb{N}$ a number, and $f : H^m \to \mathbb{F}$ be a function. An *extension polynomial* of f is any polynomial $f' \in \mathbb{F}[x_{1,\dots,m}]$ such that $f(h) = f'(h)$ for all $h \in H$.

It turns out that this polynomial needs only to be of a surprisingly low multidegree. Since polynomials of lower degree are generally easier to compute, we would like to have some measure of what a "small" polynomial actually is in this context.

Definition 1.3.5 ([7, §5.1])**.** Let $\mathbb{F}$ be a finite field, $H \subseteq \mathbb{F}$, $m \in \mathbb{N}$ a number, and $f : H^m \to \mathbb{F}$ be a function. A *low-degree extension* $\hat{f}$ of f is an extension of f with multidegree at most $|H| - 1$.

It turns out that this is the minimum possible degree of any extension polynomial. Further, it turns out that for any f, there is a *unique* low-degree extension. Neither of these statements are particularly important for our further work, so we will not endeavor to prove them here. Something of practical use to us is an explicit formula for the low-degree extension, which we shall now calculate.

Theorem 1.3.6 ([7, §5.1])**.** *Let $\mathbb{F}$ be a finite field, $H \subseteq \mathbb{F}$, $m \in \mathbb{N}$ a number, and $f : H^m \to \mathbb{F}$. Then a low-degree extension $\hat{f}$ of f is the function*

$$\hat{f}(x) = \sum_{\beta \in H^m} \delta_\beta(x) f(\beta), \tag{1.4}$$

where δ is the polynomial

$$\delta_x(y) = \prod_{i=1}^{m} \left(\sum_{\omega \in H} \left(\prod_{\gamma \in H \setminus \{\omega\}} \frac{(x_i - \gamma)(y_i - \gamma)}{(\omega - \gamma)^2} \right) \right). \tag{1.5}$$

Proof. First, we must show $\hat{f}$ has multidegree $|H| - 1$. First, note that $\hat{f}$ is a linear combination of some $\delta_x$es; hence asking about the multidegree of $\hat{f}$ is really just asking about the multidegree of δ_x. Looking at δ_x, the innermost product has $|H| - 1$ terms, each with the same y_i; thus those

terms have multidegree $|H| - 1$. Summing terms preserves their multidegree, and the outer product iterates over the variables, thus it preserves multidegree as well. Thus, δ_x has multidegree $|H| - 1$.

To understand why $\hat{f}(x)$ agrees with $f(x)$ on H, we first should look at $\delta_\beta(x)$. In particular, for all $x, y \in H^m$,

$$\delta_y(x) = [x = y] = \delta_{xy}. \tag{1.6}$$

This can be shown through some algebra which we have worked through in full detail in Appendix A. This is the reason why we have named the polynomial in Equation (1.5) as we have; it functions as the Kronecker delta function over the set H^m.

Taking the above statement, we get that for all $x \in H^m$, the only nonzero term of $\hat{f}(x)$ is the term where $\beta = x$; thus $\hat{f}(x) = f(x)$. Hence, $\hat{f}$ is a low-degree extension of f. □

Of particular interest to us will be the case of low-degree extensions where $H = \{0, 1\}$. Since every field contains both 0 and 1, this will allow us to construct a set consisting of an extension for *every* field. Further, since $|H| = 2$ here, it means our low-degree extensions will be multilinear. Not only do we thus constrain our polynomial to have a very low multidegree, the δ function also dramatically simplifies in this case, which makes it much easier to reason about.

Corollary 1.3.7 ([1, §4.1])**.** *Let $\mathbb{F}$ be a finite field, $m \in \mathbb{N}$ a number, and $f : \{0, 1\}^m \to \mathbb{F}$. Then*

$$\hat{f}(x) = \sum_{\beta \in \{0,1\}^m} \delta_\beta(x) f(\beta) \tag{1.7}$$

is a low-degree extension of f, where δ is the polynomial

$$\delta_y(x) = \left(\prod_{i : y_i = 1} x_i \right) \left(\prod_{i : y_i = 0} (1 - x_i) \right). \tag{1.8}$$

Note that in the product bound $i : y_i = 1$, we mean the product over all numbers i such that $y_i = 1$.

As we can see, the form of δ in Equation (1.8) is much more manageable than the form in Equation (1.5), and it is perhaps more immediately apparent here why δ has the property it does. Further, since this equation has no division, it turns out that it is valid for arbitrary (non-trivial) rings, while the more complex equation is only valid for fields. We show the algebra that brings us from the first to the second in Appendix A.

The form of δ_y defined in Equation (1.8) has further use to us than just being simpler. In particular, these δ_y form a basis of multilinear polynomials (and hence a generating set for the ring of all polynomials). This is a particularly useful basis because it allows us to reason about multilinear polynomials based solely on their outcomes on the Boolean cube.[3]

Theorem 1.3.8 ([1, §4.1])**.** *For any field $\mathbb{F}$, the set $\{\delta_x \mid x \in \{0, 1\}^n\}$ forms a basis for the vector space of multilinear polynomials $\mathbb{F}^n \to \mathbb{F}$.*

Proof. Since $\delta_y(x) = 0$ for all $y \neq x \in \{0, 1\}^n$, it follows that the only way to get

$$\sum_{y \in \{0,1\}^n} a_y \delta_y = 0 \tag{1.9}$$

is to have each $a_y = 0$. Hence the set of δ_x is linearly independent. Further, the vector space of multilinear polynomials has 2^n dimensions; since there are 2^n distinct δ_x polynomials, it follows that they form a basis. □

Now, we can use this fact to prove some cases where our low-degree extensions turn out to have a particularly low degree. Unfortunately, these do have a lot of qualifiers to them, but they will be useful in later theorems (in particular Lemma 1.3.10).

[3] As an aside, this fact provides a relatively slick proof of the special case of our unproven statement earlier that low-degree extensions are both of minimal degree and unique.

Theorem 1.3.9 ([1, Theorem 4.3]). *Let $\mathbb{F}$ be a field and $Y \subseteq \mathbb{F}^n$ be a set of t points $y_1, \ldots, y_t$. Then for at least $2^n - t$ Boolean points $w \in \{0,1\}^n$, there exists a multiquadratic extension polynomial $p : \mathbb{F}^n \to \mathbb{F}$ such that*

1. *$p(y_i) = 0$ for all $i \in [t]$,*
2. *$p(w) = 1$,*
3. *$p(z) = 0$ for all Boolean $z \neq w$.*

Proof. □

Lemma 1.3.10 ([1, Lemma 4.5]). *Let $\mathcal{F}$ be a collection of fields. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and for every $\mathbb{F} \in \mathcal{F}$, let $p_{\mathbb{F}} : \mathbb{F}^n \to \mathbb{F}$ be a multiquadratic polynomial over $\mathbb{F}$ extending f. Also let $\mathcal{Y}_{\mathbb{F}} \in \mathbb{F}^n$ for each $\mathbb{F} \in \mathcal{F}$, and define $t = \sum_{\mathbb{F} \in \mathcal{F}} |\mathcal{Y}_{\mathbb{F}}|$.*

Then, there exists a subset $B \subseteq \{0,1\}^n$, with $|B| \leq t$, such that for all Boolean functions $f' : \{0,1\}^n \to \{0,1\}$ that agree with f on B, there exist multiquadratic polynomials $p'_{\mathbb{F}} : \mathbb{F}_n \to \mathbb{F}$ (one for each $\mathbb{F} \in \mathcal{F}$) such that

1. *$p'_{\mathbb{F}}$ extends f', and*
2. *$p'_{\mathbb{F}}(y) = p_{\mathbb{F}}(y)$ for all $y \in \mathcal{Y}_{\mathbb{F}}$.*

Proof. Call $z \in \{0,1\}^n$ *good* if for every $\mathbb{F} \in \mathcal{F}$ there exists a multiquadratic poylnomial $u_{\mathbb{F},z} : \mathbb{F}^n \to \mathbb{F}$ such that

a. $u_{\mathbb{F},z}(y) = 0$ for all $y \in \mathcal{Y}_{\mathbb{F}}$,

b. $u_{\mathbb{F},z}(z) = 1$, and

c. $u_{\mathbb{F},z} = 0$ for all $w \in \{0,1\}^n \setminus \{z\}$.

From Theorem 1.3.9, each $\mathbb{F} \in \mathcal{F}$ can prevent at most $|\mathcal{Y}_{\mathbb{F}}|$ points from being good. Since $t = |\mathcal{Y}_{\mathbb{F}}|$, there are at least $2^n - t$ good points.

Let G be the set of good points, and thus let $B = \{0,1\}^n \setminus G$ be the set of not-good points. Define

$$p'_{\mathbb{F}}(x) = p_{\mathbb{F}}(x) + \sum_{z \in G} (f'(z) - f(z)) u_{\mathbb{F},z}(x). \tag{1.10}$$

Now, all we need is to show that $p'_{\mathbb{F}}(x)$ satisfies the two conditions from the theorem statement.

First, we show that $p'_{\mathbb{F}}$ extends f'; that is, $p'_{\mathbb{F}}(x) = f'(x)$ for all $x \in \{0,1\}^n$. There are two cases here: $x \in G$ and $x \in B$. If $x \in B$, then the sum term of Equation (1.10) is 0; hence $p'_{\mathbb{F}}(x) = p_{\mathbb{F}}(x)$. Since $p_{\mathbb{F}}(x)$ extends $f(x)$, and since $f(x) = f'(x)$ on B, this means $p'_{\mathbb{F}}(x) = f'(x)$. If $x \in G$, then the only term of the sum where $u_{\mathbb{F},z}(x)$ is nonzero is where $x = G$, as per Items b. and c. above. Hence, we have

$$p'_{\mathbb{F}}(x) = p_{\mathbb{F}}(x) + f'(x) - f(x),$$

and since $p_{\mathbb{F}}(x) = f(x)$, it follows that $p'_{\mathbb{F}}(x) = f'(x)$.

Next, we show that $p'_{\mathbb{F}}(y)$ and $p_{\mathbb{F}}(y)$ agree for all $y \in \mathcal{Y}_{\mathbb{F}}$. Since by Item a. above, we have that $u_{\mathbb{F},z}(y) = 0$, it follows that the entire sum term is zero. Therefore, $p'_{\mathbb{F}}(y) = p_{\mathbb{F}}(y)$ for all $y \in \mathcal{Y}_{\mathbb{F}}$.

As such, we have constructed a polynomial $p'_{\mathbb{F}}$ and a set B that satisfy our conditions of the theorem. □

Lemma 1.3.11 ([15, Lemma 7]). *Let $m(x_1, \ldots, x_n)$ be a multilinear monomial. Over a field of characteristic other than 2, we have*

$$\sum_{b \in \{-1,1\}} m(b) = 0. \tag{1.11}$$

Proof. For some x_i, we can write $m = x_i \cdot m'$, where the degree of x_i in m' is 0. Then

$$\begin{aligned}\sum_{b\in\{1,-1\}^n} m(b) &= \sum_{a\in\{-1,1\}} \sum_{b'\in\{1,-1\}^{n-1}} a \cdot m'(b') \\ &= \sum_{a\in\{-1,1\}} a \cdot \left(\sum_{b'\in\{1,-1\}^{n-1}} m'(b') \right) \\ &= \left(\sum_{b'\in\{1,-1\}^{n-1}} m'(b') \right) - \left(\sum_{b'\in\{1,-1\}^{n-1}} m'(b') \right) \\ &= 0.\end{aligned}$$

□

1.4 Statistics

Definition 1.4.1. A *random variable* is

Definition 1.4.2. Two random variables are *statistically independent* if

Theorem 1.4.3 ([7, Claim 2])**.** *Let $\mathbb{F}$ be a finite field and D a finite set. Let $V \subseteq \mathbb{F}^D$ be a vector space, and let v be a uniform random variable over V. For any subdomains $S, S' \subseteq D$, the restrictions $v|_S$ and $v|_{S'}$ are statistically dependent if and only if there exist constants $c \in \mathbb{F}^S$ and $d \in \mathbb{F}^{S'}$ such that*

1. *There exists $w \in V$ such that $c \cdot w \neq 0$, and*
2. *For all $w \in V$, $c \cdot w = d \cdot w$.*

Proof. □

Chapter 2

Relativization

An important prerequisite to understanding algebrization is the similar, but simpler, concept of *relativization*, also called *oracle separation*. To do this, we first must define an *oracle*.

Definition 2.0.1 ([1, Def. 2.1])**.** An *oracle* A is a collection of Boolean functions $A_m : \{0,1\}^m \to \{0,1\}$, one for each natural number m.

There are several ways to think of an oracle; this will extend the most naturally when it comes time to define an extension oracle in Definition 3.0.1. Another way to think of an oracle is as a subset $A \subseteq \{0,1\}^*$. This allows us to think of A as a language. Since we can do this, it gives us the ability to think of the complexity of the oracle. If we want to think about the subset in terms of our functions, we can write A as

$$A = \bigcup_{m \in \mathbb{N}} \{x \in \{0,1\}^m \mid A_m(x) = 1\}. \tag{2.1}$$

We will use the Iverson bracket defined in Definition 1.3.1 for this purpose: allowing us to think of A as the set and $[A]$ as the function.

Example 2.0.1.1. Let $m = 3$. The function

$$\begin{aligned} f : \{0,1\}^3 &\to \{0,1\} \\ abc &\mapsto b \end{aligned} \tag{2.2}$$

is an oracle function. We can think of f as corresponding to the set $\{010, 011, 110, 111\}$.

Example 2.0.1.2. For each $n \in \mathbb{N}$, define

$$\begin{aligned} f_n : \{0,1\}^n &\to \{0,1\} \\ a_1 a_2 \cdots a_n &\mapsto a_n. \end{aligned} \tag{2.3}$$

Then the set $\{f_n\}$ forms an oracle, whose corresponding language is the set of all binary representations of odd numbers.

An oracle is not particularly interesting mathematical object on its own (after all, it is simply a set of arbitrary Boolean functions); its utility comes from when it interacts with a Turing machine. A normal Turing machine does not have the facilities to interact with an oracle, so we need to define a small extension to a standard Turing machine to allow for this.

Definition 2.0.2 ([2, Def. 3.6])**.** A *Turing machine with an oracle* is a Turing machine with an additional tape, called the *oracle tape*, as well as three special states: q_{query}, q_{yes}, and q_{no}. Further, each machine is associated with an oracle A. During the execution of the machine, if it ever moves into the state q_{query}, the machine then (in one step) takes the output of A on the contents of the oracle tape, moving into q_{yes} if the answer is 1 and q_{no} if the answer is 0.

Of course, the question now becomes how we can effectively use an oracle in an algorithm. The previously-mentioned conception of an oracle as a set of strings is useful here. If we consider the set of strings as being a *language* in its own right, then querying the oracle is the same as determining whether a string is in the langauge, just in one step. If the language is computationally hard, this means our machine can get a significant power boost from the right oracle.

Definition 2.0.3 ([1, Def. 2.1])**.** For any complexity class $\mathcal{C}$, the complexity class $\mathcal{C}^A$ is the class of all languages determinable by a Turing machine with access to A in the number of steps defined for $\mathcal{C}$.

We will be using this definition in many places, so we should take a moment to look at it in more depth. First, it is important to realize that $\mathcal{C}^A$ is a set of *languages*, not *machines*: despite the notation, augmenting $\mathcal{C}$ with an oracle does not modify any languages, it just adds new ones that are computable. Second, since a machine can always ignore its oracle, it follows that adding an oracle can only increase the number of languages in the class, never decrease it.

Lemma 2.0.4. *For any complexity class $\mathcal{C}$ and oracle A, $\mathcal{C} \subseteq \mathcal{C}^A$.*

Proof. Let $L \in \mathcal{C}$ and M be a machine that determines L. Then the oracle machine M' that simulates M on its input and makes no queries to the oracle will also accept exactly L. Since M' is a $\mathcal{C}^A$ machine for any oracle A, it follows that $L \in \mathcal{C}^A$ and hence $\mathcal{C} \in \mathcal{C}^A$. □

While the above lemma tells us that $\mathcal{C} \subseteq \mathcal{C}^A$ always, another interesting question is when $\mathcal{C} = \mathcal{C}^A$. We do have a notion for this, called *lowness*. Lowness can be defined for both individual languages and complexity classes; we will define both here.

Definition 2.0.5. A language L is *low* for a class $\mathcal{C}$ if $\mathcal{C}^L = \mathcal{C}$.

Definition 2.0.6. A complexity class $\mathcal{D}$ is *low* for a class $\mathcal{C}$ if each language in $\mathcal{D}$ is low for $\mathcal{C}$.

Of particular interest to us will be classes that are low for *themselves*. We care about these classes because they can use other problems from the same class as a subroutine without issue; in particular recursion and iteration both work here. Thankfully, both P and PSPACE are low for themselves (it turns out NP is probably not); this allows us to easily write algorithms that recurse for classes in both of our most common classes.

Theorem 2.0.7. P *is low for itself.*

Proof. Let $L \in \mathsf{P}$ and let $K \in \mathsf{P}^L$. Let $M(L)$ be the determiner of L and $M(K)$ be the determiner of K. Further, let $\hat{M}(K)$ be the determiner of K but with access to L as an oracle. We aim to show $K \in \mathsf{P}$. Let $p_L(n)$ be a polynomial upper bound of the runtime of $M(L)$ on an input of length n, and let $p_{\hat{K}}(n)$ be similar. Since $M(K)$ can call $M(L)$ no more than $p_{\hat{K}}(n)$ times, it follows that $p_K(n) \leq p_{\hat{K}}(p_L(n))$. Hence, the runtime of $M(K)$ is bounded above by a polynomial, and thus $K \in P$. □

Theorem 2.0.8. PSPACE *is low for itself.*

Proof. The proof is very similar to that for Theorem 2.0.7, but with space instead of time. Since memory usage is bounded above by some polynomial, and polynomials are closed under composition, it follows that PSPACE is low for itself. □

2.1 Defining relativization

We are now ready to define what relativization is. First, note that relativization is a statement about a *result*: we talk about inclusions relativizing, not sets themselves.

Definition 2.1.1. Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes such that $\mathcal{C} \subseteq \mathcal{D}$. We say the result $\mathcal{C} \subseteq \mathcal{D}$ *relativizes* if $\mathcal{C}^A \subseteq \mathcal{D}^A$ for all oracles A. Conversely, if there exists A such that $\mathcal{C} \nsubseteq \mathcal{D}$, we say that the result $\mathcal{C} \subseteq \mathcal{D}$ *does not relativize*.

Definition 2.1.2. Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes such that $\mathcal{C} \nsubseteq \mathcal{D}$. We say the result $\mathcal{C} \nsubseteq \mathcal{D}$ *relativizes* if $\mathcal{C}^A \nsubseteq \mathcal{D}^A$ for all oracles A. Conversely, if there exists A such that $\mathcal{C} \subseteq \mathcal{D}$, we say that the result $\mathcal{C} \nsubseteq \mathcal{D}$ *does not relativize.*

We start with a very straightforward example of a relativizing result.

Lemma 2.1.3. *For any oracle A, $\mathsf{P}^A \subseteq \mathsf{NP}^A$. Equivalently, the result $\mathsf{P} \subseteq \mathsf{NP}$ relativizes.*

Proof. Since any deterministic Turing machine is also a nondeterministic machine, it follows that a machine that solves a P^A problem is also an NP^A machine. Hence, $\mathsf{P}^A \subseteq \mathsf{NP}^A$. □

This result tells us that not *everything* is weird in the world of relativization (although we will soon do our best to find all the weird bits): if we have a machine that can do more operations without an oracle, it can still do more operations with an oracle. Further, for the question of P vs. NP that we will discuss in Section 2.3, this means that the question we care about is whether $\mathsf{NP} \subseteq^? \mathsf{P}$ relativizes. As such, the question we are asking simplifies to determining where $\mathsf{P}^A = \mathsf{NP}^A$ and where $\mathsf{P}^A \subsetneq \mathsf{NP}^A$.

Now that we have talked about set inclusions relativizing, we need to define the other side of the coin: *proofs* can relativize as well as results. Unfortunately, this needs to be a somewhat informal definition as formally delineating different types of proof is far beyond the scope of this paper. However, the definition we offer here will be sufficient for our purposes.

Definition 2.1.4. We say a *proof relativizes* if it is not made invalid if the relevant classes are replaced with oracle classes, i.e., a proof that $\mathcal{C} \subseteq \mathcal{D}$ *relativizes* if the same proof can be used to show $\mathcal{C}^A \subseteq \mathcal{D}^A$ for all oracles A with minimal modifications.

This gives us a reason to care about relativization as a concept: if our proofs are relativizing then we know not to try to use them to prove nonrelativizing results. In particular, we will show in Section 2.3 that the famous P vs. NP problem will not relativize regardless of the outcome, and then in Section 2.4 we will show that the common proof technique of diagonalization *does* in fact relativize.

Now that we have given ourselves a reason to care about oracles and how they interact with Turing machines, we now turn to the question of how a machine can gain information about the oracle it queries. We will do this with the notion of *query complexity.*

2.2 Query complexity

The goal of query complexity is to ask questions about some Boolean function $A : \{0,1\}^n \to \{0,1\}$ by querying A itself. For this, we will interchangeably think of A as a *function* as well as a bit string of length $N = 2^n$, where each string element is A applied to the ith string of length n, arranged in some lexicographical order. We can further think of the property itself as being a Boolean function; a function that takes as input the bit-string representation of A and outputs whether or not A has the given property. We will call the function representing the property f. When viewed like this, f is a function from $\{0,1\}^N$ to $\{0,1\}$. We define three types of query complexity for three of the most common types of computing paradigms: deterministic, randomized, and quantum. Nondeterministic query complexity is interesting, but it is outside the scope of this paper.

Definition 2.2.1 ([1, p. 17])**.** Let $f : \{0,1\}^N \to \{0,1\}$ be a Boolean function. Then the *deterministic query complexity* of f, which we write $D(f)$, is the minimum number of queries made by any deterministic algorithm with access to an oracle A that determines the value of $f(A)$.

To make this more clear, let us give an example problem.

Definition 2.2.2. The OR problem is the following oracle problem:

> Let $A : \{0,1\}^n \to \{0,1\}$ be an oracle. The function $\mathsf{OR}(A)$ returns 1 if there exists a string on which A returns 1, and 0 otherwise.

The question is then what the deterministic query complexity of the OR function is.

Theorem 2.2.3. *The* OR *problem has a deterministic query complexity of* 2^n.

Proof. First, note that any algorithm that determines the OR problem can stop as soon as it queries A and gets an output of 1. Hence, for any algorithm M, let $\{s_i\}$ be the sequence of queries M makes to A on the assumption that it always recieves a response of 0. If $|\{s_i\}| \leq 2^n$, there exists some $s \in \{0,1\}^n$ not queried. In that case, M will not be able to distinguish the zero oracle from the oracle that outputs 1 only when given s. Hence, M must query every string of length n and thus the query complexity is 2^n. □

From this, we get that the OR problem cannot be solved any better than by enumerative checking. This makes intuitive sense because none of the results we get by querying A imply anything about what A will do on other values, since A can be an arbitrary function. Later on (in Section 3.1), we will look at what happens when we give ourselves access to a *polynomial*, where querying one point could tell us information about others.

For the next two definitions, since their Turing machines include some element of randomness, we only require that they succeed with a 2/3 probability. This is in line with most definitions of complexity classes involving random computers.

Definition 2.2.4 ([1, p. 17])**.** Let $f : \{0,1\}^N \to \{0,1\}$ be a Boolean function. Then the *randomized query complexity* of f, which we write $D(f)$, is the minimum number of queries made by any randomized algorithm with access to an oracle A that evaluates $f(A)$ with probability at least 2/3.

Definition 2.2.5 ([1, p. 17])**.** Let $f : \{0,1\}^N \to \{0,1\}$ be a Boolean function. Then the *quantum query complexity* of f, which we write $D(f)$, is the minimum number of queries made by any quantum algorithm with access to an oracle A that evaluates $f(A)$ with probability at least 2/3.

2.3 Relativization of P vs. NP

An important example of relativization is that of P and NP. While the question of if $\mathsf{P} = \mathsf{NP}$ is still open, we aim to show that *regardless of the answer*, the result does not algebrize. To do this, we show that there are some oracles A where $\mathsf{P}^A = \mathsf{NP}^A$, and some where $\mathsf{P}^A \neq \mathsf{NP}^A$.

Additionally, it should be noted that the similarity of relativization to algebrization means that the structure of these proofs will return in Section 3.2 when we show the algebrization of P and NP.

2.3.1 Equality

The more straightforward of the two proofs is the oracle where $\mathsf{P}^A = \mathsf{NP}^A$, so we shall begin with that.

Theorem 2.3.1 ([5, Theorem 2])**.** *There exists an oracle* A *such that* $\mathsf{P}^A = \mathsf{NP}^A$.

Proof. For this, we can let A be any PSPACE-complete language. By letting our machine in P be the reducer from A to any other language in PSPACE, we therefore get that $\mathsf{PSPACE} \subseteq \mathsf{P}^A$. Similarly, if we have a problem in NP^A, we can verify it in polynomial space without talking to A at all (by having our machine include a determiner for A). Hence, we have that $\mathsf{NP}^A \subseteq \mathsf{NPSPACE}$. Further, a celebrated result of Savitch [21] (which we briefly discussed as Theorem 1.2.17) is that $\mathsf{PSPACE} = \mathsf{NPSPACE}$. Combining all these results, we get the chain

$$\mathsf{NP}^A \subseteq \mathsf{NPSPACE} = \mathsf{PSPACE} \subseteq \mathsf{P}^A \subseteq \mathsf{NP}^A. \tag{2.4}$$

This is a circular chain of subset relations, which means everything in the chain must be equal. Hence, $\mathsf{P}^A = \mathsf{NP}^A = \mathsf{PSPACE}$. □

For a slightly more intuitive view of what this proof is doing, what we have done is found an oracle that is so powerful that it dwarfs any amount of computation our actual Turing machine can do. Hence, the power of our machine is really just the same as the power of our oracle, and since we have given both the P and NP machine the same oracle, they have the same power.

2.3.2 Inequality

Having shown that an oracle exists where $\mathsf{P}^A = \mathsf{NP}^A$, we now endeavor to find one where $\mathsf{P}^A \neq \mathsf{NP}^A$. This piece of the proof is less simple than the previous section, and it uses a diagonalization argument to construct the oracle. Before we dive in to the main proof, however, we need to define a few preliminaries.

Definition 2.3.2 ([5, p. 436])**.** Let X be an oracle. The language $L(X)$ is the set

$$L(X) = \{x \mid \text{there is } y \in X \text{ such that } |y| = |x|\}.$$

Example 2.3.2.1. Consider the language $X = \{0, 11, 0100\}$. The language $L(X)$ is the language consisting of all strings of length 1, 2, and 4.

Our eventual goal will be to construct a language X such that $L(X) \in \mathsf{NP}^X \setminus \mathsf{P}^X$. Of particular note is that we can rather nicely put a upper bound on the complexity of $L(X)$ when given X as an oracle, regardless of the value of X. This fact is what gives us the freedom to construct X in such a way that $L(X)$ will not be in P^X.

Lemma 2.3.3 ([5, p. 436])**.** *For any oracle X, $L(X) \in \mathsf{NP}^X$.*

Proof. Let S be a string of length n. If $S \in L(X)$, then a witness for S is any string S' such that $|S| = |S'|$ and $S' \in X$. Since a machine with query access to X can query whether S' is in X in one step, it follows that we can verify that $S \in L(X)$ in polynomial time. □

With this lemma as a base, we can now move on to our main theorem.

Theorem 2.3.4 ([5, Theorem 3])**.** *There exists an oracle A such that $\mathsf{P}^A \neq \mathsf{NP}^A$.*

Proof. Our goal is to construct a set B such that $L(B) \notin \mathsf{P}^B$. We shall construct B in an interative manner. We do this by taking a sequence $\{P_i\}$ of all machines that recongize some language in P^A, and then constructing B such that for each machine in the sequence, there is some part of $L(B)$ it cannot recognize. This technique is called *diagonalization*, and it is used in many places in computer science theory.[1] Additionally, we define $p_i(n)$ to be the maximum running time of P_i on an input of length n. We give the following algorithm to construct B:

Input: A sequence of P oracle machines $\{P_i\}_{i=1}^{\infty}$
Output: A set B such that $L(B) \notin \mathsf{P}^B$

1 $B(0) \leftarrow \varnothing$;
2 $n_0 \leftarrow 0$;
3 **for** *i starting at* 1 **do**
4 Let $n > n_i$ be large enough that $p_i(n) < 2^n$;
5 Run $P_i^{B(i-1)}$ on input 0^n;
6 **if** $P_i^{B(i-1)}$ *rejects* 0^n **then**
7 Let x be a string of length n not queried during the above computation;
8 $B(i) \leftarrow B(i-1) \sqcup \{x\}$;
9 **end**
10 $n_{i+1} \leftarrow 2^n$;
11 **end**
12 $B \leftarrow \bigcup_i B(i)$;

Algorithm 2.1: An algorithm for constructing B

Now that we have presented the algorithm, let us demonstrate its soundness. First, note that since P_i runs in polynomial time, $p_i(n)$ is bounded above by a polynomial, and hence there will always exist an n as defined in line 4. Next, since there are 2^n strings of length n and since $p_i(n) < 2^n$, we know that there must be some x to make line 7 well-defined. While our algorithm allows x to be any

[1] This argument style is named after *Cantor's diagonal argument*, which was originally used to prove that the real numbers are uncountable [20, Thm. 2.14].

string, if it is necessary to be explicit in which we choose, then picking x to be the smallest string in lexicographic order is a standard choice.

We should also briefly mention that this algorithm does not terminate. This is okay because we are only using it to construct the set B, which does not need to be bounded. If this were to be made practical, since the sequence of n_is is monotonically increasing, the set could be constructed "lazily" on each query by only running the algorithm until n_i is greater than the length of the query.

Next, we demonstrate that $L(B) \notin \mathsf{P}^B$. The end goal of our instruction is a set B such that if P_i^B accepts 0^n then there are no strings of length n in B, and if P_i^B rejects, then there is a string of length n in B. This means that no P_i accepts $L(B)$, and hence $L(B) \notin \mathsf{NP}^B$.

The central idea behind the proper functioning of our algorithm is that adding strings to our oracle *cannot change the output if they are not queried*. This is what we do in line 4: we need our input length to be long enough to guarantee that a non-queried string exists. Since the number of queried strings is no greater than $p_i(n)$, and there are 2^n strings of length n, there must be some string not queried.

Next, we run $P_i^{B(i-1)}$ on all the strings we have already added. If it accepts, then we want to make sure that no string of length n is in B; that is, 0^n is not in $L(B)$. Hence, in this particular loop we add nothing to $B(i)$. If $P_i^{B(i-1)}$ rejects, we then need to make sure that $0^n \in L(B)$ but in a way that does not affect the output of $P_i^{B(i-1)}$. Hence, we find a string that $P_i^{B(i-1)}$ did not query (and thus will not affect the result) and add it to $B(i)$.

Having done this, we then set n_{i+1} to be 2^n. Since $p_i(n) < 2^n$, it follows that no previous machine could have queried any strings of length n_{i+1}.[2] This way, we ensure our previous machines do not accidentally have their output change due to us adding a string they queried.

Having run this over all polynomial-time Turing machines, we have a set $L(B)$ such that no machine in P^B accepts it, which tells us $L(B) \notin \mathsf{P}^B$. But, Lemma 2.3.3 already told us $L(B) \in \mathsf{NP}^B$. Hence, $\mathsf{P}^B \neq \mathsf{NP}^B$. □

2.4 Diagonalization relativizes

Of course, determining that P vs NP does not relativize is only important if the proof techniques used in practice *do* in fact relativize. Rather unfortunately, it turns out that simple diagonalization is a relativizing result.

While diagonalization itself does not have a formal definition, we can still think about it informally. Looking at our construction of B, which we did using diagonalization, notice that our definition never really cared about how the P_i worked, just about the results it produced. Hence, if it were to be possible to modify Algorithm 2.1 to construct $B \in \mathsf{NP} \setminus \mathsf{P}$, the proof would remain the same if we were to replace our sequence $\{P_i\}$ with a sequence of machines in P^A for some PSPACE-complete A. However, this would lead to a contradiction, as we showed in Theorem 2.3.1 that in that case, $\mathsf{P}^A = \mathsf{NP}^A$! This tells us that a simple diagonalization argument would not suffice to determine separation between P and NP.

2.5 Arithmetization does not relativize

[2] A word of caution: we only care about what P_i does on input n_i, *not any other input*. This is because we only need each machine to be incorrect for some i, not all i.

Chapter 3

Algebrization

Algebrization, originally described by Aaronson and Wigderson [1], is an extension of relativization. While relativization deals with oracles that are Boolean functions, algebrization extends oracles to be a collection of polynomials over finite fields. Since any field contains the set $\{0,1\}$, we can think about our new oracles as *extending* some specific oracle A, so that both oracles agree on the set $\{0,1\}^n \subseteq \mathbb{F}^n$. We formalize this notion below.

Definition 3.0.1 ([1, Def. 2.2])**.** Let $A_m : \{0,1\}^m \to \{0,1\}$ be a Boolean function and let $\mathbb{F}$ be a finite field. Then an *extension* of A_m over $\mathbb{F}$ is a polynomial $\tilde{A}_{m,\mathbb{F}} : \mathbb{F}^m \to \mathbb{F}$ such that $\tilde{A}_{m,\mathbb{F}}(x) = A_m(x)$ whevever $x \in \{0,1\}^m$. Also, given an oracle $A = (A_m)$, an *extension* $\tilde{A}$ of A is a collection of polynomials $\tilde{A}_{m,\mathbb{F}} : \mathbb{F}^m \to \mathbb{F}$, one for each positive integer m and finite field $\mathbb{F}$, such that

1. $\tilde{A}_{m,\mathbb{F}}$ is an extension of A_m for all $m, \mathbb{F}$, and
2. there exists a constant c such that $\mathrm{mdeg}(\tilde{A}_{m,\mathbb{F}}) \leq c$ for all $m, \mathbb{F}$.

Take note that an oracle can have many different extension oracles, since one can construct an infinite number of polynomials that go through a set of points. For this reason, when dealing with oracles in practice, we will also often be interested in oracles of a particular multidegree, which limits our options for oracles in potentially-interesting ways.

Example 3.0.1.1. Consider the function we defined in Example 2.0.1.1:

$$\begin{aligned} f : \{0,1\}^3 &\to \{0,1\} \\ abc &\mapsto b. \end{aligned} \tag{3.1}$$

An extension of that function is the polynomial

$$\begin{aligned} \tilde{f} : \mathbb{F}^3 &\to \mathbb{F}^3 \\ (a,b,c) &\mapsto b. \end{aligned} \tag{3.2}$$

While this is a relatively trivial polynomial, there are more non-trivial ones, for example

$$\begin{aligned} \tilde{f} : \mathbb{F}^3 &\to \mathbb{F}^3 \\ (a,b,c) &\mapsto a^3c^3 + b^2 - ac. \end{aligned} \tag{3.3}$$

Notice that on $\{0,1\}$, $x^2 = x$, which allows us to see that $\tilde{f}$ is a valid extension of f.

Definition 3.0.2 ([1, Def. 2.2])**.** For any complexity class $\mathcal{C}$ and extension oracle $\tilde{A}$, the complexity class $\mathcal{C}^{\tilde{A}}$ is the class of all languages determinable by a Turing machine with access to $\tilde{A}$ with the requirements for $\mathcal{C}$.

Next, we need to formally define what algebrization is.

Definition 3.0.3 ([1, Def. 2.3])**.** Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes such that $\mathcal{C} \subseteq \mathcal{D}$. We say the result $\mathcal{C} \subseteq \mathcal{D}$ *algebrizes* if $\mathcal{C}^A \subseteq \mathcal{D}^{\tilde{A}}$ for all oracles A and finite field extensions $\tilde{A}$ of A. Conversely, if there exists A and $\tilde{A}$ such that $\mathcal{C} \not\subseteq \mathcal{D}$, we say that the result $\mathcal{C} \subseteq \mathcal{D}$ *does not algebrize*.

Definition 3.0.4 ([1, Def. 2.3])**.** Let $\mathcal{C}$ and $\mathcal{D}$ be complexity classes such that $\mathcal{C} \not\subseteq \mathcal{D}$. We say the result $\mathcal{C} \not\subseteq \mathcal{D}$ *algebrizes* if $\mathcal{C}^A \not\subseteq \mathcal{D}^{\tilde{A}}$ for all oracles A and finite field extensions $\tilde{A}$ of A. Conversely, if there exists A and $\tilde{A}$ such that $\mathcal{C} \subseteq \mathcal{D}$, we say that the result $\mathcal{C} \not\subseteq \mathcal{D}$ *does not algebrize*.

3.1 Algebraic query complexity

Similarly to how we defined query complexity in Section 2.2, our notion of algebrization requires a definition of *algebraic* query complexity.

Definition 3.1.1 ([1, Def. 4.1])**.** Let $f : \{0,1\}^N \to \{0,1\}$ be a Boolean function, $\mathbb{F}$ be a field, and c be a positive integer. Also, let $\mathbb{M}$ be the set of deterministic algorithms M such that $M^{\tilde{A}}$ outputs $f(A)$ for every oracle $A : \{0,1\}^n \to \{0,1\}$ and every finite field extension $\tilde{A} : \mathbb{F}^n \to \mathbb{F}$ of A with $\mathrm{mdeg}(\tilde{A}) \leq c$. Then, the deterministic algebraic query complexity of f over $\mathbb{F}$ is defined as

$$\tilde{D}_{\mathbb{F},c}(f) = \min_{M \in \mathcal{M}} \left(\max_{A,\tilde{A}:\mathrm{mdeg}(\tilde{A}) \leq c} T_M(\tilde{A}) \right), \tag{3.4}$$

where $T_M(\tilde{A})$ is the number of queries to $\tilde{A}$ made by $M^{\tilde{A}}$.

Our goal here is to find the *worst*-case scenario for the *best* algorithm that calculates the property f. The difference between this and Definition 2.2.1 is twofold: first, our algorithm M has access to an extension oracle of A, and second, that we can limit our $\tilde{A}$ in its maximum multidegree. For the most part, we will focus on equations with multidegree 2, which is enough to get the results we want.

As an example, let us look at the same OR problem we defined in Definition 2.2.2.

Theorem 3.1.2 ([1, Thm. 4.4])**.** $\tilde{D}_{\mathbb{F},2}(\mathsf{OR}) = 2^n$ *for every field* $\mathbb{F}$.

Proof. First note that 2^n is an upper bound for the number of queries necessary since we can query every point in $\{0,1\}^n$, of which there are 2^n.

Let M be a deterministic algorithm and let $\mathcal{Y}$ be the set of points queried by M in the case where M always recieves 0 as a response. So long as $|\mathcal{Y}| < 2^n$, there exists by Theorem 1.3.9 a multiquadratic extension polynomial $\tilde{A} : \mathbb{F}^n \to \mathbb{F}$ such that $\tilde{A}(y) = 0$ for all $y \in \mathcal{Y}$ but $\tilde{A}(w) = 1$ for some $w \in \{0,1\}^n$. As such, if M queries less than 2^n points then it would not be able to tell the difference between $\tilde{A}$ and the zero function. However, $\mathsf{OR}(A) = 1$ and $\mathsf{OR}(0) = 0$, so it would get the incorrect answer for one of them. Hence if M queries fewer than 2^n points it cannot solve the OR problem. □

Note that this works even if M is adaptive: if M ever recieves a nonzero response it (correctly) knows $\mathsf{OR}(A) = 1$, so it can accept immediately. As such, we know that any contradiction must come when M has only ever seen zeros as responses.

This gives us a potentially counterintuitive property of algebraic query complexity: while it would seem that giving our machine a polynomial (and a polynomial of multidegree only 2, at that) would give us the ability to solve the hardest problems more quickly, that turns out not to be the case.

Now, while this is true for polynomials of multidegree 2, it turns out that if we restrict our oracles to being simply *multilinear* polynomials, we do get a speedup.

Theorem 3.1.3 ([15, Thm. 3])**.** $\tilde{D}_{\mathbb{F},1}(\mathsf{OR}) = 1$ *for every field* $\mathbb{F}$ *with characteristic not equal to* 2.

Proof. Let $A : \{0,1\}^n \to \{0,1\}$ and $\tilde{A}$ be our extension polynomial. Consider the value of $p(1/2, \ldots, 1/2)$. We aim to show that this value is equal to 0 if and only if A is the zero oracle.

Consider the function

$$p'(x_1, \ldots, x_n) = p(1 - 2x_1, \ldots, 1 - 2x_n). \tag{3.5}$$

Since $1 - 2x$ is a linear polynomial, it follows that p' is itself a multilinear polynomial. Further, since the sum over $\{1, -1\}^n$ of a non-constant multilinear monomial is 0 as per Lemma 1.3.11, it follows that

$$\sum_{b \in \{-1,1\}^n} p'(b) = p'(0, \ldots, 0), \tag{3.6}$$

i.e., the constant term of p'. Further, from our definition of p', we have that $p'(0, \ldots, 0) = p(1/2, \ldots, 1/2)$. Hence, we have

$$\sum_{b \in \{0,1\}^n} p(b) = p(1/2, \ldots, 1/2). \tag{3.7}$$

Since $p(b) \geq 0$ for all $b \in \{0, 1\}^n$, it follows that $p(1/2, \ldots, 1/2)$ is 0 if and only if $p(b) = 0$ for all $b \in \{0, 1\}^n$, i.e. exactly when A is the zero function. □

3.2 Algebrization of P vs. NP

As with relativization, an important application of algebrization is in regards to the P vs. NP problem.

Definition 3.2.1 ([4, Def. 6.1])**.** A language L is PSPACE-*robust* if $\mathsf{P}^L = \mathsf{PSPACE}^L$.

Lemma 3.2.2. *Any* PSPACE*-complete language is also* PSPACE*-robust.*

Proof. First, we know from Lemma 2.0.4 that $\mathsf{P}^L \subseteq \mathsf{PSPACE}^L$. Next, let $M \in \mathsf{PSPACE}^L$, and we aim to show $M \in \mathsf{P}^L$. Since $L \in \mathsf{PSPACE}$ and PSPACE is low for itself, we know $M \in \mathsf{PSPACE}$. As such, we know there is a polynomial-time reduction f from M to L. Hence, we can compute M by running f on the input and then testing if that output is in L (using the oracle). Hence, $M \in \mathsf{P}^L$ and thus $\mathsf{P}^L = \mathsf{PSPACE}^L$. □

Lemma 3.2.3 ([4, Lemma 6.2])**.** *Let L be a* PSPACE*-robust language, with corresponding oracle A. Let $\tilde{A}$ be the unique multilinear extension oracle of A. Then the language*

$$\tilde{L} = \bigcup_{n \in \mathbb{N}} \{(x_1, \ldots, x_n, z) \in \mathbb{F}^{n+1} \mid \tilde{A}(x_1, \ldots, x_n) = z\} \tag{3.8}$$

is polynomially-equivalent to L; that is, $\tilde{L} \in \mathsf{P}^L$ and $L \in \mathsf{P}^{\tilde{L}}$.

The proof of this statement originally given in [4] has some apparent problems; we discuss these more thoroughly later on in Appendix B. Instead, we present our own proof of the above lemma.

Proof. First, we provide a polynomial-time reduction from L to $\tilde{L}$. Since for all $x \in \{0, 1\}^n$, $\tilde{A}(x) = 1$ if and only if $x \in L$, it follows that

$$\begin{aligned} f : \Sigma^* &\to \Sigma^* \\ x &\mapsto (x, 1) \end{aligned} \tag{3.9}$$

is a polynomial-time reduction from L to L'.

Input: $(x_1, \ldots, x_n, z) \in \mathbb{F}^{n+1}$
Output: Whether $\tilde{A}(x_1, \ldots, x_n) = z$
1 $z' \leftarrow 0$;
2 **for** $k \in \{0,1\}^n$ **do**
3 Simulate L on input k;
4 **if** $k \in L$ **then**
  // Compute $d_k(x)$
5 $d \leftarrow 1$;
6 **for** i *from* 1 *to* n **do**
7 **if** $k_i = 1$ **then**
8 $d \leftarrow d \cdot x_i$;
9 **else**
10 $d \leftarrow d \cdot (1 - x_i)$;
11 **end**
12 **end**
13 $z' \leftarrow z' + d$;
14 **end**
15 **end**
16 **return** *whether* $z = z'$;

Algorithm 3.1: Determiner for $\tilde{L}$

This algorithm simply calculates the value of $\tilde{A}(x_1, \ldots, x_n)$ directly, from the explicit definition we gave in Corollary 1.3.7, and then compares it to the value of z.

First, we demonstrate that the above algorithm runs in P^L. From the definition of PSPACE-robustness, we know that we only need to show that the algorithm runs in PSPACE^L, a much weaker bound. The inner for-loop runs in polynomial *time*, hence it must run in polynomial space. The outer for-loop runs for 2^n iterations, so determining that it is in P^L is non-trivial. Beyond the inner loop (which we have already discussed), the only thing we do in the outer loop is simulate L, which can be done in one step with access to an oracle for L.

The only memory we need to simulate this oracle (beyond that for the input) is space for d and z'. We have already shown d needs polynomial space, so what remains is z'. Since $A(x_1, \ldots, x_n) \in \{0,1\}$, each term in the sum in Equation (1.7) is bounded above by $\delta_\beta(x)$. This means that the value of z' that we compute is bounded above by

$$2^n \max_{k \in \{0,1\}^n} \delta_k(x). \tag{3.10}$$

Since each $\delta_k(x)$ can be written in polynomial space, and 2^n can be *written* in polynomial space, it follows that z' can as well. Hence, Algorithm 3.1 is in PSPACE^L, and thus is in P^L.

Next, we show that Algorithm 3.1 determines $\tilde{L}$. As mentioned earlier, our algorithm computes $\tilde{A}$ directly through the equations given in Corollary 1.3.7. First, we show the inner loop (beginning on line 6) computes $\delta_k(x)$. We compute δ directly, through the formula described at Equation (1.8). We do this by simply iterating through each i and then multiplying d by either x_i or $1 - x_i$, as appropriate.

Second, in this case Equation (1.7) simplifies to

$$\tilde{A}_n(x_1, \ldots, x_n) = \sum_{\beta \in L} \delta_\beta(x_1, \ldots, x_n). \tag{3.11}$$

This is exactly what our outer loop does: computes the sum directly through iteration. Hence, the only thing the above algorithm does is calculate $\tilde{A}_n(x_1, \ldots, x_n)$ and then compares it to the value we were given. As such, it determines $\tilde{L}$.

Since there is a reduction from L to $\tilde{L}$, we know that L is no harder than $\tilde{L}$, and Algorithm 3.1 demonstrates that $\tilde{L} \in \mathsf{PSPACE}$. Hence, $\tilde{L}$ is PSPACE-complete. □

With that as a base, we can now move on to the main theorem. As before, the more straightforward proof is the oracle where $\mathsf{P}^{\tilde{A}} = \mathsf{NP}^A$, so we begin with that.

Theorem 3.2.4 ([1, Theorem 5.1]). *There exist A, $\tilde{A}$ such that $\mathsf{NP}^A = \mathsf{P}^{\tilde{A}}$.*

Proof. For this theorem, we use the same technique we did in our proof of Theorem 2.3.1: find a PSPACE-complete language A and work from there. If we let $\tilde{A}$ be the unique multilinear extension of A, Lemma 3.2.3 tells us $\tilde{A}$ is PSPACE-complete. Hence, as mentioned before, we have $\mathsf{NP}^{\tilde{A}} \subseteq \mathsf{NP}^{\mathsf{PSPACE}} \subseteq \mathsf{NPSPACE}$, and since $\mathsf{NPSPACE} = \mathsf{PSPACE}$ and we know from Theorem 2.3.1 that $\mathsf{PSPACE} \subseteq \mathsf{P}^A$, it follows

$$\mathsf{NP}^{\tilde{A}} = \mathsf{NP}^{\mathsf{PSPACE}} = \mathsf{PSPACE} = \mathsf{P}^A.$$

□

Now it is time for the other case.

Theorem 3.2.5 ([1, Theorem 5.3]). *There exist A, $\tilde{A}$ such that $\mathsf{NP}^A \neq \mathsf{P}^{\tilde{A}}$.*

Proof. Like in Theorem 2.3.4, we aim to "diagonalize": iterate over all $\mathsf{P}^{\tilde{A}}$ machines to construct a language that none of them can recognize. Also like before, we will do this by constructing an oracle extension $\tilde{A}$ such that $L(A) \notin \mathsf{P}^{\tilde{A}}$. Since we only give an algebraic extension to P and not NP, we can resuse the result from Lemma 2.3.3 that $L(A) \in \mathsf{NP}^A$. We shall construct $\tilde{A}$ using the following algorithm:

Input: A sequence of P oracle machines $\{P_i\}_{i=1}^{\infty}$
Output: An extension oracle $\tilde{A}$ such that $L(A) \notin \mathsf{P}^{\tilde{A}}$

1 $\tilde{A} \leftarrow \varnothing$;
2 $n_0 \leftarrow 0$;
3 **for** i *starting at* 1 **do**
4 Let $n > n_i$ be large enough that $p_i(n) < 2^n$;
5 Run $P_i^{\tilde{A}}$ on input 0^n;
6 **if** $P_i^{B(i-1)}$ *rejects* 0^n **then**
7 Let $\mathcal{Y}_{\mathbb{F}}$ be the set of all $y \in \mathbb{F}^{n_i}$ queried during the above computation;
  `// See Lemma 1.3.10 for why we can do this`
8 Let $w \in \{0,1\}^n$ such that the following works;
9 **for** *all* $\mathbb{F}$ **do**
10 Set $\tilde{A}_{n_i,\mathbb{F}}$ to be a multiquadratic polynomial such that $\tilde{A}_{n_i,\mathbb{F}}(w) = 1$ and $\tilde{A}_{n_i,\mathbb{F}}(y) = 0$ for all $y \in \mathcal{Y}_{\mathbb{F}} \cup (\{0,1\}^{n_i} \setminus \{w\})$;
11 **end**
12 **else**
13 Set $\tilde{A}_{n_i,\mathbb{F}} = 0$ for all $\mathbb{F}$;
14 **end**
15 $n_{i+1} \leftarrow 2^n$;
16 **end**
17 $B \leftarrow \bigcup_i B(i)$;

Algorithm 3.2: An algorithm for constructing $\tilde{A}$

As before, we will start by demonstrating soundness and then move on to why the constructed oracle provides the separation we seek.

Perhaps the least intuitive section of the above algorithm is the section beginning at line 8. We want to leverage Lemma 1.3.10 to show that such a solution exists. We know that $p_i(n) < 2^n$, and since $p_i(n)$ is an upper bound on the number of total queries, this tells us that there is at least one $w \in \{0,1\}^{n_i}$ not queried. From the definition of $\mathcal{Y}_{\mathbb{F}}$, we also therefore know that $\sum_{\mathbb{F}} \mathcal{Y}_{\mathbb{F}} < 2^n$. Further setting up this lemma, we will let f be the zero function and $p_{\mathbb{F}}$ be the zero polynomial.

From the lemma, we know that there is some $B \in \{0,1\}^n$ with $|B| < 2^n$ such that for all f' agreeing with f there exists a series of $p'_{\mathbb{F}}$ extending f' and agreeing with $p_{\mathbb{F}}$ on $\mathcal{Y}_{\mathbb{F}}$. As such, if we pick any $w \in \{0,1\}^n \setminus B$, then the function $f'(x) = [x = w]$ agrees with f on B, and thus we know that there exists a series of $p'_{\mathbb{F}}$ that agree with the zero polynomial on $\mathcal{Y}_{\mathbb{F}}$ and each non-w Boolean point.

Now, we know that such a solution exists, and Equation (1.10) gives us an explicit formula for our $A_{n_i,\mathbb{F}}$; thus, we know that this is in fact computable. Since this algorithm is simply for *constructing* the language, we do not care about time or space complexity, so the fact that it is computable is enough. In terms of finding the w we need, we can simply iterate try the construction for each $w \in \{0,1\}^n$ and stop as soon as we are able to construct each polynomial.

The other component of soundness is determining how we can run P_i with the extension oracle $\tilde{A}$ when $\tilde{A}$ is not yet fully constructed. What we do is when simulating P_i, we assume that any $\tilde{A}_{n_i,\mathbb{F}}$ that we have not yet queried returns zero on all queried inputs. We then make sure that any time we set an $\tilde{A}_{n_i,\mathbb{F}}$, it also returns zero on any point that we queried. Further, we ensure that each n_i is large enough that no previous machine would have queried any string of length n_i on its respective input; ergo modifying these polynomials would not have any affect on their output.

Next, we show that $L(A)$ is not in $\mathsf{P}^{\tilde{A}}$. As we did in Theorem 2.3.4, the idea is that for each polynomial-time machine P_i, that machine will return the incorrect result on the string 0^{n_i}. We do this in Algorithm 3.2 by simulating P_i on the input, and then adjusting $\tilde{A}$ based on its output. We separate this into two cases: the case where $P_i^{\tilde{A}}$ rejects 0^{n_i}, and the case where it accepts. We shall begin with the case where it accepts.

When $P_i^{\tilde{A}}$ accepts, we want to ensure that no strings of length n_i is in A. The unique low-degree extension of the zero function is the zero polynomial; hence, we set $\tilde{A}_{n_i,\mathbb{F}}$ to be 0 for all $\mathbb{F}$. This ensures $\tilde{A}(x) = 0$ for all $x \in \{0,1\}^{n_i}$, and thus $A \cap \{0,1\}^{n_i} = \varnothing$. This means $0^{n_i} \notin L(A)$ and thus $P_i^{\tilde{A}}$ is incorrect.

When $P_i^{\tilde{A}}$ accepts, we want to make sure that there is at least some string $w \in A \cap \{0,1\}^{n_i}$, but also to make sure that any polynomials we add have their values align with what $P_i^{\tilde{A}}$ already saw. As we mentioned earlier, we know that such a polynomial exists, and thus we construct it. Since our constructed polynomials tell us that $w \in A$, it follows that $0^{n_i} \in L(A)$ and hence $P_i^{\tilde{A}}$ is incorrect there as well.

Since our argument earlier told us that none of the P_i machines would have their output affected by any of the polynomials modified outside of the corresponding iteration i, it follows that no machine P_i could recognize $L(A)$. Since P_i includes every machine recognizing a $\mathsf{P}^{\tilde{A}}$ language, it follows that $L(A) \notin \mathsf{P}^{\tilde{A}}$. □

3.3 Arithmetization algebrizes

Chapter 4

Interactive proof systems

Interactive proof systems are models of computation that involve multiple Turing machines exchanging messages between each other. In general, the machines are split into two categories: those that are computationally unbounded but untrustworthy (the provers), and those that are bounded but trustworthy (the verifiers). The "goal" of the system is to convince the verifier of whether or not the string is in the language. These systems almost always use randomness as part of their design: for this reason, almost all of the bounds are "with high probability" bounds and not complete mathematical certainty.

Interactive proof systems turn out to be surprisingly powerful—while the verifier only runs in polynomial time, it turns out that the interaction with the untrustworthy computer is still enough to boost the power significantly.

4.1 Single-prover systems

The simplest form of an interactive proof system is when there is one prover and one verifier.

Definition 4.1.1 ([9, Def. 4.2.1])**.** An *interactive Turing machine* is a deterministic multi-tape Turing machine with the following tapes:

- Input tape (read-only)
- Output tape (write-only)
- Two communication tapes (one read-only, one write-only)
- One-cell switch tape (read-write)
- Work tape (read-write)

In addition to these tapes, an interactive TM has a single bit $\sigma \in \{0, 1\}$ associated with it, called its *identity*. When the content of the switch tape is not equal to the machine's identity, it performs no computation and is called *idle*.

Of course, a single interactive Turing machine is not worth much: in order to do work with these we need to define how a pair of them interact. The chief mechanism of interacting Turing machines is that of shared tapes. Shared tapes are tapes where any modifications can be seen by both Turing machines immediately. While the tapes themselves are shared, the *heads* are not: the two machines are perfectly capable of looking at different entries at the same time.

Definition 4.1.2 ([9, Def. 4.2.2])**.** A pair of interactive Turing machines (M, N) are *linked* if the following are true:

1. The identity of M is distinct from the identity of N.

2. The switch tapes of M and N coincide (i.e., writing to one affects the value in both).
3. The read-only communication tape of M coincides with the write-only communication tape of N.
4. The read-only communication tape of N coincides with the write-only communication tape of M.

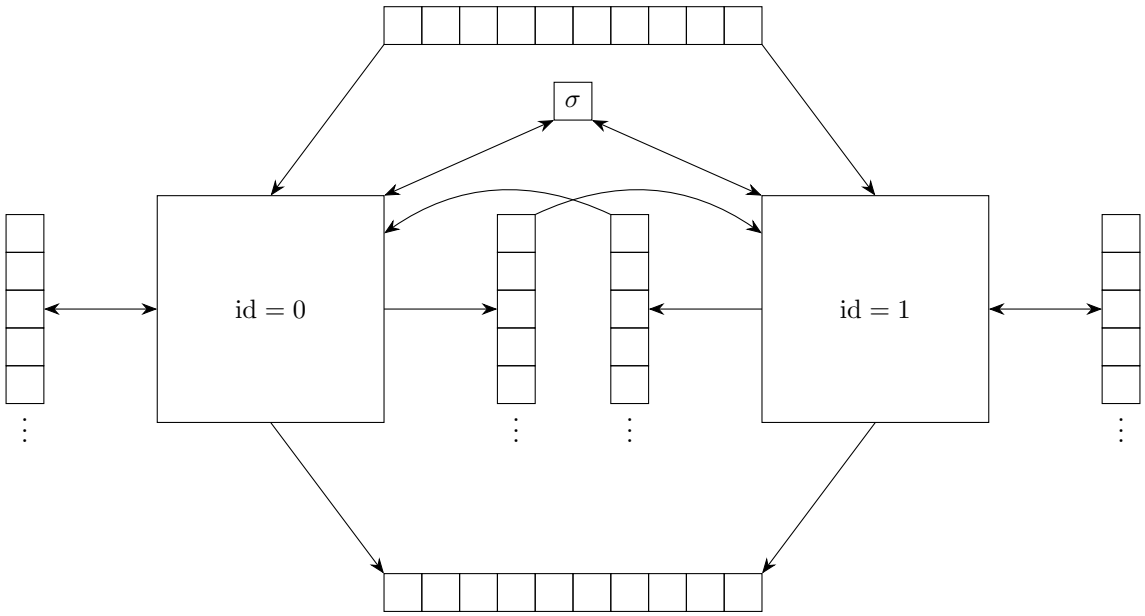

Figure 4.1: A linked pair of interactive Turing machines

We include a diagram of how a linked pair of Turing machines interact and share tape as Figure 4.1. The arrows point in the direction data is able to flow: read-only tapes have an arrow pointing from them and write-only tapes have an arrow pointing to them.

Definition 4.1.3 ([9, Def. 4.2.2])**.** The *joint computation* of a linked pair of interactive Turing machines (M, N) is, on a common input string x, is the series of computation states for both M and N when each is given x as its initial input tape and when the initial value of the shared switch tape is 0. The joint computation halts when either machine halts and the halting machine is not idle.

We will denote the joint computation of machines M and N on input x by $\langle M, N\rangle(x)$.

Now that we have a model for letting two machines talk to each other, we can define the requirements for an interactive proof. To do this, we need three pieces: to restrict the complexity of the verifier (lest it simply compute the problem itself), to require the verifier to generally accept whenever the input is in the language, and to require the verifier to generally reject whenever the input is not in the language.

Definition 4.1.4 ([9, Def. 4.2.4])**.** An *interactive proof system* is a pair of interactive machines (P, V) such that V is polynomial-time and the following holds:

- *Completeness*: For every $x \in L$,
$$\mathbb{P}[\langle P, V\rangle(x) = 1] \geq \frac{2}{3}.$$
- *Soundness*: For every $x \notin L$ and every interactive machine B,
$$\mathbb{P}[\langle B, V\rangle(x) = 1] \leq \frac{1}{3}.$$

While we require our system to be correct at least 2/3 of the time, our choice of probability is actually somewhat arbitrary, so long as it is at least 50%. This is because with a greater than 50% chance of success, we can simply run the checker multiple times and take the majority vote, which will allow us to get the probability arbitrarily high. Since this iteration is for a fixed number of times, it will only linearly scale the runtime and thus it does not affect whether our algorithm is an interactive proof system.

An additional thing to note is that for the soundness clause, we require the inequality to hold for *any* interactive machine B, and not just our chosen machine P. This is important—it says that our verifier cannot be "fooled" reliably by a lying machine, so long as x is not in the language L. In practice, what this means is that if the verifier has reason to believe that the machine it is interacting with is not P, then it should always reject immediately, as we do not care what happens with an arbitrary machine when $x \in L$. A consequence of this is that if V ever recieves back improperly-formatted or nonsense input from its prover, it will reject immediately. Similarly to what we do for ordinary Turing machines parsing their input, we will not explicitly write out that V should reject if it recieves a poorly-formatted response, as it serves little but to provide clutter.

As with all of our interactive-proof variants, we will also define a complexity class corresponding to the set of languages with the given proof. Once we have a complexity class, we will be able to work with it in the same way we have been all the "standard" classes like P or NSPACE.

Definition 4.1.5 ([9, Def. 4.2.5])**.** The class IP is the class of all languages that have an interactive proof system.

Now that we have seen the formal definition of an interactive proof, let us illustrate the formality with an example. To do so, consider the following theorem:

Theorem 4.1.6 ([19])**.** *The language* $\mathsf{Prime} = \{p \mid p \text{ is prime}\}$ *is in* IP.

Algorithm 4.1: An interactive proof for the language Prime

Once we have a complexity class, the question arises of how it relates to other complexity classes. For IP, Adi Shamir proved in 1992 [22] that a language has a standard interactive protocol if and only if it is in PSPACE.

Theorem 4.1.7 ([22])**.** $\mathsf{IP} = \mathsf{PSPACE}$.

Proof. □

4.2 Multi-prover systems

We have now seen quite a bit of single-prover interactive proofs. Having seen this, the question might arise of how things would change if we were to add more machines. Since our verifiers are trusted, increasing the number of verifiers is not useful since any pair of verifiers we would simply be able to simulate with a single verifier working twice as hard (which would keep it polynomial). However, increasing the number of provers to two turns out to give us more power than we would get with a single prover.

Definition 4.2.1 ([9, Def. 4.11.2])**.** A *multi-prover interactive proof system* is a triplet of interactive machines (P_1, P_2, V) such that P_1 and P_2 cannot communicate, V is probabilistic polynomial-time, and

- *Completeness*: For every $x \in L$,
$$\mathbb{P}[\langle P_1, P_2, V\rangle(x) = 1] \geq \frac{2}{3}.$$
- *Soundness*: For every $x \notin L$ and every pair of interactive machines B_1 and B_2,
$$\mathbb{P}[\langle B_1, B_2, V\rangle(x) = 1] \leq \frac{1}{3}.$$

The above definition should look rather similar to Definition 4.1.4; the only difference is now we have two provers instead of just one. The fact that the two provers cannot communicate is important: if they could, they would be able to "strategize"; that is, agree on a joint plan to make sure that their responses agree with each other. Since our provers are not required to be computationally bounded, if they could communicate it would be no different than simply having one prover. However, since the two provers cannot communicate, we gain some information from times where they lie in *different* ways: where each prover individually could say something plausible, but in combination, the provers' responses contradict.

Definition 4.2.2. The class MIP is the class of languages that have a multi-prover interactive proof system.

Lemma 4.2.3. $\mathsf{IP} \subseteq \mathsf{MIP}$.

Theorem 4.2.4 ([4])**.** $\mathsf{MIP} = \mathsf{NEXP}$.

Proof. We showed in Theorem 1.2.21 that O3SAT is NEXP-complete, so all we need is to demonstrate that O3SAT has a multi-prover system. □

Having seen how much more powerful systems become with two provers, one might wonder what would happen if we were to add a third. Unfortunately, it turns out that a third prover is no more powerful than just having two. We formalize this below; because we do not get any benefit from three provers we will not work with three-prover systems at all in this paper beyond this proof.

Theorem 4.2.5. *If we redefine* MIP *to have* $m(n) = \mathsf{poly}(n)$ *provers on an input of size* n*, the class is unchanged.*

Proof. □

4.3 Zero-knowledge proofs

Zero-knowledge proofs are a variant of interactive proofs that have certain cryptographic requirements. What we care about is the idea that zero-knowledge proofs transmit *no knowledge* other than precisely the statement trying to be proved. As an example, if the statement that you are trying to prove is "I have an instance of X", the conceptually-easiest way to prove it would be to produce the aforementioned instance. However, this would not be zero-knowledge since it also transmits the knowledge of exactly what your instance of X is.

The way we mathematically define zero-knowledge is a little tricky. The way we demonstrate that the proof is zero-knowledge is by creating a simulator S_V for each possible verifier V: a machine in P that *by itself* can reproduce the entire message log between P and V for any input.

This definition shows that no knowledge has been released because we are able to reproduce all the public information of the proof with relatively little work. Having said that, it is not particularly obvious that there are *any* languages that are outside of P with perfect zero-knowledge proofs.[1] Despite this, it turns out that these languages do in fact exist (and are reasonably common). Abstractly, the idea behind why many of these work is that the verifier can perform a transformation on some random value, such that undoing the transformation and reliably recovering the original value is only possible with knowledge of the language. However, a simulator would have access to the randomly-chosen value, and thus it could construct a response immediately with no reference to the problem to be solved.

Definition 4.3.1 ([9, Def. 4.3.1])**.** A proof system (P, V) for a language L is *perfect zero-knowledge* if for each probabilistic polynomial-time interactive machine V^* there exists a probabilistic polynomial-time ordinary machine M^* such that for every $x \in L$ we have the following conditions hold:

[1] To some extent, showing that there are languages *truly* outside of P would require a proof that $\mathsf{P} \neq \mathsf{NP}$ (which is unfortunately beyond the scope of this paper), but there are lots of languages strongly believed to be outside of P with zero-knowledge proofs.

1. With probability at most $1/2$, on input x, machine M^* outputs a special symbol denoted $\perp$ (i.e. $\mathbb{P}[M^*(x) = \perp] \leq 1/2$).
2. Let $m^*(x)$ be the random variable such that
$$\mathbb{P}[m^*(x) = \alpha] = \mathbb{P}[M^*(x) = \alpha \mid M^*(x) \neq \perp] \tag{4.1}$$
for all α. That is, let $m^*(x)$ be the distribution of non-$\perp$ values of M^*. Then $\langle P, V^* \rangle(x)$ and $m^*(x)$ are identically distributed for all $x \in L$.

In this case, we say the machine M^* is a *perfect simulator* for the interaction of V^* with P.

As with other interactive proof systems, zero-knowledge proofs are probabilistic; in particular this means they do *not* function as proofs in the mathematical sense.

Definition 4.3.2 ([9, Def. 4.3.5])**.** The class PZK is the class of all languages with a perfect zero-knowledge proof system.

4.4 Probabilistically-checkable proofs

So far, all of our computational proofs have focused on the interaction between two computers, but there exist non-interactive models as well. Probabilistically-checkable proofs do not use interactive Turing machines, but instead have access to a "proof" that their input is in the given language. The nontriviality is that the number of bits of the proof we can access is bounded—simply reading the entire proof will not suffice. For any string in the language, we ensure there exists a correct proof, which our algorithm must always recognize accurately. Further, for any string *not* in the language, the algorithm must reliably (but not necessarily always) reject.

Definition 4.4.1 ([2, Def. 18.1])**.** Let $L \subseteq \{0,1\}^n$ be a language and $q, r : \mathbb{N} \to \mathbb{N}$. A $(r(n), q(n))$-*verifier* for L is a polynomial-time probabilistic algorithm V such that

1. When given an input string $x \in \{0,1\}^n$ and random access to a string $\pi \in \{0,1\}^*$, V uses at most $r(n)$ random coins and makes at most $q(n)$ non-adaptive queries to locations of π before either accepting or rejecting.
2. If $x \in L$ then there exists a $\pi \in \{0,1\}^*$ such that V will always accept when given input x and random string π.
3. If $x \notin L$ then V will reject with probability $\geq 1/2$ for *all* random strings π.

We call the random string π the *proof*. We denote the output of V on input x and proof π with $V^\pi(x)$.

So far, all of our proof-complexity classes have just had a single class for all languages with the proof, regardless of internal complexity, but for probabilistically-checkable proofs we actually stratify the class further. This is for multiple reasons: first, we can actually get astonishingly tight bounds on the parameters for PCPs, and second, because these are "access" complexity (i.e. we measure the number of preexisting bits actually read by the algorithm), they are actually independent of computational model, so the need for polynomial equivalence is negated.

Definition 4.4.2 ([2, Def. 18.1])**.** For any $q, r : \mathbb{N} \to \mathbb{N}$, the class $\mathsf{PCP}(q(n), r(n))$ is the class of all languages with a $(cq(n), dr(n))$-verifier for some $c, d \in \mathbb{N}$.

We would be remiss if we were not to mention the PCP theorem, by far the most important theorem relating to probabilistically-checkable proofs.

Theorem 4.4.3 (PCP theorem, [3])**.** *Any problem in* NP *has a probabilistically-checkable proof of constant query complexity and using a maximum of* $O(\log n)$ *random bits, and vice versa. Equivalently,* $\mathsf{NP} = \mathsf{PCP}(\log n, 1)$.

Proof. □

Theorem 4.4.4 ([11])**.** *Any language in* NP *has a* PCP *that queries a maximum of* 3 *bits of the proof and uses* $O(\log n)$ *random bits.*

4.5 Zero-knowledge probabilistically-checkable proofs

A zero-knowledge probabilistically-checkable proof is a combination of the ideas of zero-knowledge proofs (as seen in Section 4.3) and probabilistically-checkable proofs (as seen in Section 4.4). Since we can model a PCP as an interaction between between a verifier and a proof (instead of a prover), we can model this interaction as being zero-knowledge as well.

Definition 4.5.1 ([10, Def. 8.6])**.** A probabilistically-checkable proof system is *zero-knowledge* if there exists a probabilistic polynomial-time simulator S such that on input x, S can simulate every interaction of V with the associated proof of x.[2]

Definition 4.5.2. The class PZK-PCP is the class of all languages that have a perfect zero-knowledge probabilistically-checkable proof.

4.6 Interactive probabilistically-checkable proofs

Interactive probabilistically-checkable proofs are a combination of the concepts of an interactive protocol and a probabilistically-checkable proof. The broad idea is our proof proceeds in two phases: first, the prover sends a purported proof to the verifier, after which they engage in an interactive protocol, during which the verifier can access the proof as an oracle.

Definition 4.6.1 ([16, §1.1])**.** Let L be a language, let $p, q, l : \mathbb{N} \to \mathbb{N}$, and let $c, s \in [0, 1]$. An *interactive probabilistically-checkable proof* for L is an interactive protocol as follows:

Input: To both P and V: a string x of length n
Input: To P alone: A string w
Output: Whether $x \in L$

Algorithm 4.2: The IPCP protocol

Definition 4.6.2. The class IPCP is

The tuple-notation we used when talking about the class PCP (see Definition 4.4.2) is rather hard to read when we have this many parameters, and as such we will us the following clearer notation when talking about the various bounds on IPCP algorithms:

$$L \in \mathsf{IPCP}\left[\begin{array}{rl} \text{round complexity:} & r \\ \text{PCP length:} & \ell \\ \text{communication complexity:} & c \\ \text{query complexity:} & q \\ \text{soundness error:} & \varepsilon \end{array}\right]$$

to mean the language L is a member of IPCP with the listed restrictions.

Definition 4.6.3. Let $\mathbb{F}$ be a field, and $d, m \in \mathbb{N}$. A *low-degree IPCP* is an IPCP instance with the following two properties:

1. The oracle sent by the honest prover P is an m-variable $\mathbb{F}$-polynomial Q with multidegree no more than d (i.e. $Q \in \mathbb{F}[X_{1,\dots,m}^{\leq d}]$)
2. Soundness is only required to hold against provers that send oracles that are polynomials in $\mathbb{F}[X_{1,\dots,m}^{\leq d}]$.

Similarly to what we did with normal IPCP oracles, we will use the following notation to talk about low-degree IPCP instances:

$$L \in \mathsf{IPCP}\left[\begin{array}{rl} \text{round complexity:} & r \\ \text{PCP length:} & \ell \\ \text{communication complexity:} & c \\ \text{query complexity:} & q \\ \text{oracle:} & \mathbb{F}[X_{1,\dots,m}^{\leq d}] \\ \text{soundness error:} & \varepsilon \end{array}\right].$$

[2] To clarify, S does *not* have access to the proof of x, just x itself.

We combine all the information about the degree of the oracle into one line because we have an efficient notation for multidegree-bounded polynomials, and so that we do not wind up with an exorbitant number of lines in our notation.[3]

[3]Having said that, there are still a lot of lines in this notation, but this is the best we can do.

Chapter 5

Quantum computation

5.1 Quantum computers

Definition 5.1.1. A *qubit* is a unit vector in $\mathbb{C}^2$.

Definition 5.1.2. A *operator* is a linear function $A : V \to V$ such that $v \cdot A \cdot v^T \geq 0$ for all $v \in V$.

5.1.1 Measurement

Definition 5.1.3. A *projective measurement* is

Definition 5.1.4. A *positive operator-valued measure* is

5.2 Quantum complexity classes

Definition 5.2.1. The class BQP is

Definition 5.2.2. The class QMA is

5.3 Quantum interactive proofs

Definition 5.3.1. The class $\mathsf{MIP}*$ is

Theorem 5.3.2 ([13])**.** $\mathsf{MIP}* = \mathsf{RE}$.

5.4 Quantum low-multidegree test

Theorem 5.4.1 ([14])**.** *There is a universal constant $C > 0$ such that the following holds. Let $(\tilde{P}_1, \tilde{P}_2, |\Psi\rangle)$ be a projective strategy that passes the $(\mathbb{F}, d, m)$-low-multidegree test with probability at least $1-\varepsilon$. For $i \in \{1,2\}$, $\alpha \in \mathbb{F}^m$, denote by $\{A^z_{i,\alpha}\}_{z\in\mathbb{F}}$ the measurement applied by $\tilde{P}_i$ upon recieving question α. Then there exist projective measurements $\{L_1^Q\}_{Q\in\mathbb{F}[X^{\leq d}_{1,\dots,m}]}$ and $\{L_2^Q\}_{Q\in\mathbb{F}[X^{\leq d}_{1,\dots,m}]}$ such that for $v \in \mathsf{poly}(m,d)(d/|\mathbb{F}|+c)^C$, the following holds:*

1. *Consistency with $\{A^z_{1,\alpha}\}_{z\in\mathbb{F},\alpha\in\mathbb{F}^m}$ and $\{A^z_{1,\alpha}\}_{z\in\mathbb{F},\alpha\in\mathbb{F}^m}$:*

$$\mathbb{E}_{\alpha\in\mathbb{F}^m} \sum_{Q\in\mathbb{F}[X^{\leq d}_{1,\dots,m}]} \sum_{z\in\mathbb{F}\setminus\{Q(\alpha)\}} \langle\Psi \,|\, A^z_{1,\alpha} \otimes L_2^Q \,|\, \Psi\rangle \leq v, \tag{5.1}$$

$$\mathbb{E}_{\alpha\in\mathbb{F}^m} \sum_{Q\in\mathbb{F}[X^{\leq d}_{1,\dots,m}]} \sum_{z\in\mathbb{F}\setminus\{Q(\alpha)\}} \langle\Psi \,|\, L_1 \otimes A^z_{2,\alpha} \,|\, \Psi\rangle \leq v. \tag{5.2}$$

2. Consistency of $\{L_1^Q\}_Q$ *and* $\{L_2^Q\}_Q$*:*

$$\sum_{Q \neq Q' \in \mathbb{F}[X_{1,\dots,m}^{\leq d}]} \langle \Psi \mid L_1^Q \otimes L_2^Q \mid \Psi \rangle \leq v. \tag{5.3}$$

Proof. □

Chapter 6

Lifting IPCP to MIP∗

6.1 Reducing query complexity

Theorem 6.1.1 ([7, Prop. 9.2]). *There exists a transformation T such that, for every $m, d \in \mathbb{N}$ and finite field $\mathbb{F}$, if*

$$(P,V) \in \mathsf{IPCP}\left[\begin{array}{rl} \textit{round complexity:} & r \\ \textit{PCP length:} & \ell \\ \textit{communication complexity:} & c \\ \textit{query complexity:} & q \\ \textit{oracle:} & \mathbb{F}[X_{1,\ldots,m}^{\leq d}] \\ \textit{soundness error:} & \varepsilon \end{array}\right],$$

then $T(P,V)$ recognizes the same language as (P,V) and

$$T(P,V) \in \mathsf{IPCP}\left[\begin{array}{rl} \textit{round complexity:} & r+1 \\ \textit{PCP length:} & \ell \\ \textit{communication complexity:} & c+\mathsf{poly}(m,d,q) \\ \textit{query complexity:} & 1 \\ \textit{oracle:} & \mathbb{F}[X_{1,\ldots,m}^{\leq d}] \\ \textit{soundness error:} & \varepsilon + \frac{mdq}{|\mathbb{F}|-q} \end{array}\right].$$

Proof. □

Theorem 6.1.2 ([7, Prop. 9.2]). *If (P,V) is perfect zero-knowledge with query bound b, then $T(P,V)$ (where T is the transformation from Theorem 6.1.1) is perfect zero-knowledge with query bound $b-(mdq+1)$.*

Proof. □

6.2 A lifting algorithm

Theorem 6.2.1 ([7, Lemma 9.1]). *Let L be a language, let $m, d, q \in \mathbb{N}$, and let $\mathbb{F}$ be a finite field of size $\mathsf{poly}(m,d,q)$ sufficiently large. Then, there exists a transformation T*

$$T : \mathsf{IPCP}\left[\begin{array}{rl} \textit{round complexity:} & r \\ \textit{PCP length:} & \ell \\ \textit{communication complexity:} & c \\ \textit{query complexity:} & q \\ \textit{oracle:} & \mathbb{F}[X_{1,\ldots,m}^{\leq d}] \\ \textit{soundness error:} & \varepsilon \end{array}\right] \to \mathsf{MIP}*\left[\begin{array}{rl} \textit{number of provers:} & 2 \\ \textit{round complexity:} & r+1 \\ \textit{communication complexity:} & c \\ \textit{soundness error:} & 1-\frac{1}{\mathsf{poly}(m,d)} \end{array}\right].$$

such that (P',V') and $T(P',V')$ recognize the same language.

Further, if the IPCP (P',V') is zero-knowledge with query bound $b \geq 2(q+1)md+3$, then the MIP∗ *(P_1,P_2,V) is zero-knowledge.*

V: Choose a random $r \in \{0, 1\}$;
if $V = 0$ **then**
  V: Perform the low multidegree test from Theorem 5.4.1;
else
  `// IPCP emulation`
  P_1 and V emulate the interaction of the IPCP $(P'', V'') = T(P', V')$ (see Theorem 6.1.1);
  The above emulation generates a uniform $\beta \in \mathbb{F}^m$, and a $c \in \mathbb{F}$ such that with probability $1 - \varepsilon$, $x \in \mathcal{L}$ if and only if $R(\beta) \in c$;
  V: ask P_2 for an evaluation of R at β;
  P_2: reply with an element $z \in \mathbb{F}$;
  V: accept if and only if $c = z$;
end

Algorithm 6.1: Construction of a MIP∗ from an IPCP [7, Construction 2]

6.2.1 Soundness of Algorithm 6.1

6.2.2 Algorithm 6.1 preserves zero-knowledge

Algorithm 6.2: A simulator for Algorithm 6.1 [7, §9.4]

Chapter 7

Low-degree IPCP with zero-knowledge

7.1 AQC of polynomial summation

Lemma 7.1.1 ([7, Lemma 12.1]). *Let $\mathbb{F}$ be a field, $m, k, d, d' \in \mathbb{N}$, and G, K, L be finite subsets of $\mathbb{F}$ such that $K \subseteq L$, $d' \geq |G| - 2$, and $|K| = d + 1$. If $S \subseteq \mathbb{F}^{m+k}$ is such that there exist matrices $C \in \mathbb{F}^{L^m \times \ell}$ and $D \in \mathbb{F}^{S \times \ell}$ such that for all $Z \in \mathbb{F}[X^{\leq d}_{1,\ldots,m}, Y^{\leq d'}_{1,\ldots,k}]$ and all $i \in \{1, \ldots, \ell\}$*

$$\sum_{\alpha \in L^m} C_{\alpha,i} \sum_{y \in G^k} Z(\alpha, y) = \sum_{q \in S} D_{q,i} Z(q), \tag{7.1}$$

then $|S| \geq \operatorname{rank}(BC)(\min(d' - |G| + 2, |G|))^k$, where $B \in \mathbb{F}^{K^m \times L^m}$ is such that the column of B indexed by α represents $Z(\alpha)$ in the basis $\{Z(\beta) \mid \beta \in K^m\}$.

Proof. □

Corollary 7.1.2 ([7, Corollary 12.2]). *Let $\mathbb{F}$ be a finite field, $G \subseteq \mathbb{F}$, and $d, d' \in \mathbb{N}$ with $d' \geq 2(|G|-1)$. If $S \subseteq \mathbb{F}^{m+k}$ is such that there exist $(c_\alpha)_{\alpha \in \mathbb{F}^m}$ and $(d_\beta)_{\beta \in \mathbb{F}^{m+k}}$ such that*

1. *for all $Z \in \mathbb{F}[X^{\leq d}_{1,\ldots,m}, Y^{\leq d}_{1,\ldots,k}]$ it holds that*

$$\sum_{\alpha \in \mathbb{F}^m} c_\alpha \sum_{y \in G^k} Z(\alpha, y) = \sum_{q \in S} d_q Z(q), \tag{7.2}$$

   and

2. *there exists $Z' \in \mathbb{F}[X^{\leq d}_{1,\ldots,m}, Y^{\leq d}_{1,\ldots,k}]$ such that*

$$\sum_{\alpha \in \mathbb{F}^m} c_\alpha \sum_{y \in G^k} Z'(\alpha, y) = 0, \tag{7.3}$$

then $|S| \geq |G|^k$.

Proof. We will leverage Theorem 1.4.3 that we proved earlier. Now, consider the vector space

$$\left\{ \left((Z(\gamma))_{\gamma \in \mathbb{F}^{m+k}}, \left(\sum_{y \in G^k} Z(\alpha, y) \right)_{\alpha \in \mathbb{F}^m} \right) \;\middle|\; Z \in \mathbb{F}[X^{\leq d}_{1,\ldots,m}, Y^{\leq d'}_{1,\ldots,k}] \right\} \tag{7.4}$$

This is a vector space over $\mathbb{F}$ with domain $\mathbb{F}^{m+k} \cup \mathbb{F}^m$. □

Corollary 7.1.3 ([7, Corollary 12.3]). *Let $\mathbb{F}$ be a finite field, $G \subseteq \mathbb{F}$, and $d, d' \in \mathbb{N}$ with $d' \geq 2(|G|-1)$. Let Q be a subset of $\mathbb{F}^{m+k}$ with $|Q| \leq |G|^k$, and let Z be uniformly random in $\mathbb{F}[X^{\leq d}_{1,\ldots,m}, Y^{\leq d'}_{1,\ldots,k}]$. Then, the random variables $(\sum_{y \in G^k} Z(\alpha, y))_{\alpha \in \mathbb{F}^m}$ and $(Z(q))_{q \in Q}$ are independent.*

Proof. □

7.2 The sumcheck problem

Definition 7.2.1 ([18])**.** The *sumcheck problem* is the following problem:

> Let H be a subset of a finite field $\mathbb{F}$, let $F \in \mathbb{F}[X_{1,\dots,m}^{\leq d}]$ a polynomial over $\mathbb{F}$, and let $a \in \mathbb{F}$. Does $\sum_{x \in H^m} F(x) = a$?

For this question, we give H and a to both the prover and verifier, but only the prover gets access to F as an algebraic oracle.

7.2.1 A non-zero-knowledge sumcheck protocol

Input: A polynomial A and number s
Output: Whether $\text{per}(A) = s$
`/* Except where specified, this protocol is written from the perspective of the verifier` V`. */`
1 P: pick a prime p and convince V that it is prime using Algorithm 4.1;
`/* All arithmetic in the remainder of this algorithm is done modulo` p `*/`
2 **while** $L \neq \langle (B, q) \rangle$ *for any* 1×1 *matrix* B **do**
`// "Expand" phase`
3 **if** L *contains exactly one pair* (B, q) **then**
4 $r \leftarrow \dim(B)$;
5 **for** i *from* 1 *to* r **do**
6 $B_i \leftarrow B_{1,i}$; `// Matrix minor`
7 Ask P for the permanent of B_i;
8 **if** $\sum_{i=1}^{r} b_{1i} q_i \neq q$ **then**
9 **return** *0*;
10 **end**
11 **end**
12 $L \leftarrow \langle (B_1, q_1), \dots, (B_r, q_r) \rangle$;
13 **else**
`// "Shrink" phase`
14 Pick two pairs (C, c) and (D, d) from L;
15 Ask P for the $r + 1$ coefficient of $f(x) = \text{per}(C + x(D - C))$;
16 Construct $g(x)$ from that coefficient;
17 **if** $g(0) = c$ *or* $g(1) = d$ **then**
18 **return** *0*;
19 **end**
20 Choose random $a \in \mathbb{Z}_p$;
21 Send a to P;
22 Replace (C, c) and (D, d) with $(C + a(D - C), g(a))$;
23 **end**
24 **end**
25 **return** $q = \text{per}(B)$;

Algorithm 7.1: The standard sumcheck protocol [18, Thm. 1]

7.2.2 A weakly zero-knowledge sumcheck protocol

Algorithm 7.2: A weakly zero-knowledge sumcheck protocol [6]

7.2.3 Making the sumcheck protocol zero-knowledge

Theorem 7.2.2 ([7])**.** *There exists a zero-knowledge variant of Algorithm 7.2.*

Proof. □

Input: An instance (H, a) to both P and V
Input: A polynomial $F \in \mathbb{F}[X_{1,\dots,m}^{\leq d}]$ as an oracle to P
Output: Whether $\sum_{x \in H^m} F(x) = a$

1 P: draw uniformly random polynomials $Z \in \mathbb{F}[X_{1,\dots,m}^{\leq d}, Y_{1,\dots,m}^{\leq 2\lambda}]$ and $A \in \mathbb{F}[Y_{1,\dots,k}^{\leq 2\lambda}]$;
2 P: send the polynomial

$$O(W, X, Y) = W \cdot Z(X, Y) + (1 - W) \cdot A(Y)$$

to V;
// Note that $Z = O(1, \cdot)$ and $A = O(0, 0, \cdot)$, so V can use both Z and A later
3 P: send $z = \sum_{a \in H^m} \sum_{\beta \in G^k} Z(\alpha, \beta)$ to V;
4 V: draw a random element $\rho_1 \in \mathbb{F} \setminus \{0\}$ and send to P;
5 Run the standard sumcheck IP (Algorithm 7.1) on the statement $\sum_{\alpha \in H^m} Q(a) = \rho_1 a + z$, where

$$Q(X_1, \dots, X_m) = \rho_1 F(X_1, \dots, X_m) + \sum_{\beta \in G^k} Z(X_1, \dots, X_m, \beta).$$

We have P play the prover and V the verifier, with the following modification: For $i = 1, \dots, m$, in the ith round, V samples its random element c_i from the set I instead of from all of $\mathbb{F}$; if P ever recieves $c_i \in \mathbb{F} \setminus I$, it immediately aborts. In particular, in the mth round, P sends a polynomial

$$g_m(X_m) = \rho_1 F(c_1, \dots, c_{m-1}, X_m) + \sum_{\beta \in G^k} Z(c_1, \dots, c_{m-1}, X_m, \beta)$$

for some $c_1, \dots, c_{m-1} \in I$.;
6 V: send $c_m \in I$ to P;
7 P: send $w \in \sum_{\beta \in G^k} Z(c, \beta)$ to V, where $c = (c_1, \dots, c_m)$;
8 Both: engage in the weak-ZK sumcheck protocol with respect to the claim $\sum_{\beta \in G^k} Z(c, \beta) = w$, using A as the masking polynomial. If the verifier in that protocol rejects, so does V;
9 V: output the claim $F(c) = \frac{g_m(c_m) - w}{\rho_1}$;

Algorithm 7.3: Strong zero-knowledge sumcheck [7, Construction 3]

Algorithm 7.4: An inefficient simulator for Algorithm 7.3 [7, p. 15:33]

Algorithm 7.5: An efficient variant of Algorithm 7.4 [7, p. 15:34]

7.3 Extending the sumcheck algorithm to NEXP

Theorem 7.3.1 ([7, Thm. 14.2]). *There exists a $c \in \mathbb{N}$ such that for any query-bound function $b(n)$, $d(n) \in \Omega(n^c)$, $m(n) \in O(n^c \log(b))$, and any sequence of fields $\mathbb{F}(n)$ that are field extensions of $\mathbb{F}_2$ with $|\mathbb{F}(n)| \in \Omega((n^c \log(b))^4)$,*

$$\mathsf{O3SAT} \in \mathsf{IPCP} \left[\begin{array}{rl} \textit{round complexity:} & O(n, b) \\ \textit{PCP length:} & \mathsf{poly}(2^n, b) \\ \textit{communication complexity:} & \mathsf{poly}(n, \log(b)) \\ \textit{query complexity:} & \mathsf{poly}(n, \log(b)) \\ \textit{oracle:} & \mathbb{F}[X_{1,\dots,m}^{\leq d}] \\ \textit{soundness error:} & 1/2 \end{array} \right],$$

which is zero-knowledge with query bound b.

repeat
  P: Draw a random $Z \in \mathbb{F}[X_{1,\dots,m}^{\leq |H|+2}, Y_{1,\dots,m}^{\leq 2|H|}]$;
until $\sum_{\beta \in G^k} Z(\alpha, \beta) = A(\gamma_2(\alpha))$ *for all* $\alpha \in H^{m_2}$;
for $i \in \{1, 2, 3\}$ **do**
  P and V implement Algorithm 7.2 on the claim $\sum_{\beta \in H^k} Z(c_i', \beta) = h_i$;
end

Algorithm 7.6: A low-degree IPCP for O3SAT [7, p. 15:36]

Proof. □

Corollary 7.3.2. NEXP $\subseteq$ PZK-IPCP.

Proof. Since O3SAT is NEXP-complete as per Theorem 1.2.21, we can perform a polynomial reduction from any other language to O3SAT and then run Algorithm 7.6. □

Chapter 8

Zero-knowledge PCPs for #P

Theorem 8.0.1 ([10, Theorem 8.1])**.** *There exists a perfect zero-knowledge probabilistically-checkable proof for* #SAT*.*

Corollary 8.0.2. #P $\subseteq$ PZK-PCP.

Appendix A

More on extension polynomials

In this appendix, we will work through some of the algebra we mentioned but did not go into detail about in Section 1.3.

A.1 A proof of Equation (1.6)

Our goal is to demonstrate the following:

$$[x = y] = \prod_{i=1}^{m} \left(\sum_{\omega \in H} \left(\prod_{\gamma \in H \setminus \{\omega\}} \frac{(x_i - \gamma)(y_i - \gamma)}{(\omega - \gamma)^2} \right) \right) \tag{A.1}$$

for all $x, y \in H^n$. We will do this in two cases: one where $x = y$ and one where $x \neq y$.

First, assume $x \neq y$ (so we want to show $\delta_y(x) = 0$). In this case, there exists at least one i where $x_i \neq y_i$. For this i, for each ω there exists some $\gamma \in H \setminus \{\omega\}$ such that either $x_i = \gamma$ or $y_i = \gamma$.[1] As such, it follows that either $(x_i - \gamma) = 0$ or $(\gamma_i - \gamma) = 0$. Hence, for this i the sum will be entirely over zero terms (since there will be at least one zero term in the product for each ω). As such, this means that the ith term of our outermost product is 0, and hence the entire product is 0, as desired.

When $x = y$ (and so we want to show $\delta_y(x) = 1$), the above equation simplifies to

$$[x = y] = \prod_{i=1}^{m} \left(\sum_{\omega \in H} \left(\prod_{\gamma \in H \setminus \{\omega\}} \frac{(x_i - \gamma)^2}{(\omega - \gamma)^2} \right) \right) \tag{A.2}$$

Whenever $\omega \neq x_i$, the innermost product becomes 0 since there will be a term where $\gamma = x_i$. Hence, we can simplify this further to

$$[x = y] = \prod_{i=1}^{m} \left(\prod_{\gamma \in H \setminus \{\omega\}} \frac{(x_i - \gamma)^2}{(x_i - \gamma)^2} \right). \tag{A.3}$$

Since $\gamma \neq x_i$, we can simplify the fraction to 1; since we have two nested products it follows that the equation as a whole simplifies to 1.

A.2 Algebra behind Equation (1.8)

Our goal is to show that the equation in Equation (1.5) simplifies to that of Equation (1.8) when $H = \{0, 1\}^n$.

[1] This piece fails in the case where $x_i = y_i$, since if $\omega = x_i = y_i$ neither of the terms will ever be zero.

As a refresher, our starting equation has the form

$$\delta_y(x) = \prod_{i=1}^{m}\left(\sum_{\omega\in H}\left(\prod_{\gamma\in H\setminus\{\omega\}}\frac{(x_i-\gamma)(y_i-\gamma)}{(\omega-\gamma)^2}\right)\right). \tag{A.4}$$

We start by manually substituting the outer sum:

$$\delta_y(x) = \prod_{i=1}^{m}\left(\left(\prod_{\gamma\in\{0,1\}\setminus\{0\}}\frac{(x_i-\gamma)(y_i-\gamma)}{(\omega-\gamma)^2}\right)+\left(\prod_{\gamma\in\{0,1\}\setminus\{1\}}\frac{(x_i-\gamma)(y_i-\gamma)}{(\omega-\gamma)^2}\right)\right). \tag{A.5}$$

Next, notice that the inner products are actually each over one term, so we can manually substitute there:

$$\delta_y(x) = \prod_{i=1}^{m}\left(\frac{(x_i-1)(y_i-1)}{(0-1)^2}+\frac{(x_i-0)(y_i-0)}{(1-0)^2}\right). \tag{A.6}$$

Next, we simplify, taking note that the denominator of both fractions is 1:

$$\delta_y(x) = \prod_{i=1}^{m}((x_i-1)(y_i-1)+x_iy_i). \tag{A.7}$$

From here, we take advantage of the fact that $y\in\{0,1\}^n$; here we split our product into two smaller products: one where $y_i=0$ and one where $y_i=1$.

$$\delta_y(x) = \left(\prod_{i:y_i=0}(x_i-1)(0-1)+0x_i\right)\left(\prod_{i:y_i=1}(x_i-1)(1-1)+x_i1\right). \tag{A.8}$$

Finally, we simplify, bringing us to Equation (1.8).

$$\delta_y(x) = \left(\prod_{i:y_i=0}(1-x_i)\right)\left(\prod_{i:y_i=1}x_i\right). \tag{A.9}$$

Appendix B

More on Lemma 3.2.3

Definition B.0.1. An *alternating Turing machine* is

Proof of Lemma 3.2.3 as written in [4]. Let L be a PSPACE-robust language. Let $g_n(x_1, \ldots, x_n)$ be the multilinear extension of the characteristic function of $L_n = L \cap \{0,1\}^n$. Clearly, $L \in \mathsf{P}^g$, where $g = \{g_n \mid n \geq 0\}$. We will describe an alternating polynomial-time Turing machine with access to L computing g. First guess the value $z = g_n(x_1, \ldots, x_n)$. Then existentially guess the linear function $h_1(y) = g(y, x_2, \ldots, x_n)$ and verify that $h_1(x_1) = z$. Then universally choose $t_1 \in \{0,1\}$ and existentially guess the linear function $h_2(y) = g(t_1, y, x_3, \ldots, x_n)$. Keep repeating this process until we have specified $t_1, \ldots, t_n$ and then verify $t_1, \ldots, t_n \in L$. Since a PSPACE machine can simulate an alternating polynomial-time Turing machine, if L is PSPACE-robust then g is Turing-reducible to L. □

Bibliography

[1] Scott Aaronson and Avi Wigderson. "Algebrization: A New Barrier in Complexity Theory". In: *ACM Trans. Comput. Theory* 1.1 (Feb. 2009). ISSN: 1942-3454. DOI: 10.1145/1490270.1490272.

[2] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. 1st. USA: Cambridge University Press, 2009. ISBN: 978-0-521-42426-4. DOI: 10.5555/1540612.

[3] Sanjeev Arora and Shmuel Safra. "Probabilistic checking of proofs: a new characterization of NP". In: *J. ACM* 45.1 (Jan. 1998), pp. 70–122. ISSN: 0004-5411. DOI: 10.1145/273865.273901. URL: https://doi.org/10.1145/273865.273901.

[4] L. Babai, L. Fortnow, and C. Lund. "Nondeterministic exponential time has two-prover interactive protocols". In: *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*. 1990, 16–25 vol.1. DOI: 10.1109/FSCS.1990.89520.

[5] Theodore Baker, John Gill, and Robert Solovay. "Relativizations of the $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$ Question". In: *SIAM Journal on Computing* 4.4 (1975), pp. 431–442. DOI: 10.1137/0204037. eprint: https://doi.org/10.1137/0204037. URL: https://doi.org/10.1137/0204037.

[6] Eli Ben-Sasson et al. "Zero Knowledge Protocols from Succinct Constraint Detection". In: *Theory of Cryptography*. Ed. by Yael Kalai and Leonid Reyzin. Cham: Springer International Publishing, 2017, pp. 172–206. ISBN: 978-3-319-70503-3.

[7] Alessandro Chiesa et al. "Spatial Isolation Implies Zero Knowledge Even in a Quantum World". In: *J. ACM* 69.2 (Jan. 2022). ISSN: 0004-5411. DOI: 10.1145/3511100. URL: https://doi.org/10.1145/3511100.

[8] Stephen A. Cook. "The complexity of theorem-proving procedures". In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC '71. Shaker Heights, Ohio, USA: Association for Computing Machinery, 1971, pp. 151–158. ISBN: 9781450374644. DOI: 10.1145/800157.805047. URL: https://doi.org/10.1145/800157.805047.

[9] Oded Goldreich. *Foundations of Cryptography*. Vol. 1. 1st ed. Cambridge University Press, 2001. 372 pp. ISBN: 978-0-511-54689-1. DOI: 10.1017/CBO9780511546891.

[10] Tom Gur, Jack O'Connor, and Nicholas Spooner. "Perfect Zero-Knowledge PCPs for #P". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. STOC 2024. Vancouver, BC, Canada: Association for Computing Machinery, 2024, pp. 1724–1730. ISBN: 9798400703836. DOI: 10.1145/3618260.3649698. URL: https://doi.org/10.1145/3618260.3649698.

[11] Johan Håstad. "Some optimal inapproximability results". In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '97. El Paso, Texas, USA: Association for Computing Machinery, 1997, pp. 1–10. ISBN: 0897918886. DOI: 10.1145/258533.258536. URL: https://doi.org/10.1145/258533.258536.

[12] Kenneth E. Iverson. *A Programming Language*. 1st ed. John Wiley and Sons, Inc., 1962. 286 pp. ISBN: 978-0471430148. URL: https://dl.acm.org/doi/10.5555/1098666.

[13] Zhengfeng Ji et al. "MIP* = RE". In: *Commun. ACM* 64.11 (Oct. 2021), pp. 131–138. ISSN: 0001-0782. DOI: 10.1145/3485628. URL: https://dl.acm.org/doi/10.1145/3485628.

[14] Zhengfeng Ji et al. "Quantum soundness of the classical low individual degree test". In: *CoRR* abs/2009.12982 (2020). arXiv: 2009.12982. URL: https://arxiv.org/abs/2009.12982.

[15] Ali Juma et al. "The Black-Box Query Complexity of Polynomial Summation". In: *Comput. Complex.* 18.1 (Apr. 2009), pp. 59–79. ISSN: 1016-3328. DOI: 10.1007/s00037-009-0263-7. URL: https://doi.org/10.1007/s00037-009-0263-7.

[16] Yael Tauman Kalai and Ran Raz. "Interactive PCP". In: *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Part II*. ICALP '08. Reykjavik, Iceland: Springer-Verlag, 2008, pp. 536–547. ISBN: 9783540705826. DOI: 10.1007/978-3-540-70583-3_44. URL: https://doi.org/10.1007/978-3-540-70583-3_44.

[17] Donald E. Knuth. "Two Notes on Notation". In: *The American Mathematical Monthly* 99.5 (1992), pp. 403–422. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2325085 (visited on 11/19/2024).

[18] Carsten Lund et al. "Algebraic methods for interactive proof systems". In: *J. ACM* 39.4 (Oct. 1992), pp. 859–868. ISSN: 0004-5411. DOI: 10.1145/146585.146605. URL: https://doi.org/10.1145/146585.146605.

[19] Vaughan R. Pratt. "Every Prime Has a Succinct Certificate". In: *SIAM Journal on Computing* 4.3 (1975), pp. 214–220. DOI: 10.1137/0204018. eprint: https://doi.org/10.1137/0204018. URL: https://doi.org/10.1137/0204018.

[20] Walter Rudin. *Principles of Mathematical Analysis*. 3rd ed. McGraw-Hill, 1976. 342 pp. ISBN: 978-0-07-085613-4.

[21] Walter J. Savitch. "Relationships between nondeterministic and deterministic tape complexities". In: *Journal of Computer and System Sciences* 4.2 (1970), pp. 177–192. ISSN: 0022-0000. DOI: 10.1016/S0022-0000(70)80006-X. URL: https://www.sciencedirect.com/science/article/pii/S002200007080006X.

[22] Adi Shamir. "IP = PSPACE". In: *J. ACM* 39.4 (Oct. 1992), pp. 869–877. ISSN: 0004-5411. DOI: 10.1145/146585.146609. URL: https://doi.org/10.1145/146585.146609.

[23] Michael Sipser. *Introduction to the Theory of Computation*. 1st ed. International Thomson Publishing, 1996. 396 pp. ISBN: 978-0-534-94728-6. DOI: 10.1145/230514.571645.

[24] L. J. Stockmeyer and A. R. Meyer. "Word problems requiring exponential time". In: *Proceedings of the Fifth Annual ACM Symposium on Theory of Computing*. STOC '73. Austin, Texas, USA: Association for Computing Machinery, 1973, pp. 1–9. ISBN: 9781450374309. DOI: 10.1145/800125.804029. URL: https://doi.org/10.1145/800125.804029.

[25] A. M. Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem". In: *Proceedings of The London Mathematical Society* 42.1 (1936), pp. 230–265. DOI: 10.1112/PLMS/S2-42.1.230.

Index