Some Results in Circuit Complexity

Yuan Li

Thesis Advisor: Alexander Razborov
## Contents

1 Subgraph Isomorphism Problem 7  
1.1 Introduction 7  
1.2 Definitions and Preliminaries 10  
1.2.1 Graphs 10  
1.2.2 Reductions 10  
1.2.3 Subgraph Isomorphism Problems 11  
1.2.4 The Average Case 12  
1.2.5 Parameters $\kappa(P)$ and $\kappa_{col}(P)$ 14  
1.3 Average-Case AC$^0$ Complexity 15  
1.3.1 The Upper Bound 16  
1.3.2 The Lower Bound 17  
1.4 Bounds on $\kappa_{col}(P)$ 20  
1.4.1 Upper Bound 20  
1.4.2 Lower Bounds 21  
1.5 Minor-Monotonicity and Monotone Projections 23  
1.6 Conclusion 28  

2 Immunity of MOD Function 29  
2.1 Introduction 29  
2.2 Preliminaries 30  
2.2.1 Composite Modulus 30  
2.2.2 Symmetrization 31  
2.3 Lower Bound for MOD$_q$ 32  
2.4 Lower Bound for $\neg$MOD$_q$ 34  
2.5 Lower Bound for Symmetric Functions in $\langle$MOD$_q$ $\rangle$ 38  
2.6 Immunity and Circuit Lower Bound 41  

3 Robust Immune Symmetric Functions 47  
3.1 Statement of the Result 47  
3.2 Proof Techniques 48  
3.3 Proof for the Case $\text{char}(F) = 2$ 52  
3.3.1 Partition $\mathcal{U}_0$ 53  
3.3.2 Partition $\mathcal{U}_1$ 53
CONTENTS

3.3.3 From $U_m$ to $U_{2m}$ ................................. 54  
3.3.4 From $U_m$ to $U_{2m+1}$, $m$ odd ..................... 55  
3.3.5 From $U_m$ to $U_{2m+1}$, $m$ odd ..................... 58  
3.4 Proof for the Case $\text{char}(F) > 2$ ......................... 62  
3.4.1 Partition $U_0$ ........................................ 63  
3.4.2 Partition $U_1$ ........................................ 64  
3.4.3 From $U_m$ to $U_{mp+r}$ ................................. 66  

4 Appendix .................................................. 73  
4.1 Proof of Lemma 1.2.6(2) ................................. 73
Abstract

The thesis consists of three parts. The first part investigates the AC$^0$ complexity of subgraph isomorphism problem that is, detecting whether an n-vertex input graph contains a P-subgraph for some fixed P. For the average-case complexity, where the input is a distribution on random graphs at the threshold and small error is allowed, we are able to explicitly characterize the minimal AC$^0$ size up to a quadratic factor. For the worst-case complexity, if P is a colored graph (each vertex has a different color, and the input graph is also colored, of course), we prove a $n^{\Omega(tw(P)/\log tw(P))} + O(1)$ lower bound, which nearly matches the upper bound $n^{tw(P)/\log tw(P)} + O(1)$ due to Alon, Yuster and Zwick [5]. For the uncolored worst-case complexity, we prove that there is no monotone projection whatsoever that reduces Subgraph(M3) to Subgraph(P3 + M2) (P3 is a path on 3 vertices, M_k is a matching with k edges, and “+” stands for the disjoint union), which suggests that the complexity of the uncolored case is not minor monotone (unlike the colored case).

The second part proves tight lower bounds on the immunity of MOD function and its negation. For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, its immunity over the field $F_p$ is defined as the minimal degree of a nontrivial polynomial $g(x) \in F_p[x_1,\ldots,x_n]$ such that $g(x) = 0$ for all $x$ with $f(x) = 0$. Improving the previous results, we prove: when $p,q$ are coprime, the immunity of $\neg$MOD_q is exactly $\lceil (n+q-1)/q \rceil$; and the immunity of MOD_q is lower bounded by $\lceil n/2 \rceil$. We observe the following connection between immunity and circuit lower bounds: if Boolean function $f$ has immunity over $F_p$ at least $n/2 - o(\sqrt{n})$ and $|f| = \Omega(2^n)$, then $f$ requires exponential size $AC^0[p] (=AC^0$ with MOD_p gates) to compute.

The third part is a complete characterization of k robust immune symmetric Boolean functions for any k, over any field, where a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is k robust immune if the immunity of $f$ and $1-f$ is always lower bounded by k no matter how you change the values of $f(x)$ with $k \leq |x| \leq n-k$.

The first part is joint with Alexander Razborov and Benjamin Rossman, and the second part is joint with Chris Beck.
Chapter 1

Subgraph Isomorphism Problem

1.1 Introduction

The subgraph isomorphism problem takes as its input two graphs $H$ and $G$ and asks to determine whether or not $G$ contains a subgraph (not necessarily induced) isomorphic to $H$. This is one of the most basic NP-complete problems that includes CLIQUE and HAMILTONIAN CYCLE as special cases, and little more can be said about its complexity in full generality.

A significant body of research, motivated both by the framework of parameterized complexity and practical applications, has been devoted to the case when the graph $H$ is fixed and possesses some useful structure (see e.g. the sources [5, 14, 15, 28] related to the subject of our paper). To stress its nature in this situation, the graph $H$ is traditionally called a pattern and designated by the letter $P$; we also follow this convention and denote by $\text{Subgraph}(P)$ the corresponding restriction of the general subgraph isomorphism problem.

The sources above (among many others!) provide quite non-trivial improvements on the obvious size bound $O(n |V(P)|)$ in many cases of interest. But for lower bounds we, given our current state of knowledge, have to resort to restricted models, and, indeed, a substantial amount of work has been done here in the context of both bounded-depth circuits and monotone circuits. In this paper we focus on the former model.

As for upper bounds, it was observed by Amano [2] that the color-coding algorithm by Alon, Yuster and Zwick [5] can be adapted to our context and gives $\mathsf{AC}^0$-circuits for $\text{Subgraph}(P)$ of size $\tilde{O}(n^{tw(P)+1})$, where $tw(P)$ is the treewidth of the pattern $P$. Our paper is motivated by the following natural question:

How tight is this bound?

Or, in other words,

**Question 1.** Is it possible to give good general lower bounds on the $\mathsf{AC}^0$-
complexity of \textsc{Subgraph}(P) in terms of the treewidth of P only?

Prior to our work, Rossman [33] answered this question in affirmative for the case of a k-clique by proving a lower bound of $\Omega(n^{k/4})$ on the $AC^0$ complexity of \textsc{Subgraph}(K_k). Generalizing his method, Amano [2] gave a general lower bound that holds for arbitrary patterns P. It in particular implied an $n^{\Omega(k)}$ lower bound (and, thus, an affirmative answer to Question 1) for the $k \times k$ grid $G_{k,k}$: this result is very interesting since $G_{k,k}$ is the "canonical" example of a sparse graph with large treewidth.

Before discussing our results, it will be convenient to introduce the following handy notation: given a pattern $P$, we let $C(P)$ be the minimal real number $c \geq 0$ for which \textsc{Subgraph}(P) is solvable on $n$-vertex graphs by $AC^0$ circuits of size $n^{c+o(1)}$. In this notation, the previous results mentioned above can be stated as $C(P) \leq \text{tw}(P) + 1$ ([5, 2], $P$ any pattern), $C(K_k) \geq k/4$ [33] and $C(G_{k,k}) \geq \Omega(k)$ [2].

Our contributions.

We formulate explicitly and study two modifications that already implicitly played a great role in the previous research. The first of them is the 
\textit{colored $P$-subgraph isomorphism problem} $\text{Subgraph}_{col}(P)$ in which the target graph $G$ comes with a coloring $\chi : V(G) \rightarrow V(P)$ (and can w.l.o.g. be assumed to be $|V(P)|$-partite), and we are looking only for properly colored $P$-subgraphs. Let $C_{col}(P)$ be defined analogously to $C(P)$. Then the very first thing the algorithm by Alon, Yuster and Zwick does is a simple reduction from $\text{Subgraph}(P)$ to $\text{Subgraph}_{col}(P)$ thus establishing $C(P) \leq C_{col}(P)$. After that they work exclusively with the colored version that leads to $C(P) \leq C_{col}(P) \leq \text{tw}(P) + 1$.

We settle in the affirmative (up to a logarithmic factor) our motivating Question 1 for the colored version by proving the following

\textbf{Theorem 1.1.1.} $\Omega(\text{tw}(P)/\log \text{tw}(P)) \leq C_{col}(P)$.

We show that the colored version is quite well-behaved by proving that it is minor-monotone: if $Q$ is a minor of $P$, then $C_{col}(Q) \leq C_{col}(P)$ (see Theorem 1.5.2)\footnote{It is worth observing that this fact, along with the recent result [10] by Chekura and Chuzhoy and Amano’s bound $C_{col}(G_{k,k}) \geq \Omega(k)$ [2] already implies the weaker bound $C_{col}(P) \geq \text{tw}(P)^{O(1)}$. But the exponent given by this approach will be disappointingly small.}. Whether a similar result holds for $C(P)$ is open, but we give a strong evidence (Theorem 1.5.6) that even if this is true, the proof will most likely require totally different techniques. One possible interpretation is that perhaps the colored version is in fact a cleaner and more natural model to study than the standard (uncolored) version. We also observe that if the pattern $P$ is a core (i.e., every homomorphism from $G$ to $G$ is an automorphism), then $C(P) = C_{col}(P)$ and thus our lower bound from Theorem 1.1.1 transfers to the uncolored case.
1.1. INTRODUCTION

What happens to \( C(P) \) at the opposite site of the spectrum, say, for bipartite patterns \( P \), remains wide open.

All lower bounds surveyed above, including our proof of Theorem 1.1.1, have been actually achieved in the context of average-case complexity. Prior to our work, the only distribution that was considered for this purpose is the Erdős-Rényi model \( G(n, n^{-\theta(P)}) \), where \( \theta(P) \) is the uniquely defined threshold exponent for which the probability to contain a copy of \( P \) is bounded away from 0 and 1 (see [21] or Section 1.2.4 below). We define \( C_{\text{ave}}(P) \) analogously to \( C(P) \), but only requiring that our circuit outputs the correct answer a.a.s. when the input is drawn accordingly to \( G(n, n^{-\theta(P)}) \). Clearly, \( C_{\text{ave}}(P) \leq C(P) \) so the whole picture now looks like

\[
C_{\text{ave}}(P) \leq C(P) \leq C_{\text{col}}(P) \approx \text{tw}(P),
\]

where \( \approx \) means approximation within a logarithmic factor. Also, \( C_{\text{ave}}(K_k) \geq k/4 \) [33] and \( C_{\text{ave}}(G_{k,k}) \geq \Omega(k) \) [2].

We explicitly define a combinatorial parameter \( \kappa(P) \) and prove the following.

**Theorem 1.1.2.** \( \kappa(P) \leq C_{\text{ave}}(P) \leq 2\kappa(P) + O(1). \)

In other words, we give lower and upper bounds on the average case \( \text{AC}^0 \) complexity for an arbitrary pattern \( P \), matching with a quadratic factor. While the lower bound is essentially implicit in [33, 34, 2], the upper bound is new\(^2\). Its proof exploits a previously overlooked duality in the definition of \( \kappa(P) \), which has equivalent min-max and max-min formulations, and the key insight behind our proof is the observation that the min-max expression for \( \kappa(P) \) leads to \( \text{AC}^0 \) circuits of size \( n^{2\kappa(P) + O(1)} \).

Finally, let us say a few words about the proof of Theorem 1.1.1. Its own worst-case lower bound, it is obtained as the maximum of a family of average-case lower bounds with respect to \( P \)-colored random graphs. These random graphs generalize Erdős-Rényi random graphs in the \( P \)-colored setting by allowing different edge probabilities according to the color classes of vertices, and we believe that this generalization may be of independent interest. Each \( P \)-colored random graph in this family is parameterized by a point in a certain convex polytope, denoted \( \theta_{\text{col}}(P) \). We rely on a lemma of Grohe and Marx [16] which characterizes the treewidth of \( P \) in terms of the existence of a certain concurrent flow on \( P \), which we convert to a suitable point in \( \theta_{\text{col}}(P) \).

The chapter is organized as follows. In Section 1.2 we give the necessary definitions and preliminaries; in particular, in Section 1.2.5 we present the parameters \( \kappa(P) \) and \( \kappa_{\text{col}}(P) \) that is our main technical tool in this chapter. Section 1.3 is devoted to the proof of Theorem 1.1.2, and it also paves way to the proof of Theorem 1.1.1 that, up to a certain point, goes in parallel to the former. The proof of Theorem 1.1.1 is completed in Section 1.4. Section 1.5 contains our

\(^2\)Amano [2] attempted to give a general upper bound on \( C_{\text{ave}}(P) \), but later Nakagawa and Watanabe [29] constructed a sequence of patterns \( P_k \) for which \( C_{\text{ave}}(P_k) \leq O(1) \) while Amano’s bound grows to infinity.
structural results about the behavior of Subgraph($P$) and Subgraph$\text{col}(P)$ with respect to minors and subgraphs. The chapter is concluded with a few open problems in Section 1.6.

1.2 Definitions and Preliminaries

Let $[k] := \{1, \ldots, k\}$.

1.2.1 Graphs

We start off with terminology and notation for graphs. Throughout this chapter, graphs are finite simple graphs $G = (V(G), E(G))$ where $E(G)$ is a subset of $\binom{V(G)}{2}$. We often write $v(G)$ for $|V(G)|$ and $e(G)$ for $|E(G)|$.

A graph $H$ is a subgraph of $G$, denoted $H \subseteq G$, if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. For arbitrary $G$ and $H$, $G + H$ and $G \times H$ respectively denote the disjoint union and Cartesian product of graphs $G$ and $H$ (where $E(G \times H) = \{(\{v, v'\}, \{w, w'\}) : \{v, w\} \in E(G) \text{ and } \{v', w'\} \in E(H)\}$).

A homomorphism from $G$ to $H$ is a function $\varphi : V(G) \rightarrow V(H)$ such that $\{\varphi(v), \varphi(w)\} \in E(H)$ for all $\{v, w\} \in E(G)$. A graph $G$ is a core if every homomorphism from $G$ to $G$ is an automorphism.

The treewidth of $G$ is denoted by $tw(G)$ (for the definition and background, see e.g. [8]). Other relevant facts about treewidth will be stated where needed (in particular, we will use a characterization of treewidth in terms of concurrent flows (Theorem 1.4.8) due to Grohe and Marx [16]).

$K_k$ is a clique on $k$ vertices, and $G_{k,k}$ is a $k \times k$ grid.

1.2.2 Reductions

With one exception (Lemma 1.2.3), all reductions between different problems employed and studied in this chapter are of the simplest form ever, called monotone projections.

Definition 1.2.1. Let $I, J$ be arbitrary sets.

(i) For a function $p : J \rightarrow I \cup \{0, 1\}$ and $x \in \{0, 1\}^J$, we write $p^*(x)$ for the unique $y \in \{0, 1\}^I$ such that $y_j = x_{p(j)}$ if $p(j) \in I$, and $y_j = 0$ if $p(j) = 0$, and $y_j = 1$ if $p(j) = 1$.

(ii) For boolean functions $f : \{0, 1\}^I \rightarrow \{0, 1\}$ and $g : \{0, 1\}^J \rightarrow \{0, 1\}$, we say that $f$ is reducible via a monotone projection to $g$, denoted $f \leq_{\text{mp}} g$, if there exists $p : J \rightarrow I \cup \{0, 1\}$ such that $f(x) = g(p^*(x))$ for all $x \in \{0, 1\}^I$.

(Perform that $\leq_{\text{mp}}$ is transitive.)

Any decision problem $L$ can be represented as a sequence of Boolean functions $\{L^n\}$ in $n$ variables. We say that $L_1$ is reducible via a monotone projec-
tion to another decision problem $L_2$ if for any $n$ there exists a $p(n)$ such that $L_1^n \leq_{mp} L_2^{p(n)}$. If in addition $p(n) \leq O(n)$, we call this projection linear.

### 1.2.3 Subgraph Isomorphism Problems

Throughout this chapter, $P$ represents an arbitrary fixed “pattern” graph with no isolated vertices (i.e. $V(P) = \bigcup_{e \in E(P)} e$). Whenever we write $Q \subseteq P$, or refer to $Q$ as “sub-pattern” of $P$, it is understood that $V(Q)$ is chosen as small as possible, so that $Q$ also has no isolated vertices. Subgraphs (not necessarily induced) of a graph $G$ which are isomorphic to $P$ are called $P$-subgraphs of $G$. We consider two versions (uncolored and colored) of the problem of detecting $P$-subgraphs:

- **Subgraph($P$)** is the problem, given a graph $G$, of determining whether or not $G$ contains a $P$-subgraph.
- **Subgraph$_\text{col}$(P)** is the problem, given $G$ together with a homomorphism $\chi : G \to P$, of determining whether or not $G$ contains a properly colored $P$-subgraph (i.e. a subgraph which is isomorphic to $P$ via $\chi$).

We refer to **Subgraph($P$)** as the $P$-subgraph isomorphism problem and to **Subgraph$_\text{col}$(P)** as the colored $P$-subgraph isomorphism problem. It will be convenient to introduce a notation for the $\text{AC}^0$ complexity of these problems. (Recall that $\text{AC}^0$ is the class of problems solvable by polynomial-size constant-depth boolean circuits with AND and OR gates of unbounded fan-in.)

**Definition 1.2.2.** Let $C(P)$ (resp. $C_{\text{col}}(P)$) denote the minimum real number $c > 0$ such that **Subgraph($P$)** (resp. **Subgraph$_\text{col}$(P)**) is solvable (in the worst-case) on $n$-vertex graphs by $\text{AC}^0$ circuits of size $O(n^{c+\varepsilon})$ for every $\varepsilon > 0$.

Note that if **Subgraph($P$)** is reducible to **Subgraph($Q$)** via a linear monotone projection then $C(P) \leq C(Q)$, and this remains true if we add the subscript col to one or both sides.

**Lemma 1.2.3. (Properties of $C(P)$ and $C_{\text{col}}(P)$)**

1. $C(P) \leq C_{\text{col}}(P) \leq tw(P) + O(1),$
2. if $P$ is a core, then $C(P) = C_{\text{col}}(P)$.

**Proof.** (1): The second inequality $C_{\text{col}}(P) \leq tw(P) + O(1)$ is by the color-coding algorithm of Alon, Yuster and Zwick [5] (adapted to the colored setting), which can be implemented in $\text{AC}^0$ as observed by Amano [2]. The first inequality $C(P) \leq C_{\text{col}}(P)$ is also implicitly proved there by reducing **Subgraph($P$)** to **Subgraph$_\text{col}$(P)**: the reduction searches through logarithmically many different colorings of the same target graph $G$, picked at random. An easy counting argument shows that a.a.s. every prospective injective mapping $V(P) \to V(G)$ will be properly colored in at least one of them.

---

3Uniformity issues do not play any role in this chapter.
(2): If \( P \) is a core, then the “forgetful functor” \( (G, \chi) \mapsto G \) is a reduction from \textsc{Subgraph}_\text{col}(P) to \textsc{Subgraph}(P) (via a linear monotone projection). To see why, it suffices to show that every \( P \)-subgraph of \( G \) is, up to an automorphism, properly colored with respect to any homomorphism \( \chi : G \to P \). Indeed, if \( H \) is a \( P \)-subgraph of \( G \), then there exists a one-to-one homomorphism \( \varphi : P \to H \); since \( P \) is a core, the composition \( \chi \circ \varphi : P \to P \) is an automorphism of \( P \); let us call it \( \alpha \). Then \( \varphi \circ \alpha^{-1} \) defines a properly colored subgraph of \( G \).

\[ \square \]

### 1.2.4 The Average Case

We now define the random graphs which appear in our average-case lower bounds for \textsc{Subgraph}(\( P \)) and \textsc{Subgraph}_\text{col}(\( P \)). In the uncolored setting, we consider the Erdős-Rényi random graph \( G(n, p(n)) \) for an appropriately chosen threshold function \( p(n) \).

**Definition 1.2.4.**

(i) The threshold exponent of \( P \) is defined by \( \theta(P) := \min_{Q \subseteq P} v(Q)/e(Q) \).

(ii) \( P \) is balanced if \( v(P)/e(P) = \theta(P) \).

(iii) Let \( \text{Bal}(P) := \bigcup\{Q \subseteq P : v(Q)/e(Q) = \theta(P)\} \).

**Lemma 1.2.5.**

1. \( P \) is balanced if and only if \( P = \text{Bal}(P) \).

2. For every \( P \), \( \text{Bal}(P) \) is balanced and \( \theta(\text{Bal}(P)) = \theta(P) \).

**Proof.** All these statements are obvious except for the “if” part in (1), and for that we have to prove that if two subgraphs \( Q_1, Q_2 \subseteq P \) have the property \( v(Q_1) = \theta(P)e(Q_1) \) and \( v(Q_2) = \theta(P)e(Q_2) \), then their union also possesses it. For that we observe that

\[
\begin{align*}
(e(Q_1) + e(Q_2)) &= e(Q_1 \cup Q_2) + e(Q_1 \cap Q_2) \\
n\frac{v(Q_1) + v(Q_2)}{e(Q_1) + e(Q_2)} &\geq \frac{v(Q_1 \cup Q_2) + v(Q_1 \cap Q_2)}{e(Q_1 \cup Q_2) + e(Q_1 \cap Q_2),}
\end{align*}
\]

and that \( v(Q_1) \cap v(Q_2) \geq \theta(P)e(Q_1 \cap Q_2) \) due to the definition of \( \theta(P) \). This implies \( \theta(Q_1 \cup Q_2) \leq \theta(P)e(Q_1 \cup Q_2) \) and, hence \( \theta(Q_1 \cup Q_2) = \theta(P)e(Q_1 \cup Q_2) \) as the opposite inequality again follows from Definition 1.2.4(i).

Recall that \( G(n, p) \) is the Erdős-Rényi random graph with vertex set \([n]\), in which each \( e \in \binom{[n]}{2} \) occurs as an edge independently with probability \( p \). The next lemma states that \( p = n^{-\theta(P)} \) is a threshold function for \textsc{Subgraph}(\( P \)) and that detecting \( P \)-subgraphs on \( G(n, n^{-\theta(P)}) \) is equivalent to detecting \( \text{Bal}(P) \)-subgraphs. (Lemma 1.2.6(1) is a standard fact about random graphs (see [21]); we include a proof of Lemma 1.2.6(2) in Appendix 4.1.)

**Lemma 1.2.6.**

1. \( \Pr[G(n, n^{-\theta(P)}) \text{ has a } P \text{-subgraph}] \) is bounded away from 0 and 1.
1.2. DEFINITIONS AND PRELIMINARIES

2. Asymptotically almost surely, if $G(n,n^{-\theta(P)})$ contains a $\text{Bal}(P)$-subgraph, then it contains a $P$-subgraph.

With slight abuse of notation, we denote by $\text{Subgraph}_{\text{ave}}(P)$ the algorithmic problem of solving $\text{Subgraph}(P)$ on $G(n,n^{-\theta(P)})$ correctly with probability that tends to 1 as $n$ tends to $\infty$. (We remark that our results are unchanged if $n^{-\theta(P)}$ is replaced by any other threshold function $p(n) \in \Theta(n^{-\theta(P)})$.)

Similarly to Definition 1.2.2, let $C_{\text{ave}}(P)$ be the smallest $c > 0$ for which this problem can be solved by $AC^0$-circuits of size $n^{c+o(1)}$.

Remark 1.2.7. Obviously, $C_{\text{ave}}(P) \leq C(P)$, but the gap between them can be arbitrarily large. Assume e.g. that $P = K_4 + G_{k,k}$ where $k \to \infty$. Then $\text{Bal}(P) = K_4$ and thus Lemma 1.2.6(2) implies that $C_{\text{ave}}(P) = C_{\text{ave}}(K_4) \leq 4$. On the other hand, $\text{Subgraph}(G_{k,k})$ is reduced to $\text{Subgraph}(P)$ via an obvious linear monotone projection that takes $G$ to $K_4 + G$. This proves $C(P) \geq C(G_{k,k}) \geq \Omega(k)$ by the result from [2].

One might argue that this example is not “fair” since it heavily exploits the fact that the pattern $P$ is highly unbalanced. It is, however, possible to give nearly the same separation (albeit, more complicated) with balanced pattern $P$. Say, let $d > 0$ be a sufficiently large constant, and $V(P) = [k]$, where $k \gg d$. We start building $E(P)$ with the clique on the set $[d]$, and then for every $i \in [d+1,k]$ pick at random $d$ different vertices $j_1, \ldots, j_d < i$ and add all $d$ edges $(j_i,i)$. Then $P$ will be balanced, and randomness in selecting the edges will imply that a.a.s. $\text{tw}(P) \geq \Omega(k)$ and that $P$ is a core. Given these facts, the bounds $C_{\text{ave}}(P) \leq O(d)$ and $C(P) \geq \Omega(k/\log k)$ readily follow from the main results of this chapter.

We now move onto the notion of average case for $\text{Subgraph}_{\text{col}}(P)$. In contrast to the uncolored setting, there is no single most obvious average-case distribution on $P$-colored random graphs. Instead, we consider a family of $P$-colored random graphs, denoted $G_{\alpha,\beta}(n)$, which are parameterized by certain pairs of functions $\alpha : V(P) \to [0,1]$ and $\beta : E(P) \to [0,2]$ called “threshold pairs”.

Definition 1.2.8. ($P$-colored random graph $G_{\alpha,\beta}(n)$)

(i) A threshold pair for $P$ is a pair $(\alpha, \beta)$ of functions $\alpha : V(P) \to [0,1]$ and $\beta : E(P) \to [0,2]$ such that

- $\alpha(P) = \beta(P)$,
- $\alpha(Q) \geq \beta(Q)$ for all $Q \subseteq P$,

where $\alpha(Q) := \sum_{v \in V(Q)} \alpha(v)$ and $\beta(Q) := \sum_{e \in E(Q)} \beta(e)$.

(As an important special case, note that $(1, \beta)$ is a threshold pair if and only if $\beta(P) = |V(P)|$ and $\beta(Q) \leq |V(Q)|$ for all $Q \subseteq P$.)

(ii) $\theta_{\text{col}}(P)$ denotes the set of threshold pairs for $P$. 
(Note that \( \theta_{\text{col}}(P) \) is a polytope in \( \mathbb{R}^{V(P)} \times \mathbb{R}^{E(P)} \), and its section \( \{ \beta : (1, \beta) \in \theta_{\text{col}}(P) \} \) is a polytope in \( \mathbb{R}^{E(P)} \). We view elements of \( \theta_{\text{col}}(P) \) as the “\( P \)-colored” analogue of \( \theta(P) \).)

(iii) For all \((\alpha, \beta) \in \theta_{\text{col}}(P)\), let \( G_{\alpha, \beta}(n) \) denote the random graph with vertex set \( V_{\alpha}(n) := \{ (v, i) : v \in V(P), 1 \leq i \leq \lfloor n^{\alpha(v)} \rfloor \} \) where each \( \{ (v, i), (w, j) \} \) with \( \{ v, w \} \in E(P) \) is independently an edge with probability \( n^{-\beta(\{ v, w \})} \).

The \( P \)-coloring of \( G_{\alpha, \beta}(n) \) is the obvious one: \( (v, i) \mapsto v \).

The following lemma justifies the terminology “threshold pair” (by analogy to the “threshold exponent”):

**Lemma 1.2.9.** For every pattern \( P \) and \((\alpha, \beta) \in \theta_{\text{col}}(P)\) such that \( \alpha \not\equiv 0 \),

\[
\Pr[G_{\alpha, \beta}(n) \text{ contains a properly colored } P\text{-subgraph}] 
\]

is bounded away from 0 to 1.

The proof of this lemma is similar with the uncolored case (for example, see Chapter 3 of [21]).

In the context of \( \text{Subgraph}_{\text{col}}(P) \), we speak of the average-case with respect to \( G_{\alpha, \beta}(P) \), meaning an \( \text{AC}^0 \) circuit which solves \( \text{Subgraph}_{\text{col}}(P) \) on \( G_{\alpha, \beta}(P) \) with probability that tends to 1 as \( n \) tends to \( \infty \). We do not introduce any special notation like \( C_{\alpha, \beta} \) as this concept is intended to be auxiliary.

### 1.2.5 Parameters \( \kappa(P) \) and \( \kappa_{\text{col}}(P) \)

We now introduce the parameters \( \kappa(P) \) and \( \kappa_{\text{col}}(P) \) which figure in our lower bounds. The definitions, that might appear unmotivated at first glance, are derived from the lower bound technique of [33], which we explain in the next section.

**Remark 1.2.10.** The max-min (or “hitting set”) form of \( \kappa(P) \), as a lower bound on the average-case \( \text{AC}^0 \) complexity of \( \text{Subgraph}(P) \), was implicit to varying degrees in [2, 29, 33, 34]. However, the dual min-max (or “union sequence”) expression \( \kappa(P) \) is new, as are parameters \( \kappa_{\alpha, \beta}(P) \) and \( \kappa_{\text{col}}(P) \).

**Definition 1.2.11.** (Union sequences and hitting sets) A union sequence for \( P \) is a sequence \( Q_1, \ldots, Q_t \) of subgraphs of \( P \) such that \( Q_t = P \) and for all \( 1 \leq k \leq t \), either \( Q_k \) is a single edge or \( Q_k = Q_i \cup Q_j \) for some \( 1 \leq i < j < k \). A hitting set for union sequences (or hitting set for short) is a set \( H \) of subgraphs of \( P \) such that \( H \) contains at least one element from every union sequence.

**Definition 1.2.12.** (Parameters \( \kappa(P) \), \( \kappa_{\alpha, \beta}(P) \) and \( \kappa_{\text{col}}(P) \))

(i) If \( P \) is balanced, then \( \kappa(P) \) is defined by

\[
\kappa(P) := \min_{\text{union seq. } Q_1, \ldots, Q_t} \max_{v \in [t]} (v(Q_1) - \theta(P)e(Q_i)).
\]

For \( P \) which is not balanced, we define \( \kappa(P) := \kappa(\text{Bal}(P)) \).
1.3. AVERAGE-CASE $AC^0$ COMPLEXITY

(ii) For all $(\alpha, \beta) \in \theta_{\text{col}}(P)$, let

$$\kappa_{\alpha, \beta}(P) := \min_{\text{union seq. } Q_1, \ldots, Q_t} \max_{i \in [t]} (\alpha(Q_i) - \beta(Q_i)).$$

(iii) Let $\kappa_{\text{col}}(P) := \max_{(\alpha, \beta) \in \theta_{\text{col}}(P)} \kappa_{\alpha, \beta}(P)$.

The next lemma is key to linking our upper and lower bounds on the average-case $AC^0$ complexity of $\text{SUBGRAPH}(P)$.

**Lemma 1.2.13. (Minimax principle for $\kappa(P)$ and $\kappa_{\alpha, \beta}(P)$)**

1. If $P$ is balanced, then

$$\kappa(P) = \max_{\mathcal{H}} \min_{Q \in \mathcal{H}} (v(Q) - \theta(P)v(Q)),$$

where $\mathcal{H}$ ranges over hitting sets for $P$.

2. Similarly, $\kappa_{\alpha, \beta}(P) = \max_{\mathcal{H}} \min_{Q \in \mathcal{H}} (\alpha(Q) - \beta(Q))$ for all $(\alpha, \beta) \in \theta_{\text{col}}(P)$.

**Proof.** The argument is the same for (1) and (2). Let $f(Q) := v(Q) - \theta(P)v(Q)$ (the proof works for any real-valued objective function). First, we will prove $\max_{\mathcal{H}} \min_{Q \in \mathcal{H}} f(Q) \leq \kappa(P)$. Since $\mathcal{H}$ is a hitting set, for any union sequence $\{Q_i\}$, there exists some $Q_i \in \mathcal{H}$. It follows that $\min_{Q \in \mathcal{H}} f(Q) \leq \max_i f(Q_i)$, and thus $\min_{Q \in \mathcal{H}} f(Q) \leq \kappa(P)$ as $\{Q_i\}$ is taken arbitrarily.

On the other hand, let us prove $\kappa(P) \leq \max_{\mathcal{H}} \min_{Q \in \mathcal{H}} f(Q)$. Enumerate all union sequences $\{Q_i^{(j)}\}$, $j = 1, 2, \ldots$ (each $\{Q_i^{(j)}\}$ is a finite sequence). For each $j$, take the subgraph $S^{(j)}$ in $\{Q_i^{(j)}\}$ with maximal $f(Q_i^{(j)})$. Let $S = \{S^{(1)}, S^{(2)}, \ldots\}$. It is easily seen that $S$ is a hitting set, as every union sequence has some element in it. By definition,

$$\max_{\mathcal{H}} \min_{Q \in \mathcal{H}} f(Q) \geq \min_{S^{(j)} \in S} f(S^{(j)}) = \min_j \max_i f(P_i^{(j)}) = \kappa(P).$$

This completes the proof. \hfill \Box

### 1.3 Average-Case $AC^0$ Complexity

We present our lower and upper bounds on the average-case $AC^0$ complexity of $\text{SUBGRAPH}(P)$ and $\text{SUBGRAPH}_{\text{ave}}(P)$.

**Theorem 1.3.1.**

1. For every pattern $P$ we have

$$\kappa(P) \leq C_{\text{ave}}(P) \leq 2\kappa(P) + O(1).$$

In words, the average-case $AC^0$ complexity of $\text{SUBGRAPH}(P)$ on $G(n, n^{-\theta(P)})$ is between $n^{\kappa(P) - o(1)}$ and $n^{2\kappa(P) + O(1)}$.
2. For every pattern $P$ and $(\alpha, \beta) \in \theta_{\text{col}}(P)$, the average-case $AC^0$ complexity of $\text{SUBGRAPH}_{\text{col}}(P)$ on $G_{\alpha, \beta}(n)$ is between $n^{\kappa_{\alpha, \beta}(P)-o(1)}$ and $n^{2\kappa_{\alpha, \beta}(P)+O(1)}$.

As an immediate corollary, we get worst-case lower bounds $\kappa(P) \leq C(P)$ and $\kappa_{\text{col}}(P) \leq C_{\text{col}}(P)$.

We remark that Theorem 1.3.1(1) is actually a special case of Theorem 1.3.1(2). Indeed, in light of Lemma 1.2.6, it suffices to prove (1) in the case where $P$ is balanced, and for balanced $P$ (1) does reduce to the special case of (2) for the threshold pair $(1, \theta(P)) \in \theta_{\text{col}}(P)$ consisting of two constant functions.

We prove the $n^{2\kappa_{\alpha, \beta}(P)+O(1)}$ upper bound first in Section 1.3.1. Afterwards, a sketch of the $n^{\kappa_{\alpha, \beta}(P)-o(1)}$ lower bound is presented in Section 1.3.2.

### 1.3.1 The Upper Bound

We present the $n^{2\kappa_{\alpha, \beta}(P)+O(1)}$ upper bound. For a $P$-colored graph $G$ and $Q \subseteq P$, let $\text{sub}(Q,G)$ denote the number of properly colored $Q$-subgraphs of $G$. Let $\mathcal{G}_{\alpha, \beta}(n)$ denote the support of $G_{\alpha, \beta}(n)$, that is, the class of $P$-colored graphs with vertex set $\{(v,i): v \in V(P), 1 \leq i \leq n^{\alpha(v)}\}$ and vertex-coloring $(v,i) \mapsto v$. For $\varepsilon > 0$, let

$$\mathcal{G}_{\alpha, \beta}^{(\varepsilon)}(n) := \{G \in \mathcal{G}_{\alpha, \beta}(n) : \text{sub}(Q,G) \leq n^{\alpha(Q)-\beta(Q)+\varepsilon} \text{ for all } Q \subseteq P\}.$$  

The next lemma is a standard inequality follows from Markov inequality says that the random graph $G_{\alpha, \beta}(n)$ is unlikely to contain significantly more than than expected number of $Q$-subgraphs for any $Q \subseteq P$.

**Lemma 1.3.2.** For all $\varepsilon > 0$, $\Pr_{G \sim G_{\alpha, \beta}(n)}[G \in \mathcal{G}_{\alpha, \beta}^{(\varepsilon)}(n)] \to 1$ as $n \to \infty$.  

To prove our upper bound, we will show:

**Lemma 1.3.3.** There exists a random $AC^0$ circuit $C$ of size $O(n^{2\kappa_{\alpha, \beta}(P)+2\varepsilon+O(1)})$ such that for every $G \in \mathcal{G}_{\alpha, \beta}^{(\varepsilon)}(n)$, $\Pr[C(G) = 1 \iff \text{sub}(P,G) \geq 1] \to 1$ as $n \to \infty$.

As an immediate corollary of Lemmas 1.3.2 and 1.3.3 (via the standard averaging argument), we have:

**Corollary 1.3.4.** There exists a (deterministic) $AC^0$ circuit $C$ of size $n^{2\kappa_{\alpha, \beta}(P)+O(1)}$ such that

$$\Pr_{G \sim G_{\alpha, \beta}(n)}[C(G) = 1 \iff \text{sub}(P,G) \geq 1] \to 1 \text{ as } n \to \infty.$$  

It remains to prove Lemma 1.3.3. Before worrying about the implementation in $AC^0$, let’s first give an $n^{2\kappa_{\alpha, \beta}(P)+O(1)}$ algorithm to solve $\text{SUBGRAPH}_{\text{col}}(P)$ on the class $\mathcal{G}_{\alpha, \beta}^{(\varepsilon)}(n)$. By definition of $\kappa_{\alpha, \beta}(P)$, there exists a union sequence $Q_1, \ldots, Q_t = P$ such that $\max_{i \in [t]}(\alpha(Q_i) - \beta(Q_i)) = \kappa_{\alpha, \beta}(P)$. The idea is simple: given $G \in \mathcal{G}_{\alpha, \beta}^{(\varepsilon)}(n)$, for $i = 1, \ldots, t$, we will make a list $L_i(G)$ of all $Q_i$-subgraphs in $G$ (in arbitrary order). If $Q_i$ is a single edge, then we construct $L_i(G)$ by
brute force in time $O(n^2)$. Otherwise, $Q_i = Q_j \cup Q_k$ for some $i \geq j > k \geq 1$, we form the list $L_i(G)$ by “merging” lists $L_j(G)$ and $L_k(G)$: this requires checking every pair of subgraphs $A \in L_j(G)$ and $B \in L_k(G)$ and adding $A \cup B$ to $L_i(G)$ whenever $A \cup B$ is a $Q_i$-subgraph of $G$. Note that the complexity of this merge step is $O(|L_j(G)| \cdot |L_k(G)|)$. At the end of the algorithm, we simply check whether $L_i(G)$ is empty or not. The complexity of this algorithm is bounded by $\max_{i \leq |t|} |L_i(G)|^2 \leq O(n^{2n_{\alpha, \beta} \cdot (P) + 2c})$, since $G \in \mathcal{G}_{\alpha, \beta}^c(n)$.

Here is how we implement this algorithm by a random AC$^0$ circuit $C$. The list $L_i(G)$ will be represented by an “array” of $n^{n_{\alpha(Q_i) - \beta(Q_i) + 2c}}$ “cells”, where each cell consists of $O(\log n)$ gates. On input $G$, a given cell will either be “blank” (all $|V(Q_j)| \cdot n$ gates have value 0), or contain the description (in binary) of a $Q_i$-subgraph of $G$. In the case $Q_i = Q_j \cup Q_k$ where $i \geq j > k \geq 1$, the list $L_i(G)$ will be randomly constructed from lists $L_j(G)$ and $L_k(G)$ in two steps. First, the circuit constructs the 2-dimensional “merge array” of size $n^{n_{\alpha(Q_j) - \beta(Q_j) + 2c}) \cdot n^{n_{\alpha(Q_k) - \beta(Q_k) + 2c})}$ which contains the merge of $L_j(G)$ and $L_k(G)$ among many blank cells. That is, for cell $x$ in $L_j(G)$ and cell $y$ in $L_k(G)$, the $(x, y)$-cell in the merge array will be blank if $x$ is blank or $y$ is blank, or the union of the graphs in these cells is not a $Q_i$-subgraph.

Finally, we must “hash” the merge array (which has $\leq n^{n_{\alpha(Q_i) - \beta(Q_i) + 2c}}$ non-blank cell) down to an array of $n^{n_{\alpha(Q_i) - \beta(Q_i) + 2c}}$ cells. This can be achieved—with high probability—by a random AC$^0$ circuit.

### 1.3.2 The Lower Bound

We begin with the observation that AC$^0$ has two equivalent definitions:

- (I) polynomial-size constant-depth $\{\text{AND}_\infty, \text{OR}_\infty, \text{NOT}\}$-circuits,
- (II) polynomial-size $\{\text{AND}_2, \text{OR}_2, \text{NOT}\}$-circuits with unbounded depth, but only $O(1)$ alternations between AND and OR gates along any path from an input to the output (where NOT gates are on the bottom level without loss of generality).

Note that the conversion from type I to type II (by replacing each $\text{AND}_\infty$ (resp. $\text{OR}_\infty$) gate with unbounded fan-in with a balanced binary tree of $\text{AND}_2$ (resp. $\text{OR}_2$) gates) transforms a circuit with $w$ wires into a circuit with $O(w)$ gates. Measuring size by the number of gates, it follows that a size lower bound of $S$ for type-II circuits implies a lower bound of $\Omega(\sqrt{S})$ for type-I circuits.

We will sketch a proof of the $n^{n_{\alpha, \beta}(P) - o(1)}$ lower bound of Theorem 1.3.1(2) for type-II circuits. This implies an $n^{n_{\alpha, \beta}(P) - o(1)}$ lower bound for type-I circuits. We mention that the stronger $n^{n_{\alpha, \beta}(P) - o(1)}$ lower bound for type-I circuits holds by an additional argument (see Chapter 3 of [34]).

The following definition, adapted from [34], is key to the proof.

#### Definition 1.3.5

Let $f$ be a boolean function on graphs, and let $H$ be any graph. The $f$-sensitive subgraph of $H$, denoted $\text{Sens}(f, H)$, defined as the unique minimal subgraph $S \subseteq H$ such that $f(H') = f(H' \cap S)$ for every $H' \subseteq H$. We say that $f$ is sensitive over $H$ if $\text{Sens}(f, H) = H$. 

Two important observations are:

- $f$ is sensitive over $\text{Sens}(f, H)$ (i.e. $\text{Sens}(f, \text{Sens}(f, H)) = \text{Sens}(f, H)$),
- if $f$ is the AND or OR of functions $f_1$ and $f_2$, then $\text{Sens}(f, H) \subseteq \text{Sens}(f_1, H) \cup \text{Sens}(f_2, H)$.

**Lemma 1.3.6.** Let $C$ be an arbitrary boolean circuit with fan-in 2, whose variables encode the potential edges in a graph. Suppose that $C$ is sensitive over some nonempty graph $H$. Then there exists a union sequence $H_1, \ldots, H_t = H$ and a sequence $C_1, \ldots, C_t$ of sub-circuits of $C$ such that $C_i$ is sensitive over $H_i$ for all $i \in [t]$.

**Proof.** We argue by induction on boolean circuits with fan-in 2. In the base case, $C$ is a variable (corresponding to a possible edge). The assumption that $C$ is sensitive over $H$ implies that $H$ is a single edge. Therefore, $H$ itself is a union sequence of length 1 which satisfies the condition of the lemma.

For the induction step, first suppose $C = \text{NOT}(C')$. Note that $C'$ is sensitive over $H$. Therefore, the lemma holds by the induction hypothesis for $C'$.

Finally, suppose $C$ is the AND or OR of sub-circuits $C_1$ and $C_2$. If $C_1$ or $C_2$ is sensitive over $H$, then appealing to the induction hypothesis, we are done. So we will assume that neither $C_1$ nor $C_2$ are sensitive over $H$. Let $H_i := \text{Sens}(C_i, H)$ for $i = 1, 2$. Then $C_i$ is sensitive over $H_i$, by the first observation above. By the second observation,

$$H = \text{Sens}(C, H) \subseteq \text{Sens}(C_1, H) \cup \text{Sens}(C_2, H) = H_1 \cup H_2.$$

Hence $H = H_1 \cup H_2$. By the induction hypothesis, there exist union sequence $S_1, \ldots, S_s = H_1$ and $T_1, \ldots, T_t = H_2$ which satisfy the condition in the lemma with respect to $C_1, H_1$ and $C_2, H_2$ respectively. Then $S_1, \ldots, S_s, T_1, \ldots, T_t, H$ is a union sequence which satisfies the condition in the lemma with respect to $C, H$.

A second bit of notation:

**Definition 1.3.7.** If $f$ is a boolean functions on graphs and $G$ is any graph, then let $f^{\cup G}$ denote the function $f^{\cup G}(H) := f(G \cup H)$.

For a boolean circuit $C$ on graphs, by considering the circuit $C^{\cup G}$ which substitutes 1 for variables corresponding to edges in $G$, we get the following corollary of Lemma 1.3.6.

**Corollary 1.3.8.** Let $C$ be an arbitrary boolean circuit with fan-in 2, whose variables encode the potential edges in a graph. Let $G$ be any graph. Suppose that $C^{\cup G}$ is sensitive over some nonempty graph $H$. Then there exists a union sequence $H_1, \ldots, H_t = H$ and a sequence $C_1, \ldots, C_t$ of sub-circuits of $C$ such that $C_i^{\cup G}$ is sensitive over $H_i$ for all $i \in [t]$. 


1.3. AVERAGE-CASE AC⁰ COMPLEXITY

Now let’s fix a pattern $P$ and a threshold pair $(\alpha, \beta) \in \theta_{col}(P)$. We will write $G$ for the $P$-colored random graph $G_{\alpha,\beta}(n)$. Let $P$ be a uniform random “planted” $P$-subgraph (independent of $G$). (That is, $P$ is the $P$-subgraph with vertex set $\{(v, i_v) : v \in V(P)\}$ where $i_v$ is uniform random in $\{1, \ldots, \lceil n^{\alpha(v)} \rceil \}$. For a sub-pattern $Q \subseteq P$, let $\mathbf{Q}$ denote the corresponding subgraph of $P$.

**Lemma 1.3.9.** Suppose $f : G_{\alpha,\beta}(n) \to \{0, 1\}$ is any function such that

$$\Pr_G[f(G) = 1 \leftrightarrow G \text{ has a } P\text{-subgraph}] = 1 - o(1).$$

Then $\Pr_{G,P}[f_{\cup P} \text{ is sensitive over } P] \geq \Omega(1)$.

In fact, $\Pr_{G,P}[f_{\cup P} \text{ is sensitive over } P \mid G \text{ has no } P\text{-subgraph}] = \Omega(1)$, which implies $\Pr_{G,P}[f_{\cup P} \text{ is sensitive over } P] \geq \Omega(1)$ by Lemma 1.2.9. The point is that $f_{\cup P}(P) = 1$ with probability 1, while if we condition on $G$ having no $P$-subgraph, then almost surely $f_{\cup P}(Q) = 0$ for every proper sub-pattern $Q \subset P$.

We now state the main technical lemma, which is straightforward generalization Proposition 3.11 in [34].

**Lemma 1.3.10.** (Proposition 3.11 in [34]) Suppose $f : G_{\alpha,\beta}(n) \to \{0, 1\}$ is $AC^0$ computable. Then for every $Q \subseteq P$,

$$\Pr_{G,Q}[f_{\cup Q} \text{ is sensitive over } Q] \leq n^{-\alpha(Q) + \beta(Q) + o(1)}.$$ 

**Theorem 1.3.11.** Suppose $C$ is a type-II circuit which solves $\text{SUBGRAPH}_P(G)$ in the average-case on $G_{\alpha,\beta}(P)$. Then $C$ has size $n^{\kappa_{\alpha,\beta}(P)-\varepsilon}$ for some constant $\varepsilon > 0$.

*Proof.* For contradiction, assume $C$ has size $\leq n^{\kappa_{\alpha,\beta}(P)-\varepsilon}$ for some constant $\varepsilon > 0$. By Lemma 1.2.13, there exists a hitting set $H$ for $P$ such that

$$\kappa_{\alpha,\beta}(P) = \min_{Q \in H} \alpha(Q) - \beta(Q).$$

Note that $|H| \leq 2^{|E(P)|} = O(1)$. For every sub-circuit $C'$ of $C$, we have

$$\Pr_G[\bigvee_{Q \in H} C_{\cup Q} \text{ is sensitive over } Q] \leq \sum_{Q \in H} n^{-\alpha(Q) + \beta(Q) + o(1)} \text{ (by Lemma 1.3.10)}$$

$$= n^{-\kappa_{\alpha,\beta}(P) + o(1)}.$$ 

By a union bound,

$$\Pr_G[\bigvee_{\text{sub-circuits } C' \subseteq H} C_{\cup C'} \text{ is sensitive over } Q] \leq n^{-\varepsilon + o(1)} = o(1).$$  \hspace{0.5cm} (1.1)

On the other hand, by Lemma 1.3.9, $\Pr_{G,P}[C_{\cup P} \text{ is sensitive over } P] \geq \Omega(1)$. Note that by Corollary 1.3.8, if $C_{\cup P}$ is sensitive over $P$, then there exists $Q \in H$ and a sub-circuit $C' \subseteq C$ such that $C_{\cup H} \text{ is sensitive over } Q$. But this implies

$$\Pr_G[\bigvee_{\text{sub-circuits } C' \subseteq H} C_{\cup C'} \text{ is sensitive over } Q] \geq \Omega(1).$$ \hspace{0.5cm} (1.2)

We get a contradiction between (1.1) and (1.2), which proves the theorem. \Box
1.4 Bounds on $\kappa_{\text{col}}(P)$

In the previous section, we proved that $C_{\text{col}}(P) \geq \kappa_{\text{col}}(P)$, that is, $n^{\kappa_{\text{col}}(P)-o(1)}$ is a lower bound on the $AC^0$ complexity of SUBGRAPH$_{\text{col}}(P)$. In this section, we complete the proof of Theorem 1.1.1 by showing that $\kappa_{\text{col}}(P) = \Omega(\text{tw}(P) / \log \text{tw}(P))$.

1.4.1 Upper Bound

We have already established that $\kappa_{\text{col}}(P) \leq C_{\text{col}}(P)$ (Theorem 1.3.1(3)) and $C_{\text{col}}(P) \leq \text{tw}(P) + O(1)$ (Lemma 1.2.3(1)). By these lower and upper bounds in circuit complexity, it follows that $\kappa_{\text{col}}(P) \leq \text{tw}(P) + O(1)$. In this subsection, we give a direct proof that $\kappa_{\text{col}}(P) \leq \text{tw}(P) + 1$.

We require the following lemma, which shows that the max in the definition of $\kappa_{\text{col}}(P) := \max_{(\alpha, \beta) \in \theta_{\text{col}}(P)} \kappa_{\alpha, \beta}(P)$ is always achieved by some $(\alpha, \beta) \in \theta_{\text{col}}(P)$ with $\alpha \equiv 1$.

Lemma 1.4.1. For all $P$, there exists $\beta : E(P) \rightarrow [0, 2]$ such that $(1, \beta) \in \theta_{\text{col}}(P)$ and $\kappa_{\text{col}}(P) = \kappa_{1, \beta}(P)$.

Proof. Fix arbitrary $(\alpha, \beta) \in \theta_{\text{col}}(P)$ such that $\kappa_{\text{col}}(P) = \kappa_{\alpha, \beta}(P)$. Define $\beta' : E(P) \rightarrow [0, 2]$ by

$$\beta'({v, w}) := \beta({v, w}) + \frac{1 - \alpha(v)}{d_P(v)} + \frac{1 - \alpha(w)}{d_P(w)}.$$

For all $Q \subseteq P$, we have

$$|V(Q)| - \beta'(Q) = |V(Q)| - \sum_{\{v, w\} \in E(Q)} \left( \beta({v, w}) + \frac{1 - \alpha(v)}{d_P(v)} + \frac{1 - \alpha(w)}{d_P(w)} \right)$$

$$= \sum_{v \in V(Q)} \left( 1 - \frac{d_Q(v)}{d_P(v)} (1 - \alpha(v)) \right) - \sum_{\{v, w\} \in E(Q)} \beta({v, w})$$

$$\geq \alpha(Q) - \beta(Q).$$

It follows that $(1, \beta') \in \theta_{\text{col}}(P)$ and $\kappa_{1, \beta'}(P) \geq \kappa_{\alpha, \beta}(P)$, therefore $\kappa_{1, \beta'}(P) = \kappa_{\alpha, \beta}(P) = \kappa_{\text{col}}(P)$. \qed

Proposition 1.4.2. $\kappa_{\text{col}}(P) \leq \text{tw}(P) + 1$.

Proof. In fact, we will prove $\kappa_{\text{col}}(P) \leq \text{bw}(P)$ where $\text{bw}(P)$ is the branch-width of $P$ (it is known that $\text{bw}(P) \leq \text{tw}(P) + 1$ by [35]). Recall that a branch decomposition of $P$ is a pair $(T, b)$ where $T$ is a binary tree and $b$ is bijection from Leaves$(T)$ to $E$. Each edge in $T$ determines a partition of Leaves$(T)$ (and hence of $E$) into two sets. The width of $(T, b)$ is the maximum of $|V(E_1) \cap V(E_2)|$ over partitions $E = E_1 \uplus E_2$ determined by the edges of $T$, where $V(E_i) = \bigcup_{e \in E_i} e$ is the set of vertices incident to edges of $E_i$. 

Let $\kappa$. For a corresponding threshold pair $(\alpha, \beta)$ of distinct vertices in $P$ of width $k$. By Lemma 1.4.1, there exists $Q_i$, $x_i$, and $P$ such that $Q_i$ is a union sequence of $P$. Since $(T, b)$ has width $k$, we have $|V(Q_i) \cap V(Q_i)| \leq k$ for all $i \in [l]$. By Lemma 1.4.1, there exists $\beta : E(P) \rightarrow [0, 2]$ such that $(1, \beta) \in \theta_{col}(P)$ and $\kappa_{col}(P) = \kappa_{1, \beta}(P)$. For all $i \in [l]$, we have

$$|V(Q_i)| - \beta(Q_i) \leq |V(Q_i)| - \beta(Q_i) + |V(Q_i)| - \beta(Q_i) \quad \text{(since } |V(Q_i)| \geq \beta(Q_i))$$

$$= |V(Q_i)| + |V(Q_i)| + |V(P)| \quad \text{(since } \beta(Q_i) + \beta(Q_i) = \beta(Q_i) = |V(P)|)$$

$$= |V(Q_i) \cap V(Q_i)| \leq k.$$

Therefore, $\kappa_{col}(P) = \kappa_{1, \beta}(P) \leq \max_{i \in [l]} |V(Q_i)| - \beta(Q_i) \leq k \leq bw(P) \leq tw(P) + 1.$

1.4.2 Lower Bounds

We now prove:

**Theorem 1.4.3.** $\kappa_{col}(P) \geq \Omega(tw(P)/ \log tw(P)).$

Together with the fact that $C_{col}(P) \geq \kappa_{col}(P)$ (Theorem 1.3.1(3)), this completes the proof of our second main theorem (Theorem 1.1.1).

Theorem 1.4.3 is proved as follows. For $P$ with $tw(P) = k$, we use a result of Grohe and Marx [16] which shows that there is a large subset $W \subseteq V(P)$ and a concurrent flow on $P$ which routes a significant amount of flow between every pair of distinct vertices in $W$. Given such a concurrent flow on $P$, we construct a corresponding threshold pair $(\alpha, \beta) \in \theta_{col}(P)$ and show that $\kappa_{\alpha, \beta}(P)$ gives the desired bound.

**Definition 1.4.4.**

(i) Let $\text{Paths}(P)$ denote the set of paths in $P$, that is, subgraphs of $P$ isomorphic to an undirected path of length $\geq 1$.

(ii) Let $\text{Flows}(P)$ denote the set of concurrent flows on $P$, that is, functions $f : \text{Paths}(P) \rightarrow [0, 1]$ such that $\sum_{\pi \in \text{Paths}(P), v \in V(\pi)} f(\pi) \leq 1$ for all $v \in V(P)$.

(iii) For $\pi \in \text{Paths}(P)$, define $\alpha_\pi : V(P) \rightarrow [0, 1]$ and $\beta_\pi : E(P) \rightarrow [0, 2]$ by

$$\alpha_\pi(v) := \begin{cases} 1/2 & \text{if } v \text{ is an endpoint of } \pi, \\ 1 & \text{if } v \text{ is a middle vertex of } \pi, \\ 0 & \text{if } v \notin V(\pi), \end{cases} \quad \beta_\pi(e) := \begin{cases} 1 & \text{if } e \in E(\pi), \\ 0 & \text{if } e \notin E(\pi). \end{cases}$$

(iv) For $f \in \text{Flows}(P)$, define $\alpha_f : V(P) \rightarrow [0, 1]$ and $\beta_f : E(P) \rightarrow [0, 2]$ by

$$\alpha_f(v) := \sum_{\pi \in \text{Paths}(P)} f(\pi) \cdot \alpha_\pi(v), \quad \beta_f(e) := \sum_{\pi \in \text{Paths}(P)} f(\pi) \cdot \beta_\pi(e).$$
Lemma 1.4.5. \((\alpha_f, \beta_f) \in \theta_{\text{col}}(P)\) for all \(f \in \text{Flows}(P)\).

Proof. We must check that \(\alpha_f(P) = \beta_f(P)\) and \(\alpha_f(Q) \geq \beta_f(Q)\) for all \(Q \subseteq P\). This follows from the (more obvious) fact that \(\alpha_\pi(P) = \beta_\pi(P) = |E(\pi)|\) and \(\alpha_\pi(Q) \geq \beta_\pi(Q)\) for all \(Q \subseteq P\). \(\square\)

Definition 1.4.6. For \(f \in \text{Flows}(P)\) and \(S, T \subseteq V(P)\), let \(\tilde{f}(S, T)\) denote the ergodic flow under \(f\) from \(S\) to \(T\), that is,

\[
\tilde{f}(S, T) := \sum_{\pi \in \text{Paths}(P) : \pi \text{ has endpoints in } S \text{ and } T} f(\pi).
\]

Lemma 1.4.7. For all \(Q \subseteq P\) and \(f \in \text{Flows}(P)\),

\[
\alpha_f(Q) - \beta_f(Q) \geq \frac{1}{2} \tilde{f}(V(Q), V(P) \setminus V(Q)).
\]

Proof. Note that \(\tilde{f}(S, T) = \sum_{\pi \in \text{Paths}(P)} f(\pi) \cdot \tilde{\pi}(S, T)\) where

\[
\tilde{\pi}(S, T) := \begin{cases} 1 & \text{if } \pi \text{ has endpoints in } S \text{ and } T, \\ 0 & \text{otherwise}. \end{cases}
\]

It suffices to show that

\[(1.3) \quad \alpha_\pi(Q) - \beta_\pi(Q) \geq \frac{1}{2} \tilde{\pi}(V(Q), V(P) \setminus V(Q))\]

for all \(\pi \in \text{Paths}(P)\). If \(\pi\) does not have endpoints in \(V(Q)\) and \(V(P) \setminus V(Q)\), then \(\frac{1}{2} \tilde{\pi}(V(Q), V(P) \setminus V(Q)) = 0\), while \(\alpha_\pi(Q) - \beta_\pi(Q) \geq 0\), so (1.3) holds. On the other hand, if \(\pi\) does have endpoints in \(V(Q)\) and \(V(P) \setminus V(Q)\), then \(\frac{1}{2} \tilde{\pi}(V(Q), V(P) \setminus V(Q)) = \frac{1}{2}\), while \(\alpha_\pi(Q) - \beta_\pi(Q) = -\frac{1}{2} + (\text{the number of times that } \pi \text{ crosses between } V(Q) \text{ and } V(P) \setminus V(Q)) \geq \frac{1}{2}\), so again (1.3) holds. \(\square\)

For our lower bound on \(\kappa_{\text{col}}(P)\), we will use the following characterization of treewidth in terms of concurrent flows:

Theorem 1.4.8. (Lemma 10 in [16]) If \(P\) has treewidth \(k\), then there exist \(W \subseteq V(P)\) with \(|W| \geq 2k/3\) and \(f \in \text{Flows}(P)\) such that \(\tilde{f}(v, w) \geq 1/ck\log k\) for all distinct \(v, w \in W\) where \(c > 0\) is a universal constant.

We now prove the main result of this section.

Proof of Theorem 1.4.3. Suppose \(tw(P) = k\) and fixed \(W \subseteq V(P)\) and \(f \in \text{Flows}(P)\) as in the Theorem 1.4.8. The set of \(Q \subseteq P\) such that \(2k/9 \leq |W \cap V(Q)| \leq 4k/9\) is clearly a hitting set for \(P\) (i.e. every union sequence for \(P\) contains a subgraph in this set). For such \(Q\), we have

\[
\alpha_f(Q) - \beta_f(Q) \geq \frac{\tilde{f}(W \cap V(Q), W \setminus V(Q)) \cdot |W \setminus V(Q)|}{2ck \log k} \geq \frac{4k}{81ck \log k}.
\]

Therefore, \(\kappa_{\text{col}}(P) \geq \kappa_{\alpha_f, \beta_f}(P) \geq 4k/81ck \log k = \Omega(k/ \log k)\). \(\square\)
1.5. MINOR-MONOTONICITY AND MONOTONE PROJECTIONS

We conclude this section by giving a second lower bound on \( \kappa_{\text{col}}(P) \), which is stronger than Theorem 1.4.3 in the case that \( P \) is an expander (such as \( K_k \) or \( \text{Grid}_{k,k} \)). Let \( \Delta(P) \) denote the maximum degree of \( P \). For \( S,T \subseteq V(P) \), let \( E_P(S,T) := \{ e \in E : e \text{ has endpoints in } S \text{ and } T \} \). Recall that the edge expansion of \( P \) is defined by

\[
\eta(P) := \min_{S : \emptyset \subset S \subseteq V(P)} \min\{|S|,|V(P) \setminus S|\}.
\]

Proposition 1.4.9. \( \kappa_{\text{col}}(P) \geq h(P)|V(P)|/3\Delta(P) \).

Proof. Define \( \lambda : E(P) \to [0,2] \) by

\[
\lambda(\{v,w\}) := \frac{1}{d_P(v)} + \frac{1}{d_P(w)}.
\]

It is easy to check that \((1,\lambda) \in \theta_{\text{col}}(P)\), as clearly \( \lambda(P) = |V(P)| \) and \( \lambda(Q) \leq |V(Q)| \) for all \( Q \subseteq P \).

Consider the hitting set for \( P \) consisting of subgraphs \( Q \) such that \( \frac{1}{3}|V(P)| \leq |V(Q)| \leq \frac{2}{3}|V(P)| \). For such \( Q \), we have

\[
|V(Q)| - \lambda(Q) = \sum_{(v,w) : v \in V(Q) \& \{v,w\} \in E(P)} \frac{1}{d_P(v)} - \sum_{(v,w) : \{v,w\} \in E(Q)} \frac{1}{d_P(v)}
\]

\[
\geq \sum_{(v,w) : v \in V(Q) \& \{v,w\} \in E(P) \setminus V(Q)} \frac{1}{d_P(v)}
\]

\[
\geq \frac{|E_P(V(Q),V(P) \setminus V(Q))|}{\Delta(P)}
\]

\[
\geq h(P) \min\{|V(Q)|,|V(P)| - |V(Q)|\}
\]

\[
\geq h(P)|V(P)|/3\Delta(P).
\]

Completing the proof, it follows that \( \kappa_{\text{col}}(P) \geq \kappa_{1,\lambda}(P) \geq h(P)|V(P)|/3\Delta(P) \). \( \square \)

1.5 Minor-Monotonicity and Monotone Projections

In this section, we prove that \( \kappa_{\text{col}}(P) \) and \( C_{\text{col}}(P) \) are minor-monotone graph parameters. First, a few definitions.

Recall that a minor of \( G \) is any graph that can be obtained from \( G \) by a sequence of vertex deletions, edge deletions, and edge contractions. A real-valued graph parameter \( f \) is minor-monotone if \( f(G) \leq f(G') \) whenever \( G \) is a minor of \( G' \).
For every $P$ and $\alpha : V(P) \to [0, 1]$, let $G_{P,\alpha}(n)$ be the class of $P$-colored graphs with vertex set $V_{P,\alpha}(n) := \{(v, i) : v \in V(P), 1 \leq i \leq \kappa^\alpha(v)\}$ and the obvious vertex-coloring $\chi : (v, i) \mapsto v$. Let $E_{P,\alpha}(n) := \{(v, i), (w, j)\} \in \{V_{\alpha,\beta}(n) : \{v, w\} \in E(P)\}$ be the set of possible edges.

**Lemma 1.5.1.** Suppose $P$ is a minor of $P'$. Then

1. for every $(\alpha, \beta) \in \theta_{\text{col}}(P)$, there exists $(\alpha', \beta') \in \theta_{\text{col}}(P')$ such that $\kappa_{\alpha,\beta}(P) = \kappa_{\alpha',\beta'}(P')$,

2. for every $\alpha : V(P) \to [0, 1]$, there exists $\alpha' : V(P') \to [0, 1]$ such that $(\text{SUBGRAPH}_{col}(P) \upharpoonright G_{P,\alpha}) \leq_{\text{mp}} (\text{SUBGRAPH}_{col}(P') \upharpoonright G_{P',\alpha'})$.

As an immediate corollary:

**Corollary 1.5.2.** $\kappa_{\text{col}}(P)$ and $C_{\text{col}}(P)$ are minor-monotone.

**Proof of Lemma 1.5.1.** It suffices to consider two cases: $P$ is a subgraph of $P'$, or $P$ is obtained from $P'$ by a single edge contraction. First, suppose $P$ is a subgraph of $P'$.

For (1): Consider any $(\alpha, \beta) \in \theta_{\text{col}}(P)$. Define $\alpha' : V(P') \to [0, 1]$ and $\beta' : E(P') \to [0, 2]$ by

$$
\alpha'(v) := \begin{cases} 
\alpha(v) & \text{if } v \in V(P), \\
0 & \text{otherwise},
\end{cases} \quad \beta'(e) := \begin{cases} 
\beta(e) & \text{if } e \in E(P), \\
0 & \text{otherwise}.
\end{cases}
$$

It is easy to check that $(\alpha', \beta') \in \theta_{\text{col}}(P')$ and $\kappa_{\alpha,\beta}(P) = \kappa_{\alpha',\beta'}(P')$.

For (2): For consider any $\alpha : V(P) \to [0, 1]$. Define $\alpha'$ be as above. Viewing $\text{SUBGRAPH}_{col}(P) \upharpoonright G_{P,\alpha}$ as a boolean function $\{0, 1\}^{E_{P,\alpha}}$ (and similarly $\text{SUBGRAPH}_{col}(P') \upharpoonright G_{P',\alpha'}$), define $p : E_{P',\alpha'} \to E_{P,\alpha} \cup \{0, 1\}$ by

$$
p([\{v, i\}, (w, j)\]) := \begin{cases} 
\{\{v, i\}, (w, j)\} & \text{if } \{v, w\} \in E(P), \\
1 & \text{otherwise}.
\end{cases}
$$

This $p$ witnesses $(\text{SUBGRAPH}_{col}(P) \upharpoonright G_{P,\alpha}) \leq_{\text{mp}} (\text{SUBGRAPH}_{col}(P') \upharpoonright G_{P',\alpha'})$.

We now consider the case that $P$ is obtained from $P'$ by contracting a single edge. That is, $P = P' \setminus \{x, y\}$ for some $\{x, y\} \in E(P')$. Let $z$ label the contracted vertex in $P$ (so that $V(P') \setminus V(P) = \{z\}$ and $V(P') \setminus V(P) = \{x, y\}$).

For (1): Consider any $(\alpha, \beta) \in \theta_{\text{col}}(P)$. Define $\alpha' : V(P') \to [0, 1]$ and $\beta' : E(P') \to [0, 2]$ by

$$
\alpha'(v) := \begin{cases} 
\alpha(z) & \text{if } v \in \{x, y\}, \\
\alpha(v) & \text{otherwise},
\end{cases} \quad \beta'(e) := \begin{cases} 
\alpha(z) & \text{if } e = \{x, y\}, \\
\beta(\{z, u\}) & \text{if } e \notin \{x, y\} = \{u\} \text{ for some } u \in V(P), \\
\beta(e) & \text{otherwise}.
\end{cases}
$$
Once again, it is easy to check that $(\alpha', \beta') \in \theta_{col}(P')$ and $\kappa_{\alpha', \beta}(P) = \kappa_{\alpha', \beta}(P')$.

For (2): Consider any $\alpha : V(P) \to [0, 1]$. Again define $\alpha' : V(P') \to [0, 1]$ as above. Let $q : V(P') \to V(P)$ map $x, y$ to $z$ and fix all other vertices. Define $p : E_{P', \alpha'} \to E_{P, \alpha} \cup \{0, 1\}$ by

$$p([(v, i), (w, j)]) := \begin{cases} 1 & \text{if } \{v, w\} = \{x, y\} \text{ and } i = j, \\ 0 & \text{if } \{v, w\} = \{x, y\} \text{ and } i \neq j, \\ \{q(v), i\}, (q(w), j) & \text{otherwise.} \end{cases}$$

This $p$ witnesses $(\text{Subgraph}_{col}(P) \mid G_{P, \alpha}) \leq_{mp} (\text{Subgraph}_{col}(P') \mid G_{P', \alpha'})$.

\subsection{Negative Results in the Uncolored Setting}

In the proof of Corollary 1.5.2, we proved that $C_{col}(P)$ is minor monotone by monotone projection reduction. (In principle, any $AC^0$ reduction works.) We doubt $C(P)$ is not minor monotone. Although we are not able to prove it, we can prove that under the restriction only monotone projection is allowed.

Now, we will prove there does not exist monotone projection that reduces detecting $M_3$ in an $n$-vertex graph to detecting $P_3 + M_2$ in an $N$-vertex graph, no matter how large $N$ is. Before proving the theorem, we need a few lemmas and claims.

\textbf{Lemma 1.5.3.} Every $P_3 + M_2$-free graph $G$ satisfies one of the following conditions:

1. $G$ has $\leq C$ edges for some absolute constant $C$,
2. $G$ is a matching,
3. $G$ has exactly two vertices of degree $\geq 6$, in which case $G$ is a union of two stars,
4. $G$ has a unique vertex of degree $\geq 6$, and moreover $G$ is the union of a star and a subgraph of $K_3$ or $S_5$ (the star of degree 5).

\textbf{Proof.} For $S \subseteq [N]$, let $D_S(G)$ be the number of vertices in $G$ with degree in $S$. Three simple claims:

- If $D_{\geq 6}(G) \geq 3$, then $G$ contains a $P_3 + M_2$-subgraph.\(^4\)
- There is a constant $C'$ such that if $D_{\geq 6}(G) = 0$ and $D_{\{2,3,4,5\}}(G) \geq C'$, then $G$ contains $P_3 + M_2$-subgraph.\(^5\)

\(^4\)Let $a, b, c$ be distinct vertices of degree $\geq 6$. There exist $v, w \in N_a \setminus \{b, c\}$ (where $N_a$ is the neighbor set of $a$ in $G$), and $x \in N_b \setminus \{a, c, u, v\}$ and $y \in N_c \setminus \{a, b, u, v, x\}$. Then $a, b, c, u, v, x, y$ are the vertices of a $P_3 + M_2$-subgraph of $G$.

\(^5\)If $C'$ is large enough, then there are vertices $a, b, c \in V(G)$ with $2 \leq d(a), d(b), d(c) \leq 5$ such that $a, b, c$ have distance $\geq 2$ in $G$. Pick any edges $e, f$ adjacent to $a$; $g$ adjacent to $b$ and $h$ adjacent to $c$. Then $e, f, g, h$ is a $P_3 + M_2$-subgraph.
CHAPTER 1. SUBGRAPH ISOMORPHISM PROBLEM

- There is a constant $C''$ such that if $D_{\geq 6}(G) = 0$ and $D_{\geq 2}(G) \geq 1$ and $D_1(G) \geq C''$, then $G$ contains a $P_3 + M_2$-subgraph.\(^6\)

It follows that, if $G$ is $P_3 + M_2$-free, then one of the following holds:

- $D_{\geq 2}(G) = 0$ (i.e. $G$ is a matching),
- $D_{\geq 6}(G) = 0$ and $1 \leq D_{\{2,3,4,5\}}(G) < C''$ and $D_1(G) < C''$ (in which case $G$ has $< 5C' + C''$ edges),
- $D_{\geq 6}(G) = 1$, or
- $D_{\geq 6}(G) = 2$.

If $G$ has exactly 2 vertices $v, w$ of degree $\geq 6$, then $G$ is a union of two stars. (If $G$ has an addition edge $e$ non-adjacent to $v$ and $w$, then we get a $P_3 + M_2$-subgraph.)

Finally, suppose $G$ has exactly one vertex $v$ of degree $\geq 6$. Let $G' = G - v$ (i.e. $G$ minus $v$ and all edges adjacent to $v$). Then $G'$ does not contain an $M_3$-subgraph (otherwise, $G$ would have a $P_3 + M_2$-subgraph). Therefore, $G'$ is either a star of degree $\leq 5$ or $K_3$. It follows that $G$ satisfies (a), (b), (c) or (d).

\begin{claim}
If $G$ is $P_3 + M_2$-free and $G$ contains a matching of size at least 4, then $G$ is a matching.
\end{claim}

\begin{lemma}
If $G$ contains a vertex $v$ of degree $\geq 6$, and $G$ contains a $P_3 + M_2$-subgraph, then $G$ contains a $P_3 + M_2$-subgraph in which $v$ is the degree-2 vertex.
\end{lemma}

\begin{proof}
Since $G$ contains $P_3 + M_2$-subgraph subgraph, then $G - v$ contains $M_2$, and then the conclusion follows.
\end{proof}

\begin{theorem}
The $M_3$-subgraph problem is not a monotone projection of the $P_3 + M_2$-subgraph problem.
\end{theorem}

\begin{proof}
For contradiction, let $n, N \in \naturals$ where $n \geq C + 2$ and assume $p : \binom{[n]}{2} \rightarrow \binom{[n]}{2} \cup \{0, 1\}$ is a monotone projection such that, for every graph $G$ with $V(G) \subseteq \naturals$,

$G$ contains an $M_3$-subgraph $\iff p^*(G)$ contains a $P_3 + M_2$-subgraph.

As before, $p^*(G)$ denotes the graph with edge set $p^{-1}(E(G) \cup \{1\})$.

The following claim simply says that the reduction essentially depends on all variables, which is clear.

\begin{claim}
$|p^{-1}(e)| \geq 1$ for all $e \in \binom{[n]}{2}$.
\end{claim}

\(^6\)Let $a$ be a vertex with degree $2 \leq d(a) \leq 5$. If $D_1(G)$ is large enough, then there exist vertices $b, c$ with $d(b) = d(c) = 1$ such that $a, b, c$ have distance $\geq 2$ in $G$. Let $e, f, g, h$ as before; this is a $P_3 + M_2$-subgraph.
Proof. For contradiction, assume that $p^{-1}(e)$ is empty for some $e \in [\binom{n}{2}]$. Let $f, g \in [\binom{n}{2}]$ be edges such that $e, f, g$ are vertex-disjoint. Then $p^*(\{e, f, g\}) = p^*\{\{f, g\}\}$, yet only $\{e, f, g\}$ contains an $M_3$-subgraph. Contradiction.

For $a \in [n]$, let $S_a$ be the $n$-vertex star centered at $a$ (i.e., $S_a$ is the graph with edge set $\{e \in \binom{[n]}{2} : a \in e\}$). Let $F_a := p^{-1}(S_a)$ (i.e., $F_a$ is the graph with edge set $p^{-1}(E(S_a))$). Since $S_a$ is $M_3$-free, $p^*(S_a) \supseteq F_a$ is $P_3 + M_2$-free. By Claim 1.5.7, $F_a$ has $\geq C + 1$ edges (since $n \geq C + 2$). By Lemma 1.5.3, $F_a$ satisfies (b), (c) or (d). The next two claims eliminate cases (b) and (c).

Claim 1.5.8. For all $a \in [n]$, $F_a$ is not a matching.

Proof. For contradiction, assume that $F_a$ is a matching for some $a \in [n]$. Then $F_a \cup F_b$ is a matching for all $a \neq b \in [n]$ (by Claim 1.5.4, since $S_a \cup S_b$ is $M_3$-free and $p^{-1}(S_a \cup S_b)$ contains a sufficiently large matching). It follows that $p^{-1}(K_n)$ is a matching, where $K_n$ is the complete graph on vertex set $[n]$.

Since $K_n$ contains an $M_3$-subgraph, $p^*(K_n) = p^{-1}(K_n) \cup p^{-1}(1)$ contains a $P_3 + M_2$-subgraph. It follows that either $p^{-1}(1)$ contains a path of length 2, or $p^{-1}(1)$ contains an edge $e$ which has an endpoint in $V(p^{-1}(K_n))$. In both cases we get a contradiction, as it follows that $p^*(S_b)$ contains a $P_3 + M_2$-subgraph for some $b \in [n]$. If $p^{-1}(1)$ contains a $P_3$-subgraph, then any $b \in [n]$ will do; if $p^{-1}(1)$ contains an edge $e$ with an endpoint $v \in V(p^{-1}(K_n))$, then any $b \in [n]$ with $v \in V(F_b)$ will do.)

Claim 1.5.9. For all $a \in [n]$, $F_a$ contains a unique vertex of degree $\geq 6$.

Proof. It follows from Lemma 1.5.3 and Claims 1.5.7 and 1.5.9 that $D_{\geq 6}(F_a) \geq 1$ for all $a \in [n]$. For contradiction, assume $F_a$ contains distinct vertices $v \neq w \in [N]$ of degree $\geq 6$. Let $K_{v-a}$ be the complete graph supported on $[n] \setminus \{a\}$. Note that $\{v, w\}$ cannot be a vertex cover of $p^*(K_{v-a})$ (since $p^*(K_{v-a})$ contains a $P_3 + M_2$-subgraph). Therefore, there exists $e \in \binom{[n]}{2}$ such that $p^*(e)$ contains an edge $\{x, y\} \in \binom{[n]}{2}$ with $\{x, y\} \cap \{v, w\} = \emptyset$.

Since $v$ has degree $\geq 6$, there exist $u_1 \neq u_2 \in N_v \setminus \{w, x, y\}$ (where $N_v$ is the neighbor set of $v$ in $F_a$). Since $w$ has degree $\geq 6$, there exists $z \in N_w \setminus \{v, x, y, u_1, u_2\}$. Note that $\{v, w, x, y, z, u_1, u_2\} \subseteq p^*(S_a \cup e)$ is a $P_3 + M_2$-subgraph. However, $S_a \cup e$ contains no $M_3$-subgraph. Contradiction.

Let $z : [n] \to [N]$ be the function which maps $a \in [n]$ to the unique vertex of degree $\geq 6$ in $F_a$.

Claim 1.5.10. $|z^{-1}(v)| \leq 2$ for all $v \in [N]$.

Proof. For contradiction, assume that there exist distinct $a, b, c \in [n]$ such that $v := z(a) = z(b) = z(c)$. By Lemma 1.5.5, $p^*(S_a \cup S_b \cup S_c)$ contains a $P_3 + M_2$-subgraph in which $v$ is the degree-2 vertex. Let $e, f \in \binom{[n]}{2}$ be the two edges in this subgraph which are not adjacent to $v$. Without loss of generality, $\{e, f\} \subseteq p^*(S_a \cup S_b)$. It follows that $p^*(S_a \cup S_b)$ contains a $P_3 + M_2$-subgraph
(since \( v \) has degree \( \geq 6 \) in \( p^*(S_a \cup S_b) \), we can find a different path of length 2 through \( v \) which is vertex-disjoint from edges \( e \) and \( f \)). Contradiction.

It follows from Claim 1.5.10, that \(|\text{Range}(z)| \geq n/2 > 3\) (as \( C \) is much larger than 6).

**Claim 1.5.11.** \( z \) is 1-to-1 (i.e. \(|z^{-1}(v)| \leq 1\) for all \( v \in [N] \)).

**Proof.** For contradiction, assume \( v := z(a) = z(b) \) for some \( a \neq b \in [n] \). Note that \( F_a \) is not a star. (If \( F_a \) were a star, we get a contradiction as follows: fix \( c \in [n] \setminus \{a, b\} \); \( p^*(S_a \cup S_b \cup S_c) \) contains \( P_3 + M_2 \)-subgraph; it follows that \( p^*(S_b \cup S_c) \) contains a \( P_3 + M_2 \)-subgraph, by replacing edges in \( F_a \) with edges in \( F_b \).) Since \( F_a \) is a not a star, there exists \( e \in E(F_a) \) such that \( v \notin e \). Since \(|\text{Range}(z)| \geq 4\), there exists \( c \in [n] \) such that \( z(c) \notin \{v\} \cup e \). Note that \( p^*(S_a \cup S_c) \) contains a \( P_3 + M_2 \)-subgraph. Contradiction.

**Claim 1.5.12.** For all \( a \in [n] \), \( F_a \) is a star of degree \( \leq n - 1 \).

**Proof.** First, assume \( F_a \) is not a star. Let \( e \in E(F_a) \) be such that \( z(a) \notin e \), \( b \in [n] \setminus \{a\} \) and \( z(b) \notin e \). Then \( p^*(S_a \cup S_b) \) contains a \( P_3 + M_2 \)-subgraph. Contradiction.

Second, assume \( F_a \) is a star of degree \( \geq n \). Then there exists an edge \( e \in \binom{[n]}{2} \) with \( a \in e \) and \(|p^{-1}(e)| \geq 2\). Let \( b \) be the other endpoint of \( e \). Note that \( F_b \) is not a star, which gives a contradiction (by the previous paragraph).

Claims 1.5.7 and 1.5.12 establish that \(|p^{-1}(e)| = 1\) for all \( e \in \binom{[n]}{2} \).

**Claim 1.5.13.** \( p^{-1}(1) \) is nonempty.

**Proof.** Assume \( p^{-1}(1) \) is empty. Let \( G \) be any \( M_3 \)-subgraph of \( K_n \) (with exactly 3 edges). Then \( p^*(G) \) has 3 edges, hence contains no \( P_3 + M_2 \)-subgraph. Contradiction.

Now fix any \( e \in p^{-1}(1) \) and any \( a \neq b \in [n] \) such that \( z(a), z(b) \notin e \). We get a final contradiction, as \( p^*(S_a \cup S_b) \) contains a \( P_3 + M_2 \)-subgraph. This completes the proof of Theorem 1.1.2.

**1.6 Conclusion**

The main open problem is to get a better understanding of \( C(P) \). Is \( C(P) \) lower bounded by any nontrivial function of \( tw(P) \)? Is \( C(P) \) minor-monotone?
Chapter 2

Immunity of MOD Function

2.1 Introduction

A fundamental task in computer science is to take simple functions like $OR$, $MAJ$, $MOD_q$, etc. and determine how difficult it is to represent them as polynomials over a field $F_p$. Usually for such questions, it is easy to determine the degree required to exactly represent such a function, but when we ask a variant such as how hard it is to compute an approximation in low degree it can become quite difficult to get tight results. We were led to the following question by way of proof complexity and circuit complexity (for example, [3] proved general hardness criterion for Polynomial Calculus based on immunity).

**Question 1.** What is the smallest degree of a nonzero polynomial in the ideal generated by $MOD_q$ or $\neg MOD_q$ in the polynomial ring $F_p[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n)$?

There are several definitions of the same concept. In [3], this value is called the *immunity* of the $MOD_q$ function, where the immunity of Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ over some field $F$ is the minimal degree of some nonzero function in the ideal $\langle f \rangle$, where $f$ here is viewed as a polynomial in the ring $F[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n)$. It is also known in the literature as the *weak p-degree* [18] of Boolean function $f$, and can alternately be defined as the smallest degree of a nontrivial polynomial $g \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$\forall x \in \{0,1\}^n, f(x) = 0 \Rightarrow g(x) \equiv 0 \pmod{p} .$$

Immunity can also be thought of as measuring how expensive it is to compute a function with unbounded one-sided error on 1 by polynomial.

In cryptography community, *algebraic immunity* of a Boolean function $f$ is defined to be the smaller one between immunity of $f$ and immunity of $1-f$ over $F_2$. In this chapter, we will call it “two-sided immunity” to differentiate with the (one-sided) immunity. In cryptography, two-sided immunity is a criterion of the security of Boolean functions used in stream cipher system [11].
For purpose of our current research, we hoped for a tight lower bound of the immunity of functions \( \text{MOD}_q \) and \( \neg \text{MOD}_q \). However, with not much trouble we were able to show an improved lower bound \( n/2 \) of \( \text{MOD}_q \) function, which relies only on the kind of analysis that appears in Razborov-Smolensky. The lower bound \( n/2 \) of \( \text{MOD}_q \) turns out to be tight when \( n \) is a multiple of \( 2q \). For \( \neg \text{MOD}_q \), we prove an exact result of immunity over \( \mathbb{F}_p \), which is \( \lfloor (n + q - 1)/q \rfloor \) (independent of \( p \)), based a symmetrization technique, which was used by Feng and Liu [25] in the case of Boolean functions.

Our result improves Green’s lower bound \( \lfloor n/2(n+1) \rfloor \) [18], which uses complex Fourier technique. Green’s lower bound improves the results of Barrington, Beigel and Rudich [6] and Tsai [38], which proved \( \Omega(n) \) lower bound of a weaker version (that is, polynomial \( g(x) \) has to be nonzero if \( f(x) = 1 \)) for slow growing \( p \).

2.2 Preliminaries

2.2.1 Composite Modulus

For the proof complexity and circuit complexity application we had in mind, we only actually care about prime characteristic. However, it is natural to try to generalize the improvement to composite characteristic as well. In fact, we can use a trick similar to what Green did, and reduce the composite case to the prime case. For extra clarity, we adopt the language which appears in his paper [18].

**Lemma 2.2.1.** The weak mod-\( m \) degree of any Boolean function \( f \) equals the minimum of weak mod-\( p \) degree of \( f \), where \( p \) ranges all prime factors of \( m \).

**Proof.** One direction is easy, that is, the weak mod-\( m \) degree is not greater than the minimum of the weak mod-\( p \) degree. Suppose the minimum weak mod-\( p \) degree of \( f \), where \( p \) ranges all prime factors of \( m \), is \( d \). That is, there exists a nonzero (multilinear) polynomial \( g \in \mathbb{Z}[x_1, \ldots, x_n] \) of degree \( d \) such that

\[
f(x) = 0 \Rightarrow g(x) \equiv 0 \pmod{m}, \forall x.
\]

Then, we claim that \( m/pg(x) \) weakly represent \( f \) mod-\( m \). Because for all \( x \) with \( f(x) = 0 \), \( g(x) \equiv 0 \pmod{p} \) implies \( m/pg(x) \equiv 0 \pmod{m} \). And \( m/pg(x) \pmod{m} \) is nonzero because there exists \( x \in \{0, 1\}^n \) such that \( g(x) \not\equiv 0 \pmod{p} \), which implies \( m/pg(x) \not\equiv 0 \pmod{m} \).

For the other direction, we need to show the weak mod-\( m \) degree of \( f \) is not less than the minimum of the weak mod-\( p \) degree. Suppose \( g \in \mathbb{Z}[x_1, \ldots, x_n] \) is some multilinear polynomial weakly represent \( f \) with minimum degree \( d \). We shall prove that there exists some \( g' \in \mathbb{Z}[x_1, \ldots, x_n] \) weakly represent \( f \) mod \( p \) with degree \( \leq d \).

Let \( x \) be any input such that \( g(x) \) is nonzero modulo \( m \). By the Chinese Remainder Theorem, for some maximal prime power \( q \) of \( m \), \( g(x) \) is nonzero modulo \( q \), so \( g \) is a nonzero polynomial modulo \( q \).
2.2. PRELIMINARIES

Now suppose that $q = p^e$. If $g$ is a nonzero polynomial modulo $p$ as well, then we are done by letting $g' = g$. If $g$ as a function is zero modulo $p$ but not modulo $q$, then it is easy to see that every coefficient of $f$ must be zero modulo $p$; if not, take a monomial $S$ such that for every $T \subseteq S$, the coefficient of $T$ is zero, then the input such that $x_i = 1$ iff $i \in S$ must have nonzero value modulo $p$. Thus, if $g$ is zero as a function modulo $p$, but not modulo $q$, its coefficients are all divisible by $p$, and the integer polynomial $g/p$ is nonzero modulo $q/p$. By iterating this, eventually we obtain a divisor $g'$ of $g$ which is nonzero modulo $p$, and hence $g'$ has degree not greater than that of $g$.

2.2.2 Symmetrization

One key ingredient of our improved lower bound for $\neg \chi_q$ is the fact that we can symmetrize any function in a symmetric ideal, where symmetric ideal is an ideal generated by a symmetric function. If the characteristic of the field is zero, this is trivial, for we can summing over all permutations of some given function to obtain a symmetric one with algebraic degree non-increasing. When working over finite field, this averaging technique does not work because we may get a zero function.

However, we could still symmetrize an annihilator to some simple form, as the following lemma says. The following lemma is proved by Feng and Liu in the case of Boolean functions, that is, $F = F_2$ [25]. For the ring $F[x_1, \ldots, x_n]/(x_i^2 = x_i, x_i^2 = x_n)$, the proof is almost the same. The idea is to symmetrize step by step in order to avoid getting a zero function in contrast to summing over all permutations in the case of characteristic zero.

**Lemma 2.2.2.** If $f \in F[x_1, \ldots, x_n]/(x_i^2 = x_1, \ldots, x_n^2 = x_n)$ is a symmetric function, there is a lowest degree $g$ in $\langle f \rangle$ of the following form

\[
(2.1) \quad g = g' \prod_{i=1}^{n}(x_{2i-1} - x_{2i}),
\]

where $g'$ is a symmetric function on variables $x_{2i+1}, \ldots, x_n$.

**Proof.** Prove by construction. Let $g$ be a function in $\langle f \rangle$ with lowest degree. If $g$ is symmetric, then we are done. Thus assume $g$ is not symmetric. Since the symmetric group $S_n$ is generated by all transpositions $(i, j), 1 \leq i < j \leq n$, the assumption that $g$ is not symmetric implies there exists some transposition $\pi = (i, j)$ such that $\pi(g) \neq g$. Let

\[
g' = g - \pi(g) \neq 0.
\]

In fact, $g' = (x_i - x_j)h$, where $h$ is a symmetric function on $\{x_1, \ldots, x_n\} \setminus \{x_i, x_j\}$. To see this, write $g = g_0 + g_1x_i + g_2x_j + g_3x_ix_j$, where $g_0, g_1, g_2, g_3$ are functions on $\{x_1, \ldots, x_n\} \setminus \{x_i, x_j\}$. And thus $\pi(g) = g_0 + g_1x_j + g_2x_i + g_3x_ix_j$, which implies

\[
g - \pi(g) = (x_i - x_j)(g_1 - g_2)
\]
Repeat this procedure on \( h = g_1 - g_2 \) until one gets a symmetric function. Finally, we find a function \( g \) in ideal \( \langle f \rangle \) with the following form

\[
g = g' \prod_{i=1}^{\ell} (x_{t_{2i-1}} - x_{t_{2i}}),
\]

indexes \( t_1, t_2, \ldots, t_{2\ell} \) can take \( 1, 2, \ldots, 2\ell \) because we could apply a permutation \( \pi \) to \( g \) which sends \( t_i \) to \( i \), which is in the ideal \( \langle \pi(f) \rangle = \langle f \rangle \) for \( f \) is invariant under all permutations.

The above lemma has the following consequence. In order to lower bound the degree of nonzero functions in some symmetric ideal \( \langle f \rangle \) in \( R \), we only need to consider all functions of the form \( g = g' \prod_{i=1}^{n} (x_{2i-1} - x_{2i}) \), where \( g' \) is symmetric on variables \( x_{2\ell+1}, \ldots, x_n \). The fact that \( f(x) = 0 \Leftrightarrow g(x) = g' \prod_{i=1}^{n} (x_{2i-1} - x_{2i}) = 0 \) is equivalent to \( f|_{\rho}(x) = 0 \Leftrightarrow g'(x) = 0 \) where \( \rho \) is the restriction setting \( x_1 = x_2 = \ldots = x_{2\ell-1} = 0 \) and \( x_2 = x_4 = \ldots = x_{2\ell} = 1 \), that is, \( g' \) is in the ideal \( \langle f|_{\rho} \rangle \). Therefore, we have the following corollary.

**Corollary 2.2.3.** Let \( f \in F[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n) \) be a symmetric function. The lowest degree of a nonzero function in \( \langle f \rangle \) equals the minimum degree of \( \deg(g) + \ell \), where \( g \in \langle f|_{\rho} \rangle \) and \( \rho \) ranges over all restrictions setting \( x_1 = x_2 = \ldots = x_{2\ell-1} = 0 \) and \( x_2 = x_4 = \ldots = x_{2\ell} = 1 \), \( 0 \leq \ell \leq n/2 \).

### 2.3 Lower Bound for \( \text{MOD}_q \)

Consider the following quotient of the polynomial ring, \( R := F_p[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n) \), sometimes called the Razborov-Smolensky ring. Each element of \( R \) has a unique multilinear polynomial representative, and generally we identify an element of \( R \) with this representative. Each polynomial also determines a map from \( \{0, 1\}^n \to F_p \) by evaluation, and in fact this induces an isomorphism of \( F_p \)-algebras between \( R \) and the algebra of functions \( \{0, 1\}^n \to F_p \). So we also will often identify an element of \( R \) with function it computes on boolean inputs.

Sometimes authors define the \( \text{MOD}_q \) function slightly differently in different contexts, and here we will focus on this one first:

**Definition 2.3.1.** Let \( \chi_q \) denote the element of \( R \) defined by

\[
\chi_q(x_1, \ldots, x_n) := \begin{cases} 
1 & \text{if } q \text{ divides } |x| \\
0 & \text{otherwise}
\end{cases}
\]

Then, by definition, the immunity/weak \( p \)-degree of \( \chi_q \) is the smallest degree of a nontrivial element of the ideal generated by \( \chi_q \) in \( R \).

**Observation 2.3.2.** \( f \in \langle \chi_q \rangle \) iff \( f = f \cdot \chi_q \).

**Proof.** By definition, \( f \in \langle \chi_q \rangle \) if \( f = g \cdot \chi_q \) for some \( g \), so \( (\rightarrow) \) holds. Now lets do \( (\rightarrow) \). Since \( \chi_q \) is zero-one valued, \( \chi_q^2 = \chi_q \), so \( f \cdot \chi_q = g \cdot \chi_q^2 = g \cdot \chi_q = f \), so \( (\rightarrow) \) holds as well. \( \square \)
Following the general Razborov-Smolensky methodology, let $\omega$ denote a primitive $q$th root of unity found in some large enough extension field of $F_p$ (if $F_p$ did not already contain $\omega$, observe that $\langle \chi_q \rangle$ contains only more polynomials when we work over a larger field). Note that this does not require that $q$ be a prime. Define new variables $y_i := 1 + (\omega - 1)x_i$. Then the $y_i$ are elements of $R$, but also $x_i$ is determined by $y_i$ so if we like for any function $f(x) \in R$, we can think of it as a function $f(y) : \{1, \omega\}^n \to F_p$. Of course it has a unique multilinear representation in the variables $y_i$ as well. While the coefficients might look different, its degree in this representation must be the same, because the degree of a polynomial cannot increase under a linear transformation of the variables, and our linear transformation is invertible.

We will also introduce variables $y'_i := 1 + (\omega^{-1} - 1)x_i$, and by the same reasoning, we know that for any $f \in R$, its degree as represented in the $x_i, y_i$, or $y'_i$ is the same. Note also that $y_i \cdot y'_i = 1$ as elements of $R$.

**Observation 2.3.3.** $f \in \langle \chi_q \rangle$ iff $f = f \cdot \prod_i y'_i$.

**Proof.** Think of $\prod_i y'_i$ as a function in the $x$-variables. Because $\omega$ is a $q$th root of unity, $\prod_i y'_i \neq 1$ if and only if $\chi_q = 0$. Thus, $\chi_q \cdot (\prod_i y'_i - 1) = 0$. Therefore, for any $f \in \langle \chi_q \rangle$,

$$f \cdot \left(\prod_i y'_i - 1\right) = f \cdot \chi_q \cdot \left(\prod_i y'_i - 1\right) = 0,$$

so $f \cdot \prod_i y'_i = f$. \hfill \square

Now we use this to prove the main result.

**Theorem 2.3.4.** If $f \in \langle \chi_q \rangle$, then $f = 0$ or $f$ has degree $\geq n/2$.

**Proof.** Suppose not. Consider $f$’s representation as a polynomial in the $y_i$,

$$f = \sum_S c_S \prod_{i \in S} y_i.$$

For any monomial $S$, we have that

$$\prod_{i \in S} y_i \cdot \prod_{i \in S} y'_i = \prod_{i \in S} y'_i.$$

Since $f = f \cdot \prod_i y'_i$, we deduce that $f$’s representation as a $y'_i$ polynomial is

$$f = \sum_S c_S \prod_{i \in S} y'_i.$$

If the polynomial $f(y)$ is nonzero and has degree less than $n/2$, then this polynomial representation of $f(y')$ has at least one nonzero monomial of degree strictly larger than $n/2$, and so has degree greater than $n/2$. But this is a contradiction, since as we saw before, the degree of the polynomials $f(y)$ and $f(y')$ must be the same, as they are linear transformations of one another. \hfill \square
CHAPTER 2. IMMUNITY OF MOD FUNCTION

Note that nowhere did we assume that \( q \) was not composite, only that it is coprime with \( p \), which is sufficient to find a \( q \)'th root of unity in a large enough extension of \( F_p \).

The idea in the above proof also can be used to show an upper bound of the immunity of \( \neg \chi_q \). Again, \( \omega \) is a \( q \)th root of unity, and \( y_i = (\omega - 1)x_i + 1 \) and \( y'_i = (\omega^{-1} - 1)x_i + 1 \), which is the inverse of \( y_i \). It’s easy to see that

\[
\prod_{i \leq n/2} y_i = \prod_{i > n/2} y'_i
\]

holds for all \( x \) with \( |x| \equiv 0 \) (mod \( q \)), since \( 1 = \prod_{i \leq n} y_i = \prod_{i \leq n/2} y_i (\prod_{i > n/2} y'_i)^{-1} \), which implies

\[
\prod_{i \leq n/2} y_i - \prod_{i > n/2} y'_i \in \langle \neg \chi_q \rangle.
\]

Thus, the immunity of \( \neg \chi_q \) is upper bounded by \( \lceil n/2 \rceil \).

The tightness of the lower bound \( n/2 \) is shown by the following example. Let \( n \) be even and \( n/2 \equiv 0 \) (mod \( q \)), and let

\[
g = \prod_{i=0}^{n/2} (x_{2i-1} - x_{2i}).
\]

It’s easy to see \( g \in \langle \chi_q \rangle \), because \( g(x) = 0 \) for all \( x \) with \( |x| \neq n/2 \), and thus, \( g(x) = 0 \) for all \( x \) with \( |x| \equiv 0 \) (mod \( q \)).

2.4 Lower Bound for \( \neg \text{MOD}_q \)

By Corollary 2.2.3, in order to prove symmetric \( f \) has immunity not less less than \( d \), it’s equivalent to prove any nonzero symmetric function in \( \langle f|_{\rho_i} \rangle \) has degree not less than \( d - i \), for \( i = 0, 1, \ldots, \min\{n/2, d\} \), where restriction \( \rho_i \) sets \( x_1, x_3, \ldots, x_{2i-1} \) to 1, and \( x_2, x_4, \ldots, x_{2i} \) to 0.

It’s easily checked that if the truth value table of symmetric function \( f \) is

\[
v_f = (v_f(0), v_f(1), \ldots, v_f(n)) \in F_2^{n+1},
\]

then the truth value table of \( f|_{\rho_i} \) is

\[
v_{f|_{\rho_i}} = (v_f(i), v_f(i+1), \ldots, v_f(n-i)) \in F_2^{n+1-2i}.
\]

Assume function \( g \) is a symmetric function in \( \langle f \rangle \) of degree less than \( d \), and we can write \( g = \sum_{i<d} c_i \sigma_i \), where \( \sigma_i \) is the elementary symmetric polynomial of degree \( i \). For convenience, we define function \( \psi_d : N \to F_2^d \) by

\[
\psi_d(i) = \left( \begin{array}{c} i \\ 0 \end{array} \right), \left( \begin{array}{c} i \\ 1 \end{array} \right), \ldots, \left( \begin{array}{c} i \\ d-1 \end{array} \right) \in F_2^{d},
\]
which is the evaluation $\sigma_0, \sigma_1, \ldots, \sigma_{d-1}$ at value $i$. The fact $g \in \langle f \rangle$ implies $g(w) = 0$ for all $w$ with $v_f(w) = 0$, that is

$$
\begin{pmatrix}
\psi_d(i_1) \\
\psi_d(i_2) \\
\vdots \\
\psi_d(i_k)
\end{pmatrix} = 
\begin{pmatrix}
e_0 \\
e_1 \\
\vdots \\
e_d
\end{pmatrix} = 0,
$$

where $v_f(i_1) = \ldots = v_f(i_k) = 0$. Therefore, $\langle \neg\chi_q \rangle$ has nonzero symmetric function of degree less than $d$ if and only if the rank of $\{\psi_d(w) : \chi_q(w) = 1\}$ is smaller than $d$. It turns out the rank of $\{\psi_d(w) : \chi_q(w) = 1\}$ is always full (equals the number of vectors).

The lower bound of immunity of $\neg\chi_q$ follows from the following lemma. We will present two proofs of the following lemma, and the first one is much simpler. However, we are reluctant to discard the second one since it has a byproduct as we will later see.

**Lemma 2.4.1.** Fix a prime $p$. Let integers $a \geq 0$ and $d > 0$, and $q$ is coprime to $p$. Vectors

$$
\psi_d(a), \psi_d(a + q), \ldots, \psi_d(a + (d - 1)q) \in F_p^d
$$

is a basis $F_p^d$.

**Proof.** It suffices to prove the determinant of $\psi_d(a), \psi_d(a + q), \ldots, \psi_d(a + (d - 1)q)$ is nonzero, which turns out to have a simple closed form.

For convenience, let $a_i = a + iq$.

$$
\det \begin{pmatrix}
\binom{a_0}{0} & \binom{a_1}{0} & \cdots & \binom{a_0}{d-1} \\
\binom{a_1}{0} & \binom{a_1}{1} & \cdots & \binom{a_1}{d-1} \\
\vdots & \vdots & \ddots & \vdots \\
\binom{a_{d-1}}{0} & \binom{a_{d-1}}{1} & \cdots & \binom{a_{d-1}}{d-1}
\end{pmatrix} = \frac{1}{\prod_{k=1}^{d-1} k!} \det \begin{pmatrix}
1 & a_0 & a_0(a_0 - 1) & \cdots & a_0(a_0 - 1)\cdots(a_0 - d + 1)
\vdots & a_1 & a_1(a_1 - 1) & \cdots & a_1(a_1 - 1)\cdots(a_1 - d + 1)
\vdots & \vdots & \ddots & \vdots
1 & a_{d-1} & a_{d-1}(a_{d-1} - 1) & \cdots & a_{d-1}(a_{d-1} - 1)\cdots(a_{d-1} - d + 1)
\end{pmatrix}
= \frac{1}{\prod_{k=1}^{d-1} k!} \det \begin{pmatrix}
1 & a_0 & a_0^2 & \cdots & a_0^{d-1}
\vdots & a_1 & a_1^2 & \cdots & a_1^{d-1}
\vdots & \vdots & \ddots & \vdots
1 & a_{d-1} & a_{d-1}^2 & \cdots & a_{d-1}^{d-1}
\end{pmatrix}
= \frac{\prod_{0 \leq i < j \leq d-1} (a_j - a_i)}{\prod_{k=1}^{d-1} k!}
= \frac{\prod_{0 \leq i < j \leq d-1} q(j - i)}{\prod_{k=1}^{d-1} k!}
= q^{d(d-1)/2},
$$
which is nonzero for $q$ is coprime to $p$. In the above calculation, the first step is by the definition of binomial coefficients; the second step is by adding column $i$ to column $i+1$ for $i=1,2,\ldots,d-1$; and the third step is by Vandermonde determinant formula.

Now we can calculate the immunity of $\neg \chi_q$, which is defined to be the minimal degree of a nonzero function in the ideal $\langle \neg \chi_q \rangle$.

**Theorem 2.4.2.** Let $p$ be a prime, and $q \geq 2$ an integer coprime to $p$. The immunity of $\neg \chi_q$ over $F_p$ is $\lfloor \frac{n+q-1}{q} \rfloor$, which is independent of $p$.

**Proof.** By Lemma 2.4.1, the minimal degree of nonzero symmetric function in $\langle \neg \chi_q \rangle$ is the weight of $\chi_q$, which is $\lfloor \frac{n}{q} \rfloor + 1$; the minimal degree of nonzero symmetric function in $\langle \neg \chi_q |_{\rho_i} \rangle$ is the weight of $\chi_q |_{\rho_i}$, which is $\lfloor \frac{n-1}{q} \rfloor$; ...; the minimal degree of nonzero symmetric function in $\langle \neg \chi_q |_{\rho} \rangle$ is $\lfloor \frac{n+i-1}{q} \rfloor$.

Therefore, the immunity of of $\neg \chi_q$ is

$$\min \{ \lfloor \frac{n}{q} \rfloor + 1, \lfloor \frac{n-i}{q} \rfloor - \lfloor \frac{i-1}{q} \rfloor + i : i = 1, \ldots, \lfloor n/2 \rfloor \},$$

which is easy to check.

Now, let’s present the second proof Lemma 2.4.1 by proving a more general result about the rank of tensor product of matrices.

**Definition 2.4.3.** Call $A \in M_{n \times n}(F)$ strong nondegenerate matrix if for any $1 \leq t \leq n$ and $1 \leq i_1 < \ldots < i_t \leq n$, submatrix $M(i_1, \ldots, i_t; 1, \ldots, t)$ always has full rank $t$.

Call $A \in M_{n \times n}(F)$ weak nondegenerate matrix if for any $1 \leq t \leq n$ and any integer $a$, and any $q$ coprime to $n$, submatrix $M(a, a+q, \ldots, a+(t-1)q; 1, \ldots, t)$ always has full rank $t$, where the row indexes are computed mod the size of matrix $A$.

By the definition, a strong nondegenerate matrix is always weak nondegenerate. The following theorem says we can construct many weak nondegenerate matrices by taking tensors products of strong nondegenerate ones.

**Theorem 2.4.4.** The tensor product of strong nondegenerate matrices is weak nondegenerate.

**Proof.** Suppose $A_1, \ldots, A_m$ are strong nondegenerate matrices, and $q > 0$ is coprime to the size of each $A_i$. We need to prove matrix

$$(A_1 \otimes \cdots \otimes A_m)(a, a+q, \ldots, a+(d-1)q; 1, \ldots, d)$$

has full rank $d$. Let $\ell$ be the size of $B$, and let $A_1$ be $p \times p$ matrix, and thus $q$ is coprime to both $p$ and $\ell$. 

Prove by induction on \( m \). For the basis \( m = 1 \), the conclusion is trivial by the definition of nondegenerate matrix. Let’s assume it’s true for \( m - 1 \), and prove it for \( m \). Let \( B = A_2 \otimes \ldots \otimes A_m \). Recalling the definition of tensor product,

\[
A_1 \otimes B = \begin{pmatrix}
a_{11}B & a_{12}B & \ldots & a_{1p}B \\
a_{21}B & a_{22}B & \ldots & a_{2p}B \\
\vdots & \vdots & \ddots & \vdots \\
a_{p1}B & a_{p2}B & \ldots & a_{pp}B
\end{pmatrix}
\]

Let \( d = \lfloor d/\ell \rfloor \ell + d' \).

**Case 1:** \( d \leq \ell \). By the definition the non-degenerate matrix (Definition 2.4.3), \( a_{1i}, i = 1, \ldots, p \), are nonzero in the field \( F \). Thus,

\[
\langle A(a; 1, \ldots, d), A(a + q; 1, \ldots, d) \rangle = \langle B(a; 1, \ldots, d), B(a + q; 1, \ldots, d) \rangle,
\]

which has full rank by induction hypothesis on \( m - 1 \).

**Case 2:** \( d > \ell \) and \( d' = 0 \). Since \( q \) is coprime to \( p\ell \), \( d = \lfloor d/\ell \rfloor \ell \) numbers \( a, a + q, \ldots, a + (d - 1)q \) runs over \( \{0, 1, \ldots, \ell - 1\} \) for exactly \( t = d/\ell \) times, which implies for any \( j \in \{0, 1, \ldots, \ell - 1\} \), there exists \( t \) distinct numbers \( i_1, i_2, \ldots, i_t \in \{a, a + q, \ldots, a + (d - 1)q\} \) which is congruent to \( j \) mod \( \ell \).

For convenience, let \( B(i) \) denotes the \( i \)th row of \( B \), and let

\[
B^{(c)}(i) = (0, \ldots, 0) \oplus B(i) \oplus (0, \ldots, 0),
\]

where \( c = 1, \ldots, t \). Let \( F^d = S_1 \oplus \ldots \oplus S_t \), where \( S_i \) is the subspace of \( F^d \) of dimension \( \ell \), generated by \( e_{(i-1)\ell + 1}, \ldots, e_{i\ell} \).

By definition of tensor product (2.3),

\[
A(i; 1, \ldots, d) = a_{i1}B^{(1)}(j) + a_{i2}B^{(2)}(j) + \ldots + a_{ip}B^{(p)}(j)
\]

\[
A(i; 1, \ldots, d) = a_{i1}B^{(1)}(j) + a_{i2}B^{(2)}(j) + \ldots + a_{ip}B^{(p)}(j)
\]

\[
\ldots
\]

\[
A(i; 1, \ldots, d) = a_{i1}B^{(1)}(j) + a_{i2}B^{(2)}(j) + \ldots + a_{ip}B^{(p)}(j),
\]

where \( i'_k = \lfloor i_k/\ell \rfloor \). Since matrix \( A_1 \) is non-degenerate, the coefficient matrix \( (a_{i'k})_{i,k=1,\ldots,t} \) is invertible, which implies

\[
\langle B^{(1)}(j), \ldots, B^{(t)}(j) \rangle \subseteq \langle A(i; 1, \ldots, d), \ldots, A(i; 1, \ldots, d) \rangle
\]

\[
\subseteq \langle A(a; 1, \ldots, d), \ldots, A(a + (d - 1)q; 1, \ldots, d) \rangle
\]

Since \( j \in \{0, \ldots, \ell - 1\} \) is arbitrary, we have \( B^{(c)}(0), \ldots, B^{(c)}(\ell - 1), c = 1, \ldots, t \), is in the linear span of \( A(a; 1, \ldots, d), \ldots, A(a + (d - 1)q; 1, \ldots, d) \). By induction hypothesis, \( B^{(c)}(0), \ldots, B^{(c)}(\ell - 1) \) is a basis of subspace \( S_c \) of dimension \( \ell \) in \( F^d \); since \( F^d \) is the direct sum of \( S_1, \ldots, S_t \), we complete the proof of this case.
Case 3: \( d > \ell \) and \( d' > 0 \). Since \( q \) and \( pl \) are coprime, \( d - d' \) numbers \( a + d'q, \ldots, a + (d - 1)q \) runs over \( \{0, 1, \ldots, \ell - 1\} \) for exactly \( t = \lfloor d/\ell \rfloor \) times, and the extra \( d' \) numbers \( a, \ldots, a + (d' - 1)q \) numbers are distinct mod \( \ell \). This implies for any \( j \in \{a, \ldots, a + (d' - 1)q\} \), there exists \( t + 1 \) distinct numbers \( i_1, i_2, \ldots, i_t \in \{a, a + q, \ldots, a + (d - 1)q\} \) which is congruent to \( j \) mod \( \ell \).

Similar to Case 2, let \( B(i) \) denotes the \( i \)th row of \( B \), and let

\[
B^{(c)}(i) = (0, \ldots, 0) \oplus B(i) \oplus (0, \ldots, 0),
\]

where \( c = 1, \ldots, t \). However, for \( c = t + 1 \), let

\[
B^{(t+1)}(i) = (0, \ldots, 0) \oplus B(i; 1, \ldots, d').
\]

Again, by definition of tensor product (2.3),

\[
A(i; 1, \ldots, d) = a_{i'1}B^{(1)}(j) + a_{i'2}B^{(2)}(j) + \ldots + a_{i't+1}B^{(t+1)}(j)
\]

\[
A(i; 1, \ldots, d) = a_{i'1}B^{(1)}(j) + a_{i'2}B^{(2)}(j) + \ldots + a_{i't+1}B^{(t+1)}(j)
\]

\[
\ldots \ldots \ldots \ldots 
\]

\[
A(i; 1, \ldots, d) = a_{i't+1}B^{(t+1)}(j) + a_{i't+1}B^{(2)}(j) + \ldots + a_{i't+1}B^{(t+1)}(j),
\]

where \( i'_k = \lfloor i_k/\ell \rfloor \). Since matrix \( A_1 \) is non-degenerate, the coefficient matrix \( (a_{i'k,j})_{k=1,\ldots,t+1} \) is invertible, which implies

\[
\langle B^{(1)}(j), \ldots, B^{(t)}(j) \rangle \subseteq \langle A(i; 1, \ldots, d), \ldots, A(i; 1, \ldots, d) \rangle.
\]

Since \( j \in \{a, a + (d' - 1)q\} \) is arbitrary, we conclude \( B^{(t+1)}(a), \ldots, B^{(t+1)}(a + (d' - 1)q) \), is in the linear span of \( A(a; 1, \ldots, d), \ldots, A(a + (d - 1)q; 1, \ldots, d) \). By induction hypothesis, \( B^{(t+1)}(a), \ldots, B^{(t+1)}(a + (d' - 1)q) \) is a basis of \( S_{t+1} \). After mod out \( S_{t+1} \) from \( F^d \), and repeat the argument as in Case 2, the proof is complete. \( \square \)

Lemma 2.4.1 follows from the above theorem by taking \( A = {\binom{i}{j}}_{i,j=0,\ldots,p-1} \) and thus \( \psi_q(i) = (A \otimes A \otimes \cdots \otimes A)(i; 1, \ldots, d) \) by Lucas formula. The fact that \( A \) is a non-degenerate matrix can be shown by computing its determinant as in the proof of Lemma 2.4.1.

2.5 Lower Bound for Symmetric Functions in \( \langle \text{MOD}_q \rangle \)

By the result in Section 4, to lower bound the immunity of \( \chi_q \), it’s equivalent to lower bound the degree of symmetric functions in the ideal \( \langle \chi_q \rangle, \langle \chi_q | _{\rho_1} \rangle, \ldots \), where \( \rho_i \) is the restriction sending \( x_{2j-1} \) to 0 and \( x_{2j} \) to 1 for \( j = 1, 2, \ldots, i \).
When restricting our attention to only symmetric functions, it becomes much easier to deal with.

In this section, we will lower bound the degree of symmetric functions in \(\langle \chi_q \rangle\), and the result here is not strong enough to prove \(\lceil n/2 \rceil\) lower bound for every \(n\). However, in some special cases, such as \(n + 1\) is a power of \(p\), we will prove better lower bound on the degree of nonzero symmetric functions in \(\langle \chi_q \rangle\) which is close to optimal.

Let \(f : \{0, 1\}^n \to F\) be a symmetric function in \(R\), and let \(v_f : \{0, 1, \ldots, n\} \to F\) be its value vector, i.e., \(v_f(|x|) = f(x)\). It’s clear that any symmetric function in \(R\) can be written as a linear combination of elementary symmetric polynomials \(\sigma_0, \ldots, \sigma_n\), that is,

\[
f(x) = \sum_{i=0}^{n} c_f(i)\sigma_i(x),
\]

where \(c_f = (c_f(0), \ldots, c_f(n)) \in F^{n+1}\) is the coefficients of \(f\) in the above form. Given \(c_f\), the value of \(v_f\) is determined by

\[
v_f(i) = \sum_{j=0}^{i} \binom{i}{j} c_f(j).
\]

By a special case of Mobius inversion on the Boolean lattice, \(c_f\) can be written in \(v_f\) as follows,

\[
c_f(i) = \sum_{j=0}^{i} (-1)^{i+j} \binom{i}{j} v_f(j).
\]

The following proposition is an immediate consequence from equations (2.5) and (2.6).

**Proposition 2.5.1.** There is a symmetric function in \(R\) of degree less than \(d\) supported only on points of hamming weight in \(S \subseteq \{0, 1, \ldots, n\}\) if and only if there is a symmetric function in \(R\) supported only on monomials of weight in \(S\) which takes value zero on every input point of hamming weight not less than \(d\).

By the above proposition, the following lemma implies the lower bound of the degree of symmetric functions in the ideal \(\langle \chi_q \rangle\), when \(n + 1\) is a power of \(p\).

**Lemma 2.5.2.** Let \(f \in R\) be a nonzero symmetric function supported only on monomials of weight in \(S_a = \{a, a + q, a + 2q, \ldots\} \subseteq \{0, 1, \ldots, N = p^n - 1\}\), which takes value zero on every input point of hamming weight not less than \(d\). Then,

\[
d \geq N(1 - \frac{1}{p^\ell}),
\]

where \(\ell = \lceil \log_p(q - 1) \rceil\).
**Proof.** If \( f \) is symmetric supported only on monomials of weight in \( S_n \), and \( w \) is an integer variable representing the weight \( |x| \) of \( x \), we can express \( f : \{0, 1, \ldots, N = p^n - 1\} \to \mathbb{F}_p \) as
\[
f(w) = \sum_k c_k \binom{w}{k}.
\]

Now we employ Lucas’ Theorem, in the mod \( p \) case.

**Claim 2.5.3.**
\[
\binom{w}{k} \equiv \prod_{i=0}^{n-1} \binom{w_i}{k_i} \pmod{p}
\]
where \( w_i, k_i \) are the \( i \)'th bits in the \( p \)-adic representation of \( w, k \) respectively.

It is easy to see that \( \binom{w_0}{0} = 1, \binom{w_1}{1} = w_1, \ldots, \binom{w_j}{j} = w_j(w_i - 1)\ldots(w_j - j + 1)/j! \), \cm{\binom{w_i}{j} = w_i(w_i-1)\cdots(w_i-j+1)/j!} \ldots \binom{w_{p-1}}{p-1} = w_1(w_1-1)\cdots(w_1-p+2)/(p-1)! \] which are linearly independent in the polynomial ring \( \mathbb{F}_p[w] \). Let’s view \( \binom{w}{k} \) as a polynomial of \( w_0, w_1, \ldots, w_{n-1} \). From the linear independence of \( \{w_0, w_1, \ldots, w_{p-1}\} \), we claim terms \( \binom{w_0}{0}, \binom{w_1}{1}, \ldots, \binom{w_{p-1}}{p-1} \) are linearly independent as polynomials in \( \mathbb{F}[w_0, \ldots, w_{n-1}] \).

Let’s write
\[
f(w) = \sum_k c_k \binom{w}{k} = \sum_k c_k \prod_{i=0}^{n-1} \binom{w_i}{k_i},
\]
and view it as a polynomial in \( \mathbb{F}_p[w_0, \ldots, w_{n-1}] \). We will show that if \( c_k = 0 \) except when \( k \in S_n \), then \( f \) takes a nonzero value of large hamming weight as a function \( \{0, 1, \ldots, N\} \to \mathbb{F}_2 \). To achieve this, fix a parameter \( \ell \). We will hit \( f \) with a restriction which sets the \( \ell \) highest order bits of input \( w \) to \( p - 1 \) if we can prove that the restricted polynomial is nonzero, it implies there is a nonzero point of value at least \( (p^{\ell} - 1)p^n = N(1 - p^{-\ell}) \). Thus we would like to do this with \( \ell \) as large as possible. Let \( \rho \) denote this restriction.

What happens when we restrict a term (here, term is specifically refer to a multiple of \( \binom{w_0}{0}, \binom{w_1}{1}, \ldots, \binom{w_{p-1}}{p-1} \)) and obtain \( \prod_{i=0}^{n-1} \binom{w_i}{k_i}_p \)? We get exactly the term \( \prod_{i=n-\ell}^{n-1} \binom{w_i}{k_i}_p \prod_{i=n-\ell}^{n-1} \binom{w_i}{k_i} \), where the constant factor \( \prod_{i=n-\ell}^{n-1} \binom{w_i}{k_i} \) is always nonzero. Thus, this linear map maps every term to (nonzero multiple of) a term. If all terms corresponding to \( a, a + q, a + 2q, \ldots \) map to distinct terms, it implies this map is injective on the domain of all such \( f \), and thus that the image of a nonzero \( f \) is a nonzero polynomial as desired.

When do the terms corresponding to two multiples \( a + k_1 q, a + k_2 q \) of \( q \mapsto \) map to the same term under this restriction? As we saw, this happens if and only if they agree on their \( n - \ell \) lowest order bits, which happens if and only if \( 2^{n-\ell} \) divides \( (k_1 - k_2)q \). Since \( q \) is coprime to \( p \), this implies \( 2^{n-\ell} \) divides \( k_1 - k_2 \). But \( k_1 - k_2 \leq N/q \). Thus \( \ell \leq \log_p q \) implies this can only happen if \( k_1 - k_2 = 0 \), that map is injective. Therefore, we take \( \ell = \lfloor \log_p (q - 1) \rfloor \), which is the maximal integer less than \( \log_p q \), and our conclusion follows. \( \square \)
2.6. IMMUNITY AND CIRCUIT LOWER BOUND

As a consequence of the above lemma and Proposition 2.5.1, we can lower bound the degree of a symmetric nonzero function in the idea \( \langle \chi_q \rangle \), when \( n + 1 \) is a power of \( p \).

**Corollary 2.5.4.** Let \( n > 1 \) be an integer such that \( n + 1 \) is a power of \( p \). Let \( f \in \langle \chi_q \rangle \) be a nonzero symmetric function, then

\[
\deg(f) \geq n(1 - \frac{1}{p^\ell}),
\]

where \( \ell = \lfloor \log_p(q-1) \rfloor \).

In the case that \( n + 1 \) is a power of \( p \), and \( q + 1 \) is a power of \( p \), the above corollary gives lower bound \( n(1 - \frac{1}{q-1}) \), which is close to the optimal. Because if we view \( \chi_q \) as a symmetric function from \( \{0, 1, \ldots, n\} \) to \( F \), it takes zero on \( n - \lfloor n/q \rfloor - 1 \) points, which implies there must exist a nonzero symmetric function in \( \langle \chi_q \rangle \) of degree \( n - \lfloor n/q \rfloor - 1 \) by solving \( n - \lfloor n/q \rfloor - 1 \) in \( n - \lfloor n/q \rfloor \) variables in the form (2.4).

In the case that \( n + 1 \) is not a power of \( p \), we can reduce to the former case by applying a restriction \( \rho \) with support size \( n' \) such that \( n - n' + 1 \) is a power of \( p \). However, we may lose a lot if \( n + 1 \) is much above a power of \( p \).

**Corollary 2.5.5.** Let \( n > 1 \) be an integer, and \( n' = n + 1 - p^{\lfloor \log_p(n+1) \rfloor} \) and thus \( n - n' + 1 \) is a power of \( p \). Let \( f \in \langle \chi_q \rangle \) be a nonzero symmetric function, then

\[
\deg(f) \geq (n - n')(1 - \frac{1}{p^\ell}),
\]

where \( \ell = \lfloor \log_p(q-1) \rfloor \).

**Proof.** Let \( f \in \langle \chi_q \rangle \) be a nonzero symmetric function with minimum degree. Let \( \rho \) be a restriction restrict \( n' \) bits to constant, either 0 or 1, such that \( f|_\rho \neq 0 \). It’s easy to see such restriction exists, because if all restrictions of size \( n' \) restricts \( f \) to zero, then \( f \) is a zero function. Moreover, \( f|_\rho \) is also symmetric, and in the ideal \( \langle \chi_q \rangle \). By Proposition 2.5.1 and Lemma 2.5.2, we know that

\[
\deg(f|_\rho) \geq (n - n')(1 - \frac{1}{p^\ell}).
\]

The conclusion follows by observing \( \deg(f|_\rho) \leq \deg(f) \). \( \square \)

**2.6 Immunity and Circuit Lower Bound**

In this section, we will prove that high immunity over \( \mathbb{R} \) plus some weight condition will imply circuit lower bound for \( AC^0 \) circuit, and high immunity over \( \mathbb{F}_p \) will imply circuit lower bound for \( AC^0[p] \) circuit, where \( AC^0[p] \) circuit is constant-depth circuit with MOD\( _p \) gates. The high level idea is that high immunity implies correlation bound (of low degree polynomial), which will imply circuit lower bound.

The following is a classical result due to Razborov, which says functions computed by \( AC^0[p] \) circuits correlates with low degree polynomials.
CHAPTER 2. IMMUNITY OF MOD FUNCTION

Theorem 2.6.1. [31] Let $C$ be an AC$^0[p]$ circuit of size $S$ and depth $d$. For every $\ell > 0$, there is a polynomial $p(x)$ in $F_p[x_1, \ldots, x_n]$ of degree at most $((p-1)\ell)^d$ such that
\[
\Pr_{x \in \{0,1\}^n}[C(x) \neq p(x)] \leq \frac{S}{2^\ell}.
\]

For AC$^0$ circuit, we can still approximate (in the sense of Hamming distance) each AND, OR gates over $\mathbb{R}$.

Lemma 2.6.2. [1] For every integer $\ell \geq 1$, there exists a polynomial $p(x) \in \mathbb{R}[x_1, \ldots, x_n]$ of degree $O(\ell \log n)$ such that
\[
\Pr_x[\text{AND}(x) \neq p(x)] \leq 2^{-\ell}.
\]

As a consequence, if $C$ can be computed by AC$^0$ circuit of depth $d$ and size $S$, for every $\ell \geq 1$, there exists a polynomial $p(x) \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most $O((\ell \log n)^d)$ such that
\[
\Pr_x[C(x) \neq p(x)] \leq \frac{S}{2^\ell}.
\]

Therefore, one approach to prove AC$^0[p]$ circuit lower bound is to prove correlation bound of low degree polynomials. In Smolensky’s 1993 paper [37], he proved Hilbert function is an “invariant” for low degree polynomials.

Definition 2.6.3. Fix the field $F$. The Hilbert function $h_m(S)$, where $S \subseteq \{0,1\}^n$, is defined as the dimension of the following subspace
\[
\{f|_S : f \in F[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n), \deg(f) \leq m\}.
\]

Smolensky proved that high Hilbert function implies correlation bound with low degree polynomials.

Theorem 2.6.4. [37] The distance of $f$, where $S$ is the zero set of $f$, to any degree $d$ polynomials (all nonzero is viewed as 1) is lower bounded by
\[
2h_m(S) - |S|,
\]
where $m \leq (n - d - 1)/2$.

The following observation relates Hilbert function with immunity. By the definition of Hilbert function,
\[
h_m(S) = \dim\{f|_S : \deg(f) \leq m\}
\]
\[
= \binom{n}{\leq m} - \dim\{f \in \langle S \rangle : \deg(f) \leq m\},
\]
where $\langle S \rangle$ denotes the ideal of functions vanishing on $S$ (the ring $R = F[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$), and $\binom{n}{\leq m} = \sum_{i \leq m} \binom{n}{i}$. If the immunity of $S$ is greater than $m$, which means $\dim\{f \in \langle S \rangle : \deg(f) \leq m\} = 0$, and thus $h_m(S)$ achieves the maximal $\binom{n}{\leq m}$. 

2.6. IMMUNITY AND CIRCUIT LOWER BOUND

Since the immunity of \( \chi_q \) is lower bounded by \( n/2, h_m(S) = \binom{n}{\leq m} \) for any \( m = (n - d - 1)/2 < n/2 \), where \( S \) is the zero set of \( \chi_q \). For all \( d = o(\sqrt{n}) \), we have

\[
2h_m(S) - |S| = 2\left( \binom{n}{\leq m} \right) - 2^n(1 - \frac{1}{q} + o(1)) = 2^n(1 - o(1)) - 2^n(1 - \frac{1}{q} + o(1)) = \frac{2^n}{q} - o(2^n),
\]

By Theorem 2.6.4, function \( \chi_q \) is different from any degree \( o(\sqrt{n}) \) polynomials on at least \( 2^\ell(1/q - o(1)) \) points. Taking \( \ell = O(\log n) \) and \( S = n^{O(1)} \) in Theorem 2.6.1, thus \( C(x) \) can be approximated by a \( o(\sqrt{n}) \) function with error \( o(1) \). Combining these two facts implies any polynomial size \( AC^0[p] \) circuit can only output the correct answer on at most \( 2^n(1 - 1/q + o(1)) \) points, and this was proved by Smolensky [37].

Note that above argument works as long as Boolean function \( f \) has immunity (over \( \mathbb{F}_p \)) \( \geq n/2 - o(\sqrt{n}) \) and \( |f| = \Omega(2^n) \), then \( f \) has exponential \( AC^0[p] \) circuit lower bound. The same conclusion holds for \( AC^0 \) circuit, i.e., if \( f \) has immunity (over \( \mathbb{R} \)) \( \geq n/2 - o(\sqrt{n}) \) and \( |f| = \Omega(2^n) \), then \( f \) has exponential \( AC^0 \) circuit lower bound.

For another example, let’s consider the \( q \)th residue character function, \( \Lambda_q : \{0,1\}^n \rightarrow \{0,1\} \) on finite field \( F_{2^n} \). Fix a basis \( b_1, \ldots, b_n \) of \( F_{2^n} \) over \( F_2 \). Map \( \phi : \{0,1\}^n \rightarrow F_{2^n} \) is defined as

\[
\phi(x) = \sum_{i=1}^{n} x_i b_i \in F_{2^n}.
\]

Then \( \Lambda_q(x) = 1 \) if and only if there exists \( y \in F_{2^n} \) such that \( y^q = x \). Kopparty [23] proved exponential \( AC^0[p] \) circuit lower bound of the \( q \)th residue character over \( F_{2^n} \). In fact, he proved something stronger, which is the lower bound of computing a large power in \( F_{2^n} \). Here, we present a simple proof by immunity.

Carlet and Feng [12] proves the quadratic residue function has one sided immunity not less than \( n/2 \), and their proof also works for \( q \)th residue character function. Since it’s a nice and simple proof, we reproduce the proof here.

**Theorem 2.6.5.** Assume \( q \) divides \( 2^n - 1 \). The immunity of \( \neg \Lambda_q(x) \) over \( F_2 \) is greater than \( d \), as long as \( \binom{n}{\leq d} \leq 2^n/q \).

**Proof.** Let \( f \) be a polynomial in \( \langle \neg \Lambda_q(x) \rangle \) with degree \( \leq d \), and we shall prove \( f = 0 \).

The trick is to view \( f \) as a function \( \tilde{f} \) from \( F_{2^n} \rightarrow F_{2^n} \) by the natural map \( \phi \), given the basis \( b_1, \ldots, b_n \) of \( F_{2^n} \) over \( F_2 \). Given \( f : F_{2^n} \rightarrow F_2 \), define \( \tilde{f} : F_{2^n} \rightarrow F_{2^n} \) by

\[
\tilde{f}(x) = f(x_1, x_2, \ldots, x_n),
\]
where \(x = x_1b_1 + \ldots + x_nb_n\). It’s easy to see any function from \(F_{2^n} \to F_{2^n}\) can be written as a univariate polynomial of degree less than \(2^n\). Thus, write

\[
\tilde{f}(x) = \sum_{0 \leq i \leq 2^n-1} c_i x^i
\]

where \(i = \sum_{s \in S} i_s 2^s\) is the binary representation of \(i\). Imagining (2.7) is expanded, it’s easy to see the coefficients of \(\prod_{i \in S} x_i\) for any \(S \subseteq [n]\) should be in \(\{0, 1\}\), and coincides with the expansion of \(f : F_{2^n} \to F_2\), for they are taking the same value on every \(x_1, \ldots, x_n\). From this, we see the degree \(f : F_{2^n} \to F_2\) is

\[
\max\{w_2(i) : c_i \neq 0\},
\]

where \(w_2(i)\) is defined as the number of 1's in the binary representation of \(i\). Hence, assume

\[
\tilde{f}(x) = \sum_{0 \leq i \leq 2^n-1} c_i x^i,
\]

and we will show \(\tilde{f}(x) = 0\), that is, \(c_i = 0\) for all \(i\).

Let \(\xi\) be a primitive root of \(F_{2^n}\). Since \(f\) is in \(\langle \neg \Lambda_q(x) \rangle\), \(\tilde{f}\) has to take 0 on \(\xi^0, \xi^q, \xi^{2q}, \ldots, \xi^{2^n-1}\), that is,

\[
\left(\begin{array}{cccc}
\xi^0 & \xi^q & \cdots & \xi^{2^n-1} \\
\xi^{iq_1} & \xi^{iq_2} & \cdots & \xi^{iq_m} \\
& \cdots & \cdots & \\
& & & \\
& & & \\
& & & \\
\end{array}\right)
\left(\begin{array}{c}
c_{i_1} \\
c_{i_2} \\
\vdots \\
c_{i_m}
\end{array}\right) = 0,
\]

where \(t = (2^n - 1)/q\) and \(i_1, \ldots, i_m\) enumerates all \(i\) with \(w_2(i) \leq d\). By assumption \(\binom{n}{\leq d} \leq 2^n/q\), we have \(m \leq t\). Since the matrix on the left hand side of (2.8) has full rank \(m\) by Vandermonde determinant formula, \(c_{i_1} = c_{i_2} = \ldots = c_{i_m} = 0\), which completes the proof. \(\Box\)

Let \(S\) be the one-set of \(\Lambda_q\). For integer \(m\) such that \(\binom{n}{\leq m} \geq 2^n/q\), by the above theorem, we have

\[
2h_m(S) - |S| \geq 2h_{m'}(S) - |S| \geq 2^n\left(\frac{1}{q} - o(1)\right),
\]

where \(m'\) is the largest integer such that \(\binom{n}{\leq m'} \leq 2^n/q\), and thus \(m' = n/2 - \Theta(\sqrt{n})\) for fixed \(q\). Combining with Theorem 2.6.4, function \(\Lambda_q\) is different from
any degree $o(\sqrt{n})$ polynomials at $2^n(1/q - o(1))$ points. Following the same argument as we did for MOD function, any polynomial size $\text{AC}^0[\oplus]$ circuit can agree with $\Lambda_q$ on at most $2^n(1 - 1/q + o(1))$ points.

Moreover, by the immunity argument, we can prove the following result, which improves the size bound by Kopparty [23] from $2^{n^{1/2(2d)}}$ to $2^{n^{1/(2+\varepsilon)d}}$, where $\varepsilon > 0$ is arbitrarily small, where the constant $1/(2d)$ on the double exponent seems to be the best we can get by the direct Razborov-Smolensky approach.

**Theorem 2.6.6.** For every $\text{AC}^0[\oplus]$ circuit $C : \{0,1\}^n \rightarrow \{0,1\}$ of depth $d$ and size $S \leq 2^{n^{1/(2+\varepsilon)d}}$, where $\varepsilon > 0$ is arbitrarily small, we have

\begin{equation}
Pr_x[C(x) = \Lambda_q(x)] \leq 1 - \frac{1}{q} + o_n(1),
\end{equation}

where $o_n(1)$ goes to 0 as $n$ goes to infinity after $q$ and $\varepsilon$ are fixed.

**Proof.** Applying Razborov’s Theorem 2.6.1 by taking $\ell = n^{1/(2+0.5\varepsilon)d}$, there exists a polynomial of degree $\leq \ell^d = n^{1/(2+0.5\varepsilon)}$, such that,

\begin{equation}
Pr_x[C(x) \neq g(x)] \leq \frac{S}{2^{n^{1/(2+0.5\varepsilon)d}}} = o_n(1).
\end{equation}

Meanwhile, by Theorem 2.6.4 and Theorem 2.6.5,

\begin{align*}
Pr_x[\Lambda_q(x) \neq g(x)] &\geq (2h_{m}(S) - |S|)/2^n \\
&\geq (2h_{(n-\ell^{-1})/2}(S) - |S|)/2^n \\
&\geq (2h_{n/2-o(\sqrt{n})}(S) - |S|)/2^n \\
&= \frac{1}{q} - o_n(1).
\end{align*}

By triangle inequality,

\begin{equation*}
Pr[\Lambda_q(x) \neq C(x)] \geq Pr[\Lambda_q(x) \neq g(x)] - Pr[C(x) \neq g(x)] = \frac{1}{q} - o_n(1),
\end{equation*}

which proves the theorem. $\square$

In fact, what Kopparty proved in [23] is for $q$th residue function $\Lambda_q : F_{2^n} \rightarrow \{0,1,\ldots,q-1\}$ instead of the $q$th residue character function. We can easily modify the above argument for $q$th residue function as follows, where the right hand side of (2.9) will become $1/q + o(1)$. Given $\varepsilon > 0$, suppose for contradiction that there exists a circuit $C$ of depth $d$ and size $2^{n^{1/(2+\varepsilon)d}}$ agrees with $\Lambda_q$ on $\geq 1/q'$ fractions, where $1/q' > 1/q$. Again, taking $\ell = n^{1/(2+0.5\varepsilon)d}$ in Theorem 2.6.1, there exist polynomials $g_0,\ldots,g_{q-1}$ of degree $\leq \ell^d = n^{1/(2+0.5\varepsilon)} = o(\sqrt{n})$ which agrees with $P_0,\ldots,P_{q-1}$ on $1 - o(1)$ fraction respectively, which implies,

\begin{equation*}
\sum_{i} Pr_x[g_i(x) = 1] \geq 1/q' - o(1),
\end{equation*}
where \( P_i = \{ x \in F_{2^n} : \Lambda_i(x) = i \} \). Denote by \( S = \{ x : g_i(x) = 1 \text{ for some } i \in P_i \} \), where \( S \geq (1/q' - o(1))2^n \). By the Hilbert function and immunity argument, all polynomials of degree \( \leq d \), where \( \binom{n}{\leq d} \geq 2^n(1/q + o(1)) \), can represent any function restricting on \( P_i \). Since the existence of \( g_0, g_1, \ldots, g_{q-1} \), degree \( d + \max \deg(g_i) \) polynomials are sufficient to represent any functions on \( S \). The contradiction comes from a double counting: the number of such polynomials is upper bounded by \( 2^{\binom{n}{\leq d+\deg(g)}} = 2^{2^n(1/q+o(1))} \), while the number of Boolean functions on \( S \) is \( 2^{|S|} \geq 2^{2^n(1/q' - o(1))} \), where \( 1/q' \) is strictly greater than \( 1/q \).
Chapter 3

Robust Immune Symmetric Functions

3.1 Statement of the Result

Before stating our main result, we need some notations and definitions. Fix a field $F$. Let

$$\psi_k(i) = \binom{i}{0}, \binom{i}{1}, \ldots, \binom{i}{k-1} \in \mathbb{F}_k,$$

where $\binom{i}{j} = 1 + \ldots + 1$.

Definition 3.1.1. ($m,t$-sound partition) Let $U = \{S_0, S_1, \ldots\}$ be a partition of $\{0,1,\ldots,t-1\}$, that is, $\{0,1,\ldots,t-1\}$ is the disjoint union of $S_0, S_1, \ldots$. If for any integer $1 < k \leq t$, $\cup_{i \geq 0} E_i$ is always a basis of $\mathbb{F}_k$, we say $U$ is a $(m,t)$-sound partition, where

$A_i = \{\psi_k(k-1-j) : j \in S_i \cap \{0,1,\ldots,k-1\}\}$,

$B_i = \{\psi_k(k+m+j) : j \in S_i \cap \{0,1,\ldots,k-1\}\}$,

$E_i \in \{A_i, B_i\}$.

The following theorem is our main result, and furthermore, all such partitions are explicitly constructed. We point out that the following theorem is proved implicitly in [39] for the case $F = F_2$ and $m = 1$, which can be viewed as a baby version. The above mentioned result is a key ingredient leading to the characterization of all even-number variable symmetric Boolean functions with maximum algebraic immunity (see Definition 3.1.4).

Theorem 3.1.2. For any field $F$, any integer $m \geq 0$ and $t \geq 1$, there exists a $(m,t)$-sound partition $U_m$ which is a refinement of any $(m,t)$-sound partition.

\[1\] Here we write $U_m$ instead of $U_{m,t}$ for convenience, where $U_m$ is a partition of natural numbers, and for given $t$, we think of it as a partition of $\{0,1,\ldots,t-1\}$. 47
CHAPTER 3. ROBUST IMMUNE SYMMETRIC FUNCTIONS

If $\mathcal{U}$ is a refinement of any $(m, t)$-sound partition, we say it's $(m, t)$-complete. Of course, the trivial partition $\{\{0\}, \{1\}, \{2\}, \ldots\}$ is always complete. The above theorem asserts that, for any $m \geq 0$, $t > 0$, there exists a partition $\mathcal{U}_m$ which is both $(m, t)$-sound and $(m, t)$-complete. Equivalently, the above theorem can be rephrased as follows: if both $\mathcal{U}$ and $\mathcal{V}$ are $(m, t)$-sound, their least common refinement is also $(m, t)$-sound.

Definition 3.1.3. Fix a field $\mathbb{F}$. The degree of Boolean function $f : \{0, 1\}^n \to \{0, 1\}$ over $\mathbb{F}$ is the degree of the unique multilinear polynomial $g(x) \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f(x) = g(x)$ for any $x \in \{0, 1\}^n$, which is denoted by $\deg_\mathbb{F}(f)$ or simply $\deg(f)$.

Definition 3.1.4. Given field $\mathbb{F}$, the immunity of $f$ is defined as the minimal degree of a nonzero function $g \in \mathbb{F}[x_1, \ldots, x_n]$ such that $g(x) = 0$ for all $x$ with $f(x) = 0$. Algebraic immunity over $\mathbb{F}$ (or two-sided immunity) is defined as the smaller one between the immunity of $f$ and $1 - f$.

Notice that the degree and immunity of a Boolean function depends on the field we are working on. When there is no ambiguity, we will omit the field. Following is the definition of $k$ robust immune, which looks a bit artificial.

Definition 3.1.5. Function $f$ is called $k$ robust immune if the algebraic immunity of $f$ is always lower bounded by $k$ no matter how you change the value of $f(x)$ with $k \leq |x| \leq n - k$.

Our main theorem (Theorem 3.1.2) has the following consequence, which will be proved in the next section.

Corollary 3.1.6. Let $f : \{0, 1\}^n \to \{0, 1\}$ be a symmetric Boolean function (a symmetric Boolean function is a function invariant under symmetric group $S_n$, and thus can be represented by a value vector $v_f : \{0, 1, \ldots, n\} \to \{0, 1\}$ such that $f(x) = v_f(|x|)$), and $n = 2k + m - 1$. Function $f$ is $k$ robust immune if and only if its value vector $v_f : \{0, 1, \ldots, n\} \to \{0, 1\}$ satisfies

$$v_f(k - 1 - i) = 1 - v_f(k + m + j),$$

for any $0 \leq i, j \leq k - 1$ which belong to the same set in the partition $\mathcal{U}_m$ (in the notation of Theorem 3.1.2).

This chapter is organized as follows. In Section 2, we will introduce the proof techniques of our theorem, and the proof of Corollary 3.1.6 from Theorem 3.1.2. In Section 3, we will prove our theorem for $\mathbb{F}$ with characteristic 2. In Section 4, we will prove our theorem for field with characteristic $p > 2$, which turns out to be simpler than characteristic 2.

3.2 Proof Techniques

Our proof is based on the following simple observation in [7]. Let $\psi_k(a_0), \psi_k(a_1), \ldots, \psi_k(a_{k-1}) \in \mathbb{F}^k$ be $k$ vectors, which is a basis of $\mathbb{F}^k$ having full rank $k$, if and
only if, the determinant of the $k$ by $k$ matrix

\[
(\psi_k(a_0), \psi_k(a_1), \ldots, \psi_k(a_{k-1}))
\]

is nonzero over $F$. The determinant of the above matrix turns out to have a simple closed form.

\[
\det(\psi_k(a_0), \psi_k(a_1), \ldots, \psi_k(a_{k-1})) = \prod_{i=0}^{k-1} \left( \begin{array}{cccc}
1 & a_0 & \cdots & (a_0 - a_{k-1}) \\
1 & a_1 & \cdots & (a_1 - a_{k-1}) \\
\vdots & \vdots & \ddots & \vdots \\
1 & a_{k-1} & \cdots & (a_{k-1} - a_{k-1}) \\
\end{array} \right)
\]

\[
= \prod_{0 \leq i < j \leq k-1} \frac{a_j - a_i}{j - i},
\]

which is nonzero over field $F$ with characteristic $p$ if $a_0, a_1, \ldots, a_{k-1}$ are distinct when $p = 0$; if

\[
\sum_{0 \leq i < j \leq k-1} \text{ord}_p(a_j - a_i) = \sum_{0 \leq i < j \leq k-1} \text{ord}_p(j - i)
\]

when $p > 0$. Here, $\text{ord}_p(i)$ for nonzero integer $i$ is the maximum integer $m$ such that $p^m$ divides $i$. The following proposition is an immediate consequence.

**Proposition 3.2.1.** Let $\bigcup_{i \geq 0} I_i = \{0, 1, \ldots, k\}$. If $\bigcup_{i \geq 0} E_i$ is always a basis of $F^{k+1}$, where

\[
A_i = \{\psi_{k+1}(k - j) : j \in I_i, 0 \leq j \leq k\},
\]

\[
B_i = \{\psi_{k+1}(k + m + 1 - j) : j \in I_i, 0 \leq j \leq k\},
\]

\[
E_i \in \{A_i, B_i\},
\]

then

\[
\sum_{x \in I_i, y \in I_j} \text{ord}_p(x - y) = \sum_{x \in I_i, y \in I_j} \text{ord}_p(x + y + m + 1)
\]

holds for all $i \neq j$. 
In the case char(\mathbb{F}) = 0, since \psi_k(a_0), \ldots, \psi_k(a_{k-1}) will always be a basis as long as a_0, \ldots, a_{k-1} are distinct, it’s easy to see that, for any m \geq 0, any partition of N is (m, t)-sound, and thus the trivial partition

\[ U_m = \{\{0\}, \{1\}, \{2\}, \ldots\] is both (m, t)-sound and (m, t)-complete. In the following sequel, we will focus on the case when the filed \mathbb{F} has characteristic p > 0.

The next two propositions characterize when a partition is (m, t)-sound and (m, t)-complete by the sum of ord_p(\cdot), and they will be used to prove our main theorem. For convenience, if I is a subset of \mathbb{N}, let \text{I}_{<k} \text{ denotes } \text{I \cap \{0, 1, \ldots, k - 1\}}. Let k - I := \{k - i : i \in I\}, and let \text{ord}_p(I) := \sum_{i \in I} \text{ord}_p(i).

**Proposition 3.2.2.** Partition \text{U}_m is (m, t)-sound if and only if

\[ \text{ord}_p(k - I_{<k}) = \text{ord}_p(k + I_{<k} + m + 1) \]

for all 0 < k \leq t and I \in \text{U}_m with k \notin I.

**Proof.** Fix t. Let’s prove by induction on k. For k = 1, it’s easy to verify. Let’s assume that the conclusion is true for k, let’s prove for k + 1.

Let \text{U}_m = \{I_0, I_1, \ldots\}. By Proposition 3.2.1, we have

\[ (3.1) \quad \sum_{x \in I_{<k-1}^z, y \in I_{<k-1}^y} \text{ord}_p(x - y) = \sum_{x \in I_{<k-1}^z, y \in I_{<k-1}^y} \text{ord}_p(x + y + m + 1) \]

for any i \neq j.

Similarly, by Proposition 3.2.1, the condition that either \psi_{k+1}(k - I_{<k}^0) or \psi_{k+1}(k + m + 1 + I_{<k}^0), and either \psi_{k+1}(k - I_{<k}^1) or \psi_{k}(k + m + 1 + I_{<k}^1), \ldots form a basis of \mathbb{F}^{k+1} is equivalent to

\[ (3.2) \quad \sum_{x \in I_{<k}^i, y \in I_{<k}^j} \text{ord}_p(x - y) = \sum_{x \in I_{<k}^i, y \in I_{<k}^j} \text{ord}_p(x + y + m + 1) \]

for any i \neq j. Given that (3.1) is true by induction hypothesis, (3.2) holds if and only if

\[ \text{ord}_p(k - I) = \text{ord}_p(k + I + m + 1) \]

for any k \notin I. \hfill \Box

**Proposition 3.2.3.** Suppose \text{U}_m is a (m, t)-sound partition. Then \text{U}_m is (m, t)-complete if

\[ \text{ord}_p(k - I_{<k}) < \text{ord}_p(k + I_{<k} + m + 1) \]

for all k \in I \in \text{U}_m with |I_{<k}| > 0.

**Proof.** Fix t. It’s equivalent to prove the contrapositive, that is, if there exists k \in I \in \text{U}_m with |I_{<k}| > 0, such that,

\[ \text{ord}_p(k - I_{<k}) \geq \text{ord}_p(k + I_{<k} + m + 1), \]
Let $g$ be a symmetric Boolean function in $f$ of degree less than $k$, then $\langle f \langle \rangle \rangle$ has degree less than $k$. By Lemma 3.2.4, it suffices to prove, inside $\langle f \langle \rangle \rangle$, has no symmetric nonzero function with degree $< k - l$, where $\rho$ sets $x_1, x_3, \ldots, x_{2l-1}$ to 0 and $x_2, x_4, \ldots, x_2l$ to 1, for all $l = 0, 1, \ldots, k - 1$. If $v_f : \{0, 1\}^n \rightarrow \{0, 1\}$ is the value vector of $f$, then
\[ v_{f|_\rho} = (v_f(l), v_f(l + 1), \ldots, v_f(n - l)) \]
is the value vector for all $l = 0, 1, \ldots, k$.

Let $g$ be a symmetric Boolean function in $f$ of degree less than $k$. One could write $f$ as linear combinations of elementary symmetric polynomials $s_0, s_1, \ldots, s_{k-1}$, that is,
\[ f(x) = \sum_{i=0}^{k-1} c_i s_i(x). \]
Since \( g \in \langle f \rangle \), \( f(x) = 0 \) implies \( g(x) = 0 \) for all \( x \). Notice that \( s_j(x) = \binom{x}{j} \) for all \( x \) with weight \( i \), that is why we define \( \psi_k(i) \) in this way. By linear algebra that a linear system of equations has a nonzero solution if and only if the rank is less than the number of variables, we claim such nonzero \( g \) exists if and only if \( \{ \psi_k(i) : f(x) = 0 \text{ for } x \text{ with weight } i \} \) has full rank.

If \( U_m \) is \((m,k)\)-sound partition, and \( f \) satisfies

\[
v_f(k - 1 - i) = 1 - v_f(k + m + j),
\]

for any \( 0 \leq i, j \leq k - 1 \) belongs to the same set in the \((m,k)\)-sound partition \( U_m \). The rank condition holds for \( k, k - 1, \ldots \). On the other hand, since \( U_m \) is \((m,k)\)-complete, which exhaust all the possibilities. 

3.3 Proof for the Case \( \text{char}(\mathbb{F}) = 2 \)

Let’s first introduce some notations about 2-adic (binary) expansion of integers. Any integer \( k \geq 0 \) can be written as a binary number,

\[
(3.3) \quad k = (k_0, k_1, \ldots, k_l)_2,
\]

where \( k_0, \ldots, k_{l-1} \in \{0,1\} \), and \( k = \sum_{i \geq 0} a_i 2^i \). Notice that we always write lower bits from the left. The subscript 2 in (3.3) will be omitted. Let \( k_{\geq n} \) denote \((k_n, k_{n+1}, \ldots)\).

A pattern \( \alpha \), which represents a subset of \( \mathbb{N} \), is a string consisting of 0, 1, ?, *, where ? represents either 0 or 1, and * can be a binary string of arbitrary length. We say a natural number \( k \) matches a pattern if the bits of the binary expansion (3.3) matches. For example, pattern \( 0* \) is the set of all even natural numbers.

Our partition \( U_m \) is recursively defined as follows. Sorry that we use the “pattern” notation instead of the standard set notation, since it will be more convenient for the proof. Let

\[
U_0 = \{ \mathbb{N} \},
\]

\[
U_1 = \{ (0*), (10*), (110*), (1110*), \ldots \}.
\]

For any integer \( m > 0 \),

\[
U_{2m} = \bigcup_{\alpha \in U_m} \{ ?\alpha \}.
\]

For odd number \( m > 0 \),

\[
U_{2m+1} = \bigcup_{\alpha \in U_m} \{ 00\alpha \} \cup \bigcup_{\alpha \in U_m} \{ 1?\alpha, 01\alpha \}.
\]

For odd number \( m > 0 \) and integer \( e > 1 \), let

\[
U_{2^{e}m+1} = \bigcup_{\alpha \in U_m} \bigcup_{i=0}^{e-1} \{ 1^n?e^{-i}\alpha \} \cup \bigcup_{\alpha \in U_{m+1}} \{ 1^e\alpha \}.
\]

It’s easy to prove by induction that partition \( U_m \) is well-defined for any integer \( m \geq 0 \), that is, it is a partition of \( \mathbb{N} \).
3.3. PROOF FOR THE CASE CHAR($\mathbb{F}$) = 2

3.3.1 Partition $U_0$

For partition $U_0 = \{\mathbb{N}\}$, it’s easy to see $U_0$ is $(0,t)$-sound for any $t$. To prove it’s $(0,t)$-complete, by Proposition 3.2.3, we need to verify

$$\sum_{0 \leq i < k} \text{ord}_2(k - i) < \sum_{0 \leq i < k} \text{ord}_2(k + i + 1)$$

for any $k > 0$, that is, \( \text{ord}_2(k!) < \text{ord}_2((2k)!/k!) \),

which is true because \( (2k)^k \equiv 0 \pmod{2} \) for any $k > 0$. For the first time using the result, we give a proof as follows.

**Claim 3.3.1.** For any integer $k > 0$, \( (2k)^k \equiv 0 \pmod{2} \).

**Proof.** Let $k = (k_0, k_1, \ldots, k_l)$ be the binary expansion of $k$. By Lucas’ Theorem,

$$\binom{2k}{k} \equiv \binom{0}{k_0} \binom{k_0}{k_1} \cdots \binom{k_l-1}{k_l} \binom{k_l}{0} \pmod{2},$$

which is nonzero if and only if $0 \geq k_0 \geq k_1 \geq \ldots \geq k_l$, that is, $k = 0$. \( \square \)

3.3.2 Partition $U_1$

For partition $U_1 = \{I_0, I_1, I_2, \ldots\}$, where

$$I_i = \{(1^i0^{n-i})\} = \{x \in \mathbb{N} : \text{ord}_2(x + 1) = i\}.$$ 

To prove $U_1$ is $(1,t)$-sound for any $t$, by Proposition 3.2.2, it’s equivalent to prove \( \text{ord}_2(k - I_j^{<k}) = \text{ord}_2(k + I_j^{<k} + 2) \) holds for any $k \notin I_j \subset U_1$. Let $k \in I_i$, that is,

$$k = (k_0 = 1, \ldots, k_{i-1} = 1, k_i = 0, k_{i+1}).$$

Take $x \in I_j$, where $i \neq j$, then,

$$x = (x_0 = 1, \ldots, x_{j-1} = 1, x_j = 0, x_{j+1}).$$

It’s easy to verify \( \text{ord}_2(k - x) = \text{ord}_2(k + x + 2) = \min(i,j) \), which implies \( \text{ord}_2(k - I_j^{<k}) = \text{ord}_2(k + I_j^{<k} + 2) \). Thus, $U_1$ is $(1,t)$-sound for any $t$.

To prove $U_1$ is $(1,t)$-complete for any $t$, by Proposition 3.2.3, we need to prove

$$\text{ord}_2(k - I_i^{<k}) < \text{ord}_2(k + I_i^{<k} + 2),$$

for any $k \in I_i$ with $I_i^{<k}$ nonempty. For $x \in I_i$, write

$$x = (x_0 = 1, \ldots, x_{i-1} = 1, x_i = 0, x_{i+1}).$$
It’s easy to see \( \text{ord}_2(k - x) = (i + 1) + \text{ord}_2(x > i - k > i) \) and \( \text{ord}_2(k + x + 2) = (i + 1) + \text{ord}_2(x > i + k_x > i + 1) \). Thus, (3.5) is equivalent to
\[
\sum_{0 \leq x < k > i} \text{ord}_2(k > i - x) < \sum_{0 \leq x < k > i} \text{ord}_2(k > i + x + 1)
\]
for \( k > i > 0 \), which is already proved in (3.4).

3.3.3 From \( U_m \) to \( U_{2m} \)

By induction hypothesis \( U_m \) is both \((m, t)\)-sound and \((m, t)\)-complete for any \( t \), let’s prove that \( U_{2m} \) is \((2m, t)\)-sound and \((2m, t)\)-complete for any \( t \).

Recall the definition
\[
U_{2m} = \bigcup_{\alpha \in U_m} \{?\alpha\}.
\]

To prove \( U_{2m} \) is \((2m, t)\)-sound for any \( t \), by Proposition 3.2.2, one needs to prove for any \( k > 1 \),
\[
(3.6) \quad \text{ord}_2(k - I^{<k}) = \text{ord}_2(k + I^{<k} + 2m + 1),
\]
where \( k \not\in I \in U_{2m} \). By the definition of \( U_{2m} \), we may assume \( I = ?\alpha \), where \( \alpha \in U_m \). The left hand side of (3.6) is
\[
\text{ord}_2(k - I^{<k})
= \text{ord}_2((k_0, k \geq 1) - (?\alpha)^{<k})
= \text{ord}_2((k_0, k \geq 1) - (k_0, \alpha)^{<k_{\geq 1}})
= |\alpha^{<k_{\geq 1}}| + \text{ord}_2(k \geq 1 - \alpha^{<k_{\geq 1}}).
\]
The right hand side of (3.6) is
\[
\text{ord}_2(k + I^{<k} + 2m + 1)
= \text{ord}_2((k_0, k \geq 1) + (?\alpha)^{<k} + (1, m))
= \text{ord}_2((k_0, k \geq 1) + (1 - k_0, \alpha^{<k_{\geq 1}}) + (1, m))
= |\alpha^{<k_{\geq 1}}| + \text{ord}_2(k \geq 1 + \alpha^{<k_{\geq 1}} + m + 1)
\]
By induction hypothesis, partition \( U_m \) is a \((m, t)\)-sound partition, \( \alpha \in U_m \), and by Proposition 3.2.2,
\[
\text{ord}_2(k \geq 1 - \alpha^{<k_{\geq 1}}) = \text{ord}_2(k \geq 1 + \alpha^{<k_{\geq 1}} + m + 1)
\]
holds for any \( k \geq 1 \not\in \alpha \), and thus, the left hand side of (3.6) equals the right hand side.

Now, let’s prove \( U_{2m} \) is \((2m, t)\)-complete, that is, by Proposition 3.2.3,
\[
(3.7) \quad \text{ord}_2(k - I^{<k}) < \text{ord}_2(k + I^{<k} + 2m + 1),
\]
3.3. PROOF FOR THE CASE $\text{CHAR}(\mathbb{F}) = 2$

where $k \in I$, and $I^{<k}$ is nonempty. By the definition of $U_{2m}$, let $I = ? \alpha$. The left hand side of (3.7) is

\[
\text{ord}_2(k - I^{<k}) = \text{ord}_2((k_0, k_{\geq 1}) - (? \alpha)^{<k}) = \text{ord}_2((k_0, k_{\geq 1}) - (k_0, \alpha^{<k_{\geq 1}})) = |\alpha^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} - \alpha^{<k_{\geq 1}}}).
\]

Similarly, the right hand side of (3.7) is

\[
\text{ord}_2(k + I^{<k} + 2m + 1) = \text{ord}_2((k_0, k_{\geq 1} + (? \alpha)^{<k} + (1, m)) = \text{ord}_2((k_0, k_{\geq 1}) + (1 - k_0, \alpha^{<k_{\geq 1}}) + (1, m))) = |\alpha^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} + \alpha^{<k_{\geq 1}} + m + 1) + \delta_{k_0,1}(1 + \text{ord}_2(2k_{\geq 1} + m + 1))
\]

By induction hypothesis that $U_m$ is $(m,t)$-complete,

\[
\text{ord}_2(k_0 - \alpha^{<k_{\geq 1}}) < \text{ord}_2(k_{\geq 1} + \alpha^{<k_{\geq 1}} + m + 1)
\]

is true for all $\alpha^{<k_{\geq 1}}$ nonempty, which implies (3.7) is true. For the case that $\alpha^{<k_{\geq 1}}$ is empty, and $I^{<k} = (? \alpha)^{<k}$ is nonempty, we must have $k_0 = 1$, and then (3.7) is also true.

3.3.4 From $U_m$ to $U_{2m+1}$, $m$ odd

Recall the definition,

\[
U_{2m+1} = \bigcup_{0 \alpha \in U_m} \{00\alpha\} \cup \bigcup_{1 \alpha \in U_m} \{1? \alpha, 01\alpha\},
\]

where by induction hypothesis, all patterns in $U_m$ are of the form $0\alpha$ or $1\alpha$.

To prove $U_{2m+1}$ is $(2m + 1, t)$-sound for any $t$, by Proposition 3.2.2, one needs to prove

(3.8) \[
\text{ord}_2(k - I^{<k}_j) = \text{ord}_2(k + I^{<k}_j + 2m + 2),
\]

for any $k > 0$ and $k \notin I_j \in U_{2m+1}$. Let’s prove by case analysis.

**Case 1:** $k \in 0\alpha$ and $I_j \in 1? \beta$. Both left hand side and right hand side of (3.8) are 0.

**Case 2:** $k \in 0\alpha$ and $I_j \in 01 \beta$. The left hand side of (3.8) is $|I^{<k}_j|$, and the right hand side of (3.8) is $\text{ord}_2(k + I^{<k}_j + 2m + 2) = \text{ord}_2((0, 0, k_{\geq 2}) + (0, 1, \alpha) + (0, m + 1)) = |I^{<k}_j|.$

**Case 3:** $k \in 1? \alpha$ and $I_j \in 00 \beta$. Both left hand side and right hand side of (3.8) are 0.

**Case 4:** $k \in 1? \alpha$ and $I_j \in 01 \beta$. Both left hand side and right hand side of (3.8) are 0.
CHAPTER 3. ROBUST IMMUNE SYMMETRIC FUNCTIONS

Case 5: $k \in 0\alpha$ and $I_j \in 0\beta$. The left hand side of (3.8) is $|I_j^{<k}|$, and the right hand side of (3.8) is $\text{ord}_2(k + I_j^{<k} + 2m + 2) = \text{ord}_2((0, 1, k_{\geq 2}) + (0, 0, \alpha) + (0, m + 1)) = |I_j^{<k}|$.

Case 6: $k \in 0\alpha$ and $I_j \in 1?\beta$. Both the left hand side and the right hand side of (3.8) are 0.

Case 7: $k \in I_i = 00\alpha$ and $I_j \in 0?\beta$. By the definition of $\mathcal{U}_{2m+1}$, $I_i = 0\alpha \in \mathcal{U}_m$, $I_j = 0\beta \in \mathcal{U}_m$. The left hand side of (3.8) is

$$\text{ord}_2(k - I_j^{<k}) = \text{ord}_2((0, k_{\geq 1}) + (0, I_j^{<k})) = |I_j^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} - I_j^{<k_{\geq 1}}),$$

and the right hand side of (3.8) is

$$\text{ord}_2(k + I_j^{<k} + 2m + 2) = \text{ord}_2((0, k_{\geq 1}) + (0, I_j^{<k}) + (0, m + 1)) = |I_j^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} + I_j^{<k_{\geq 1}} + m + 1).$$

By induction hypothesis that $\mathcal{U}_m$ is $(m, t)$-sound partition, and thus

$$\text{ord}_2(k_{\geq 1} - I_j^{<k_{\geq 1}}) = \text{ord}_2(k_{\geq 1} + I_j^{<k_{\geq 1}} + m + 1)$$

holds, which implies (3.8) is true.

Case 8: $k \in I_i = 1?\alpha$ and $I_j \in 1?\beta$. By the definition of $\mathcal{U}_{2m+1}$, $I_i = 1\alpha \in \mathcal{U}_m$, $I_j = 1\beta \in \mathcal{U}_m$, and $(1, k_{\geq 2}) \in I_i$. The left hand side of (3.8) is

$$\text{ord}_2(k - I_j^{<k}) = \text{ord}_2((1, k_1, k_{\geq 2}) - (1, ?, \alpha)^{<k})$$

$$= \text{ord}_2((1, k_1, k_{\geq 2}) - (1, 1 - k_1, \alpha)^{<k}) + \text{ord}_2((1, k_1, k_{\geq 2}) - (1, k_1, \alpha)^{<k})$$

$$= 2|\alpha^{<k_{\geq 2}}| + \text{ord}_2((1, k_{\geq 2}) - I_j^{<(1, k_{\geq 2})}).$$

The right hand side of (3.8) is

$$\text{ord}_2(k + I_j^{<k} + 2m + 2) = \text{ord}_2((1, k_1, k_{\geq 2}) + (1, ?, \alpha)^{<k} + (0, m + 1))$$

$$= \text{ord}_2((1, k_1, k_{\geq 2}) + (1, k_1, \alpha)^{<k} + (0, m + 1)) + \text{ord}_2((1, k_1, k_{\geq 2}) + (1, 1 - k_1, \alpha)^{<k} + (0, m + 1))$$

$$= 2|\alpha^{<k_{\geq 2}}| + \text{ord}_2((1, k_1, k_{\geq 2}) + (1 - k_1, \alpha^{<k_{\geq 2}}) + m + 2)$$

$$= 2|\alpha^{<k_{\geq 2}}| + \text{ord}_2((1, k_{\geq 2}) + (1, \alpha^{<k_{\geq 2}}) + m + 1).$$

By induction hypothesis that $\mathcal{U}_m$ is $(m, t)$-sound, and $1\alpha \in \mathcal{U}_m$,

$$\text{ord}_2((1, k_{\geq 2}) - I_j^{<(1, k_{\geq 2})}) = \text{ord}_2((1, k_{\geq 2}) + (1, \alpha^{<k_{\geq 2}}) + m + 1),$$

for any $(1, k_{\geq 2}) \notin (1, \alpha)$, which proves (3.8).
3.3. PROOF FOR THE CASE $\text{CHAR} (\mathbb{F}) = 2$

**Case 9:** \( k \in I = 01\alpha \) and \( I_j = 01\beta \). By the definition of \( U_{2m+1} \), \( (1, k_{\geq 2}) \in I'_i = 1\alpha \in U_m \), and \( I'_j = 1\beta \in U_m \). The left hand side of (3.8) is

\[
\text{ord}_2(k - I^<_k)
\]

\[
= \text{ord}_2((0, 1, k_{\geq 2}) - (0, 1, \beta)^<_k)
\]

\[
= |\beta^<_k| + \text{ord}_2((1, k_{\geq 2}) - (1, \beta)^{\leq (1, k_{\geq 2})}),
\]

and the right hand side of (3.8) is

\[
\text{ord}_2(k + I^<_k + 2m + 2)
\]

\[
= \text{ord}_2((0, 1, k_{\geq 2}) + (0, 1, \beta)^<_k + (0, m + 1))
\]

\[
= |\beta^<_k| + \text{ord}_2((1, k_{\geq 2}) + (1, \beta)^{\leq (1, k_{\geq 2})} + m + 1).
\]

By induction hypothesis that \( U_m \) is \((m, t)-\text{sound}\) partition and \((1, \beta) \in U_m\),

\[
\text{ord}_2((1, k_{\geq 2}) - (1, \beta)^{\leq (1, k_{\geq 2})}) = (1, \beta)^{\leq (1, k_{\geq 2})} + m + 1
\]

holds for any \((1, k_{\geq 2}) > 0\), which implies (3.8) is true in this case.

We have proved that \( U_{2m+1} \) is \((2m + 1, t)-\text{sound}\) for any \( t \), and let’s prove it’s \((2m + 1, t)-\text{complete}\), that is, by Proposition 3.2.3

(3.9) \[
\text{ord}_2(k - I^<_k) < \text{ord}_2(k + I^<_k + m + 1)
\]

holds for any \( k \in I \in U_{2m+1} \) and \( |I^<_k| > 0 \). Again, we do it by case analysis.

**Case 1:** \( k \in I = 00\alpha \). By definition, \( I' = 0\alpha \in U_m \) and \( k_{\geq 1} \in I' \). The left hand side of (3.9) is

\[
\text{ord}_2(k - I^<_k)
\]

\[
= \text{ord}_2((0, k_{\geq 1}) - (0, I^<_k^{<k_{\geq 1}}))
\]

\[
= |I^<_k^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} - I^<_k^{<k_{\geq 1}}),
\]

and the right hand side of (3.9) is

\[
\text{ord}_2(k + I^<_k + 2m + 2)
\]

\[
= \text{ord}_2((0, k_{\geq 1}) + (0, I^<_k^{<k_{\geq 1}}) + (0, m + 1))
\]

\[
= |I^<_k^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} + I^<_k^{<k_{\geq 1}} + m + 1).
\]

By induction hypothesis that \( U_m \) is complete, then

\[
\text{ord}_2(k_{\geq 1} - I^<_k^{<k_{\geq 1}}) < \text{ord}_2(k_{\geq 1} + I^<_k^{<k_{\geq 1}} + m + 1)
\]

holds if \( I^<_k^{<k_{\geq 1}} \) is nonempty, which is nonempty for \( I^<_k \) is nonempty. This implies (3.9).
Recalling the definition of $U$

3.3.5 From $U$

implies (3.9) is true.

By induction hypothesis that

and the right hand side of (3.9) is

is nonempty or

then

and the right hand side of (3.9) is

Case 2: $k \in I = 1\alpha$. By definition, $I' = 1\alpha \in U_m$ and $(1, k_{\geq 2}) \in I'$. The left hand side of (3.9) is

\[ \text{ord}_2(k - I^{<k}) = \text{ord}_2((1, k_1, k_{\geq 2}) - (1, ?, \alpha)^{<k}) \]

\[ = \text{ord}_2((1, k_1, k_{\geq 2}) - (1, 1 - k_1, \alpha)^{<k}) + \text{ord}_2((1, k_1, k_{\geq 2}) - (1, k_1, \alpha)^{<k}) \]

\[ = 2|\alpha^{<k_{\geq 2}}| + \delta_{k, 1} + \text{ord}_2((1, k_{\geq 2}) - (1, \alpha^{<k_{\geq 2}})), \]

and the right hand side of (3.9) is

\[ \text{ord}_2(k + I^{<k} + 2m + 2) = \text{ord}_2((1, k_1, k_{\geq 2}) + (1, ?, \alpha)^{<k} + (0, m + 1)) \]

\[ = \text{ord}_2((1, k_1, k_{\geq 2}) + (1, k_1, \alpha)^{<k} + (0, m + 1)) + \text{ord}_2((1, k_1, k_{\geq 2}) + (1, 1 - k_1, \alpha)^{<k} + (0, m + 1)) + \text{ord}_2((1, k_1, k_{\geq 2}) + (1, \alpha^{<k_{\geq 2}}) + m + 1). \]

By induction hypothesis that $U_m$ is $(m, t)$-complete, and $(1, k_{\geq 2}) \in I' \in U_m$, then

\[ \text{ord}_2((1, k_{\geq 2}) - (1, \alpha^{<k_{\geq 2}})) < \text{ord}_2((1, k_{\geq 2}) + (1, \alpha^{<k_{\geq 2}}) + m + 1) \]

holds for any $(1, \alpha)^{<k(1, k_{\geq 2})}$ nonempty. If $I^{<k}$ is nonempty, then either $(1, \alpha)^{<k(1, k_{\geq 2})}$ is nonempty or $k_1 = 1$, in both case, inequality (3.9) holds.

Case 3: $k \in I = 01\alpha$. By definition, $I' = 1\alpha \in U_m$ and $k_{\geq 1} \in I'$. The left hand side of (3.9) is

\[ \text{ord}_2(k - I^{<k}) = \text{ord}_2((0, k_{\geq 1}) - (0, I')^{<k}) \]

\[ = |I'^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} - I'^{<k_{\geq 1}}) \]

and the right hand side of (3.9) is

\[ \text{ord}_2(k + I^{<k} + 2m + 2) = \text{ord}_2((0, k_{\geq 1}) + (0, I')^{<k} + (0, m + 1)) \]

\[ = |I'^{<k_{\geq 1}}| + \text{ord}_2(k_{\geq 1} + I'^{<k_{\geq 1}} + m + 1) \]

By induction hypothesis that $U_m$ is $(m, t)$-complete, and $k_{\geq 1} \in I' \in U_m$, then

\[ \text{ord}_2(k_{\geq 1} - I'^{<k_{\geq 1}}) < \text{ord}_2(k_{\geq 1} + I'^{<k_{\geq 1}} + m + 1) \]

holds for any nonempty $I'^{<k_{\geq 1}}$, which is nonempty since $I^{<k}$ is nonempty, which implies (3.9) is true.

3.3.5 From $U_m$ to $U_{2^m+1}$, $m$ odd

Recalling the definition of $U_{2^m+1}$, $m$ odd, and $e > 1$,

\[ U_{2^m+1} = \bigcup_{\alpha \in U_m} \bigcup_{i=0}^{e-1} (1^i \alpha^{e-1-i}) \cup \bigcup_{\alpha \in U_{m+1}} \{1^e \alpha\}. \]
First, let’s prove $U_{2^{m+1}}$ is $(2^m+1,t)$-sound for any $t$, that is, by Proposition 3.2.2, we need to prove

\[(3.10) \quad \text{ord}_2(k - I_j^{<k}) = \text{ord}_2(k + I_j^{<k} + 2^m + 2)\]

holds for all $k \notin I \in U_{2^{m+1}}$. Again, we prove by case analysis, according to the pattern of $k$ and $I$.

**Case 1:** $k \in I_i = 1^e \alpha$, $I_j = 1^t 0^{e-1-t} \beta$. Then, the left hand side of (3.10) is

\[
\text{ord}_2(k - I_j^{<k}) = \text{ord}_2((1^e, k_{\geq e}) - (1^t, 0, \beta^e)_{<k}) = t|\beta|_{<k_{\geq e}}.
\]

The right hand side of (3.10) is

\[
\text{ord}_2(k + I_j^{<k} + 2^m + 2) = \text{ord}_2((1^e, k_{\geq e}) + (1^t, 0, \beta^e)_{<k} + 2^m + 2) = t|\beta|_{<k_{\geq e}}.
\]

which equals the left hand side.

**Case 2:** $k \in I_i = 1^e 0^{e-1-t} \alpha$, $I_j = 1^t \beta$. Similar to case 1, and both the left hand side and right hand side of (3.10) is $s|\beta|_{<k_{\geq e}}$.

**Case 3:** $k \in I_i = 1^e \alpha$, $I_j = 1^t \beta$. By the definition of $U_{2^{m+1}}$, $\alpha \in U_{m+1}$ and $\beta \in U_{m+1}$. The left hand side of (3.10) is

\[
\text{ord}_2(k - I_j^{<k}) = \text{ord}_2((1^e, k_{\geq e}) - (1^t, 0, \beta^e)_{<k}) = e|\beta|_{<k_{\geq e}} + \text{ord}_2(k_{\geq e} - \beta|_{<k_{\geq e}}),
\]

and the right hand side of (3.10) is

\[
\text{ord}_2(k + I_j^{<k} + 2^m + 2) = \text{ord}_2((1^e, k_{\geq e}) + (1^t, \beta^e)_{<k} + (0^e, m) + (0, 1)) = e|\beta|_{<k_{\geq e}} + \text{ord}_2(k_{\geq e} + \beta|_{<k_{\geq e}} + m + 2).
\]

By induction hypothesis that $U_{m+1}$ is $(m + 1, t)$-sound for any $t$ and $\beta \in U_{m+1}$,

\[
\text{ord}_2(k_{\geq e} - \beta|_{<k_{\geq e}}) = \text{ord}_2(k_{\geq e} + \beta|_{<k_{\geq e}} + m + 2)
\]

holds, which proves (3.10).

**Case 4:** $k \in I_i = 1^e 0^{e-1-t} \alpha$, $I_j = 1^t 0^{t-1-t} \beta$. If $s \neq t$, then the left hand side of (3.10) is

\[
\text{ord}_2(k - I_j^{<k}) = \text{ord}_2((1^e, 0, k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) - (1^t, 0, \beta^{e-1-t})_{<k}) = \min(s, t)|I_j^{<k}|
\]
and the right hand side of (3.10) is

\[
\text{ord}_2(k + I_j^{<k} + 2^e m + 2)
\]

\[
= \text{ord}_2(1^e, 0, k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) + (1^e, 0, ?^{e-1-s}, \beta^{<k} + (0^e, m) + (0, 1))
\]

\[
= \text{min}(s, t)|I_j^{<k}|
\]

which equals the left hand side.

If \( s = t \), then \( \alpha \neq \beta \). The left hand side of (3.10) is

\[
\text{ord}_2(k - I_j^{<k})
\]

\[
= \text{ord}_2((1^e, 0, k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) - (1^e, 0, ?^{e-1-s}, \beta^{<k}))
\]

\[
= (s + 1)|I_j^{<k}| + \text{ord}_2((k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) - (\beta^{<k_{s+1}})
\]

\[
= (s + 1)|I_j^{<k}| + |\beta^{<k_{\geq e}}| \left( \sum_{l=0}^{e-s-2} 2^{e-s-2-l} + (e - s - 1) \right)
\]

\[
\text{ord}_2(k_{\geq e} - \beta^{<k_{\geq e}})
\]

and the right hand side of (3.10) is

\[
\text{ord}_2(k + I_j^{<k} + 2^e m + 2)
\]

\[
= \text{ord}_2((1^e, 0, k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) + (1^e, 0, ?^{e-1-s}, \beta^{<k}) + (0^e, m) + (0, 1))
\]

\[
= (s + 1)|I_j^{<k}| + \text{ord}_2((k_{s+1}, \ldots, k_{e-1}, k_{\geq e}) + (\beta^{<k_{s+1}}) + (0^e, m) + (0, 1))
\]

\[
= (s + 1)|I_j^{<k}| + |\beta^{<k_{\geq e}}| \left( \sum_{l=0}^{e-s-2} 2^{e-s-2-l} + (e - s - 1) \right)
\]

\[
\text{ord}_2(k_{\geq e} + \beta^{<k_{\geq e}} + m + 1).
\]

By induction hypothesis that \( U_m \) is \((m, t)\)-sound for any \( t \), and \( I_j' = \beta \in U_m \), we have

\[
\text{ord}_2(k_{\geq e} - \beta^{<k_{\geq e}}) = \text{ord}_2(k_{\geq e} + \beta^{<k_{\geq e}} + m + 1)
\]

for any \( k_{\geq e} \), which implies (3.10).

We have proved that \( U_{2^e m + 1} \) is \((2^e m + 1, t)\)-sound for any \( t \), and now let’s prove \( U_{2^e m + 1} \) is \((2^e m + 1, t)\)-complete, that is,

(3.11) \[
\text{ord}_2(k - I^{<k}) < \text{ord}_2(k + I^{<k} + 2^e m + 2)
\]

holds for any \( 0 < k \in I \) and \(|I^{<k}| > 0\).

**Case 1:** \( k \in I = 1^e \alpha \in U_{2^e m + 1} \). By the definition of \( U_{2^e m + 1} \), we know \( \alpha \in U_{m+1} \). The left hand side of (3.11) is

\[
\text{ord}_2(k - I^{<k})
\]

\[
= \text{ord}_2((1^e, k_{\geq e}) - (1^e, \alpha))
\]

\[
= e|I^{<k}| + \text{ord}_2(k_{\geq e} - \alpha^{<k_{\geq e}}),
\]
and the right hand side of (3.11) is
\[ \text{ord}_2(k + I^{<k} + 2^e m + 2) = \text{ord}_2((1^e, k_{ge}) + (1^e, \alpha) + (0^e, m) + (0, 1)) \]
\[ = e|I^{<k}| + \text{ord}_2(k_{ge} + \alpha^{<k_{ge}} + m + 2), \]
which is greater than left hand side by the induction hypothesis that \( U \) and the right hand side of (3.11) is complete, and \( \alpha \in U_{m+1} \), thus
\[ \text{ord}_2(k_{ge} - \alpha^{<k_{ge}}) < \text{ord}_2(k_{ge} + \alpha^{<k_{ge}} + m + 2). \]
holds for any \( \alpha^{<k_{ge}} \) nonempty, which is true because \( I^{<k} \) is nonempty.

**Case 2**: \( k \in I = 1^00^{e-1-s}\alpha \in U_{2^em+1} \). By the definition of \( U_{2^em+1} \), \( \alpha \in U_m \).

The left hand side of (3.11) is
\[ \text{ord}_2(k - I^{<k}) = \text{ord}_2((1^s, 0, k_{s+1}, \ldots, k_{e-1}, k_{ge}) - (1^s, 0, \alpha^{<k_{ge}}, \alpha^{<k_{ge}})) \]
\[ = (s + 1)|I^{<k}| + \text{ord}_2((k', k_{ge}) - (\alpha^{<k_{ge}}, \alpha^{<k_{ge}})) + \text{ord}_2((k', k_{ge}) - (\alpha^{<k_{ge}}, k_{ge})), \]
where \( k' = (k_{s+1}, \ldots, k_{e-1}) \). The right hand side of (3.11) is
\[ \text{ord}_2(k + I^{<k} + 2^e m + 2) = \text{ord}_2((1^s, 0, k_{s+1}, \ldots, k_{e-1}, k_{ge}) + (1^s, 0, \alpha^{<k_{ge}}, \alpha^{<k_{ge}}) + (0^e, m) + (0, 1)) \]
\[ = (s + 1)|I^{<k}| + \text{ord}_2((k', k_{ge}) + (\alpha^{<k_{ge}}, \alpha^{<k_{ge}}) + (0^e, m) + 1) \]
\[ + \text{ord}_2((k', k_{ge}) - (\alpha^{<k_{ge}}, k_{ge}) + (0^e, m) + 1). \]
Comparing the left hand side and right hand side, if we could prove
\[ \text{ord}_2((k', k_{ge}) - (\alpha^{<k_{ge}}, \alpha^{<k_{ge}})) \]
\[ \leq \text{ord}_2((k', k_{ge}) + (\alpha^{<k_{ge}}, \alpha^{<k_{ge}}) + (0^e, m) + 1) \]
(3.12)
and
\[ \text{ord}_2((k', k_{ge}) - (\alpha^{<k_{ge}}, k_{ge})) \]
\[ \leq \text{ord}_2((k', k_{ge}) + (\alpha^{<k_{ge}}, k_{ge}) + (0^e, m) + 1), \]
(3.13)
and the equalities in (3.12) and (3.13) can not hold at the same time, we are done.

For (3.12), the left hand side is
\[ |\alpha^{<k_{ge}}| \left( \sum_{l=0}^{e-s-2} l2^{e-s-2-l} + (e - s - 1) \right) + \text{ord}_2(k_{ge} + \alpha^{<k_{ge}} + m + 1), \]
and the right hand side is
\[ |\alpha^{<k_s}| \left( e^{s-2} - \sum_{l=0}^{e-s-2} l^2 e^{s-2-l} + (e - s - 1) \right) + \text{ord}_2(k_{\geq e} - \alpha^{<k_s}). \]

By induction hypothesis that \( \alpha \in U_m \), we have
\[ \text{ord}_2(\alpha^{<k_s} + m + 1) \geq \text{ord}_2(k_{\geq e} - \alpha^{<k_s}), \]
and the equality is strict if \( |\alpha^{<k_s}| > 0 \).

For (3.13), the left hand side is
\[ \sum_{x=0}^{k'-1} \text{ord}_2(k' - x) = \text{ord}_2(k!), \]
and the right hand side is lower bounded by
\[ \sum_{x=0}^{k'-1} \text{ord}_2(k' + x + 1) = \text{ord}_2((2k')!/k'!). \]
Thus, (3.13) is true, and the equality holds only if \( k' = 0 \).

If both \( k' = 0 \) and \( |\alpha^{<k_s}| = 0 \), then \( |I^{<k_s}| = 0 \), which is a contradiction.
Therefore, the equalities in (3.12) and (3.13) cannot both hold.

### 3.4 Proof for the Case \( \text{char}(\mathbb{F}) > 2 \)

It’s a little surprising that the case \( \text{char}(\mathbb{F}) > 2 \) is simpler than the case \( \text{char}(\mathbb{F}) = 2 \). The idea is similar: define the complete partition recursively and prove by induction.

Let
\[ U_0 = \{ I_0, I_1, \ldots \}, \]
where \( I_i = \{ j \in \mathbb{N} : v_p(j) = i \} \). Function \( v_p : \mathbb{N} \to \mathbb{N} \) is defined as follows,
\[ v_p(x) = \sum_{i : x_i \leq (p-1)/2} x_i \left( \frac{p+1}{2} \right)^i + \sum_{i : x_i > (p-1)/2} (p - x_i - 1) \left( \frac{p+1}{2} \right)^i, \]
where \( x = (x_0, x_1, x_2, \ldots) \) is the \( p \)-adic expansion.

For convenience, notation \([a, b]\) denotes a pattern which is either \( a \) or \( b \).
Again, our \( m \)-sound complete partition \( U_m \) is defined recursively by patterns.

Let
\[ U_1 = \bigcup_{\alpha \in U_0} \bigcup_{i \geq 0} \bigcup_{0 \leq j \leq (p-3)/2} \{(p-1)^i[j, p-j-2]\alpha\}, \]
and
\[ U_{m+r} = \bigcup_{\alpha \in U_m} \bigcup_{i+j \geq 0} \{[i, j]\alpha\} \bigcup \bigcup_{\alpha \in U_{m+1}} \bigcup_{i+j \geq 0} \{[i, j+1]\alpha\} \]
for \( m \geq 0 \) and \( 0 \leq r \leq p - 1 \).
3.4. PROOF FOR THE CASE CHAR($\mathbb{F}$) > 2

3.4.1 Partition $U_0$

For convenience, let $\overline{t} = \{i, p - 1 - i\}$. Then any set in $U_0$ can be described by pattern $(i_0, i_1, \ldots)$ for some $i_0, i_1, \ldots \in \{0, 1, \ldots, (p-1)/2\}$.

First, let’s prove that $U_0$ is $(0, t)$-sound for any $t$, that is, by Proposition 3.2.2, for any $k \not\in I \subseteq U_0$,

$$\text{ord}_p(k - I^{<k}) = \text{ord}_p(k + I^{<k} + 1).$$

Assume $I = (\overline{i_0}, \overline{i_1}, \ldots)$. Since $k \not\in I$, there exists the minimal index $s$ such that $k_s \not\in \overline{i_s}$. Then

$$\text{ord}_p(k - I^{<k}) = \text{ord}_p((k_0, k_1, \ldots) - (\overline{i_0}, \overline{i_1}, \ldots)^{<k}) = \text{ord}_p((k_0, \ldots, k_{s-1}, k_s, k_{s+1}, \ldots) - (\overline{i_0}, \ldots, \overline{i_{s-1}}, \overline{i_s}, \overline{i_{s+1}}, \ldots)^{<k^{<s}})) = \left|\overline{i_s^{<k^{<s}-1}}\right| \left(\sum_{l=1}^{s-1} p^l - t + s\right),$$

and

$$\text{ord}_p(k + I^{<k} + 1) = \text{ord}_p((k_0, k_1, \ldots) + (\overline{i_0}, \overline{i_1}, \ldots)^{<k} + 1) = \text{ord}_p((k_0, \ldots, k_{s-1}, k_s, k_{s+1}, \ldots) + (\overline{i_0}, \ldots, \overline{i_{s-1}}, \overline{i_s}, \overline{i_{s+1}}, \ldots)^{<k^{<s} + 1}) = \left|\overline{i_s^{<k^{<s}-1}}\right| \left(\sum_{l=1}^{s-1} p^l - t + s\right),$$

which proves (3.14).

Let’s prove that $U_0$ is $(0, t)$-complete for any $t$. By Proposition 3.2.3, we shall prove

$$\text{ord}_p(k - I^{<k}) < \text{ord}_p(k + I^{<k} + 2)$$

for any $k \in I$ and $|I^{<k}| > 0$.

Let $k \in I \subseteq U_0$. Cut the $p$-adic expansion of $k$ into consecutive pieces $k = (k_1, k_2, \ldots, k_m)$ or $k = (k_1, k_2, \ldots, k_m, l_m)$, where $k_i$ is consecutive bits of $k$ such that none of them equals $(p - 1)/2$; $l_i$ is consecutive bits of $(p - 1)/2$. Without loss of generality, assume $k = (k_1, k_2, \ldots, k_m)$.

If $i \in I$ runs over from 0 to $k$, and $i = (i_1, i_1, \ldots, i_m)$ as we did for $k$, that is, $i_1$ has the same length as $k_1$, etc, then $i < k$ is equivalent to $i_m < k_m$ or $(i_m = k_m, i_m - 1 < k_m - 1)$, or $(i_m = k_m, i_m - 1 = k_m - 1, i_{m-2} < k_{m-2}, \ldots$. Therefore, if we can prove for $m = 1$ or $m = 2$, we are done.

If $m = 1$, i.e., $k = (k_1)$, where $k_1$ consists of bits $j$ or $p - 2 - j$. Define $\phi$ be the map mapping $j$ to 0 and $p - 2 - j$ to 1, and then read it as a binary number, then

$$\text{ord}_p(k - I^{<k}) = \sum_{0 \leq x < k} \text{ord}_2(\phi(k) - x) = \text{ord}_2(\phi(k)!),$$
and
\[
\text{ord}_p(k + I^{<k} + 2) = \sum_{0 \leq x < k} \text{ord}_2(\phi(k) + x + 1) = \text{ord}_2((2\phi(k))!/\phi(k)!).
\]

Since \(\text{ord}_2((2\phi(k))!/\phi(k)! > \text{ord}_2(\phi(k)!)) \) for all \(\phi(k) > 0\), we are done.

If \(m = 2\),
\[
\sum_{i \in I^{<k}} \text{ord}_p(k - i) = \sum_{i \in I^{<k}} \text{ord}_p((k_1, l_1, k_2) - (i_1, l_1, i_2)) = \sum_{i_1 \neq k_1} \text{ord}_p(k_1 - i_1) \phi(k_2) + \sum_{i_2 < k_2} \text{ord}_p((k_1, l_1, k_2) - (k_1, l_1, i_2)) = \sum_{i_1 \neq k_1} \text{ord}_p(k_1 - i_1) \phi(k_2) + \sum_{i_2 < k_2} (\text{ord}_p(k_2 - i_2) + |k_1| + |l_1|),
\]
and, let \(k'_1\) denote the conjugate of \(k_1\) by flipping every bit in \(p\)-adic expansion to the other choice,
\[
\sum_{i \in I^{<k}} \text{ord}_p(k + i + 2) = \sum_{i \in I^{<k}} \text{ord}_p((k_1, l_1, k_2) + (i_1, l_1, i_2) + 2) = \sum_{i_1 \neq k'_1} \text{ord}_p(k_1 + i_1 + 2) \phi(k_2) + \sum_{i_2 < k_2} \text{ord}_p((k_1, l_1, k_2) + (k_1, l_1, i_2) + 2) = \sum_{i_1 \neq k'_1} \text{ord}_p(k_1 + i_1 + 2) \phi(k_2) + \sum_{i_2 < k_2} (\text{ord}_p(k_2 + i_2 + 2) + |k_1| + |l_1|),
\]
where \(\sum_{i_2 < k_2} \text{ord}_p(k_2 + i_2 + 2) > \sum_{i_2 < k_2} \text{ord}_p(k_2 - i_2)\) as long as \(\phi(k_2) > 0\). It’s easy to see
\[
\sum_{i_1 \neq k'_1} \text{ord}_p(k_1 + i_1 + 2) = \sum_{i_1 \neq k_1} \text{ord}_p(k_1 - i_1),
\]
because the sum runs over all numbers in \(I_1\) except 0. If \(\phi(k_2) = 0\), then it can be reduced to case 1.

3.4.2 Partition \(U_1\)
First, let’s prove that \(U_1\) is \((1, t)\)-sound for every \(t\), that is, by Proposition 3.2.2, one needs to prove
\[
\text{ord}_p(k - I^{<k}) = \text{ord}_p(k + I^{<k} + 2)
\]
3.4. PROOF FOR THE CASE $\text{CHAR}(\mathbb{F}) > 2$

holds for any $k \not\in I \in \mathcal{U}_1$. Assume $k \in (p - 1)^i[j, p - 2 - j] \alpha$, and $I = (p - 1)^i[j', p - 2 - j'] \beta$, where $\alpha, \beta \in \mathcal{U}_0$.

If $i \neq i'$,

$$\text{ord}_p(k - I^{<k}) = \min(i, j)|I^{<k}| = \text{ord}_p(k + I^{<k} + 2),$$

which implies (3.15).

If $i = i'$ and $j \neq j'$,

$$\text{ord}_p(k - I^{<k}) = i|I^{<k}| = \text{ord}_p(k + I^{<k} + 2),$$

which also implies (3.15).

If $i = i'$ and $j = j'$, by assumption that $k \not\in I$, we have $\alpha \neq \beta$. Then,

$$\text{ord}_p(k - I^{<k}) = (i + 1)|\beta^{<k_{z+1}}| + \text{ord}_p(k_{z+1} - \beta^{<k_{z+1}}),$$

$$\text{ord}_p(k + I^{<k} + 2) = (i + 1)|\beta^{<k_{z+1}}| + \text{ord}_p(k_{z+1} + \beta^{<k_{z+1}} + 1).$$

Since $\mathcal{U}_0$ is $(0, t)$-sound for any $t$, and $k \not\in I \in \mathcal{U}_0$, we have

$$\text{ord}_p(k_{z+1} - \beta^{<k_{z+1}}) = \text{ord}_p(k_{z+1} + \beta^{<k_{z+1}} + 1),$$

which implies (3.15).

Now, let’s prove $\mathcal{U}_1$ is $(1, t)$-complete for any $t$, that is, by Proposition 3.2.3, one needs to prove

(3.16) $$\text{ord}_p(k - I^{<k}) < \text{ord}_p(k + I^{<k} + 2)$$

for any $k \in I \in \mathcal{U}_1$ with $|I^{<k}| > 0$. Assume $I = (p - 1)^i[j, p - 2 - j] \alpha$, where $\alpha \in \mathcal{U}_0$. Let’s compute the left hand side and right hand side of (3.16).

$$\text{ord}_p(k - I^{<k}) = \text{ord}_p((p - 1)^i, k_i, k_{z+1}) - ((p - 1)^i, [j, p - 2 - j], \alpha)^{<k}$$

$$= (2i + 1)|\alpha^{<k_{z+1}}| + \delta_{k_i, p - 2 - j}i + \text{ord}_p(k_{z+1} - \alpha^{<k_{z+1}})$$

$$\text{ord}_p(k + I^{<k} + 2) = \text{ord}_p((p - 1)^i, k_i, k_{z+1} + 1) + ((p - 1)^i, [j, p - 2 - j], \alpha)^{<k} + 2$$

$$\geq (2i + 1)|\alpha^{<k_{z+1}}| + \delta_{k_i, p - 2 - j}(i + 1) + \text{ord}_p(k_{z+1} + \alpha^{<k_{z+1}} + 1).$$

Since $\mathcal{U}_0$ is complete, we have

$$\text{ord}_p(k_{z+1} - \alpha^{<k_{z+1}}) < \text{ord}_p(k_{z+1} + \alpha^{<k_{z+1}} + 1)$$

for all $|\alpha^{<k_{z+1}}| > 0$, which implies (3.16). If $|\alpha^{<k_{z+1}}| = 0$, the equality holds. By the assumption that $I^{<k}$ is nonempty, $k_i = p - 2 - j$, then $\delta_{k_i, p - 2 - j}(i + 1) > \delta_{k_i, p - 2 - j}i$, which also implies (3.16).
3.4.3 From $U_m$ to $U_{mp+r}$

Recall the definition of $U_{mp+r}$, $0 \leq m$, $0 \leq r \leq p - 1$, and $mp + r > 1$,

$$U_{pm+r} = \bigcup_{\alpha \in U_m} \bigcup_{0 \leq i, j \leq p - 1 \atop i + j + r + t \geq 2p} \{[i, j]_{\alpha}\} \cup \bigcup_{\alpha \in U_{mp + r + t}} \bigcup_{0 \leq i, j \leq p - 1 \atop i + j + r + t \geq 2p} \{[i, j]_{\alpha}\}. $$

First, let’s prove that $U_{mp+r}$ is $(mp + r, t)$-sound for any $t$, that is, by Proposition 3.2.2, one needs to prove

$$\ord_p(k - I^{<k}) = \ord_p(k + I^{<k} + mp + r + 1)$$

holds for any $k \notin I \in U_{mp+r+1}$.

Assume $k \in [i, j]_{\alpha}$, and $I = [i^*, j^*]_{\beta}$. Without loss of generality, let’s assume $i = i^*$ and $j = j^*$, because otherwise both the left hand side and right hand side of (3.17) are 0. Let $i + j + r + 1 = bp$, where $b \in \{1, 2\}$, and thus $\alpha, \beta \in U_{m-b+1}$. The left hand side of (3.17) is

$$\ord_p(k - I^{<k}) = \ord_p((k_0, k_{\geq 1}) - ([i, j], \beta)^{<k})$$

$$\ord_p((k_0, k_{\geq 1}) - (k_0, \beta^{<k_{\geq 1}}))$$

$$|\beta^{<k_{\geq 1}}| + \ord_p(k_{\geq 1} - \beta^{<k_{\geq 1}}),$$

and the right hand side of (3.17) is

$$\ord_p(k + I^{<k} + pm + r + 1) = \ord_p((k_0, k_{\geq 1}) + ([i, j], \beta)^{<k} + pm + r + 1)$$

$$\ord_p((k_0, k_{\geq 1}) + (bp - r - 1 - k_0, \beta^{<k_{\geq 1}}) + pm + r + 1)$$

$$|\beta^{<k_{\geq 1}}| + \ord_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b).$$

By the assumption that $U_{m-b-1}$ is $(m + b - 1, t)$-sound for any $t$, we have

$$\ord_p(k_{\geq 1} - \beta^{<k_{\geq 1}}) = \ord_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b),$$

which implies (3.17).

Now, let’s prove $U_{mp+r}$ is $(mp + r, t)$-complete for any $t$, that is, by Proposition 3.2.3, one needs to prove

$$\ord_p(k - I^{<k}) < \ord_p(k + I^{<k} + mp + r + 1)$$

holds for any $k \in I \in U_{mp+r+1}$ with $|I^{<k}| > 0$. Assume $k \in I = [i, j]_{\alpha}$, where $i < j$, $i + j + r + 1 = bp$, $b \in \{1, 2\}$, and $\alpha \in U_{m-b+1}$. The left hand side of (3.18) is

$$\ord_p(k - I^{<k}) = |\beta^{<k_{\geq 1}}| + \ord_p(k_{\geq 1} - \beta^{<k_{\geq 1}})$$

and the right hand side of (3.18) is

$$\ord_p(k + I^{<k} + pm + r + 1) = |I^{<k}| + \ord_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b).$$

Without loss of generality, let’s assume $i = i^*$ and $j = j^*$, because otherwise both the left hand side and right hand side of (3.18) are 0. Let $i + j + r + 1 = bp$, where $b \in \{1, 2\}$, and thus $\alpha, \beta \in U_{m-b+1}$. The left hand side of (3.18) is

$$\ord_p(k - I^{<k}) = \ord_p((k_0, k_{\geq 1}) - ([i, j], \beta)^{<k})$$

$$\ord_p((k_0, k_{\geq 1}) - (k_0, \beta^{<k_{\geq 1}}))$$

$$|\beta^{<k_{\geq 1}}| + \ord_p(k_{\geq 1} - \beta^{<k_{\geq 1}}),$$

and the right hand side of (3.18) is

$$\ord_p(k + I^{<k} + pm + r + 1) = \ord_p((k_0, k_{\geq 1}) + ([i, j], \beta)^{<k} + pm + r + 1)$$

$$\ord_p((k_0, k_{\geq 1}) + (bp - r - 1 - k_0, \beta^{<k_{\geq 1}}) + pm + r + 1)$$

$$|\beta^{<k_{\geq 1}}| + \ord_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b).$$

By the assumption that $U_{m-b-1}$ is $(m + b - 1, t)$-sound for any $t$, we have

$$\ord_p(k_{\geq 1} - \beta^{<k_{\geq 1}}) = \ord_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b),$$

which implies (3.18).
and the right hand side of (3.17) is

\[
\text{ord}_p(k + I^{<k} + pm + r + 1) = \text{ord}_p((k_0, k_{\geq 1}) + ([i, j], \beta)^{<k} + pm + r + 1) = \text{ord}_p((k_0, k_{\geq 1}) + (bp - r - 1 - k_0, \beta)^{<k} + pm + r + 1) \geq |\beta^{<k_{\geq 1}}| + \text{ord}_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b) + \delta_{k_0,j}.
\]

By the assumption that \(U_{m+b-1}\) is \((m + b - 1, t)\)-complete for any \(t\),

\[
\text{ord}_p(k_{\geq 1} - \beta^{<k_{\geq 1}}) < \text{ord}_p(k_{\geq 1} + \beta^{<k_{\geq 1}} + m + b),
\]

if \(\beta^{<k_{\geq 1}}\) is nonempty, which implies (3.18). If \(|\beta^{<k_{\geq 1}}| = 0\), then by assumption that \(I^{<k}\) is nonempty, we must have \(k_0 = j\), in which (3.18) is also true.
Bibliography


Chapter 4

Appendix

4.1 Proof of Lemma 1.2.6(2)

We need the following well-known fact [20] (also see Chapter 8 of [4]).

**Lemma 4.1.1** (Janson’s inequality). Let \( \Omega \) be a finite set and let \( R \) be a random subset of \( \Omega \) given by
\[
\Pr[r \in R] = p_r,
\]
these events being mutually independent over \( r \in \Omega \). Let \( \{A_i\}_{i \in I} \) be subsets of \( \Omega \), \( I \) a finite index set. Let \( B_i \) be the event \( A_i \subseteq R \). For distinct \( i, j \in I \), we write \( i \sim j \) if \( A_i \cap A_j \neq \emptyset \). Define
\[
\Delta := \sum_{i \sim j} \Pr[B_i \land B_j],
\]
and
\[
\mu := \sum_{i \in I} \Pr[B_i].
\]
Then
\[
\Pr[\bigwedge_{i \in I} \overline{B_i}] \leq e^{-\frac{1}{2} \min\{\mu, \mu^2/\Delta\}}.
\]

**Proof.** (of Lemma 1.2.6(2)) Let \( B = \text{Bal}(P) \). Let \( R \subseteq P \) be the “residual” graph with \( E(R) = E(P) \setminus E(B) \). Let \( G = G(n, n^{-\theta(P)}) \).

Let \( f : V(B) \rightarrow [n] \) be an arbitrary 1-1 function. We will say that “\( G \) has an \( R \)-subgraph extending \( f \)” if there exists a 1-1 function \( g : V(P) \rightarrow [n] \) such that \( g \) extends \( f \) and \( g \) is an embedding of \( R \) into \( G \).

**Claim 4.1.2.** For every fixed function \( f \),
\[
\Pr[G \text{ does not have an } R \text{-subgraph extending } f] \leq \exp(-n^{\Omega(1)}).
\]
We put the proof of the above claim (which is an application of Janson’s inequality) at the end.

Let (*) be the following property: for every 1-1 function $f : V(B) \to [n]$, $G$ has an $R$-subgraph extending $f$.

From the claim, it follows that $G$ has (*) a.a.s. (by a union bound over $< n^{|V(B)|}$ functions $f$).

Finally, note that trivially (*) $\Rightarrow$ “$G$ has a $P$-subgraph iff $G$ has a $B$-subgraph”.

Proof. (of Claim 4.1.2) Let $\theta := \theta(P)$ and $W := V(P) \setminus V(B)$. Given $f : V(B) \to [n]$, let $i$ run over the set $I$ of all injective mappings $W \to [n] \setminus \text{im}(f)$, that is, all potential extensions of $f$. Let $B_i$ denote the event that $i$ is a valid extension, that is, the image of every edge in $E(R)$ appears in $G$. We are going to apply Lemma 4.1.1, and for that we need to show that in the notation of that lemma we have $\mu \geq n^{\Omega(1)}$ and $\mu^2/\Delta \geq n^{\Omega(1)}$.

First, denoting $\ell := |W|$ and $p := \sqrt{n}/\theta(P)$, we have

$$\Pr[B_i] = p^{\ell(R)},$$

and thus

$$\mu = \sum_{i \in I} \Pr[B_i] = \Theta(n^{\ell(R)}p^{\ell(R)}) = \Theta(n^{v(P) - v(B)} \cdot n^{\theta_{B}(E(B)) - \theta_{E(B)}}) = \Theta(n^{v(P) - \theta_{E}(P)}).$$

Since $P$ is imbalanced (otherwise there is nothing to prove), $v(P) > \theta_{E}(P)$ and the first necessary fact $\mu \geq n^{\Omega(1)}$ follows.

Let us now turn our attention to $\Delta$. For $i, j \in I$, we call $|\text{im}(i) \cap \text{im}(j)|$ the index of the pair $(i, j)$; note that $i \sim j$ implies that the index of this pair is strictly greater than 0. We split the sum (4.1) according to the index $h$ of the pair $(i, j)$, and we separately estimate each part from the above.

So, let us fix $h > 0$. The overall number of pairs $(i, j)$ of index $h$ is bounded by $O(n^{2h-2})$. For $i \in I$, let $\text{im}(i) \in \mathcal{P}(P) \to [n]$ be its extension by the base function $f$. Then for any fixed pair $(i, j)$ of index $h$ we have

$$\Pr[B_i \cap B_j] = p^{\ell(\text{im}(E(R)) \cup \text{im}(E(R))) - \ell(B)} = p^{\ell(E(R)) - \ell(E(R)) - \ell(B)} \leq p^{\ell(E(R)) - \ell(E(R)) \cdot \ell(B)},$$

where $\text{im}(\hat{E}(R))_{|K}$ is the subgraph induced on the set of vertices $K := \text{im}(i) \cap \text{im}(j)$ of size $v(B) + h$. Since $h > 0$ and $\hat{E}(R))_{|K}$ is isomorphic to an (induced) subgraph of $P$ with $v(B) + h$ vertices, we conclude that $\theta|\text{im}(\hat{E}(R))_{|K}$ is strictly less than $v(B) + h$.

Putting everything together, the contribution of pairs of index $h > 0$ to the sum (4.1) is bounded by

$$O(n^{2h-\ell}) \cdot p^{\ell(E(R)) - n^{v(B) + h - \ell(\Omega(1))}} \cdot n^{-\theta_{E}(B)} \leq \mu^2 \cdot n^{-\Omega(1)}$$

(recall that $\mu = \Theta(n^{\ell(R)})$). The second necessary bound $\mu^2/\Delta \geq n^{\Omega(1)}$ and hence Claim 4.1.2 follow. □