NORTHWESTERN
UNIVERSITY

Computer Science Department

Technical Report
Number: NU-CS-2022-08

May, 2022

Exposition of The Kushilevitz Function

Adam Wathieu

Abstract

This project studies the suboptimal degree upper bound on sensitivity for total Boolean functions. The Kushilevitz Boolean function provides the largest known gap between the sensitivity of a function and its degree: $s(f) = deg(f)^{1.63}$. Creating a function with a larger gap would not only tighten the bound between sensitivity and degree, but also between other complexity measures that are bounded by the Kushilevitz function. This project reasons about creating similar functions which have high sensitivity but low degree by defining well balanced sets. A constrained exhaustive search over Boolean functions with $n = 10$, $deg(f) = 4$, $s(f) = n$ reveals what properties such a Boolean function might have, should one exist. Such a Boolean function would provide a larger gap between the sensitivity and degree: $s(f) = deg(f)^{1.66}$.

Keywords

Boolean Function Complexity Theory, Sensitivity, Degree, Binary Constant Weight Codes

Exposition of The Kushilevitz Function

Northwestern University
Department of Computer Science

An undergraduate senior thesis submitted in partial fulfillment of the honors requirements for the degree of BA in Computer Science at Northwestern University.

Adam Wathieu
Advisor: Dr. Shravas Rao

May 2022

Acknowledgements

Thank you to my advisor Dr. Shravas Rao for being a great mentor and for showing me how to reason about formalizing intuitions and creating proofs. Shravas dealt with me for an entire summer and was patient when I was slow to learn something.

Thank you to Professor Aravindan Vijayaraghavan and Professor Konstantin Makarychev for taking the time to review this thesis and provide feedback.

Thank you to Professor Haoqi Zhang and Professor Sara Sood for organizing the senior thesis program at Northwestern University.

Thank you to Professor Brouwer from Eindhoven University of Technology for responding to my emails and helping me avoid calculating orbits.

Thank you to the Northwestern University WCAS Baker Grant for providing funding for this research project for Summer 2021.

Thank you to the Northwestern University Computer Science Department for giving me the opportunity to work on this project for credit.

Abstract

While it is known that all Boolean function complexity measures are equivalent up to polynomial factors, some exact relationships are unknown and separations still exist. This project focuses on the suboptimal degree upper bound on sensitivity, and begins by reproving the best known separation, $s(f) \leq deg(f)^2$. The Kushilevitz Boolean function provides the largest known gap between the sensitivity of a function and its degree: $s(f) = deg(f)^{1.63}$. Creating a function with a larger gap would not only tighten the bound between sensitivity and degree, but also between other complexity measures that are bounded by the Kushilevitz function. This project reasons about creating similar functions which have high sensitivity but low degree. By defining well balanced sets, this project gives a framework to the properties such a function might possess. Using what is learned about well balanced sets, a constrained exhaustive search over Boolean functions with $n = 10, deg(f) = 4, s(f) = n$ reveals what properties such a Boolean function might have, should one exist. Such a Boolean function would provide a larger gap between the sensitivity and degree: $s(f) = deg(f)^{1.66}$. Using results from the search, a $n = i, deg(f) = 4, s(f) = i$ function is presented for $i \in \{7, 8, 9\}$. This project concludes with a discussion of maximal binary constant weight codes as a source for generating well balanced sets.

Notation

$[n]$	The set $\{1, 2, \ldots, n\}$
$\binom{[n]}{k}$	The set of all subsets $s \subseteq [n]$ with size k.
$\binom{n}{k}$	The Binomial Coefficient indexed at $n, k. \binom{n}{k} = \frac{n!}{k!(n-k)!}$
$f : \{0,1\}^n \to \{0,1\}$	A function that maps elements from $\{0,1\}^n$ to 0 or 1
$\lvert x \rvert$	Hamming weight (number of 1's) of binary string $x \in \{0,1\}^n$.
$f^{=k} = \sum_{\lvert S \rvert = k} \hat{f}(S)\chi_S$	The function f with terms with degree $\neq k$ zeroed out.
$f^{\leq k} = \sum_{\lvert S \rvert \leq k} \hat{f}(S)\chi_S$	The function f with terms with degree $> k$ zeroed out.

Contents

1 Introduction **3**
1.1 Boolean Function Complexity Measures . . . 3
1.2 Sensitivity and Degree . . . 4
1.3 Thesis Outline . . . 4

2 Sensitivity vs Degree **5**
2.1 Sensitivity . . . 5
2.2 Degree . . . 5
2.3 Spectral Sensitivity . . . 6
2.4 Sensitivity vs. Degree Proof . . . 6

3 The Kushilevitz Function **11**
3.1 Definition . . . 11
3.2 Sensitivity and Degree of the Kushilevitz Function . . . 11
3.3 Kushilevitz Output Table . . . 13
3.4 Orbit of the Kushilevitz Function . . . 13

4 Well Balanced Sets **15**
4.1 Introduction . . . 15
4.2 Lower Well Balanced Subsets . . . 15
4.3 Upper Well Balanced Subsets . . . 19
4.4 Upper $\iff$ Lower . . . 23

5 Results of Scan **29**
5.1 Introduction . . . 29
5.2 n=7 . . . 32
5.3 n=8 . . . 36
5.4 n=9 . . . 38
5.5 n=10 . . . 40
5.6 Conclusion . . . 40

6 Creating Well Balanced Sets **41**
6.1 Maximal Binary Constant Weight Codes . . . 41
6.2 A Least Squares Approach . . . 43

7 Conclusion **45**
7.1 Future Work . . . 45

8 Appendix **46**

Chapter 1

Introduction

1.1 Boolean Function Complexity Measures

A fundamental model for computational problems are Boolean functions, a function $f : \{0,1\}^n \to \{0,1\}$ which given some n bit binary string, outputs 0 or 1. Boolean functions are a useful model for decision problems in which the answer is either yes or no. Examples of such functions include *AND*, *Dictator*, and *Parity*. The *AND* Boolean function outputs 1 if all of the input bits are 1, and outputs 0 if any of them are 0. The *Dictator* Boolean function outputs the first bit of the input. The *Parity* function outputs 1 if there are an odd number of 1's in the input and 0 if there are an even number of 1's.

A central measure of complexity for a Boolean function is its query complexity, which quantifies the complexity of the function by analyzing its resource consumption with respect to input use. Specifically, the *Deterministic Query Complexity*, $D(f)$, of a Boolean function f is the minimum number of queries an optimal deterministic algorithm that computes f needs to make on any input string to compute the output.

We can imagine that non-deterministic algorithms that also compute f, such as randomized or quantum algorithms, query the input strings with different behavior. A randomized algorithm might query the input string, or choose to make a random decision, while a quantum algorithm uses quantum queries. Therefore, we also define Randomized, and Quantum Query Complexity, denoted as $R(f)$ and $Q(f)$, respectively, as the minimum number of queries that an optimal randomized, and quantum algorithm that computes f needs to make on any input string in order to compute an output [BE90]. Understanding the relationship between query complexity measures under these different models of computation could help us understand their comparative strengths across problem classes.

To help compare $D(f)$, $R(f)$, and $Q(f)$ to each other, several other measures of Boolean function complexity are used. Such Boolean complexity measures include sensitivity, block sensitivity, degree, and approximate degree, among others. These measures help bound the deterministic, randomized, and quantum query complexities. For example, it has been shown that $D(f) \leq bs(f)deg(f) \leq O(Q(f)^4)$, where $bs(f)$ is the block sensitivity of f, and $deg(f)$ is the degree of f [ABDK$^+$21b]. While it is known that these complexity measures are all polynomially related to each other, some exact relationships are still unknown, and separations still exist [BE90]. Table 1 from [ABDK$^+$21b] depicts the most up-to-date separations between these measures. Tightening some of the gaps between these complexity measures would ultimately lead to stronger guarantees between the query complexities under the different models of computation.

1.2 Sensitivity and Degree

This thesis focuses on the polynomial separation between sensitivity and degree. The sensitivity of a Boolean function, $s(f)$, is the maximum number of bits that can be individually flipped which would change the output bit. For example, the AND function is fully sensitive, with $s(f) = n$, since a bit flip on any of the input bits will change the output of the function for the input $1, 1, \ldots, 1$.

It is known that every Boolean function can be represented as a unique multilinear polynomial [O'D14]. The degree of a function $deg(f)$ is the degree of the unique multilinear polynomial that represents the Boolean function f exactly. The degree of the AND function is $deg(f) = n$, since the polynomial representation of the AND function is $x_1 \cdot x_2 \cdot \cdots \cdot x_n$, where x_i is the value of the ith bit of the input string.

Currently, Huang [Hua19] and Nisan [NS94] have proven the best-known separations between the sensitivity and the degree for all Boolean functions f:

$$deg(f)^{0.5} \leq s(f) \leq deg(f)^2$$

Huang [Hua19] was able to prove that for all Boolean functions, $deg(f)^{0.5} \leq s(f)$, and since the AND-of-ORs Boolean function has $deg(f)^{0.5} = s(f)$, the lower bound is optimal. Nisan [NS94] shows by approximation theory that there does not exist a Boolean function for which $s(f) > deg(f)^2$. It is not known whether there exists a Boolean function for which $s(f) = deg(f)^2$, and the Boolean function with the largest separation so far is the Kushilevitz function, with $s(f) = deg(f)^{1.63}$. To create this separation, Eyal Kushilevitz constructed a Boolean function $f : \{0,1\}^6 \to \{0,1\}$ with $s(f) = 6$ and $deg(f) = 3$, to create a power separation of $\log(6)/\log(3) = 1.63$. This function was found in [HKP10] and can be found in Chapter 3 of this thesis.

With this relationship in mind, this thesis aims to construct and prove a tighter upper bound on sensitivity by degree by constructing a Boolean function with a larger gap between its sensitivity and degree than the Kushilevitz function. Constructing such a Boolean function would lead to a closer indication of the true polynomial separation between sensitivity and degree. This result would also tighten the degree upper bound on communication complexity $C(f)$, randomized communication $RC(f)$, and block sensitivity $bs(f)$, all of which are bounded by the Kushilevitz function [ABDK+21a].

1.3 Thesis Outline

This thesis begins by reproving the best known upper bound on sensitivity by degree in Chapter 2. Then, the Kushilevitz function is reviewed in Chapter 3, and its degree and sensitivity are proved. In Chapter 4, the notion of well balanced subsets are introduced. A subset $S \subseteq \binom{[n]}{m}$ is said to be *lower well balanced* if every subset of $[n]$ of size $i < m$ is included the same amount of times in S. A subset $S \subseteq \binom{[n]}{m}$ is said to *upper well balanced* if elements of S are included in every subset of $[n]$ of size $i > m$ the same amount of times. Using properties of well balanced subsets that are proved in Chapter 4, Chapter 5 reviews an exhaustive search conducted over Boolean functions $f : \{0,1\}^i \to \{0,1\}$ for $i \in \{7, 8, 9, 10\}$ that have upper well balanced degree 3 terms and degree 4 terms and that have $deg(f) = 4, s(f) = i$. Using results from this search, a Boolean function $f : \{0,1\}^7 \to \{0,1\}$ with $s(f) = 7$ and $deg(f) = 4$ is constructed. Chapter 6 reviews strategies to construct upper well balanced subsets, including the use of maximal binary constant weight codes.

Chapter 2

Sensitivity vs Degree

Sensitivity and Degree are two complexity measures for Boolean functions. For any Boolean function f, we know that its sensitivity is less than its degree squared. The following chapter formally defines sensitivity, degree, and reproves the degree upper bound on sensitivity.

2.1 Sensitivity

Let $f : \{0,1\} \to \{0,1\}$ be a Boolean function, and let $x \in \{0,1\}^n$ be a binary string. We say a bit i is sensitive for x if the $f(x) \neq f(x \oplus \mathbb{1}_i)$, where $\mathbb{1}_i$ is the n-bit string that is 1 at bit i and 0 otherwise. The number of sensitive bits for x is called the sensitivity of x, denoted by $s_x(f)$. We define the sensitivity of function f as $s(f) = \max_{x \in \{0,1\}} s_x(f)$.

Example 2.1.1. *Let $f : \{0,1\}^n \to \{0,1\}$ be the AND function on n bits. We note that for $x = \{1,1,\ldots,1\}$, $f(x) = 1$. Furthermore, we note that $f(x) \neq f(x \oplus \mathbb{1}_i)$ for all $i \in \{1,\ldots,n\}$. We see then that $s_x(f) = n$. It follows that the sensitivity of the AND Boolean function is n.*

2.2 Degree

A polynomial $q \in \mathbb{R}[x_1,\ldots,x_n]$ is said to represent the function $f : \{0,1\} \to \{0,1\}$ if $q(x) = f(x)$ for all $x \in \{0,1\}^n$. As mentioned in the introduction, it is known that every Boolean function has a unique multilinear polynomial expansion called its Fourier expansion [O'D14]. The degree of a function f is defined as $deg(f) = \max\{|S| : |\hat{f}(S)| \neq 0\}$, where $\hat{f}(S)$ is the coefficient of S in f.

Example 2.2.1. *Let $f : \{0,1\}^n \to \{0,1\}$ be the AND function on n bits. The Fourier expansion of f is:*

$$f(x_1,\ldots,x_n) = \prod_{i=1}^{n} x_i$$

We see that $|\hat{f}(S)| \neq 0$ only for $S = \{1,\ldots,n\}$. It follows that the degree of the AND function is n.

2.3 Spectral Sensitivity

Spectral Sensitivity is a Boolean function complexity measure which is used to bound sensitivity and degree. Thus we provide the definition here.

Let $f : \{0,1\} \to \{0,1\}$ be a Boolean function. The sensitivity graph of f, $G_f = (V, E)$ is a subgraph of the Boolean hypercube, where $V = \{0,1\}^n$, and $E = \{(x, x \oplus e_i) \in V \times V : i \in [n], f(x) \neq f(x \oplus e_i)\}$. In other words, G_f is the subgraph of the Boolean hypercube such that an edge exists between two vertices v_1 and v_2 if and only if $f(v_1) \neq f(v_2)$. Let A_f be the adjacency matrix of the graph G_f. We define the spectral sensitivity of f as $\lambda(f) = ||A_f||$.

2.4 Sensitivity vs. Degree Proof

The current best known upper bound on sensitivity by degree is reproved below for completeness. We know from [ABDK+21b] that

$$\sqrt{s(f)} \leq \lambda(f) \leq deg(f). \tag{2.1}$$

We reprove the bounds below. We start with the lower bound.

Theorem 2.4.1. *For all total Boolean functions $f : \{0,1\}^n \to \{0,1\}$, $\sqrt{s(f)} \leq \lambda(f)$.*

Proof. Consider any input x with sensitivity $s(f)$. This means x has $s(f)$ neighbors x' on the hypercube such that $f(x) \neq f(x')$. The sensitivity graph restricted to these $s(f) + 1$ vertices is a star graph centered at x. The spectral norm of the adjacency matrix of a star graph on $k + 1$ vertices is $\sqrt{k}$. Note that for any graph, the norm of a subgraph is less than the norm of the original graph, since the adjacency matrix of the subgraph is the adjacency matrix of the original graph with some entries zeroed out. It follows that the spectral norm of A_f is lower bounded by that of the star graph centered at x, so $\sqrt{s(f)} \leq \lambda(f)$.

□

We now prove the upper bound.

Theorem 2.4.2. *For all total Boolean functions $f : \{0,1\}^n \to \{0,1\}$, $\lambda(f) \leq \deg(f)$.*

Proof. The proof is split into 4 lemmas. We begin with the first lemma which expresses $\lambda(f)$ in a way that relates it to a polynomial representing f.

Lemma 2.4.3. *Let $f : \{0,1\}^n \to \{0,1\}$ be a total Boolean function and $g : \{0,1\}^n \to \{-1,1\}$ be defined as $g = 1-2f$. Let $diag(g)$ be the diagonal matrix such that $diag(g)_{xx} = g(x)$. Then the spectral sensitivity $\lambda(f) = \max_{v:||v||=1} v^T(RXR - X)v$, where $R = Hdiag(g)H$, and $H = H_n \in \{-1,1\}^{2^n \times 2^n}$ is the Hadamard matrix.*

Proof. By definition, we know know that $\lambda(f) = ||A_f||$. Since A_f is an adjacency matrix, it is symmetric, and so $\lambda(f)$ is equal to the max eigenvalue of A_f. $\lambda(f)$ can then be expressed as $\lambda(f) = \max_{v:||v||=1} |v^T A_f v|$. Furthermore, G_f is a bipartite graph, since there are no edges between any pair of vertices with even hamming weight, and there are

no edges between any pair of vertices with odd hamming weight. This means that the spectrum of A_f is symmetric about 0, and so $\lambda(f) = \max_{v:||v||=1} v^T A_f v$ [GR01].

$$\begin{aligned}\lambda(f) &= \max_{v:||v||=1} v^T A_f v \\ &= \max_{v:||v||=1} v^T H A_f H v, \end{aligned} \tag{2.2}$$

where $H = H_n \in \{-1,1\}^{2^n \times 2^n}$ is the Hadamard matrix. The second line uses the fact that $H^T = H$ and $||Hv|| = ||v||$. Let A_H be the adjacency matrix of the hypercube graph, which is defined as the graph (V, E) where $V = \{0,1\}^n$ and $E = \{(x, x \oplus e_i) \in V \times V | x \in \{0,1\}^n \text{ and } i \in [n]\}$. A_f can be expressed as

$$2A_f = A_H - diag(g) A_H diag(g), \tag{2.3}$$

where $g = 1 - 2f$ is the function f mapped on the set $\{-1, 1\}$, and $diag(g)$ is the diagonal matrix such that $diag(g)_{xx} = g(x)$. Equation 2.3 follows from the right hand side equaling $1 - g(x)g(y)$ for entries (x, y) with an edge in the Boolean hypercube.

It is known that H diagonalizes A_H, and that $A_H = H(nI - 2X)H$, where I is the identity matrix and X is the matrix such that $X_{xx} = |x|$.

Substituting equation 2.3 into equation 2.2, we get

$$\begin{aligned}\lambda(f) &= \max_{v:||v||=1} \frac{1}{2} v^T H (A_H - diag(g) A_H diag(g)) H v, \\ &= \max_{v:||v||=1} \frac{1}{2} v^T (H A_H H - H diag(g) A_H diag(g) H) v, \\ &= \max_{v:||v||=1} \frac{1}{2} v^T (nI - 2X - H diag(g) H (nI - 2X) H diag(g) H) v, \\ &= \max_{v:||v||=1} v^T (-X + H diag(g) H X H diag(g) H) v, \\ &= \max_{v:||v||=1} v^T (RXR - X) v, \end{aligned}$$

where $R = H diag(g) H$. □

We note that R is a symmetric, orthonormal matrix. The following lemma proves that $R_{xy} = 0$ if $|x \oplus y| > deg(g) = deg(f)$.

Lemma 2.4.4. *Let $g : \{0,1\}^n \to \mathbb{R}$ have real degree d and let $R = H diag(g) H$. Then for all $x, y \in \{0,1\}^n$, $R_{xy} = \hat{g}(x \oplus y)$, where for all $z \in \{0,1\}^n$, $\hat{g}(z) = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} (-1)^{\langle z,y \rangle} g(y)$. Consequently, $R_{xy} = 0$ if $|x \oplus y| > d$.*

Proof. By matrix multiplication, we can rewrite R_{xy} as

$$R_{xy} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{\langle x,z \rangle} (-1)^{\langle z,y \rangle} g(z) = \frac{1}{2^n} \sum_{z \in \{0,1\}^n} (-1)^{\langle x \oplus y, z \rangle} g(z) = \hat{g}(x \oplus y), \tag{2.4}$$

where the last equality follows by definition of Fourier coefficients [O'D14]. Since g has degree d, all Fourier coefficients $\hat{g}(z)$ with $|z| > d$ are 0. It follows that if $|x \oplus y| > d$, we have $R_{xy} = \hat{g}(x \oplus y) = 0$. □

Recall that $\lambda(f) = \max_{v:||v||=1} v^T(RXR - X)v$. By definition of matrix multiplication, $v^T(RXR - X)v$ can be expressed as

$$v^T(RXR - X)v = \sum_{x\in\{0,1\}^n} |x|(Rv)_x^2 - \sum_{x\in\{0,1\}^n} |x|v_x^2 = \sum_{i=1}^n ic_i - \sum_{j=1}^n jb_j, \tag{2.5}$$

where we define $c_i := \sum_{x:|x|=i}(Rv)_x^2$ and $b_j := \sum_{x:|x|=j} v_x^2$. In order to upper bound equation 2.5, the two summations must be compared. The following lemma shows that the first summation is bounded above by the second summation when the bounds of the summation are restricted. This is useful for the last lemma, which uses this fact to complete the proof.

Lemma 2.4.5. *Let R be a matrix with $||R|| \leq 1$ satisfying $R_{xy} = 0$ when $|x \oplus y| > d$. For any vector v, define $c_i := \sum_{x:|x|=i}(Rv)_x^2$ and $b_j := \sum_{x:|x|=j} v_x^2$. Then for any $r \in \{d+1, \ldots, n\}$, we have*

$$\sum_{i=r}^n c_i \leq \sum_{j=r-d}^n b_j \tag{2.6}$$

Proof. By definition, we can express c_i as

$$\sum_{i=r}^n c_i = \sum_{y:|y|\geq r} (Rv)_y^2 = \sum_{y:|y|\geq r} \left(\sum_{x\in\{0,1\}^n} R_{yx} v_x \right)^2 \tag{2.7}$$

Define $\Pi_{(\geq r)}$ to be the diagonal projector that satisfies the following for any vector v:

$$(\Pi_{(\geq r)} v)_x = \begin{cases} v_x & \text{if } |x| \geq r \\ 0 & \text{otherwise} \end{cases} \tag{2.8}$$

Since $R_{yx} = 0$ when $|x \oplus y| > d$, we note that for x with $|x| < r - d$, $R_{yx} = 0$. We can therefore express equation 2.7 as

$$\sum_{i=r}^n c_i = \sum_{y:|y|\geq r} \left(\sum_{x\in\{0,1\}^n} R_{yx} \Pi_{(\geq r-d)} v_x \right)^2 = \sum_{y:|y|\geq r} \left(R\Pi_{(\geq r-d)} v \right)_y^2 \tag{2.9}$$

By relaxing the constraints on y, we have

$$\sum_{i=r}^n c_i \leq \sum_{y\in\{0,1\}^n} \left(R\Pi_{(\geq r-d)} v \right)_y^2 = ||R\Pi_{(\geq r-d)} v||^2 \tag{2.10}$$

We note that since $||R|| \leq 1$, $||R\Pi_{(\geq r-d)} v||^2 \leq ||\Pi_{(\geq r-d)} v||^2$. By definition $||\Pi_{(\geq r-d)} v||^2 = \sum_{x:|x|\geq r-d} v_x^2$:

$$\begin{aligned} \sum_{i=r}^n c_i &\leq \sum_{x:|x|\geq r-d} v_x^2, \\ \sum_{i=r}^n c_i &\leq \sum_{j=r-d}^n b_j, \end{aligned} \tag{2.11}$$

where the second line follows by definition. This completes the lemma. □

We now prove the final lemma which completes the proof for Theorem 2.4.2.

Lemma 2.4.6. *Let R be a matrix with $||R|| \leq 1$ satisfying $R_{xy} = 0$ when $|x \oplus y| > d$. For any unit vector v, we have*

$$v^T(RXR - X)v \leq d. \tag{2.12}$$

Proof. Recall from equation 2.5 that

$$v^T(RXR - X)v = \sum_{i=1}^{n} ic_i - \sum_{j=1}^{n} jb_j, \tag{2.13}$$

where $c_i := \sum_{x:|x|=i}(Rv)_x^2$ and $b_j := \sum_{x:|x|=j} v_x^2$. We know from Lemma 2.4.5 that for any $r \in \{d+1, \ldots, n\}$,

$$\sum_{i=r}^{n} c_i \leq \sum_{j=r-d}^{n} b_j, \tag{2.14}$$

Summing over all $r \in \{d+1, \ldots, n\}$, this equation changes to:

$$\sum_{r\in\{d+1,\ldots,n\}} \sum_{i=r}^{n} c_i \leq \sum_{r\in\{d+1,\ldots,n\}} \sum_{j=r-d}^{n} b_j, \tag{2.15}$$

$$\sum_{i=d+1}^{n} (i-d)c_i \leq \sum_{j=1}^{n-d-1} jb_j + \sum_{j=n-d}^{n} (n-d)b_j, \tag{2.16}$$

where the second line follows after simplifying. Note that for any $r \in \{1, \ldots, d\}$, we have

$$\sum_{i=r}^{n} c_i \leq 1, \tag{2.17}$$

since $\sum_{i=r}^{n} c_i \leq \sum_{i=0}^{n} c_i = ||Rv||^2 \leq 1$ (recall $||R|| \leq 1$ and $||v|| = 1$). Summing over all $r \in \{1, \ldots, d\}$, we have

$$\sum_{r\in\{1,\ldots,d\}} \sum_{i=r}^{n} c_i \leq \sum_{r\in\{1,\ldots,d\}} 1, \tag{2.18}$$

$$\sum_{i=1}^{d-1} ic_i + \sum_{i=d}^{n} dc_i \leq d, \tag{2.19}$$

where the second line follows after simplifying. Also note that for any $k \in \{0, \ldots, d-1\}$, we trivially have

$$0 \leq \sum_{n-k}^{n} b_j \tag{2.20}$$

Summing over all $k \in \{0, \ldots, d-1\}$, we have

$$0 \leq \sum_{k\in\{0,\ldots,d-1\}} \sum_{n-k}^{n} b_j, \tag{2.21}$$

$$\leq \sum_{j=n-d+1}^{n} (d-n+j)b_j \tag{2.22}$$

Combining equations 2.16, 2.19, and 2.22, we have

$$\sum_{i=d+1}^{n}(i-d)c_i + \sum_{i=1}^{d-1} ic_i + \sum_{i=d}^{n} dc_i \leq \sum_{j=1}^{n-d-1} jb_j + \sum_{j=n-d}^{n}(n-d)b_j + \sum_{j=n-d+1}^{n}(d-n+j)b_j + d,$$

$$\sum_{i=1}^{n} ic_i \leq \sum_{j=1}^{n} jb_j + d \tag{2.23}$$

where the second line follows after simplifying. This shows that $v^T(RXR - X)v \leq d$ for all unit vectors v. □

We can now establish Theorem 2.4.2. From lemma 2.4.3, we know that $\lambda(f) = \max_{v:||v||=1} v^T(RXR - X)v$, and from lemma 2.4.6 we know that for any unit vector, $v^T(RXR - X)v \leq d = deg(g) = deg(f)$.

□

From equation 2.1, we get the best known upper bound on sensitivity by degree:

$$s(f) \leq deg(f)^2. \tag{2.24}$$

Chapter 3

The Kushilevitz Function

In the previous chapter, we proved that $s(f) \leq deg(f)^2$ for all Boolean functions f. However, it is not known whether a Boolean function with $s(f) = deg(f)^2$ exists, and the function with largest separation between sensitivity and degree is the Kushilevitz function. This chapter studies the family of Kushilevitz functions, and proves their sensitivity and degree.

3.1 Definition

3.1.1 Kushilevitz Function

The Kushilevitz Function is the Boolean function $f_k : \{0,1\}^{6^k} \to \{0,1\}$ defined as $f_k = g \diamond g \diamond \cdots \diamond g$ (k times), where $g : \{0,1\}^6 \to \{0,1\}$ is defined as:

$$g(x_1, \ldots, x_6) = \sum_{i=1}^{6} x_i - \sum_{\{i,j\} \in \binom{[6]}{2}} x_i x_j + \sum_{\{i,j,k\} \in K} x_i x_j x_k \tag{3.1}$$

and

$$\begin{aligned} K = \{&\{1,2,5\}, \{1,2,6\}, \{1,3,4\}, \{1,3,6\}, \{1,4,5\}, \\ &\{2,3,4\}, \{2,3,5\}, \{2,4,6\}, \{3,5,6\}, \{4,5,6\}\}. \end{aligned}$$

Note that the Kushilevitz function leads to a family of functions by composition. Most of this thesis studies $f_1 = g$ for simplicity.

3.1.2 Composition Function

For a Boolean function $f : \{0,1\}^m \to \{0,1\}$ and a Boolean function $g : \{0,1\}^n \to \{0,1\}$, [HKP10] defines the composition function $f \diamond g$ on mn variables as follows:

$$(f \diamond g)(x_1, \ldots, x_{mn}) = f(g(x_1, \ldots, x_n), \ldots, g(x_{mn-n+1}, \ldots, x_{mn}))$$

3.2 Sensitivity and Degree of the Kushilevitz Function

We give with proof, the values of $s(f_k)$ and $d(f_k)$ in order to show that $s(f_k) = d(f_k)^{1.63}$. This is the largest known separation between sensitivity and degree for Boolean functions.

Claim 3.2.1. $s(f_k) = 6^k$

Proof. A proof by induction is used:
Base Case: It is easy from Equation 3.1 see above that

$$f_1(0,0,0,0,0,0) = 0,$$
$$f_1(x) = 1 \text{ for inputs } x \in \{0,1\}^6 \text{ with } |x| = 1.$$

It follows that $s(f_1) = 6$.
Induction: Assume that $s(f_n) = 6^n$, and that f_n is fully sensitive on the input $x = (0,\ldots,0)$. We will show that $f_{n+1} : \{0,1\}^{6^{n+1}} \to \{0,1\}$ has $s(f_{n+1}) = 6^{n+1}$.
We know that

$$f_{n+1}(x_1,\ldots,x_{6^{n+1}}) = f_n(\underbrace{f_1(x_1,\ldots,x_6),\ldots,f_1(x_{6^{n+1}-5},\ldots,x_{6^{n+1}})}_{6^n \text{ times}})$$

We know from the base case that on the input with all 0's,

$$\begin{aligned} f_{n+1}(0,\ldots,0) &= f_n(f_1(0,\ldots,0),\ldots,f_1(0,\ldots,0)), \\ &= f_n(0,\ldots,0), \\ &= 0 \end{aligned}$$

where the last equation follows from our assumption.
For inputs $x = x_1,\ldots,x_{6^{n+1}} \in \{0,1\}^{6^{n+1}}$ with hamming weight one, we know from the base case that all but 1 of the inside f_1 functions will evaluate to 0, and the f_1 that takes on the input that has the 1 bit will evaluate to 1. Thus,

$$\begin{aligned} f_{n+1}(x_1,\ldots,x_{6^{n+1}}) &= f_n(x'_1,\ldots,x'_{6^n}), \text{ where } |x'_1,\ldots,x'_{6^n}| = 1 \\ &= 1 \end{aligned}$$

where the last equation follows from our assumption. This completes the proof. □

Claim 3.2.2. $deg(f_k) = 3^k$

Proof. A proof by induction is used:
Base Case: It is easy from Equation 3.1 that $deg(f_1) = 3$.
Induction: Assume that $deg(f_n) = 3^n$. We will show that $f_{n+1} : \{0,1\}^{6^{n+1}} \to \{0,1\}$ has $deg(f_{n+1}) = 3^{n+1}$.
Let

$$f_n(x_1,\ldots,x_{6^n}) = \sum_{S \subseteq [6^n], |S| \leq 3^n} \hat{f}_n(S) \prod_{i \in S} x_i \tag{3.2}$$

be the Fourier expansion of f_n. We note by assumption that for all S such that $|S| > 3^n$, $\hat{f}(S) = 0$. We know that

$$f_{n+1}(y_1,\ldots,y_{6^{n+1}}) = f_n(\underbrace{f_1(y_1,\ldots,y_6),\ldots,f_1(y_{6^{n+1}-5},\ldots,y_{6^{n+1}})}_{6^n \text{ times}})$$

Substituting equation 3.2 into the equation above, we get

$$f_{n+1}(y_1,\ldots,y_{6^{n+1}}) = \sum_{S \subseteq [6^n], |S| \leq 3^n} \hat{f}(S) \prod_{i \in S} f_1(y_{6i-5},\ldots,y_{6i}), \tag{3.3}$$

Where x_i in equation 3.2 is determined by $f_1(y_{6i-5},\ldots,y_{6i})$. Let S be the term for which $|S| = deg(f_n) = 3^n$. We note from equation 3.3 that for each $i \in S$, i is determined by a Kushilevitz function f_1, which has degree 3. Then the term S has degree $3^n \times 3 = 3^{n+1}$ in f_{n+1}. This concludes the proof. □

It follows from Claims 3.2.1 and 3.2.2 that the power separation between sensitivity and degree of the Kushilevitz function is $s(f_k) = d(f_k)^{\log(6^k)/\log(3^k)} = d(f_k)^{1.63}$. The Kushilevitz function retains the largest known separation between sensitivity and degree of any known Boolean function. It also provides the bounds between several other complexity measures [ABDK+21a, NW95].

3.3 Kushilevitz Output Table

Recall from the notation section that $f_1^{=3}$ is equal to the Fourier expansion of f_1 where terms with degree $\neq 3$ are zeroed out. Similarly, $f_1^{\leq 2}$ is equal to the Fourier expansion of f_1, where terms with degree > 2 are zeroed out. These definitions help us analyze how polynomials across the same degree affect the output of a Boolean function.

For some input $x = (x_1, \ldots, x_6)$, the Kushilevitz function $f_1(x)$ can be represented by the following output table:

$\lvert x \rvert$	$f_1^{\leq 2}(x)$	$f_1^{=3}(x)$	$f_1(x)$
0	0	0	0
1	1	0	1
2	1	0	1
3	0	0 10/20 times 1 10/20 times	0 10/20 times 1 10/20 times
4	-2	2	0
5	-5	5	0
6	-9	10	1

Where for inputs x with hamming weight 3,

$$\begin{aligned} f_1(x) = 1 \text{ if } x =& 110010, 110001, 101100, 101001, 100110, 011100, \\ & 011010, 010101, 001011, 000111, \\ f_1(x) = 0 \text{ if } x =& 001101, 001110, 010011, 010110, 011001, 100011, \\ & 100101, 101010, 110100, 111000 \end{aligned}$$

3.4 Orbit of the Kushilevitz Function

We note from the table above that for inputs with hamming weight $0, 1, 2, 4, 5, 6$, the value of Kushilevitz function depends only on the hamming weight of the input, and not on the permutation of the input bits. The Kushilevitz function f_1 is symmetric for all hamming weights but 3.

In order to more fully understand the structure of the Kushilevitz f_1 degree 3 terms, the orbit of the Kushilevitz function is computed with respect to the symmetric group S_6 in order to find all Boolean functions isomorphic to f_1. O'Donnell [O'D14] defines a Boolean function $g : \{0,1\}^n \to \{0,1\}$ to be *isomorphic* to f if $g = f^\pi$ for some $\pi \in S_n$.

Claim 3.4.1. *Let $S_6 \cdot f_1 = \{\sigma \cdot f_1 = f_1(x_{\sigma(1)}, \ldots, x_{\sigma(6)}) | \sigma \in S_6\}$ be the orbit of f_1 when acted on by the symmetric group S_6. $|S_6 \cdot f_1| = 12$, and the degree-3 terms of the 12*

functions are listed below.

$$\{\{1,2,3\},\{1,2,4\},\{1,3,5\},\{1,4,6\},\{1,5,6\},\{2,3,6\},\{2,4,5\},\{2,5,6\},\{3,4,5\},\{3,4,6\}\}$$
$$\{\{1,2,3\},\{1,2,4\},\{1,3,6\},\{1,4,5\},\{1,5,6\},\{2,3,5\},\{2,4,6\},\{2,5,6\},\{3,4,5\},\{3,4,6\}\}$$
$$\{\{1,2,3\},\{1,2,5\},\{1,3,4\},\{1,4,6\},\{1,5,6\},\{2,3,6\},\{2,4,5\},\{2,4,6\},\{3,4,5\},\{3,5,6\}\}$$
$$\{\{1,2,3\},\{1,2,5\},\{1,3,6\},\{1,4,5\},\{1,4,6\},\{2,3,4\},\{2,4,6\},\{2,5,6\},\{3,4,5\},\{3,5,6\}\}$$
$$\{\{1,2,3\},\{1,2,6\},\{1,3,4\},\{1,4,5\},\{1,5,6\},\{2,3,5\},\{2,4,5\},\{2,4,6\},\{3,4,6\},\{3,5,6\}\}$$
$$\{\{1,2,3\},\{1,2,6\},\{1,3,5\},\{1,4,5\},\{1,4,6\},\{2,3,4\},\{2,4,5\},\{2,5,6\},\{3,4,6\},\{3,5,6\}\}$$
$$\{\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,6\},\{1,5,6\},\{2,3,5\},\{2,3,6\},\{2,4,6\},\{3,4,5\},\{4,5,6\}\}$$
$$\{\{1,2,4\},\{1,2,5\},\{1,3,5\},\{1,3,6\},\{1,4,6\},\{2,3,4\},\{2,3,6\},\{2,5,6\},\{3,4,5\},\{4,5,6\}\}$$
$$\{\{1,2,4\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,5,6\},\{2,3,5\},\{2,3,6\},\{2,4,5\},\{3,4,6\},\{4,5,6\}\}$$
$$\{\{1,2,4\},\{1,2,6\},\{1,3,5\},\{1,3,6\},\{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,5,6\},\{3,4,6\},\{4,5,6\}\}$$
$$\{\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,4,6\},\{2,3,4\},\{2,3,6\},\{2,4,5\},\{3,5,6\},\{4,5,6\}\}$$
$$\{\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,6\},\{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,6\},\{3,5,6\},\{4,5,6\}\}$$

Proof. The following algorithm was used to determine the orbit:

Algorithm 1 Algorithm that computes all Boolean functions isomorphic to the Kushilevitz function

Require: $K \leftarrow$ Kushilevitz deg 3 terms

```
n ← {1, 2, 3, 4, 5, 6}
perms ← P(n, 6)                                  ▷ List of size 720
orbit ← {K}
for perm ∈ perms do
    deg_three_terms ← permute(K, perm)
    if deg_three_terms ∉ orbit then
        orbit.append(deg_three_terms)
    end if
end for
return orbit
```

□

The orbit of the Kushilevitz function generates all functions isomorphic to the Kushilevitz function. These functions are useful in order to recognize patterns between their structures, which helps to better understand the Kushilevitz function. The next chapter introduces a new class of subsets which formalizes such properties found across the 12 subsets above.

Chapter 4

Well Balanced Sets

4.1 Introduction

Note from the table in Section 3.3 that for any pair of inputs with the same hamming weight greater than 3, the output of the Kushilevitz function degree 3 terms, $f_1^{=3}(x)$, is the same. This means that the number of degree 3 terms of the Kushilevitz function that are included in any permutation of bits with the same hamming weight are the same.

The following chapter formalizes the notion of such subsets $S \subseteq \binom{[n]}{m}$ which are "well balanced" with respect to their representation in every subset of $[n]$ of size $i \neq m$. Learning more about the properties and structure of the Kushilevitz degree 3 terms helps to understand how the Kushilevitz function retains such a large separation between its sensitivity and degree. Furthermore, creating subsets that have similar properties to the Kushilevitz degree 3 terms could help in the construction of a Boolean function with larger separation.

4.2 Lower Well Balanced Subsets

We begin the chapter by defining lower well balanced subsets, which is a subset $S \subseteq \binom{[n]}{m}$ such that every subset of $[n]$ of size $i < m$ is included the same amount of times in S. We give trivial examples of lower well balanced subsets ($S = \emptyset$ and $S = \binom{[n]}{m}$), then show more interesting examples.

4.2.1 Definition and Examples

Definition 4.2.1. *A subset $S \subseteq \binom{[n]}{m}$ is level i lower well balanced, where $i \in \{1, \ldots, m-1\}$, if for every $t \in \binom{[n]}{m-i}$, $|\{s \in S | t \subseteq s\}|$ is the same for all t, which we denote by $X_{m,i}$.*

Remark 1. *The set $S = \emptyset \subseteq \binom{[n]}{m}$ is level 1 lower well balanced, since for every $t \in \binom{[n]}{m-1}$, $|\{s \in S | t \subseteq s\}| = 0$.*

Remark 2. *The set $S = \binom{[n]}{m}$ is level 1 lower well balanced, since for every $t \in \binom{[n]}{m-1}$, $|\{s \in S | t \subseteq s\}| = n - m + 1$.*

We call the sets $S = \emptyset$ and $S = \binom{[n]}{m}$ trivial lower balanced subsets.

Example 4.2.2. *The degree 3 terms $S \subseteq \binom{[6]}{3}$ of the Kushilevitz function $f_1 : \{0,1\}^6 \to \{0,1\}$ are level 1 lower well balanced, since for every $t \in \binom{[6]}{2}$, $|\{s \in S | t \subseteq s\}| = X_{3,1} = 2$. The degree 3 terms $S \subseteq \binom{[6]}{3}$ of the Kushilevitz function are as follows:*

$$S = \{\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,6\},\{1,4,5\},\\ \{2,3,4\},\{2,3,5\},\{2,4,6\},\{3,5,6\},\{4,5,6\}\}.$$

The table below shows $\{s \in S | t \subseteq s\}$ for every $t \in \binom{[6]}{2}$:

$t \in \binom{[6]}{2}$	$\{s \in S \mid t \subseteq s\}$
$\{1,2\}$	$\{1,2,5\},\{1,2,6\}$
$\{1,3\}$	$\{1,3,4\},\{1,3,6\}$
$\{1,4\}$	$\{1,3,4\},\{1,4,5\}$
$\{1,5\}$	$\{1,2,5\},\{1,4,5\}$
$\{1,6\}$	$\{1,2,6\},\{1,3,6\}$
$\{2,3\}$	$\{2,3,4\},\{2,3,5\}$
$\{2,4\}$	$\{2,3,4\},\{2,4,6\}$
$\{2,5\}$	$\{1,2,5\},\{2,3,5\}$
$\{2,6\}$	$\{1,2,6\},\{2,4,6\}$
$\{3,4\}$	$\{1,3,4\},\{2,3,4\}$
$\{3,5\}$	$\{2,3,5\},\{3,5,6\}$
$\{3,6\}$	$\{1,3,6\},\{3,5,6\}$
$\{4,5\}$	$\{1,4,5\},\{4,5,6\}$
$\{4,6\}$	$\{2,4,6\},\{4,5,6\}$
$\{5,6\}$	$\{3,5,6\},\{4,5,6\}$

Example 4.2.3. *The subset $S = \{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{3,4,6\},\{3,5,6\},\{4,5,6\}\} \subseteq \binom{[6]}{3}$ is level 2 lower well balanced, since for every $t \in \binom{[6]}{1}$, $|\{s \in S | t \subseteq s\}| = X_{3,2} = 3$. The table below shows $\{s \in S | t \subseteq s\}$ for all $t \in \binom{[6]}{1}$:*

$t \in \binom{[6]}{5}$	$\{s \in S \mid t \subseteq s\}$
$\{1\}$	$\{1,2,3\},\{1,2,4\},\{1,2,5\}$
$\{2\}$	$\{1,2,3\},\{1,2,4\},\{1,2,5\}$
$\{3\}$	$\{1,2,3\},\{3,4,6\},\{3,5,6\}$
$\{4\}$	$\{1,2,4\},\{3,4,6\},\{4,5,6\}$
$\{5\}$	$\{1,2,5\},\{3,5,6\},\{4,5,6\}$
$\{6\}$	$\{3,4,6\},\{3,5,6\},\{4,5,6\}$

The following claim shows that a level i lower well balanced subset $S \subseteq \binom{[n]}{m}$ is also level k lower well balanced for $k > i$. This claim is useful because it determines how many times any subset of $[n]$ of size $m-k$ is included in S, as a function of $X_{m,i}$.

Claim 4.2.4. *Let $S \subseteq \binom{[n]}{m}$ be a level i lower well balanced subset and let k be an integer such that $i+1 \leq k \leq m$. Then for every $t \in \binom{[n]}{m-k}$, $|\{s \in S | t \subseteq s\}| = X_{m,k} = \binom{k}{i}^{-1}\binom{n-m+k}{k-i}X_{m,i}$. This implies that S is a level k lower well balanced subset.*

Proof. Fix a $t \in \binom{[n]}{m-k}$. Define $L := \left\{l \in \binom{[n]}{m-i} | t \subseteq l\right\}$. If follows that $|L| = \binom{n-(m-k)}{(m-i)-(m-k)} = \binom{n-m+k}{k-i}$. For each $l \in L$, define $S_l := \{s \in S | l \subseteq s\}$ to be the set

of elements in S that contain l. Define $S_L := \cup_{l\in L} S_l$ to the set of elements in S that contain some $l \in L$. It follows directly that $X_t = \left|S_L\right|$.
The Principle of Inclusion Exclusion states that for finite sets $A_1, \ldots, A_n$,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} \left|A_i\right| - \sum_{1\le i<j\le n} \left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n} \left|A_i \cap A_j \cap A_k\right| - \cdots + (-1)^{n+1}\left|A_1 \cap \cdots \cap A_n\right|.$$

Applied to S_L, we get:

$$X_t = |S_L| = \left|\bigcup_{l\in L} S_l\right| = \sum_{l\in L} \left|S_l\right| - \sum_{\{l_1,l_2\}\subseteq L} \left|S_{l_1} \cap S_{l_2}\right| + \sum_{\{l_1,l_2,l_3\}\subseteq L} \left|S_{l_1} \cap S_{l_2} \cap S_{l_3}\right| - \cdots + (-1)^{|L|+1}\left|S_{l_1} \cap \cdots \cap S_{l_{|L|}}\right|.$$

Note that by definition, for all $l \in L, |S_l| = X_{m,i}$:

$$X_t = \binom{n-m+k}{k-i} X_{m,i} - \sum_{\{l_1,l_2\}\subseteq L} \left|S_{l_1} \cap S_{l_2}\right| + \sum_{\{l_1,l_2,l_3\}\subseteq L} \left|S_{l_1} \cap S_{l_2} \cap S_{l_3}\right| - \cdots + (-1)^{|L|+1}\left|S_{l_1} \cap \cdots \cap S_{l_{|L|}}\right|.$$

Define $\mathbb{1}_{l,s} : L \times S \to \{0,1\}$ such that $\mathbb{1}_{l,s} = 1$ if and only if $l \subseteq s$.

$$\begin{aligned}
X_t &= \binom{n-m+k}{k-i} X_{m,i} - \sum_{\{l_1,l_2\}\subseteq L} \sum_{c\in S_L} \mathbb{1}_{l_1,c}\mathbb{1}_{l_2,c} + \sum_{\{l_1,l_2,l_3\}\subseteq L} \sum_{c\in S_L} \mathbb{1}_{l_1,c}\mathbb{1}_{l_2,c}\mathbb{1}_{l_3,c} \\
&\quad - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \prod_{l\in L} \mathbb{1}_{l,c} \\
&= \binom{n-m+k}{k-i} X_{m,i} - \sum_{c\in S_L} \sum_{\{l_1,l_2\}\subseteq L} \mathbb{1}_{l_1,c}\mathbb{1}_{l_2,c} + \sum_{c\in S_L} \sum_{\{l_1,l_2,l_3\}\subseteq L} \mathbb{1}_{l_1,c}\mathbb{1}_{l_2,c}\mathbb{1}_{l_3,c} \\
&\quad - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \prod_{l\in L} \mathbb{1}_{l,c}
\end{aligned}$$

where the second line follows from switching the order of summations. Note that for each $c \in S_L$ (recall that $|c| = m$), as we iterate through subsets $\{l_1, \ldots, l_j\} \subseteq L$, there exists $\binom{m+\binom{k}{i}-m}{j} = \binom{\binom{k}{i}}{j}$ subsets $\{l_1, \ldots, l_j\}$ such that $\Pi_{i=1}^{j} \mathbb{1}_{l_i,c} = 1$:

$$\begin{aligned}
X_t &= \binom{n-m+k}{k-i} X_{m,i} - \sum_{c\in S_L} \binom{\binom{k}{i}}{2} + \sum_{c\in S_L} \binom{\binom{k}{i}}{3} - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \binom{\binom{k}{i}}{|L|}, \\
&= \binom{n-m+k}{k-i} X_{m,i} - X_t \binom{\binom{k}{i}}{2} + X_t \binom{\binom{k}{i}}{3} - \cdots + (-1)^{|L|+1} X_t \binom{\binom{k}{i}}{|L|}, \\
&= \binom{n-m+k}{k-i} X_{m,i} + \sum_{j=2}^{\binom{k}{i}} (-1)^{j+1} X_t \binom{\binom{k}{i}}{j}, \\
&= \binom{n-m+k}{k-i} X_{m,i} - X_t \left(\binom{k}{i} - 1\right) + \sum_{j=0}^{\binom{k}{i}} (-1)^{j+1} Y_t \binom{\binom{k}{i}}{j}, \qquad (4.1)
\end{aligned}$$

where the second equation follows from $|S_L| = X_t$, the third equation expresses the equation as a summation, and Equation 4.1 relaxes the summation. By the Binomial Theorem, Equation 4.1 becomes

$$X_t = \binom{n-m+k}{k-i} X_{m,i} - X_t \left(\binom{k}{i} - 1 \right),$$
$$X_t = \binom{k}{i}^{-1} \binom{n-m+k}{k-i} X_{m,i} \tag{4.2}$$

Since t was chosen arbitrarily, Equation 4.2 can be generalized to:

$$X_{m,k} = \binom{k}{i}^{-1} \binom{n-m+k}{k-i} X_{m,i} \tag{4.3}$$

Since for every $t \in \binom{[n]}{m-k}$, $\left|\{s \in S | t \subseteq s\}\right| = \binom{k}{i}^{-1} \binom{n-m+k}{k-i} X_{m,i}$, S is level k lower well balanced. □

Note that $\binom{[n]}{0}$ trivially appears in all elements of S. Using this fact, the following useful remark gives $|S|$ as a function of $X_{m,i}$.

Remark 3. *Let $S \subseteq \binom{[n]}{m}$ be a level i lower well balanced subset with $X_{m,i}$. Then $|S| = X_{m,m} = \binom{m}{i}^{-1} \binom{n}{m-i} X_{m,i}$.*

As will be further discussed in Chapter 5, creating lower well balanced subsets is not a trivial task. It is useful then to discuss conditions under which lower well balanced subsets cannot exist. The following claim and corollary provide some of these conditions.

Claim 4.2.5. *If $m > n/2$, then there does not exist a level i nontrivial lower well balanced subset $S \subseteq \binom{[n]}{m}$ for all $1 \leq i \leq 2m - n$.*

Proof. We begin by proving that there does not exist a level $i = 2m - n$ lower well balanced subset.
As defined in [Rao21], let $P^{\downarrow}_{n,i,m} \in \mathbb{R}^{\binom{[n]}{m-i} \times \binom{[n]}{m}}$ be the matrix defined by

$$P^{\downarrow}_{n,i,m}(x, y) = \begin{cases} 1 & \text{if } x_j = 1 \text{ implies } y_j = 1 \\ 0 & \text{otherwise} \end{cases} \tag{4.4}$$

Suppose that for some $m > n/2$, there exists a level $2m-n$ nontrivial lower well balanced subset $S \subseteq \binom{[n]}{m}$ with $X_{m,2m-n}$. Let $\mathbb{1}_S \in \mathbb{R}^{\binom{[n]}{m}}$ be the matrix defined by

$$\mathbb{1}_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$$

We note that $P^{\downarrow}_{n,2m-n,m} \mathbb{1}_S(y) = |\{x \in S | y \subseteq x\}|$:

$$P^{\downarrow}_{n,2m-n,m} \mathbb{1}_S = X_{m,2m-n} \mathbf{1},$$

We replace the all ones matrix $\mathbf{1}$ with an equivalent $\binom{m}{2m-n}^{-1} P^{\downarrow}_{n,2m-n,m} \mathbf{1}$:

$$P^{\downarrow}_{n,2m-n,m} \mathbb{1}_S = X_{m,2m-n} \binom{m}{2m-n}^{-1} P^{\downarrow}_{n,2m-n,m} \mathbf{1},$$

$$P^{\downarrow}_{n,2m-n,m}\left(\mathbb{1}_S - X_{m,2m-n}\binom{m}{2m-n}^{-1}\mathbf{1}\right) = 0.$$

where the second line follows from moving around terms. We note that there exists a nontrivial $\mathbb{1}_S - X_{m,2m-n}\binom{m}{2m-n}^{-1}\mathbf{1}$ if and only if $P^{\downarrow}_{n,2m-n,m}$ does not have full rank. We know from [Rao21] that $P^{\downarrow}_{n,2m-n,m}$ has full rank.

$$\mathbb{1}_S - X_{m,2m-n}\binom{m}{2m-n}^{-1}\mathbf{1} = 0,$$

$$\mathbb{1}_S = X_{m,2m-n}\binom{m}{2m-n}^{-1}\mathbf{1}$$

where the second line follows from moving around terms. Since the above statement is true if and only if $S = \binom{[n]}{m}$ or $S = \emptyset$, which are trivial lower well balanced subsets, we have reached a contradiction. It follows that there does not exist a level $2m-n$ lower well balanced subset $S \subseteq \binom{[n]}{m}$ if $m > n/2$.

For $1 \leq i < 2m-n$, a very similar proof follows. We note that $P^{\downarrow}_{n,i,m}$ has full rank, since $P^{\downarrow}_{n,2m-n,m}$ can be expressed as:

$$P^{\downarrow}_{n,2m-n,m} = P^{\downarrow}_{n,2m-n-i,m-i}P^{\downarrow}_{n,i,m}$$

Since $rank(P^{\downarrow}_{n,2m-n,m}) \leq min\{rank(P^{\downarrow}_{n,2m-n-i,m-i}), rank(P^{\downarrow}_{n,i,m})\}$, the rank of $P^{\downarrow}_{n,i,m}$ must be at least that of $P^{\downarrow}_{n,2m-n,m}$, and so it has full rank. □

Corollary 4.2.6. *If a nontrivial subset $S \subseteq \binom{[n]}{m}$ is level i lower well balanced, then $m \leq \frac{n+i-1}{2}$.*

Proof. Suppose there exists a subset $S \subseteq \binom{[n]}{m}$ that is level i lower well balanced with $m > \frac{n+i-1}{2}$. We have two cases:
Case 1: $n+i$ is odd. Then $m \geq \frac{n+i+1}{2} > n/2$. Claim 4.2.5 states that there does not exist a level j lower well balanced subset for all $1 \leq j \leq 2(\frac{n+i+1}{2}) - n$. This simplifies to $1 \leq j \leq i+1$. This is a contradiction.
Case 2: $n+i$ is even. Then $m \geq \frac{n+i}{2} > n/2$. Claim 4.2.5 states that there does not exist a level j lower well balanced subset for all $1 \leq j \leq 2(\frac{n+i}{2}) - n$. This simplifies to $1 \leq j \leq i$. This is a contradiction.

□

4.3 Upper Well Balanced Subsets

The following section defines upper well balanced subsets, which is a subset $S \subseteq \binom{[n]}{m}$ such that the number of elements of S that are included in any subset of $[n]$ of size $i > m$ is the same amount. We give trivial examples of upper well balanced subsets ($S = \emptyset$ and $S = \binom{[n]}{m}$), then show more interesting examples. Note that this section follows a similar outline to the previous section.

4.3.1 Definition and Examples

Definition 4.3.1. *A subset $S \subseteq \binom{[n]}{m}$ is level i upper well balanced, where $i \in \{1, \ldots, n-m-1\}$, if for every $t \in \binom{[n]}{m+i}$, $|\{s \in S | s \subseteq t\}|$ is the same for all t, which we denote by $Y_{m,i}$.*

Remark 4. *The set $S = \emptyset \subseteq \binom{[n]}{m}$ is level 1 upper well balanced, since for every $t \in \binom{[n]}{m+1}$, $|\{s \in S | s \subseteq t\}| = Y_{m,1} = 0$.*

Remark 5. *The set $S = \binom{[n]}{m}$ is level 1 upper well balanced, since for every $t \in \binom{[n]}{m+1}$, $|\{s \in S | s \subseteq t\}| = Y_{m,1} = m+1$.*

We call the sets $S = \emptyset$ and $S = \binom{[n]}{m}$ trivial upper balanced subsets.

Example 4.3.2. *The degree 3 terms $S \subseteq \binom{[6]}{3}$ of the Kushilevitz function $f_1 : \{0,1\}^6 \to \{0,1\}$ are level 1 upper well balanced, since for every $t \in \binom{[6]}{4}$, $|\{s \in S | s \subseteq t\}| = Y_{3,1} = 2$. The table below shows $\{s \in S | s \subseteq t\}$ for all $t \in \binom{[6]}{4}$:*

$t \in \binom{[6]}{4}$	$\{s \in S \mid s \subseteq t\}$
$\{1,2,3,4\}$	$\{1,3,4\}, \{2,3,4\}$
$\{1,2,3,5\}$	$\{1,2,5\}, \{2,3,5\}$
$\{1,2,3,6\}$	$\{1,2,6\}, \{1,3,6\}$
$\{1,2,4,5\}$	$\{1,2,5\}, \{1,4,5\}$
$\{1,2,4,6\}$	$\{1,2,6\}, \{2,4,6\}$
$\{1,2,5,6\}$	$\{1,2,5\}, \{1,2,6\}$
$\{1,3,4,5\}$	$\{1,3,4\}, \{1,4,5\}$
$\{1,3,4,6\}$	$\{1,3,4\}, \{1,3,6\}$
$\{1,3,5,6\}$	$\{1,3,6\}, \{3,5,6\}$
$\{1,4,5,6\}$	$\{1,4,5\}, \{4,5,6\}$
$\{2,3,4,5\}$	$\{2,3,4\}, \{2,3,5\}$
$\{2,3,4,6\}$	$\{2,3,4\}, \{2,4,6\}$
$\{2,3,5,6\}$	$\{2,3,5\}, \{3,5,6\}$
$\{2,4,5,6\}$	$\{2,4,6\}, \{4,5,6\}$
$\{3,4,5,6\}$	$\{3,5,6\}, \{4,5,6\}$

Similar to Claim 4.2.4, the following claim shows that a level i upper well balanced subset $S \subseteq \binom{[n]}{m}$ is also level k upper well balanced for $k > i$. This claim is useful because it determines how many elements of S are included in any subset of $[n]$ of size $m+k$ as a function of $Y_{m,i}$.

Claim 4.3.3. *Let $S \subseteq \binom{[n]}{m}$ be a level i upper well balanced subset and let k be an integer such that $i+1 \leq k \leq n-m$. Then for every $t \in \binom{[n]}{m+k}$, $\left|\{s \in S | s \subseteq t\}\right| = Y_{m,k} = \binom{k}{i}^{-1}\binom{m+k}{m+i} Y_{m,i}$. This implies that S is a level k upper well balanced subset.*

Proof. The proof follows a procedure similar to that of Claim 4.2.4. Fix a $t \in \binom{[n]}{m+k}$. Define $L := \left\{l \in \binom{[n]}{m+i} | l \subseteq t\right\}$. It follows that $|L| = \binom{m+k}{m+i}$. For each $l \in L$, define $S_l := \{s \in S | s \subseteq l\}$ to be the set of elements in S that are contained in l. Define $S_L := \cup_{l \in L} S_l$ to be the set of elements in S that are contained in some $l \in L$. It follows

directly that $Y_t = \left|S_L\right|$.
The Principle of Inclusion Exclusion tells us that for finite sets $A_1, \ldots, A_n$,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} \left|A_i\right| - \sum_{1\le i<j\le n} \left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n} \left|A_i \cap A_j \cap A_k\right| - \cdots + (-1)^{n+1}\left|A_1 \cap \cdots \cap A_n\right|.$$

Applied to set S_L, we get:

$$Y_t = |S_L| = \left|\bigcup_{l\in L} S_l\right| = \sum_{l\in L} \left|S_l\right| - \sum_{\{l_1,l_2\}\subseteq L} \left|S_{l_1} \cap S_{l_2}\right| + \sum_{\{l_1,l_2,l_3\}\subseteq L} \left|S_{l_1} \cap S_{l_2} \cap S_{l_3}\right| - \cdots + (-1)^{|L|+1}\left|S_{l_1} \cap \cdots \cap S_{l_{|L|}}\right|.$$

We note that by definition, for all $l \in L, |S_l| = Y_{m,i}$:

$$Y_t = \binom{m+k}{m+i} Y_{m,i} - \sum_{\{l_1,l_2\}\subseteq L} \left|S_{l_1} \cap S_{l_2}\right| + \sum_{\{l_1,l_2,l_3\}\subseteq L} \left|S_{l_1} \cap S_{l_2} \cap S_{l_3}\right| - \cdots + (-1)^{|L|+1}\left|S_{l_1} \cap \cdots \cap S_{l_{|L|}}\right|.$$

Define $\mathbb{1}_{s,l} : S \times L \to \{0,1\}$ such that $\mathbb{1}_{s,l} = 1$ if and only if $s \subseteq l$.

$$\begin{aligned}
Y_t &= \binom{m+k}{m+i} Y_{m,i} - \sum_{\{l_1,l_2\}\subseteq L} \sum_{c\in S_L} \mathbb{1}_{c,l_1}\mathbb{1}_{c,l_2} + \sum_{\{l_1,l_2,l_3\}\subseteq L} \sum_{c\in S_L} \mathbb{1}_{c,l_1}\mathbb{1}_{c,l_2}\mathbb{1}_{c,l_3} \\
&\quad - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \prod_{l\in L} \mathbb{1}_{c,l} \\
&= \binom{m+k}{m+i} Y_{m,i} - \sum_{c\in S_L} \sum_{\{l_1,l_2\}\subseteq L} \mathbb{1}_{c,l_1}\mathbb{1}_{c,l_2} + \sum_{c\in S_L} \sum_{\{l_1,l_2,l_3\}\subseteq L} \mathbb{1}_{c,l_1}\mathbb{1}_{c,l_2}\mathbb{1}_{c,l_3} \\
&\quad - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \prod_{l\in L} \mathbb{1}_{c,l}
\end{aligned}$$

where the second line follows from switching the order of summations. We note that for each $c \in S_L$ (recall that $|c| = m$), as we iterate through subsets $\{l_1, \ldots, l_j\} \subseteq L$, there exists $\binom{m+\binom{k}{i}-m}{j} = \binom{\binom{k}{i}}{j}$ subsets $\{l_1, \ldots, l_j\}$ such that $\Pi_{i=1}^{j} \mathbb{1}_{c,l_i} = 1$:

$$\begin{aligned}
Y_t &= \binom{m+k}{m+i} Y_{m,i} - \sum_{c\in S_L} \binom{\binom{k}{i}}{2} + \sum_{c\in S_L} \binom{\binom{k}{i}}{3} - \cdots + (-1)^{|L|+1} \sum_{c\in S_L} \binom{\binom{k}{i}}{|L|}, \\
&= \binom{m+k}{m+i} Y_{m,i} - Y_t \binom{\binom{k}{i}}{2} + Y_t \binom{\binom{k}{i}}{3} - \cdots + (-1)^{|L|+1} Y_t \binom{\binom{k}{i}}{|L|}, \\
&= \binom{m+k}{m+i} Y_{m,i} + \sum_{j=2}^{\binom{k}{i}} (-1)^{j+1} Y_t \binom{\binom{k}{i}}{j}, \\
&= \binom{m+k}{m+i} Y_{m,i} - Y_t \left(\binom{k}{i} - 1\right) + \sum_{j=0}^{\binom{k}{i}} (-1)^{j+1} Y_t \binom{\binom{k}{i}}{j}, \qquad (4.5)
\end{aligned}$$

where the second equation follows from $|S_L| = Y_t$, the third equation expresses the equation as a summation, and Equation 4.5 relaxes the summation. By the Binomial Theorem, Equation 4.5 becomes

$$Y_t = \binom{m+k}{m+i} Y_{m,i} - Y_t \left(\binom{k}{i} - 1 \right),$$
$$Y_t = \binom{k}{i}^{-1} \binom{m+k}{m+i} Y_{m,i} \tag{4.6}$$

Since t was chosen arbitrarily, Equation 4.6 can be generalized to:

$$Y_{m,k} = \binom{k}{i}^{-1} \binom{m+k}{m+i} Y_{m,i} \tag{4.7}$$

Since for every $t \in \binom{[n]}{m+k}$, $\left|\{s \in S | s \subseteq t\}\right| = \binom{k}{i}^{-1} \binom{m+k}{m+i} Y_{m,i}$, S is level k upper well balanced. □

Similar to Remark 3, the following remark makes use of the fact that every element in S is included in $\binom{[n]}{n}$. Thus, we give $|S|$ as a function of $Y_{m,i}$.

Remark 6. *Let $S \subseteq \binom{[n]}{m}$ be a level i upper well balanced subset with $Y_{m,i}$. Then $|S| = Y_{m,n-m} = \binom{n-m}{i}^{-1} \binom{n}{m+i} Y_{m,i}$.*

The following claim and corollary provide some constraints under which no upper well balanced subsets exist. Again, note that the proof follows a similar procedure to that of Claim 4.2.5

Claim 4.3.4. *If $m < n/2$, then there does not exist a nontrivial level i upper well balanced subset $S \subseteq \binom{[n]}{m}$ for all $1 \leq i \leq n - 2m$.*

Proof. We begin by proving that there does not exist a level $i = n - 2m$ upper well balanced subset. As defined in [Rao21], let $P^{\uparrow}_{n,i,m} \in \mathbb{R}^{\binom{[n]}{m+i} \times \binom{[n]}{m}}$ be the matrix defined by

$$P^{\uparrow}_{n,i,m}(x, y) = \begin{cases} 1 & \text{if } y_j = 1 \text{ implies } x_j = 1 \\ 0 & \text{otherwise} \end{cases} \tag{4.8}$$

Suppose that for some $m < n/2$, there exists a level $n-2m$ nontrivial upper well balanced subset $S \subseteq \binom{[n]}{m}$ with $Y_{m,n-2m}$. Let $\mathbb{1}_S \in \mathbb{R}^{\binom{[n]}{m}}$ be the matrix defined by

$$\mathbb{1}_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$$

We note that $P^{\uparrow}_{n,n-2m,m} \mathbb{1}_S(y) = |\{x \in S | x \subseteq y\}|$:

$$P^{\uparrow}_{n,n-2m,m} \mathbb{1}_S = Y_{m,n-2m} \mathbf{1}$$

We replace the all ones matrix $\mathbf{1}$ with an equivalent $\binom{n-m}{m}^{-1} P^{\uparrow}_{n,n-2m,m} \mathbf{1}$:

$$P^{\uparrow}_{n,n-2m,m} \mathbb{1}_S = Y_{m,n-2m} \binom{n-m}{m}^{-1} P^{\uparrow}_{n,n-2m} \mathbf{1},$$

$$P^{\uparrow}_{n,n-2m,m}\left(\mathbb{1}_S - Y_{m,n-2m}\binom{n-m}{m}^{-1}\mathbf{1}\right) = 0.$$

where the second line follows from moving around terms. We note that there exists a nontrivial $\mathbb{1}_S - Y_{m,n-2m}\binom{n-m}{m}^{-1}\mathbf{1}$ if and only if $P^{\uparrow}_{n,n-2m,m}$ does not have full rank. We know from [Rao21] that $P^{\uparrow}_{n,n-2m,m}$ has full rank:

$$\mathbb{1}_S - Y_{m,n-2m}\binom{n-m}{m}^{-1}\mathbf{1} = 0,$$

$$\mathbb{1}_S = Y_{m,n-2m}\binom{n-m}{m}^{-1}\mathbf{1}.$$

where the second line follows from moving around terms. We note that the above statement is true if and only if $S = \binom{[n]}{m}$ or $S = \emptyset$, which are trivial upper well balanced subsets. Therefore, we have reached a contradiction. It follows that there does not exist a level $n-2m$ upper well balanced subset $S \subseteq \binom{[n]}{m}$ if $m < n/2$.

For $1 \leq i < n-2m$, a very similar proof follows. We note that $P^{\uparrow}_{n,i,m}$ has full rank, since $P^{\uparrow}_{n,n-2m,m}$ can be expressed as:

$$P^{\uparrow}_{n,n-2m,m} = P^{\uparrow}_{n,n-2m-i,m+i}P^{\uparrow}_{n,i,m}$$

Since $rank(P^{\uparrow}_{n,n-2m,m}) \leq min\{rank(P^{\uparrow}_{n,n-2m-i,m+i}), rank(P^{\uparrow}_{n,i,m})\}$, the rank of $P^{\uparrow}_{n,i,m}$ must be at least that of $P^{\uparrow}_{n,n-2m,m}$, and so it has full rank. □

Corollary 4.3.5. *If a nontrivial subset $S \subseteq \binom{[n]}{m}$ is level i upper well balanced, then $m \geq \frac{n-i+1}{2}$.*

Proof. Suppose there exists a subset $S \subseteq \binom{[n]}{m}$ that is level i upper well balanced with $m < \frac{n-i+1}{2}$. We have two cases:
Case 1: $n-i$ is odd. Then $m \leq \frac{n-i-1}{2} < n/2$. Claim 4.3.4 states that there does not exist a level j upper well balanced subset for all $1 \leq j \leq n - 2(\frac{n-i-1}{2})$. This simplifies to $1 \leq j \leq i+1$. This is a contradiction.
Case 2: $n-i$ is even. Then $m \leq \frac{n-i}{2} < n/2$. Claim 4.3.4 states that there does not exist a level j upper well balanced subset for all $1 \leq j \leq n - 2(\frac{n-i}{2})$. This simplifies to $1 \leq j \leq i$. This is a contradiction.

□

4.4 Upper $\iff$ Lower

The following section proves that a subset $S \subseteq \binom{[n]}{m}$ is upper well balanced if and only if it is lower well balanced. This implies that any proposition that is made about upper well balanced subsets can be made about lower well balanced subsets, and vice versa.

Claim 4.4.1. *If $S \subseteq \binom{[n]}{m}$ is a level i lower well balanced subset with $X_{m,i}$, then it is level $n-2m+i$ upper well balanced with $Y_{m,n-2m+i} = \binom{m}{i}^{-1}\binom{n-m}{m-i}X_{m,i}$*

Proof. Fix a $t \in \binom{[n]}{m+(n-2m+i)}$. Define $L := [n] \setminus t$. It follows that $|L| = n - (m + (n - 2m + i)) = m - i$. For each $l \in L$, define $S_l := \{s \in S | l \in s\}$ to be the set of elements in S that contain l. Define $S_L := \cup_{l \in L} S_l$ to be the set of elements in S that contain any $l \in L$. It follows directly that $Y_t = |S| - |S_L|$.
The Principle of Inclusion Exclusion states that for finite sets $A_1, \ldots, A_n$,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|.$$

Applied to set S_L, we get:

$$|S_L| = \left|\bigcup_{l \in L} S_l\right| = \sum_{l \in L} |S_l| - \sum_{\{l_1, l_2\} \subseteq L} |S_{l_1} \cap S_{l_2}| + \sum_{\{l_1, l_2, l_3\} \subseteq L} |S_{l_1} \cap S_{l_2} \cap S_{l_3}| - \cdots + (-1)^{|L|+1} |S_{l_1} \cap \cdots \cap S_{l_{|L|}}|.$$

Note that for all $l \in L, |S_l| = X_{m,m-1}$:

$$|S_L| = (m-i) X_{m,m-1} - \sum_{\{l_1, l_2\} \subseteq L} |S_{l_1} \cap S_{l_2}| + \sum_{\{l_1, l_2, l_3\} \subseteq L} |S_{l_1} \cap S_{l_2} \cap S_{l_3}| - \cdots + (-1)^{|L|+1} |S_{l_1} \cap \cdots \cap S_{l_{|L|}}|. \quad (4.9)$$

We note that as we iterate through subsets $\{l_1, \ldots, l_j\} \subseteq L$, where $j \le |L| = m - i$,

$$\left|\bigcap_{l \in \{l_1, \ldots, l_j\}} S_l\right| = |\{s \in S | \{l_1, \ldots, l_j\} \subseteq s\}| = X_{m,m-j}.$$

Applying this to Equation 4.9, we get

$$|S_L| = (m-i) X_{m,m-1} - \binom{m-i}{2} X_{m,m-2} + \binom{m-i}{3} X_{m,m-3} - \cdots + (-1)^{|L|+1} \binom{m-i}{|L|} X_{m,m-|L|}.$$

Expressed as a summation, this becomes

$$\begin{aligned} |S_L| &= \sum_{a=1}^{m-i} (-1)^{a+1} \binom{m-i}{a} X_{m,m-a}, \\ &= X_{m,m} + \sum_{a=0}^{m-i} (-1)^{a+1} \binom{m-i}{a} X_{m,m-a} \end{aligned}$$

The equation for $Y_t = |S| - |S_L|$ is now

$$\begin{aligned} Y_t &= |S| - X_{m,m} - \sum_{a=0}^{m-i} (-1)^{a+1} \binom{m-i}{a} X_{m,m-a}, \\ &= -\sum_{a=0}^{m-i} (-1)^{a+1} \binom{m-i}{a} X_{m,m-a}, \\ &= \sum_{a=0}^{m-i} (-1)^{a} \binom{m-i}{a} X_{m,m-a} \end{aligned}$$

where the second line follows by remark 3.
Using Equation 4.3, $X_{m,m-a} = \binom{m-a}{i}^{-1}\binom{n-a}{m-a-i}X_{m,i}$:

$$\begin{aligned} Y_t &= \sum_{a=0}^{m-i}(-1)^a\binom{m-i}{a}\binom{m-a}{i}^{-1}\binom{n-a}{m-a-i}X_{m,i}, \\ &= X_{m,i}\sum_{a=0}^{m-i}(-1)^a\binom{m-i}{a}\binom{m-a}{i}^{-1}\binom{n-a}{m-a-i}, \\ &= X_{m,i}\binom{n}{m-i}\binom{m}{i}^{-1}{}_2F_1(i-m,-m;-n;1), \end{aligned} \tag{4.10}$$

where the third line follows from the definition of the Gaussian hypergeometric function.
We know from Lemma 4.4.4 that ${}_2F_1(i-m,-m;-n;1) = \binom{n-m}{m-i}\binom{n}{m-i}^{-1}$:

$$\begin{aligned} Y_t &= X_{m,i}\binom{n}{m-i}\binom{m}{i}^{-1}\binom{n-m}{m-i}\binom{n}{m-i}^{-1}, \\ &= X_{m,i}\binom{m}{i}^{-1}\binom{n-m}{m-i}. \end{aligned}$$

Since t was chosen arbitrarily, this equation can be generalized to:

$$Y_{m,n-2m+i} = \binom{m}{i}^{-1}\binom{n-m}{m-i}X_{m,i} \tag{4.11}$$

□

Claim 4.4.2. *If $S \subseteq \binom{[n]}{m}$ is a level i upper well balanced subset with $Y_{m,i}$, then it is level $2m-n+i$ lower well balanced with $X_{m,2m-n+i} = \binom{n-m}{i}^{-1}\binom{m}{n-m-i}Y_{m,i}$*

Proof. Fix a $t \in \binom{[n]}{m-(2m-n+i)}$. Define $L := t$. It follows that $|L| = m-(2m-n+i) = n-m-i$. For each $l \in L$, define $S_l := \{s \in S | l \in s\}$ to be the set of elements in S that contain l. Define $S_L := \cap_{l\in L} S_l$ to be the set of elements in S that contain all L. It follows directly that $X_t = |S_L|$.
The Principle of Inclusion Exclusion [jh] states that for finite sets $A_1, \ldots, A_n$,

$$\left|\bigcap_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| - \sum_{1\le i<j\le n}|A_i \cup A_j| + \sum_{1\le i<j<k\le n}|A_i\cup A_j\cup A_k| - \cdots + (-1)^{n+1}|A_1\cup\cdots\cup A_n|.$$

Applied to set S_L, we get:

$$\begin{aligned} X_t = |S_L| = \left|\bigcap_{l\in L} S_l\right| = \sum_{l\in L}|S_l| - \sum_{\{l_1,l_2\}\subseteq L}|S_{l_1}\cup S_{l_2}| + \sum_{\{l_1,l_2,l_3\}\subseteq L}|S_{l_1}\cup S_{l_2}\cup S_{l_3}| \\ - \cdots + (-1)^{|L|+1}|S_{l_1}\cup\cdots\cup S_{l_{|L|}}|. \end{aligned}$$

We note that for any $l \in L, |S_l| = |S| - |\{s \in S | l \notin s\}|$. From remark 6, we know that $|S| = Y_{m,n-m}$. Since S is upper well balanced, $|\{s \in S | l \notin s\}| = Y_{m,n-m-1}$ for any l:

$$\begin{aligned} X_t = (n-m-i)(Y_{n,n-m} - Y_{n,n-m-1}) - \sum_{\{l_1,l_2\}\subseteq L}|S_{l_1}\cup S_{l_2}| + \sum_{\{l_1,l_2,l_3\}\subseteq L}|S_{l_1}\cup S_{l_2}\cup S_{l_3}| \\ - \cdots + (-1)^{|L|+1}|S_{l_1}\cup\cdots\cup S_{l_{|L|}}|. \end{aligned} \tag{4.12}$$

We note that as we iterate through subsets $\{l_1, \ldots, l_j\} \subseteq L$,

$$\left| \bigcup_{l \in \{l_1, \ldots, l_j\}} S_l \right| = |S| - |\{s \in S | \{l_1, \ldots, l_j\} \nsubseteq s\}| = (Y_{m,n-m} - Y_{m,n-m-j}).$$

Applying this to Equation 4.12, we get

$$\begin{aligned} X_t = (n-m-i)(Y_{m,n-m} - Y_{m,n-m-1}) - \binom{n-m-i}{2}(Y_{m,n-m} - Y_{m,n-m-2}) \\ + \cdots + (-1)^{|L|+1}\binom{n-m-i}{|L|}(Y_{m,n-m} - Y_{m,n-m-|L|}). \end{aligned} \tag{4.13}$$

Expressed as a summation, this becomes

$$\begin{aligned} X_t &= \sum_{a=0}^{n-m-i} (-1)^{a+1}\binom{n-m-i}{a}(Y_{m,n-m} - Y_{m,n-m-a}) \\ &= \sum_{a=0}^{n-m-i} (-1)^{a+1}\binom{n-m-i}{a}Y_{m,n-m} + \sum_{a=0}^{n-m-i} (-1)^{a}\binom{n-m-i}{a}Y_{m,n-m-a} \\ &= \sum_{a=0}^{n-m-i} (-1)^{a}\binom{n-m-i}{a}Y_{m,n-m-a}, \end{aligned}$$

where the third line follows from the Binomial Theorem. Using Equation 4.7, $Y_{m,n-m-a} = \binom{n-m-a}{i}^{-1}\binom{n-a}{m+i}Y_{m,i}$:

$$\begin{aligned} X_t &= \sum_{a=0}^{n-m-i} (-1)^{a}\binom{n-m-i}{a}\binom{n-m-a}{i}^{-1}\binom{n-a}{m+i}Y_{m,i}, \\ &= Y_{m,i}\binom{n}{m+i}\binom{n-m}{i}^{-1} {}_2F_1(m-n, i+m-n; -n; 1) \end{aligned}$$

where the second line follows from the definition of the Gaussian hypergeometric function. We know from Lemma 4.4.5 that ${}_2F_1(m-n, i+m-n; -n; 1) = \binom{m+i}{n-m}\binom{n}{n-m}^{-1}$:

$$\begin{aligned} X_t &= Y_{m,i}\binom{n}{m+i}\binom{n-m}{i}^{-1}\binom{m+i}{n-m}\binom{n}{n-m}^{-1} \\ &= Y_{m,i}\binom{n-m}{i}^{-1}\binom{m}{n-m-i} \end{aligned}$$

where the second line follows from simplifying. Since t was chosen arbitrarily, this equation can be generalized to:

$$X_{m,2m-n+i} = \binom{n-m}{i}^{-1}\binom{m}{n-m-i}Y_{m,i} \tag{4.14}$$

□

Corollary 4.4.3. *If a nontrivial subset $S \subseteq \binom{[n]}{m}$ is level 1 upper well balanced and level 1 lower well balanced, then $m = n/2$.*

Proof. If a subset $S \subseteq \binom{[n]}{m}$ is level 1 upper well balanced, then we know from Claim 4.3.5 that $m \geq n/2$. If the same subset is level 1 lower well balanced, then we know from Claim 4.2.6 that $m \leq n/2$. Therefore $m = n/2$. □

Lemma 4.4.4. *Let* $0 < i < m < n$. *Then* ${}_2F_1(i-m, -m; -n; 1) = \binom{n-m}{m-i}\binom{n}{m-i}^{-1}$

Proof. The Jacobi Polynomial $P_n^{(\alpha,\beta)}(z)$ is defined as

$$P_n^{(\alpha,\beta)}(z) = \binom{\alpha+n}{n} {}_2F_1(-n, 1+\alpha+\beta+n; \alpha+1; \frac{1}{2}(1-z))$$

Using this definition we know that

$$P_{m-i}^{(-n-1,n-2m+i)}(-1) = \binom{m-n-i-1}{m-i} {}_2F_1(i-m, -m; -n; 1)$$

Following the symmetry relation of Jacobi Polynomials, $P_{m-i}^{(-n-1,-2m+i+n)}(-1)$ can be normalized to $(-1)^{m-i}\binom{m-i-2m+i+n}{m-i} = (-1)^{m-i}\binom{n-m}{m-i}$:

$$(-1)^{m-i}\binom{n-m}{m-i} = \binom{m-n-i-1}{m-i} {}_2F_1(i-m, -m; -n; 1) \tag{4.15}$$

Note that $m-n-i-1 < 0$, so the binomial coefficient for negative arguments is used [Kro11]:

$$\binom{m-n-i-1}{m-i} = (-1)^{m-i}\binom{n+i+1-m+m-i-1}{m-i} = (-1)^{m-i}\binom{n}{m-i}$$

Equation 4.15 becomes

$$\begin{aligned}(-1)^{m-i}\binom{n-m}{m-i} &= (-1)^{m-i}\binom{n}{m-i} {}_2F_1(i-m, -m; -n; 1)\\ \binom{n-m}{m-i}\binom{n}{m-i}^{-1} &= {}_2F_1(i-m, -m; -n; 1)\end{aligned}$$

□

Lemma 4.4.5. *Let* $0 < i < m < n$. *Then* ${}_2F_1(m-n, i+m-n; -n; 1) = \binom{m+i}{n-m}\binom{n}{n-m}^{-1}$

Proof. The Jacobi Polynomial $P_n^{(\alpha,\beta)}(z)$ is defined as

$$P_n^{(\alpha,\beta)}(z) = \binom{\alpha+n}{n} {}_2F_1(-n, 1+\alpha+\beta+n; \alpha+1; \frac{1}{2}(1-z))$$

Using this definition we know that

$$P_{n-m}^{(-n-1,i+2m-n)}(-1) = \binom{-m-1}{n-m} {}_2F_1(m-n, i+m-n; -n; 1)$$

Following the symmetry relation of Jacobi Polynomials, $P_{n-m}^{(-n-1,i+2m-n)}(-1)$ can be normalized to $(-1)^{n-m}\binom{n-m+i+2m-n}{n-m} = (-1)^{n-m}\binom{m+i}{n-m}$:

$$(-1)^{n-m}\binom{m+i}{n-m} = \binom{-m-1}{n-m} {}_2F_1(m-n, i+m-n; -n; 1) \tag{4.16}$$

Note that $-m-1<0$, so the binomial coefficient for negative arguments is used [Kro11]:

$$\binom{-m-1}{n-m} = (-1)^{n-m}\binom{m+1+n-m-1}{n-m} = (-1)^{n-m}\binom{n}{n-m}$$

Equation 4.16 becomes

$$\begin{aligned}
(-1)^{n-m}\binom{m+i}{n-m} &= (-1)^{n-m}\binom{n}{n-m}\,{}_2F_1(m-n, i+m-n; -n; 1) \\
\binom{m+i}{n-m}\binom{n}{n-m}^{-1} &= {}_2F_1(i-m, -m; -n; 1)
\end{aligned}$$

□

Chapter 5

Results of Scan

5.1 Introduction

This chapter reviews an exhaustive search conducted to find the properties that a Boolean function that is fully sensitive on the input with all 0's with upper well balanced degree 3 and degree 4 terms might have.

Specifically, in an effort to find a Boolean function with a larger separation between sensitivity and degree than the Kushilevitz function, the goal of this search is to find what characteristics a Boolean function $f : \{0,1\}^{10} \to \{0,1\}$ with $deg(f) = 4$ and $s(f) = 10$ might have, if such a function exists. These constraints are chosen because the power separation between its sensitivity and degree is $s(f) = deg(f)^{log(10)/log(4)} = deg(f)^{1.66}$, which is a greater separation than the Kushilevitz function. We do not search for functions with $deg(f) = 3$, since there does not exist a Boolean function with $f : \{0,1\}^n \to \{0,1\}$ such that $n \geq 7, s(f) \geq 7, deg(f) = 3$ [MMST21].

5.1.1 Constraints and Assumptions

In order to ensure that any function that is found in the search is fully sensitive, without loss of generality we let the input with hamming weight 0 be the input with full sensitivity. For this to be true, $f(0,\ldots,0) = 0$, and $f(x_0,\ldots,x_n) = 1$ for inputs $x_0,\ldots,x_n$ with hamming weight 1.

Note that in order for inputs x with hamming weight 2 to have an output of 0 or 1, a degree 2 term must be added with coefficient -1 or -2 for each permutation of x such that $|x| = 2$. For this search, we assume the degree 2 terms have coefficient -1.

Thus we search for functions which are constrained to the following stub:

$$f(x_0,\ldots,x_n) = \sum_{i=0}^{n} x_i - \sum_{\{i,j\}\subseteq[n]} x_i x_j + \cdots$$

For some input $x = (x_1,\ldots,x_{10})$, a function with this stub is represented by the following

table:

$\|x\|$	$f^{=1}(x)$	$f^{=2}(x)$	$f^{\leq 2}(x)$
0	0	0	0
1	1	0	1
2	2	-1	1
3	3	-3	0
4	4	-6	-2
5	5	-10	-5
6	6	-15	-9
7	7	-21	-14
8	8	-28	-20
9	9	-36	-27
10	10	-45	-35

We note that for the function to be Boolean, $f^{=3}(x) + f^{=4}(x)$ should equal 2 or 3 for inputs x with hamming weight $|x| = 4$, $+5$ or $+6$ for inputs x with hamming weight $|x| = 5$, and so on. An exhaustive search through all possible combinations of degree 3 and degree 4 terms to find those that satisfy these constraints is not possible ($2^{\binom{10}{3}} * 2^{\binom{10}{4}}$ different combinations of degree 3 and degree 4 terms, before considering variations of coefficients). A better strategy is then to constrain the search space.

We constrain the search to those Boolean functions that have upper well balanced degree 3 and degree 4 terms. The reasons for this are twofold:

- The degree 3 terms of the Kushilevitz function are upper well balanced. Like the Kushilevitz function, a function with the properties $n = 10, deg(f) = 4, s(f) = 10$ may also have upper well balanced degree 3 and degree 4 terms.

- Since level i upper well balanced subsets are deterministic with respect to their inclusion in any subset of $[n]$ of size greater than $m + i$ (see Claim 4.3.3), it is easy to set up a system of equations for solutions to the characteristics of the upper well balanced subset (i.e. scanning for n, m, i, Y), as will soon be seen.

For now, we assume the degree 3 and degree 4 terms are level 1 upper well balanced subsets. The following system of equations adequately describe the constraints above:

$\|x\|$	$f^{\leq 2}(x)$	$f^{=3}(x) + f^{=4}(x)$	$f(x)$
5	-5	$cY_{3,2} + cY_{4,1}$	$\{0, 1\}$
6	-9	$cY_{3,3} + cY_{4,2}$	$\{0, 1\}$
7	-14	$cY_{3,4} + cY_{4,3}$	$\{0, 1\}$
8	-20	$cY_{3,5} + cY_{4,4}$	$\{0, 1\}$
9	-27	$cY_{3,6} + cY_{4,5}$	$\{0, 1\}$
10	-35	$cY_{3,7} + cY_{4,6}$	$\{0, 1\}$

Since for inputs x with hamming weight 3, the function stub $f(x) = 0$, note that any degree 3 terms that may be in the Boolean function must have a coefficient of $+1$.

Furthermore, we assume that any degree 4 terms that may be in the function will

have a coefficient of -1. Thus the system of equations is modified to:

$$\begin{aligned}
-5 + Y_{3,2} - Y_{4,1} &= \{0,1\} \\
-9 + Y_{3,3} - Y_{4,2} &= \{0,1\} \\
-14 + Y_{3,4} - Y_{4,3} &= \{0,1\} \\
-20 + Y_{3,5} - Y_{4,4} &= \{0,1\} \\
-27 + Y_{3,6} - Y_{4,5} &= \{0,1\} \\
-35 + Y_{3,7} - Y_{4,6} &= \{0,1\}
\end{aligned}$$

Recall from Claim 4.3.3 that for a level 1 upper well balanced subset $S \subseteq \binom{[n]}{m}$ with $Y_{m,1}$,

$$Y_{m,k} = \frac{1}{k}\binom{m+k}{m+1} Y_{m,1},$$

where k is an integer such that $2 \leq k \leq n - m$. Thus, the equations can be further simplified to:

$$\begin{aligned}
-5 + \frac{1}{2}\binom{5}{4} Y_{3,1} - Y_{4,1} &= \{0,1\} \\
-9 + \frac{1}{3}\binom{6}{4} Y_{3,1} - \frac{1}{2}\binom{6}{5} Y_{4,1} &= \{0,1\} \\
-14 + \frac{1}{4}\binom{7}{4} Y_{3,1} - \frac{1}{3}\binom{7}{5} Y_{4,1} &= \{0,1\} \\
-20 + \frac{1}{5}\binom{8}{4} Y_{3,1} - \frac{1}{4}\binom{8}{5} Y_{4,1} &= \{0,1\} \\
-27 + \frac{1}{6}\binom{9}{4} Y_{3,1} - \frac{1}{5}\binom{9}{5} Y_{4,1} &= \{0,1\} \\
-35 + \frac{1}{7}\binom{10}{4} Y_{3,1} - \frac{1}{6}\binom{10}{5} Y_{4,1} &= \{0,1\}
\end{aligned}$$

This simplifies to

$$\begin{aligned}
-5 + 2.5Y_{3,1} - Y_{4,1} &= \{0,1\} \\
-9 + 5Y_{3,1} - 3Y_{4,1} &= \{0,1\} \\
-14 + 8.75Y_{3,1} - 7Y_{4,1} &= \{0,1\} \\
-20 + 14Y_{3,1} - 14Y_{4,1} &= \{0,1\} \\
-27 + 21Y_{3,1} - 25.2Y_{4,1} &= \{0,1\} \\
-35 + 30Y_{3,1} - 42Y_{4,1} &= \{0,1\}
\end{aligned}$$

In order to accommodate upper well balanced subsets of levels $i > 1$, we relax the right side of the system of equations to allow some fraction of inputs of a certain hamming

weight to be 0, and the others to have 1.

$$
\begin{aligned}
-5 + 2.5Y_{3,1} - Y_{4,1} &= \left\{ \frac{0}{\binom{10}{5}}, \frac{1}{\binom{10}{5}}, \dots \frac{\binom{10}{5}}{\binom{10}{5}} \right\} \\
-9 + 5Y_{3,1} - 3Y_{4,1} &= \left\{ \frac{0}{\binom{10}{6}}, \frac{1}{\binom{10}{6}}, \dots \frac{\binom{10}{6}}{\binom{10}{6}} \right\} \\
-14 + 8.75Y_{3,1} - 7Y_{4,1} &= \left\{ \frac{0}{\binom{10}{7}}, \frac{1}{\binom{10}{7}}, \dots \frac{\binom{10}{7}}{\binom{10}{7}} \right\} \\
-20 + 14Y_{3,1} - 14Y_{4,1} &= \left\{ \frac{0}{\binom{10}{8}}, \frac{1}{\binom{10}{8}}, \dots \frac{\binom{10}{8}}{\binom{10}{8}} \right\} \\
-27 + 21Y_{3,1} - 25.2Y_{4,1} &= \left\{ \frac{0}{\binom{10}{9}}, \frac{1}{\binom{10}{9}}, \dots \frac{\binom{10}{9}}{\binom{10}{9}} \right\} \\
-35 + 30Y_{3,1} - 42Y_{4,1} &= \{0, 1\}
\end{aligned}
$$

We also allow $Y_{m,1}$ to be rational numbers as well as integers in the scan. In order to interpret rational number solutions for $Y_{m,1}$, we use the following remark.

Remark 7. *If $S \subseteq \binom{[n]}{m}$ is a level i upper well balanced subset with $Y_{m,i}$, then for $t \in \binom{[n]}{m+1}$, the average value of $Y_{m,1}$ is $\mathbb{E}(|\{s \in S | s \subseteq t\}|) = i\binom{m+i}{m+1}^{-1} Y_{m,i}$*

5.1.2 Search Setup and Interpreting Results

We begin by searching for Boolean functions with $n = 7, deg(f) = 4, s(f) = 7$, then expand the search until we reach $n = 10, deg(f) = 4, s(f) = 10$. For each $n \in \{7, 8, 9, 10\}$, the system of equations above is checked for exact solutions up to hamming weight n.

For a solution pair $(Y_{3,1}, Y_{4,1}) = (a, b)$, we use Remark 7 to map the solution to $(Y_{3,i}, Y_{4,j}) = (a', b')$, where i, j are the smallest positive integers such that $a' = (a/i) * \binom{m+i}{m+1}$ and $b' = (b/j) * \binom{m+j}{m+1}$ are integers, respectively. Solutions with a (*) are solutions that involve degree 3 terms that are level $n-3$ upper well balanced, or degree 4 terms that are level $n-4$ upper well balanced. By definition, these are not upper well balanced subsets. They are included here for completeness. Solution rows that are gray represent solutions whose explicit Boolean function is presented in the section after.

5.2 n=7

The least squares solution to the following system of equations is computed.

$$
\begin{bmatrix} 2.5 & -1 \\ 5 & -3 \\ 8.75 & -7 \end{bmatrix} \begin{bmatrix} Y_{3,1} \\ Y_{4,1} \end{bmatrix} = \begin{bmatrix} h_5 \\ h_6 \\ h_7 \end{bmatrix}
$$

where $h_5 \in \left\{ 5\frac{0}{\binom{7}{5}}, 5\frac{1}{\binom{7}{5}}, \dots 5\frac{\binom{7}{5}}{\binom{7}{5}} \right\}, h_6 \in \left\{ 9\frac{0}{\binom{7}{6}}, 9\frac{1}{\binom{7}{6}}, \dots 9\frac{\binom{7}{6}}{\binom{7}{6}} \right\}, h_7 \in \{14, 15\}$.

5.2.1 Solutions

Exact solutions are shown in the table below. Solutions are enumerated for reference.

	$\mathbf{h_5}$	$\mathbf{h_6}$	$\mathbf{h_7}$	$(\mathbf{Y_{3,1}}, \mathbf{Y_{4,1}})$	**map**
1	5	9	14	$(2.4, 1)$	$(Y_{3,2}, Y_{4,1}) = (6, 1)$
2	6	10	14	$(3.2, 2)$	$(Y_{3,2}, Y_{4,1}) = (8, 2)$
3	5	65/7	15	$(2.286, 0.714)$	$(Y_{3,4}, Y_{4,3}) = (20, 5)*$
4	36/7	64/7	14	$(2.514, 1.143)$	$(Y_{3,4}, Y_{4,3}) = (22, 8)*$
5	36/7	66/7	15	$(2.4, 0.857)$	$(Y_{3,2}, Y_{4,3}) = (6, 6)*$
6	37/7	65/7	14	$(2.629, 1.286)$	$(Y_{3,4}, Y_{4,3}) = (23, 9)*$
7	37/7	67/7	15	$(2.514, 1)$	$(Y_{3,4}, Y_{4,1}) = (22, 1)*$
8	38/7	66/7	14	$(2.743, 1.429)$	$(Y_{3,4}, Y_{4,3}) = (24, 10)*$
9	38/7	68/7	15	$(2.629, 1.143)$	$(Y_{3,4}, Y_{4,3}) = (23, 8)*$
10	39/7	67/7	14	$(2.857, 1.571)$	$(Y_{3,4}, Y_{4,3}) = (25, 11)*$
11	39/7	69/7	15	$(2.743, 1.286)$	$(Y_{3,4}, Y_{4,3}) = (24, 9)*$
12	40/7	68/7	14	$(2.971, 1.714)$	$(Y_{3,4}, Y_{4,3}) = (26, 12)*$
13	40/7	10	15	$(2.857, 1.429)$	$(Y_{3,4}, Y_{4,3}) = (25, 10)*$
14	41/7	69/7	14	$(3.086, 1.857)$	$(Y_{3,4}, Y_{4,3}) = (27, 13)*$

5.2.2 Boolean Functions

We present four Boolean functions with $n = 7, deg = 4, s = 7$.

(1) Ledins [LO] shows a Boolean function $f : \{0,1\}^7 \to \{0,1\}$ with $s(f) = 7, deg(f) = 4$:

$$f(x_1, \ldots, x_7) = \sum_{i=1}^{7} x_i - \sum_{\{i,j\} \in \binom{[7]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$\begin{aligned} A = \{&\{1,2,3\}, \{1,2,5\}, \{1,2,7\}, \{1,3,6\}, \{1,3,7\}, \{1,4,5\}, \{1,4,6\}, \\ &\{1,4,7\}, \{1,5,6\}, \{2,3,4\}, \{2,3,5\}, \{2,4,6\}, \{2,4,7\}, \{2,5,6\}, \\ &\{2,6,7\}, \{3,4,5\}, \{3,4,6\}, \{3,5,7\}, \{3,6,7\}, \{4,5,7\}, \{5,6,7\}\}, \\ B = \{&\{1,2,3,7\}, \{1,2,5,6\}, \{1,3,4,6\}, \{1,4,5,7\}, \{2,3,4,5\}, \{2,4,6,7\}, \{3,5,6,7\}\} \end{aligned}$$

For some input $x = (x_1, \ldots, x_7)$, the function $f(x)$ can be represented by the following table:

$\boldsymbol{\lvert x \rvert}$	$\boldsymbol{f^{<=2}(x)}$	$\boldsymbol{f^{=3}(x)}$	$\boldsymbol{f^{=4}(x)}$	$\boldsymbol{f(x)}$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	1 21/35 times 0 14/35 times	0	1 21/35 times 0 14/35 times
4	-2	2 21/35 times 3 14/35 times	0 28/35 times -1 7/35 times	1 7/35 times 0 28/35 times
5	-5	6	-1	0
6	-9	12	-3	0
7	-14	21	-7	0

Note that the degree 3 terms are level 2 upper well balanced, with $Y_{3,2} = 6$, and the degree 4 terms are level 1 upper well balanced, with $Y_{4,1} = 1$. This Boolean function is an explicit form of solution 1 from the table in Section 5.2.1.

(2) We construct a Boolean function $f : \{0,1\}^7 \to \{0,1\}$ with $s(f) = 7, deg(f) = 4$, with the properties of solution 2 from the table in Section 5.2.1:

$$f(x_1, \ldots, x_7) = \sum_{i=1}^{7} x_i - \sum_{\{i,j\} \in \binom{[7]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$\begin{aligned} A = \{&\{1,2,3\}, \{1,2,4\}, \{1,2,6\}, \{1,2,7\}, \{1,3,5\}, \{1,3,6\}, \{1,3,7\}, \{1,4,5\}, \\ &\{1,4,6\}, \{1,4,7\}, \{1,5,6\}, \{1,5,7\}, \{2,3,4\}, \{2,3,5\}, \{2,3,7\}, \{2,4,5\}, \\ &\{2,4,6\}, \{2,5,6\}, \{2,5,7\}, \{2,6,7\}, \{3,4,5\}, \{3,4,6\}, \{3,4,7\}, \{3,5,6\}, \\ &\{3,6,7\}, \{4,5,7\}, \{4,6,7\}, \{5,6,7\}\} \\ B = \{&\{2,5,6,7\}, \{3,4,6,7\}, \{1,4,5,7\}, \{2,3,4,5\}, \{1,2,4,6\}, \{1,3,5,6\}, \{1,2,3,7\}, \\ &\{4,5,6,7\}, \{2,3,4,7\}, \{2,3,5,6\}, \{1,3,4,6\}, \{1,3,5,7\}, \{1,2,4,5\}, \{1,2,6,7\}\} \end{aligned}$$

For some input $x = (x_1, \ldots, x_7)$, the function $f(x)$ can be represented by the following table:

$\|x\|$	$f^{<=2}(x)$	$f^{=3}(x)$	$f^{=4}(x)$	$f(x)$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	1 28/35 times 0 7/35 times	0	0 7/35 times 1 28/35 times
4	-2	3 28/35 times 4 7/35 times	0 21/35 times -1 14/35 times	0 7/35 times 1 28/35 times
5	-5	8	-2	1
6	-9	16	-6	1
7	-14	28	-14	0

Note that the degree 3 terms are level 2 upper well balanced, with $Y_{3,2} = 8$, and the degree 4 terms are level 1 upper well balanced, with $Y_{4,1} = 2$. This function was created by using Algorithm 6.2 with parameters $(n = 7, m = 4, i = 1, Y = 2, res = 1)$ to find the degree 4 terms, and then doing a scan over all $\binom{\binom{[7]}{3}}{28}$ sets of 28 degree 3 terms to find the set that fit the degree 4 terms. This Boolean function is an explicit form of solution 2 from the table in Section 5.2.1.

(3) The following Boolean function $f : \{0,1\}^7 \to \{0,1\}$ has $deg(f) = 4$ and $s(f) = 7$. It is constructed by retrieving the polynomial of $f : \{0,1\}^9 \to \{0,1\}$ from Section 5.4.2 on the input $(0, x_2, \ldots, x_8, 0)$:

$$f(x_1, \ldots, x_7) = \sum_{i=1}^{7} x_i - \sum_{\{i,j\} \in \binom{[7]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$A = \{\{1,3,4\},\{1,3,5\},\{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,6,7\},\{2,6,7\},\{1,2,6\},\{1,2,7\},\{3,6,7\},\{4,6,7\},\{5,6,7\},\{3,4,6\},\{3,4,7\},\{3,5,6\},\{3,5,7\},\{4,5,6\},\{4,5,7\}\}$$
$$B = \{\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,2,6,7\},\{3,4,6,7\},\{3,5,6,7\},\{4,5,6,7\}\}$$

For some input $x = (x_1, \ldots, x_7)$, the function $f(x)$ can be represented by the following table:

$\|x\|$	$f^{<=2}(x)$	$f^{=3}(x)$	$f^{=4}(x)$	$f(x)$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	0 13/35 times 1 22/35 times	0	0 13/35 times 1 22/35 times
4	-2	2 24/35 times 3 4/35 times 4 7/35 times	0 28/35 times -1 7/35 times	0 24/35 times 1 11/35 times
5	-5	6 19/21 times 9 2/21 times	0 4/21 times -1 15/21 times -3 2/21 times	0 15/21 times 1 6/21 times
6	-9	12 3/7 times 13 4/7 times	-3	0 3/7 times 1 4/7 times
7	-14	22	-7	1

This Boolean function is an explicit form of solution 7 from the table in Section 5.2.1.

(4) The following Boolean function $f : \{0,1\}^7 \to \{0,1\}$ has $deg(f) = 4$ and $s(f) = 7$. It is constructed by retrieving the polynomial of $f : \{0,1\}^9 \to \{0,1\}$ from Section 5.4.2 on the input $(x_1, \ldots, x_7, 0, 0)$:

$$f(x_1, \ldots, x_7) = \sum_{i=1}^{7} x_i - \sum_{\{i,j\} \in \binom{[7]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$A = \{\{1,4,5\},\{1,4,6\},\{1,5,6\},\{2,4,5\},\{2,4,6\},\{2,5,6\},\{3,4,5\},\{3,4,6\},\{3,5,6\},\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,3,6\},\{2,3,4\},\{2,3,5\},\{2,3,6\},\{1,2,7\},\{1,3,7\},\{2,3,7\},\{4,5,7\},\{4,6,7\},\{5,6,7\}\}$$
$$B = \{\{1,2,4,5\},\{1,2,4,6\},\{1,2,5,6\},\{1,3,4,5\},\{1,3,4,6\},\{1,3,5,6\},\{2,3,4,5\},\{2,3,4,6\},\{2,3,5,6\}\}$$

For some input $x = (x_1, \ldots, x_7)$, the function $f(x)$ can be represented by the following

table:

$\|x\|$	$f^{<=2}(x)$	$f^{=3}(x)$	$f^{=4}(x)$	$f(x)$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	0 11/35 times 1 24/35 times	0	0 11/35 times 1 24/35 times
4	-2	2 18/35 times 3 8/35 times 4 9/35 times	0 26/35 times -1 9/35 times	0 18/35 times 1 17/35 times
5	-5	6 15/21 times 9 6/21 times	0 6/21 times -1 9/21 times -3 6/21 times	0 9/21 times 1 12/21 times
6	-9	13 6/7 times 18 1/7 times	-3 6/7 times -9 1/7 times	0 1/7 times 1 6/7 times
7	-14	24	-9	1

This Boolean function is an explicit form of solution 11 from the table in Section 5.2.1.

5.3 n=8

The following system of equations is checked for solutions:

$$\begin{bmatrix} 2.5 & -1 \\ 5 & -3 \\ 8.75 & -7 \\ 14 & -14 \end{bmatrix} \begin{bmatrix} Y_{3,1} \\ Y_{4,1} \end{bmatrix} = \begin{bmatrix} h_5 \\ h_6 \\ h_7 \\ h_8 \end{bmatrix}$$

where

$$h_5 \in \left\{ 5\frac{0}{\binom{8}{5}}, 5\frac{1}{\binom{8}{5}}, \ldots 5\frac{\binom{8}{5}}{\binom{8}{5}} \right\}, \qquad h_6 \in \left\{ 9\frac{0}{\binom{8}{6}}, 9\frac{1}{\binom{8}{6}}, \ldots 9\frac{\binom{8}{6}}{\binom{8}{6}} \right\}$$

$$h_7 \in \left\{ 14\frac{0}{\binom{8}{7}}, 14\frac{1}{\binom{8}{7}}, \ldots 14\frac{\binom{8}{7}}{\binom{8}{7}} \right\}, \qquad h_8 \in \{20, 21\}.$$

5.3.1 Solutions

Exact solutions are shown in the table below. Solutions are enumerated for reference.

	$\mathbf{h_5}$	$\mathbf{h_6}$	$\mathbf{h_7}$	$\mathbf{h_8}$	$(\mathbf{Y_{3,1}}, \mathbf{Y_{4,1}})$	**map**
1	40/7	10	15	20	$(2.857, 1.429)$	$(Y_{3,4}, Y_{4,3}) = (25, 10)$
2	66/13	129/14	117/8	21	$(2.357, 0.857)$	$(Y_{3,5}, Y_{4,3}) = (33, 6)*$
3	71/14	64/7	57/4	20	$(2.429, 1)$	$(Y_{3,5}, Y_{4,1}) = (34, 1) *$ [1]
4	36/7	131/14	59/4	21	$(2.429, 0.929)$	$(Y_{3,5}, Y_{4,4}) = (34, 13)*$
5	145/28	65/7	115/8	20	$(2.5, 1.071)$	$(Y_{3,5}, Y_{4,4}) = (35, 15)*$
6	21/4	19/2	119/8	21	$(2.5, 1)$	$(Y_{3,5}, Y_{4,1}) = (35, 1) *$ [1]
7	37/7	66/7	29/2	20	$(2.571, 1.143)$	$(Y_{3,5}, Y_{4,3}) = (36, 8)*$
8	75/14	135/14	15	21	$(2.571, 1.071)$	$(Y_{3,5}, Y_{4,4}) = (36, 15)*$
9	151/28	67/7	117/8	20	$(2.643, 1.214)$	$(Y_{3,5}, Y_{4,4}) = (37, 17)*$
10	11/2	68/7	59/4	20	$(2.714, 1.286)$	$(Y_{3,5}, Y_{4,3}) = (38, 9)*$
11	157/28	69/7	119/8	20	$(2.786, 1.357)$	$(Y_{3,5}, Y_{4,4}) = (39, 19)*$

5.3.2 Boolean Functions

The following Boolean function $f : \{0,1\}^8 \to \{0,1\}$ has $deg(f) = 4$ and $s(f) = 8$. It is constructed by retrieving the polynomial of $f : \{0,1\}^9 \to \{0,1\}$ from Section 5.4.2 on the input $(x_1, \ldots, x_8, 0)$:

$$f(x_1, \ldots, x_8) = \sum_{i=1}^{8} x_i - \sum_{\{i,j\} \in \binom{[8]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$\begin{aligned} A = \{&\{1,4,5\}, \{1,4,6\}, \{1,5,6\}, \{2,4,5\}, \{2,4,6\}, \{2,5,6\}, \{3,4,5\}, \{3,4,6\}, \{3,5,6\}, \\ &\{1,2,4\}, \{1,2,5\}, \{1,2,6\}, \{1,3,4\}, \{1,3,5\}, \{1,3,6\}, \{2,3,4\}, \{2,3,5\}, \{2,3,6\}, \\ &\{1,7,8\}, \{2,7,8\}, \{3,7,8\}, \{1,2,7\}, \{1,2,8\}, \{1,3,7\}, \{1,3,8\}, \{2,3,7\}, \{2,3,8\}, \\ &\{4,7,8\}, \{5,7,8\}, \{6,7,8\}, \{4,5,7\}, \{4,5,8\}, \{4,6,7\}, \{4,6,8\}, \{5,6,7\}, \{5,6,8\}\} \\ B = \{&\{1,2,4,5\}, \{1,2,4,6\}, \{1,2,5,6\}, \{1,3,4,5\}, \{1,3,4,6\}, \{1,3,5,6\}, \{2,3,4,5\}, \\ &\{2,3,4,6\}, \{2,3,5,6\}, \{1,2,7,8\}, \{1,3,7,8\}, \{2,3,7,8\}, \{4,5,7,8\}, \{4,6,7,8\}, \\ &\{5,6,7,8\}\} \end{aligned}$$

For some input $x = (x_1, \ldots, x_8)$, the function $f(x)$ can be represented by the following

table:

$\lvert x\rvert$	$f^{<=2}(x)$	$f^{=3}(x)$	$f^{=4}(x)$	$f(x)$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	0 20/56 times 1 36/56 times	0	0 20/56 times 1 36/56 times
4	-2	2 45/70 times 3 10/70 times 4 15/70 times	0 55/70 times -1 15/70 times	0 45/70 times 1 25/70 times
5	-5	6 48/56 times 8 8/56 times	0 12/56 times -1 36/56 times -3 8/56 times	0 36/56 times 1 20/56 times
6	-9	12 9/28 times 13 18/28 times 18 1/28 times	-3 27/28 times -9 1/28 times	0 10/28 times 1 18/28 times
7	-14	22 6/8 times 24 2/8 times	-7 6/8 times -9 2/8 times	1
8	-20	36	-15	1

Note that this function is an explicit form of solution 8 from the table in Section 5.3.1.

5.4 n=9

The following system of equations is checked for solutions:

$$\begin{bmatrix} 2.5 & -1 \\ 5 & -3 \\ 8.75 & -7 \\ 14 & -14 \\ 21 & -25.2 \end{bmatrix} \begin{bmatrix} Y_{3,1} \\ Y_{4,1} \end{bmatrix} = \begin{bmatrix} h_5 \\ h_6 \\ h_7 \\ h_8 \\ h_9 \end{bmatrix}$$

where

$$h_5 \in \left\{ 5\frac{0}{\binom{9}{5}}, 5\frac{1}{\binom{9}{5}}, \ldots 5\frac{\binom{9}{5}}{\binom{9}{5}} \right\}, \qquad h_6 \in \left\{ 9\frac{0}{\binom{9}{6}}, 9\frac{1}{\binom{9}{6}}, \ldots 9\frac{\binom{9}{6}}{\binom{9}{6}} \right\},$$

$$h_7 \in \left\{ 14\frac{0}{\binom{9}{7}}, 14\frac{1}{\binom{9}{7}}, \ldots 14\frac{\binom{9}{7}}{\binom{9}{7}} \right\}, \quad h_8 \in \left\{ 20\frac{0}{\binom{9}{8}}, 20\frac{1}{\binom{9}{8}}, \ldots 20\frac{\binom{9}{8}}{\binom{9}{8}} \right\}, h_9 \in \{27, 28\}.$$

5.4.1 Solutions

Exact solutions are shown in the table below. Solutions are enumerated for reference.

	$\mathbf{h_5}$	$\mathbf{h_6}$	$\mathbf{h_7}$	$\mathbf{h_8}$	$\mathbf{h_9}$	$(\mathbf{Y_{3,1}}, \mathbf{Y_{4,1}})$	**map**
1	75/14	135/14	15	21	27	$(2.571, 1.071)$	$(Y_{3,5}, Y_{4,4}) = (36, 15)$
2	5	55/6	175/12	21	28	$(2.333, 0.833)$	$(Y_{3,6}, Y_{4,5}) = (49, 21)*$
3	635/126	55/6	130/9	185/9	27	$(2.381, 0.913)$	$(Y_{3,6}, Y_{4,5}) = (50, 23)*$
4	215/42	65/7	175/12	62/3	27	$(2.429, 0.952)$	$(Y_{3,5}, Y_{4,5}) = (34, 24)*$
5	655/126	395/42	265/18	187/9	27	$(2.476, 0.992)$	$(Y_{3,6}, Y_{4,5}) = (52, 25)*$
6	95/18	200/21	535/36	188/9	27	$(2.524, 1.032)$	$(Y_{3,6}, Y_{4,5}) = (53, 26)*$

5.4.2 Boolean Functions

Using composition on the function $f' : \{0,1\}^3 \to \{0,1\}$ with $s(f') = 3$, $deg(f') = 2$, found in [NW95], the following function $f : \{0,1\}^9 \to \{0,1\}$ with $s(f) = 9, deg(f) = 4$ is constructed:

$$f(x_1, \ldots, x_9) = f' \diamond f' = \sum_{i=1}^{9} x_i - \sum_{\{i,j\} \in \binom{[9]}{2}} x_i x_j + \sum_{\{i,j,k\} \in A} x_i x_j x_k - \sum_{\{i,j,k,l\} \in B} x_i x_j x_k x_l,$$

where

$$\begin{aligned} A = \{&\{1,4,5\},\{1,4,6\},\{1,5,6\},\{2,4,5\},\{2,4,6\},\{2,5,6\},\{3,4,5\},\{3,4,6\},\{3,5,6\},\\ &\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,3,6\},\{2,3,4\},\{2,3,5\},\{2,3,6\},\\ &\{1,7,8\},\{1,7,9\},\{1,8,9\},\{2,7,8\},\{2,7,9\},\{2,8,9\},\{3,7,8\},\{3,7,9\},\{3,8,9\},\\ &\{1,2,7\},\{1,2,8\},\{1,2,9\},\{1,3,7\},\{1,3,8\},\{1,3,9\},\{2,3,7\},\{2,3,8\},\{2,3,9\},\\ &\{4,7,8\},\{4,7,9\},\{4,8,9\},\{5,7,8\},\{5,7,9\},\{5,8,9\},\{6,7,8\},\{6,7,9\},\{6,8,9\},\\ &\{4,5,7\},\{4,5,8\},\{4,5,9\},\{4,6,7\},\{4,6,8\},\{4,6,9\},\{5,6,7\},\{5,6,8\},\{5,6,9\}\} \\ B = \{&\{1,2,4,5\},\{1,2,4,6\},\{1,2,5,6\},\{1,3,4,5\},\{1,3,4,6\},\{1,3,5,6\},\{2,3,4,5\},\\ &\{2,3,4,6\},\{2,3,5,6\},\{1,2,7,8\},\{1,2,7,9\},\{1,2,8,9\},\{1,3,7,8\},\{1,3,7,9\},\\ &\{1,3,8,9\},\{2,3,7,8\},\{2,3,7,9\},\{2,3,8,9\},\{4,5,7,8\},\{4,5,7,9\},\{4,5,8,9\},\\ &\{4,6,7,8\},\{4,6,7,9\},\{4,6,8,9\},\{5,6,7,8\},\{5,6,7,9\},\{5,6,8,9\}\} \end{aligned}$$

For some input $x = (x_1, \ldots, x_9)$, the function $f(x)$ can be represented by the following table:

$\lvert x \rvert$	$f^{<=2}(x)$	$f^{=3}(x)$	$f^{=4}(x)$	$f(x)$
0	0	0	0	0
1	1	0	0	1
2	1	0	0	1
3	0	0 30/84 times 1 54/84 times	0	0 30/84 times 1 54/84 times
4	-2	2 81/126 times 3 18/126 times 4 27/126 times	0 99/126 times -1 27/126 times	0 81/126 times 1 45/126 times
5	-5	6 108/126 times 9 18/126 times	0 27/126 times -1 81/126 times -3 18/126 times	0 81/126 times 1 45/126 times
6	-9	12 27/84 times 13 54/84 times 18 3/84 times	-3 81/84 times -9 3/84 times	0 30/84 times 1 54/84 times
7	-14	22 27/36 times 24 9/36 times	-7 27/36 times -9 9/36 times	1
8	-20	36	-15	1
9	-27	54	-27	0

Note that the degree 3 terms are level 5 upper well balanced, with $Y_{3,5} = 36$, and the degree 4 terms are level 4 upper well balanced, with $Y_{4,4} = 15$. This Boolean function is an explicit form of solution 1 from the table in Section 5.4.1.

5.5 n=10

The following system of equations is checked for solutions:

$$\begin{bmatrix} 2.5 & -1 \\ 5 & -3 \\ 8.75 & -7 \\ 14 & -14 \\ 21 & -25.2 \\ 30 & -42 \end{bmatrix} \begin{bmatrix} Y_{3,1} \\ Y_{4,1} \end{bmatrix} = \begin{bmatrix} h_5 \\ h_6 \\ h_7 \\ h_8 \\ h_9 \\ h_{10} \end{bmatrix}$$

where

$$h_5 \in \left\{ 5\frac{0}{\binom{10}{5}}, 5\frac{1}{\binom{10}{5}}, \ldots 5\frac{\binom{10}{5}}{\binom{10}{5}} \right\}, \qquad h_6 \in \left\{ 9\frac{0}{\binom{10}{6}}, 9\frac{1}{\binom{10}{6}}, \ldots 9\frac{\binom{10}{6}}{\binom{10}{6}} \right\},$$

$$h_7 \in \left\{ 14\frac{0}{\binom{10}{7}}, 14\frac{1}{\binom{10}{7}}, \ldots 14\frac{\binom{10}{7}}{\binom{10}{7}} \right\}, \qquad h_8 \in \left\{ 20\frac{0}{\binom{10}{8}}, 20\frac{1}{\binom{10}{8}}, \ldots 20\frac{\binom{10}{8}}{\binom{10}{8}} \right\},$$

$$h_9 \in \left\{ 27\frac{0}{\binom{10}{9}}, 27\frac{1}{\binom{10}{9}}, \ldots 27\frac{\binom{10}{9}}{\binom{10}{9}} \right\}, \qquad h_{10} \in \{35, 36\}$$

5.5.1 Solutions

Exact solutions are shown in the table below. Solutions are enumerated for reference.

	$\mathbf{h_5}$	$\mathbf{h_6}$	$\mathbf{h_7}$	$\mathbf{h_8}$	$\mathbf{h_9}$	$\mathbf{h_{10}}$	$(\mathbf{Y_{3,1}}, \mathbf{Y_{4,1}})$	**map**
1	5	55/6	175/12	21	28	35	$(2.333, 0.833)$	$(Y_{3,6}, Y_{4,5}) = (49, 21)$

Using Remark 6, note that the above mapping corresponds to a set of 70 degree 3 terms and 35 degree 4 terms.

5.6 Conclusion

This exhaustive search reveals what properties a function $f : \{0,1\}^k \to \{0,1\}$ with $deg(f) = 4, s(f) = k$ that has upper well balanced degree 3 and degree 4 terms might have for $k \in \{7, 8, 9, 10\}$. Specifically, the search answers the following question: What pairs $(i, Y_{3,i})$ and $(j, Y_{4,j})$ exist such that their expected sum, combined with $f^{\leq 2}$, are within the bounds of $[0, 1]$ with respect to each hamming weight level? For inputs x with hamming weight greater than $m + i$ or $m + j$, Claim 4.3.3 is used to calculate their expected sum. For inputs x with hamming weight less than $m + i$ or $m + j$, Remark 7 is used to calculate their expected sum. While the properties of the functions are given, verifying whether a function with the properties exists, and then creating upper well balanced subsets that fit these properties is a hard task. The next chapter discusses methods to generate well balanced sets.

Chapter 6

Creating Well Balanced Sets

In Chapter 4, well balanced sets were defined, and Claims 4.2.5 and 4.3.4 introduced conditions under which no such sets exist. These claims are important because generating well balanced sets is not a trivial task, so it is useful to know when they cannot exist. This chapter explores two methods to generate well balanced sets.

The first method of creating well balanced sets is by using the explicit form of a maximal binary constant weight code. A maximal binary constant weight code $A(n, 4, m)$ is the maximum amount of binary strings of length n with hamming weight m such that any two of the strings have a hamming distance greater than or equal to 4.

The second method of creating well balanced sets is through an algorithm which sequentially picks elements $t \in \binom{[n]}{m}$ such that the distance from the subset being generated to an upper well balanced subset is minimized.

6.1 Maximal Binary Constant Weight Codes

A Binary Constant Weight Code with parameters n, d, w is a set of binary strings each of size n with hamming weight w such that any pair of strings have a hamming distance greater than or equal to d. Recall that the hamming distance between strings $x, y \in \{0, 1\}^n$, denoted $|x \oplus y|$, is the number of positions i such that $x_i \neq y_i$.

A central problem for binary constant weight codes is finding the maximum size of a binary code. We denote this value as $A(n, d, w)$. A partial table is shown below for lower bounds on values $A(n, 4, w)$ [BE90]. Note that values with a period indicate optimal values.

n\w	**3**	**4**	**5**	**6**	**7**	**8**
6	4.					
7	7.					
8	8.	14.				
9	12.	18.				
10	13.	30.	36.			
11	17.	35.	66.			
12	20.	51.	80.	132.		
13	26.	65.	123	166		
14	28.	91.	169	278	325	
15	35.	105.	242	399	585	
16	37.	140.	322	624	836	1170

Note that there exists a bijection $f : \{0,1\}^n \to P([n])$ between the set of all binary strings of length n and the power set of $[n]$. Therefore, there is a one-to-one correspondence between binary strings $\{0,1\}^n$ with hamming weight w to elements in $\binom{[n]}{w}$. We say that the hamming distance between two subsets $a, b \in \binom{[n]}{w}$, denoted $|a \oplus b|$, is equal to $|f^{-1}(a) \oplus f^{-1}(b)|$. For the rest of the section, note that elements of $\binom{[n]}{w}$ are used when working with binary constant weight codes.

We notice that many, but not all, of the explicit forms of optimal $A(n,4,w)$ are upper and lower well balanced. Below are some examples of maximal binary constant weight codes that are well balanced.

Example 6.1.1. *The explicit form of $A(12,4,6) \subseteq \binom{[12]}{6}$ is level 1 upper well balanced, with $Y_{6,1} = 1$, and level 1 lower well balanced, with $X_{6,1} = 1$. The explicit form of $A(12,4,6)$ can be found in the appendix.*

Example 6.1.2. *The explicit form of $A(9,4,3) \subseteq \binom{[9]}{3}$ is level 4 upper well balanced, with $Y_{3,4} = 5$, and level 1 lower well balanced, with $X_{3,1} = 1$. The explicit form of $A(9,4,3)$ can be found in the appendix.*

Example 6.1.3. *The explicit form of $A(10,4,4) \subseteq \binom{[10]}{4}$ is level 3 upper well balanced, with $Y_{4,3} = 5$, and is level 1 lower well balanced, with $X_{4,1} = 1$. The explicit form of $A(10,4,4)$ can be found in the appendix.*

Example 6.1.4. *The explicit form of $A(11,4,5) \subseteq \binom{[11]}{5}$ is level 2 upper well balanced, with $Y_{5,2} = 3$, and is level 1 lower well balanced, with $X_{5,1} = 1$. The explicit form of $A(11,4,5)$ can be found in the appendix.*

The following claim provides a bound on the Y value of an upper well balanced subset retrieved from an explicit code $A(n,4,m)$. This is useful in order to understand the limitations of using maximal binary constant weight codes as a source for well balanced sets.

Claim 6.1.5. *If the explicit form of $A(n,4,m)$ is level i upper well balanced, then $Y_{m,i} \leq \frac{1}{i}\binom{m+i}{m+1}$.*

Proof. Let $A \subseteq \binom{[n]}{m}$ be the explicit subset of $A(n,4,m)$. We begin by proving that elements of A do not appear in subsets of $[n]$ of size $m+1$ more than once.

Lemma 6.1.6. *Let $A \subseteq \binom{[n]}{m}$ be the explicit subset of $A(n,4,m)$. Then for every $t \in \binom{[n]}{m+1}$, $|\{a \in A | a \subseteq t\}| \leq 1$.*

Proof. Assume for contradiction that there exists a $t \in \binom{[n]}{m+1}$ for which $|\{a \in A | a \subseteq t\}| > 1$. Let $a_1, a_2 \in A$ such that $a_1 \subseteq t, a_2 \subseteq t$. It follows directly that $|a_1 \cap a_2| = m-1$. This corresponds to a pairwise hamming distance of $2 < 4$. Thus we have reached a contradiction. □

Lemma 6.1.6 implies that A cannot be level 1 upper well balanced such that $Y_{m,1} > 1$. Using Claim 4.3.3, we can say that A cannot be level i upper well balanced such that $Y_{m,i} > \frac{1}{i}\binom{m+i}{m+1}$. Since A is level i upper well balanced, it follows that $Y_{m,i} \leq \frac{1}{i}\binom{m+i}{m+1}$ □

The following claim makes an equivalence between optimal explicit forms of $A(n,4,n/2)$ and level 1 upper well balanced subsets $S \subseteq \binom{[n]}{n/2}$ with $Y_{n/2,1} = 1$.

Claim 6.1.7. *There exists a subset $S \subseteq \binom{[n]}{n/2}$ that is level 1 upper well balanced with $Y_{n/2,1} = 1$ if and only if the optimal value of $A(n, 4, n/2) = \frac{2}{n}\binom{n}{n/2+1}$.*

Proof. We begin by proving that if $S \subseteq \binom{[n]}{n/2}$ is a level 1 upper well balanced subset with $Y_{n/2,1} = 1$, then it is an explicit code of the optimal value of $A(n, 4, n/2) = |S|$.

First, we show that S is a binary constant weight code. For any two elements $s_1, s_2 \in S$, we note that the hamming distance between them is at least 4. If it were 0, they would be the same element, and if it were 2, then $s_1 \cup s_2 \in \binom{[n]}{n/2+1}$, which is a contradiction to their upper well balanced property. It follows that S is a valid binary constant weight code with parameters $n, 4, n/2$. Using Remark 6, $|S| = \frac{2}{n}\binom{n}{n/2+1}$.

We will now prove that the optimal value of $A(n, 4, n/2) \leq |S|$. Assume that there exists an explicit code A for which $A(n, 4, n/2) > |S|$.

Note that for each $a \in A$, $|\{t \in \binom{[n]}{n/2+1} | a \subseteq t\}| = n - n/2 = n/2$. Note also that for every $a_1, a_2 \in A$, $|\{t \in \binom{[n]}{n/2+1} | a_1 \subseteq t\} \cap \{t \in \binom{[n]}{n/2+1} | a_2 \subseteq t\}| = 0$. To see this, assume there exists an $a_1, a_2 \in A$ such that $a_1 \subseteq t, a_2 \subseteq t$ for some $t \in \binom{[n]}{n/2+1}$. Then $|a_1 \cap a_2| = m - 1$, so their hamming distance would be $2 < 4$. This is a contradiction.

It follows that $|\{t \in \binom{[n]}{n/2+1} | a \in A, a \subseteq t\}| > n/2 \cdot |S| = \binom{n}{n/2+1}$. By the Pigeonhole Principle, there exists a $t \in \binom{n}{n/2+1}$ for which $|\{a \in A | a \subseteq t\}| > 1$. Let $a_1, a_2 \in \{a \in A | a \subseteq t\}$. Then $|a_1 \cap a_2| = m - 1$, so their hamming distance would be $2 < 4$. This is a contradiction. Therefore the optimal value of $A(n, 4, n/2) \leq |S|$.

We now prove that if the optimal value of $A(n, 4, n/2) = \frac{2}{n}\binom{n}{n/2+1}$, then the explicit code of $A(n, 4, n/2)$ is level 1 upper well balanced with $Y_{n/2,1} = 1$.

Let A be the explicit code of $A(n, 4, n/2)$. Note that for every element $a \in A$, $|\{t \in \binom{[n]}{n/2+1} | a \subseteq t\}| = n - n/2 = n/2$. Note also that for every $a_1, a_2 \in A$, $|\{t \in \binom{[n]}{n/2+1} | a_1 \subseteq t\} \cap \{t \in \binom{[n]}{n/2+1} | a_2 \subseteq t\}| = 0$ (as discussed earlier in the proof). Thus if $A(n, 4, n/2) = \frac{2}{n}\binom{n}{n/2+1}$, $|\{t \in \binom{[n]}{n/2+1} | a \in A, a \subseteq t\}| = \frac{n}{2} \cdot \frac{2}{n}\binom{n}{n/2+1} = \binom{n}{n/2+1}$. This implies that each element $t \in \binom{n}{n/2+1}$ includes exactly 1 element of A. By definition, this means that A is level 1 upper well balanced, with $Y_{n/2,1} = 1$.

□

Using this claim and the table above, we know that there exists a level 1 upper well balanced subset $S \subseteq \binom{[n]}{m}$ with $Y_{m,1} = 1$ for $(n, m) = (8, 4)$ and $(12, 6)$, and there does not exist such a subset for $(n, m) = (10, 5)$.

6.2 A Least Squares Approach

The following distance metric measures the $l2$ proximity of a subset $S \subseteq \binom{[n]}{m}$ to it being a level i upper well balanced subset with $Y_{m,i}$:

$$dist(S) = \left(\sum_{t \in \binom{[n]}{m+i}} (Y_{m,i} - |\{s \in S | s \subseteq t\}|)^2 \right)^{1/2}$$

Note that a similar metric could be used to measure the proximity of a subset S to it being lower well balanced. The choice to use upper well balanced is arbitrary due to Claim 4.4.2. The following remark notes that if $dist(S) = 0$ for a subset S, then S is upper well balanced, and vice versa.

Remark 8. *$dist(S) = 0$ if and only if $S \subseteq \binom{[n]}{m}$ is a level i upper well balanced subset with $Y_{m,i}$.*

The following algorithm attempts to create an upper well balanced subset $S \subseteq \binom{[n]}{m}$ by iterating through groups of $\binom{[n]}{m}$ of size res and adding those that minimize $dist(S)$ the most.

Algorithm 2 Algorithm that attempts to create upper well balanced subsets by appending elements from $\binom{[n]}{m}$ to S that minimize $dist(S)$ the most.

```
Require: n, m, i, Y, res                                  ▷ where 0 < Y < (m+1)/i · C(m+k, m+1)
S ← {}
choose ← C([n], m)                                        ▷ List C([n], m)
S_size ← C(n − m, i)^−1 * C(n, m + i) * Y                 ▷ See Remark 6
candidates ← C(choose, res)                               ▷ where 1 ≤ res ≤ S_size

while get_size(S) < S_size do
    min_dist ← MAXINT
    min_c ← None
    for c ∈ candidates do
        curr_dist = dist(S ∪ c)
        if curr_dist < min_dist then
            min_dist ← curr_dist
            min_c ← c
        end if
    end for

    S.append(min_c)
    for c ∈ min_c do
        choose.remove(c)
    end for
    candidates ← C(choose, res)
end while

return S
```

We note that as $resolution \to S\_size$, the algorithm will generate an upper well balanced subset with the desired properties, if one exists. However, as $resolution \to S\_size$, the size of $candidates = \binom{\binom{[n]}{m}}{S\_size}$ grows quickly.
The algorithm run with parameters $alg\_2(6, 3, 1, 2, res)$ was able to find the Kushilevitz function degree 3 terms for $res \in \{3, 5, 6, 7, 8, 9, 10\}$. The algorithm run with parameters $alg\_2(8, 4, 1, 1, res)$ was able to find a subset $S \subseteq \binom{[8]}{4}$ which is level 1 upper well balanced, with $Y_{4,1} = 1$ when tested with $res \in \{1, 2, 3\}$.

Chapter 7

Conclusion

This thesis studies the degree upper bound on sensitivity for Boolean functions. In Chapter 2, we reprove the best known separation $s(f) \leq deg(f)^2$, and we analyze the Kushilevitz function in Chapter 3. The Kushilevitz Boolean function provides the largest known gap between the sensitivity of a function and its degree: $s(f) = deg(f)^{1.63}$. We then define well balanced sets, which gives a framework to many Boolean functions that have high sensitivity and low degree. Boolean functions $f : \{0,1\}^i \to \{0,1\}$ with $deg(f) = 4, s(f) = i$ are presented for $i \in \{7,8,9\}$. Using construction methods from Chapter 6, we present a novel function $f : \{0,1\}^7 \to \{0,1\}$ with $deg(f) = 4, s(f) = 7$ which has upper well balanced degree 3 and degree 4 terms. Furthermore, we suggest what properties a function $f' : \{0,1\}^{10} \to \{0,1\}$ with $deg(f') = 4, s(f') = 10$ and upper well balanced degree 3 and degree 4 terms might have. Constructing such a function f' would lead to a gap larger than the Kushilevitz function: $s(f') = deg(f')^{1.66}$. Finally, this thesis reviews two methods of generating well balanced subsets. Maximal binary constant weight codes are a source of some well balanced subsets, while we also present an algorithm that can generate well balanced subsets given reasonably small parameters.

7.1 Future Work

Future work involves generating degree 3 and degree 4 terms which comprise a fully sensitive Boolean function on 10 bits. Also, analyzing the proof in [ABDK+21a] and seeing where there are opportunities for stronger claims could help tighten the degree upper bound on sensitivity. We present suggested problems:

1. Does there exist an upper well balanced subset $S \subseteq \binom{[10]}{3}$ and an upper well balanced subset $S \subseteq \binom{[10]}{4}$ which comprise the degree 3 and degree 4 terms of a fully sensitive Boolean function on 10 bits?

2. What are the necessary and sufficient conditions for a level i well balanced subset $S \subseteq \binom{[n]}{m}$ to exist?

3. Gathan [vzGR97] states that for $n \geq 2$ and randomly chosen symmetric Boolean function $f : \{0,1\}^n \to \{0,1\}$, $P(n - deg(f) \geq 1) < 2^{-n/3}$. Many of the Boolean functions studied in this thesis are symmetric for some hamming weights, but not others. How does $P(n - deg(f) \geq 1)$ compare for a randomly chosen "semi-symmetric" function f, such as those seen in this thesis?

Chapter 8

Appendix

The following subset $S \subseteq \binom{[8]}{4}$ is level 1 upper well balanced with $Y_{4,1} = 1$. Note that this is also the explicit form of $A(8,4,4)$.

$$\{\{1,2,3,7\},\{1,2,5,6\},\{1,3,4,6\},\{1,4,5,7\},\{2,3,4,5\},\{2,4,6,7\},\{3,5,6,7\},\\ \{4,5,6,8\},\{3,4,7,8\},\{2,5,7,8\},\{2,3,6,8\},\{1,6,7,8\},\{1,3,5,8\},\{1,2,4,8\}\}$$

The following subset $S \subseteq \binom{[9]}{3}$ is an explicit form of $A(9,4,3)$:

$$\{\{5,7,9\},\{4,7,8\},\{4,5,6\},\{3,6,8\},\{3,4,9\},\{2,8,9\},\{2,6,7\},\{2,3,5\},\{1,6,9\},\\ \{1,5,8\},\{1,3,7\},\{1,2,4\}\}$$

The following subset $S \subseteq \binom{[10]}{4}$ is an explicit form of $A(10,4,4)$:

$$\{\{5,7,9,10\},\{5,6,8,9\},\{4,7,8,10\},\{4,6,7,9\},\{4,5,6,10\},\{3,7,8,9\},\{1,2,5,6\},\\ \{3,5,6,7\},\{3,4,9,10\},\{3,4,5,8\},\{2,8,9,10\},\{2,6,7,10\},\{2,5,7,8\},\{2,4,6,8\},\\ \{2,4,5,9\},\{2,3,6,9\},\{2,3,5,10\},\{2,3,4,7\},\{1,6,9,10\},\{1,6,7,8\},\{1,5,8,10\},\\ \{1,4,8,9\},\{1,4,5,7\},\{1,3,7,10\},\{1,3,5,9\},\{1,3,4,6\},\{1,2,4,10\},\{3,6,8,10\},\\ \{1,2,7,9\},\{1,2,3,8\}\}$$

The following subset $S \subseteq \binom{[8]}{4}$ is level 3 upper well balanced, with $Y_{4,3} = 10$.

$$\{\{1,2,3,7\},\{1,2,5,6\},\{1,3,4,6\},\{1,4,5,7\},\{2,3,4,5\},\{2,4,6,7\},\{3,5,6,7\},\\ \{4,5,6,8\},\{3,4,7,8\},\{2,5,7,8\},\{2,3,6,8\},\{1,6,7,8\},\{1,3,5,8\},\{1,2,4,8\},\\ \{2,4,5,6\},\{2,3,6,7\},\{2,3,5,8\},\{1,4,6,7\},\{1,4,5,8\},\{1,3,7,8\}\}$$

The following subset $S \subseteq \binom{[10]}{4}$ is level 5 upper well balanced with $Y_{4,5} = 21$:

$$\{\{5,7,9,10\},\{5,6,8,9\},\{4,7,8,10\},\{4,6,7,9\},\{4,5,6,10\},\{3,7,8,9\},\{3,6,8,10\},\\ \{3,5,6,7\},\{3,4,9,10\},\{3,4,5,8\},\{2,8,9,10\},\{2,6,7,10\},\{2,5,7,8\},\{2,4,6,8\},\\ \{2,4,5,9\},\{2,3,6,9\},\{2,3,5,10\},\{2,3,4,7\},\{1,6,9,10\},\{1,6,7,8\},\{1,5,8,10\},\\ \{1,4,8,9\},\{1,4,5,7\},\{1,3,7,10\},\{1,3,5,9\},\{1,3,4,6\},\{1,2,7,9\},\{1,2,5,6\},\\ \{1,2,4,10\},\{1,2,3,8\},\{7,8,9,10\},\{3,4,5,6\},\{1,2,9,10\},\{5,6,7,8\},\{1,2,3,4\}\}$$

The following subset $S \subseteq \binom{[12]}{6}$ is an explicit form of $A(12,4,6)$:

$$\{\{2,3,4,5,6,7\},\{1,2,4,6,7,8\},\{1,3,5,6,7,8\},\{1,2,3,4,5,8\},\{1,3,4,5,7,9\},$$
$$\{2,3,5,6,8,9\},\{1,2,3,4,6,9\},\{2,4,5,7,8,9\},\{1,2,5,6,7,9\},\{3,4,6,7,8,9\},$$
$$\{1,4,5,6,8,9\},\{1,2,3,7,8,9\},\{1,2,4,5,6,10\},\{2,3,4,7,8,10\},\{1,2,3,5,7,10\},$$
$$\{3,4,5,6,8,10\},\{4,5,6,7,9,10\},\{2,3,6,7,9,10\},\{2,4,6,8,9,10\},\{3,5,7,8,9,10\},$$
$$\{1,2,5,8,9,10\},\{1,3,4,8,9,10\},\{1,3,5,6,9,10\},\{1,2,4,7,9,10\},\{1,6,7,8,9,10\},$$
$$\{1,2,3,6,8,10\},\{1,4,5,7,8,10\},\{1,3,4,6,7,10\},\{2,5,6,7,8,10\},\{2,3,4,5,9,10\},$$
$$\{1,3,4,6,8,11\},\{1,2,5,7,8,11\},\{2,3,6,7,8,11\},\{1,4,5,6,7,11\},\{1,2,4,5,9,11\},$$
$$\{1,3,6,7,9,11\},\{3,4,5,6,9,11\},\{2,3,4,8,9,11\},\{5,6,7,8,9,11\},\{1,4,7,8,9,11\},$$
$$\{2,3,5,7,9,11\},\{1,2,6,8,9,11\},\{1,2,3,4,7,11\},\{2,4,5,6,8,11\},\{1,3,5,8,9,11\},$$
$$\{1,2,3,5,6,11\},\{3,4,5,7,8,11\},\{2,4,6,7,9,11\},\{2,4,5,7,10,11\},\{1,3,4,5,10,11\},$$
$$\{1,2,6,7,10,11\},\{1,5,6,8,10,11\},\{2,3,5,8,10,11\},\{4,6,7,8,10,11\},\{2,3,4,6,10,11\},$$
$$\{1,3,7,8,10,11\},\{1,2,3,9,10,11\},\{4,5,8,9,10,11\},\{2,5,6,9,10,11\},\{3,4,7,9,10,11\},$$
$$\{3,5,6,7,10,11\},\{1,4,6,9,10,11\},\{2,7,8,9,10,11\},\{1,2,4,8,10,11\},\{1,5,7,9,10,11\},$$
$$\{3,6,8,9,10,11\},\{4,5,6,7,8,12\},\{1,2,3,6,7,12\},\{1,2,5,6,8,12\},\{1,3,4,7,8,12\},$$
$$\{2,3,4,7,9,12\},\{1,2,3,5,9,12\},\{1,4,6,7,9,12\},\{1,3,6,8,9,12\},\{3,4,5,8,9,12\},$$
$$\{2,6,7,8,9,12\},\{2,4,5,6,9,12\},\{1,5,7,8,9,12\},\{1,3,4,5,6,12\},\{2,3,5,7,8,12\},$$
$$\{1,2,4,8,9,12\},\{1,2,4,5,7,12\},\{2,3,4,6,8,12\},\{3,5,6,7,9,12\},\{1,2,3,4,10,12\},$$
$$\{1,5,6,7,10,12\},\{2,3,5,6,10,12\},\{2,4,5,8,10,12\},\{3,6,7,8,10,12\},\{1,2,7,8,10,12\},$$
$$\{3,4,5,7,10,12\},\{1,4,6,8,10,12\},\{3,4,6,9,10,12\},\{2,5,7,9,10,12\},\{1,4,5,9,10,12\},$$
$$\{2,3,8,9,10,12\},\{2,4,6,7,10,12\},\{1,3,7,9,10,12\},\{5,6,8,9,10,12\},\{1,3,5,8,10,12\},$$
$$\{1,2,6,9,10,12\},\{4,7,8,9,10,12\},\{1,2,4,6,11,12\},\{1,3,5,7,11,12\},\{3,4,6,7,11,12\},$$
$$\{2,5,6,7,11,12\},\{1,2,3,8,11,12\},\{1,4,5,8,11,12\},\{3,5,6,8,11,12\},\{2,4,7,8,11,12\},$$
$$\{2,3,4,5,11,12\},\{1,5,6,9,11,12\},\{3,7,8,9,11,12\},\{1,2,7,9,11,12\},\{4,6,8,9,11,12\},$$
$$\{2,3,6,9,11,12\},\{4,5,7,9,11,12\},\{2,5,8,9,11,12\},\{1,3,4,9,11,12\},\{1,6,7,8,11,12\},$$
$$\{1,4,7,10,11,12\},\{2,6,8,10,11,12\},\{1,3,6,10,11,12\},\{5,7,8,10,11,12\},$$
$$\{3,5,9,10,11,12\},\{2,4,9,10,11,12\},\{1,8,9,10,11,12\},\{6,7,9,10,11,12\},$$
$$\{3,4,8,10,11,12\},\{1,2,5,10,11,12\},\{4,5,6,10,11,12\},\{2,3,7,10,11,12\}\}$$

Bibliography

[ABDK+21a] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. Degree vs. approximate degree and quantum implications of huang's sensitivity theorem. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1330–1342, 2021.

[ABDK+21b] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. Degree vs. approximate degree and quantum implications of Huang's sensitivity theorem. In *STOC '21—Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1330–1342. ACM, New York, [2021] ©2021.

[BE90] Andries E Brouwer and T Etzion. Bounds for binary constant weight codes. *IEEE Trans. Inf. Theory*, 36:1334–1380, 1990.

[GR01] Chris Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[HKP10] Pooya Hatami, Raghav Kulkarni, and Denis Pankratov. Variations on the sensitivity conjecture. *arXiv preprint arXiv:1011.0354*, 2010.

[Hua19] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Ann. of Math. (2)*, 190(3):949–955, 2019.

[jh] joriki (https://math.stackexchange.com/users/6622/joriki). Can the principle of inclusion/exclusion be used to count elements in the intersection of a sequence of sets? Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/3483688 (version: 2019-12-21).

[Kro11] MJ Kronenburg. The binomial coefficient for negative arguments. *arXiv preprint arXiv:1105.3689*, 2011.

[LO] Peteris Ledins and Rihards Opmanis. Boolean functions of low polynomial degree. *Databases and Information Systems*, page 25.

[MMST21] Subhamoy Maitra, Chandra Sekhar Mukherjee, Pantelimon Stanica, and Deng Tang. On boolean functions with low polynomial degree and higher order sensitivity, 2021.

[NS94] Noam Nisan and Márió Szegedy. On the degree of Boolean functions as real polynomials. volume 4, pages 301–313. 1994. Special issue on circuit complexity (Barbados, 1992).

[NW95] Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Combinatorica*, 15(4):557–565, 1995.

[O'D14] Ryan O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, New York, 2014.

[Rao21] Shravas Rao. The fourier transform of restrictions of functions on the slice. *arXiv preprint arXiv:2111.03213*, 2021.

[vzGR97] Joachim von zur Gathen and James R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997.