Zero-error communication over adder MAC

by

Yuzhou Gu

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2018

Author .....
Department of Electrical Engineering and Computer Science
May 25, 2018

Certified by .....
Yury Polyanskiy
Associate Professor
Thesis Supervisor

Accepted by .....
Katrina LaCurts
Chair, Master of Engineering Thesis Committee

Zero-error communication over adder MAC

by

Yuzhou Gu

Submitted to the Department of Electrical Engineering and Computer Science
on May 25, 2018, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

Adder MAC is a simple noiseless multiple-access channel (MAC), where if users send messages $X_1, \ldots, X_h \in \{0,1\}^n$, then the receiver receives $Y = X_1 + \cdots + X_h$ with addition over $\mathbb{Z}$. Communication over the noiseless adder MAC has been studied for more than fifty years. There are two models of particular interest: uniquely decodable code tuples, and B_h-codes. In spite of the similarities between these two models, lower bounds and upper bounds of the optimal sum rate of uniquely decodable code tuple asymptotically match as number of users goes to infinity, while there is a gap of factor two between lower bounds and upper bounds of the optimal rate of B_h-codes.

The best currently known B_h-codes for $h \geq 3$ are constructed using random coding. In this thesis, we study variants of the random coding method and related problems, in hope of achieving B_h-codes with better rate. Our contribution include the following.

1. We determine the rate achieved by changing the underlying distribution used in random coding.

2. We determine the rate of a list-decoding version of B_h-codes achieved by the random coding method.

3. We study several related problems about Rényi entropy.

Thesis Supervisor: Yury Polyanskiy
Title: Associate Professor

Acknowledgments

I am deeply grateful to my advisor Yury Polyanskiy for his support and guidance in various aspects. Without him I would not have learnt the beauty of information theory. I would like to thank Ganesh Ajjanagadde, Alexey Frolov, and all people who has discussed the material with me for their helpful advice. I also thank my family and friends, in particular my partner Zhulin Li, for their support and encouragement.

Contents

Chapter 1

Introduction

1.1 Overview

Adder MAC is a simple noiseless multiple-access channel (MAC), where if users send messages $X_1, \ldots, X_h \in \{0,1\}^n$, then the receiver receives $Y = X_1 + \cdots + X_h$ with addition over $\mathbb{Z}$.

Communication over the noiseless adder MAC has been studied for more than fifty years. In the most well-studied version, each user i $(1 \leq i \leq h)$ has their own codebook $\mathcal{C}_i \subseteq \{0,1\}^n$, and X_i is picked from $\mathcal{C}_i$. We insist our protocol to be zero-error, i.e., we can uniquely determine $X_1, \ldots, X_k$ given Y. More formally, if we have $u_1, \ldots, u_h, v_1, \ldots, v_h$ with $u_i, v_i \in \mathcal{C}_i$ $(1 \leq i \leq h)$ and

$$u_1 + \cdots + u_h = v_1 + \cdots + v_h,$$

then we must have $u_i = v_i$ for all $1 \leq i \leq h$. A code tuple $(\mathcal{C}_1, \ldots, \mathcal{C}_h)$ satisfying the above property is called uniquely decodable. The quantity we would like to optimize is the sum rate, defined as

$$R(\mathcal{C}_1, \ldots, \mathcal{C}_h) = \sum_{1 \leq i \leq h} \frac{\log |\mathcal{C}_i|}{n}$$

where the logarithm is taken over base 2. Let

$$R_h = \limsup_{n\to\infty} \sup_{\substack{\mathcal{C}_1,\ldots,\mathcal{C}_h\subseteq\{0,1\}^n \\ \text{uniquely decodable}}} R(\mathcal{C}_1,\ldots,\mathcal{C}_h).$$

By standard information theory (e.g., [20] Chapter 29), we have

$$R_h \le H(B(h,\frac{1}{2})) = (1+o(1))\frac{\log h}{2}$$

where $B(h,\frac{1}{2})$ is the binomial distribution and H is Shannon entropy. On the other hand, Cantor and Mills [6] and Lindström [14] constructed code tuples whose sum rate grow as $(1+o(1))\frac{\log h}{2}$ as $h\to\infty$. Therefore lower bound and upper bound match.

There is another version of communication over the noiseless adder MAC, where all the users share a single codebook $\mathcal{C}\subseteq\{0,1\}^n$. In this case, we cannot expect to be able to uniquely determine $X_1,\ldots,X_h$ given Y, because permuting X_i's does not change Y. Instead, we require that we can uniquely determine the multiset $\{X_1,\ldots,X_h\}$ given Y. Formally, if we have $u_1,\ldots,u_h,v_1,\ldots,v_h\in\mathcal{C}$ and

$$u_1+\cdots+u_h = v_1+\cdots+v_h,$$

then the multisets $\{u_1,\ldots,u_h\}$ and $\{v_1,\ldots,v_h\}$ are equal. Codes $\mathcal{C}$ satisfying this property are called B_h-codes.

In this setting the quantity we would like to optimize is the rate

$$R(\mathcal{C}) = \frac{\log|\mathcal{C}|}{n}.$$

We define

$$R_h^* = \limsup_{n\to\infty} \sup_{\substack{\mathcal{C}\subseteq\{0,1\}^n \\ B_h\text{-code}}} R(\mathcal{C}).$$

Again, standard information theory gives

$$R_h^* \leq \frac{1}{h} H(B(h, \frac{1}{2})) = (1 + o(1)) \frac{\log h}{2h}.$$

The best known lower bound so far is $R_2^* \geq \frac{1}{2}$ given by Lindström [15] and

$$R_h^* \geq \frac{\log \left(\frac{2^{2h}}{\binom{2h}{h}} \right)}{2h - 1} = (1 + o(1)) \frac{\log h}{4h}$$

for $h \geq 3$ given by Poltyrev [19]. Therefore there is a gap of factor 2 between the lower bound and the upper bound.

Poltyrev's construction is based on random coding. In this work, we study variants of the random coding method and related problems, in hope of achieving B_h-codes with better rate. Our contribution includes the following.

1. We determine the rate achieved by changing the underlying distribution used in random coding.

2. We determine the rate of a list-decoding version of B_h-codes achieved by the random coding method.

3. We study several related problems about Rényi entropy.

1.2 Related work

In this section we review previous works on uniquely decodable code tuples and B_h-codes.

In both settings, the case $h = 2$ is studied most. A uniquely decodable code tuple with $h = 2$ is called uniquely decodable code pair (UDCP) in literature. Lindström [15] prove that $\frac{1}{2} \log 6 \leq R_2 \leq \frac{3}{2}$. Since then, a lot of constructions of UDCPs have been given, improving the lower bound on R_2, including 1.30366 by Coebergh van den Braak and van Tilborg [8], 1.30369 by Ahlswede and Balakirsky [1], 1.30565 by Coebergh van den Braak [7], 1.30999 by Urbanke and Li [21], 1.31782 by Mattas and

Östergård [17]. These constructions are all explicit constructions, and usually have small n. There has been no upper bound of R_2 better than the entropy bound $\frac{3}{2}$.

For UDCPs, people have also considered the following question: when $\alpha = \frac{\log |\mathcal{C}_1|}{n}$ is close to one, how large can $\beta = \frac{\log |\mathcal{C}_2|}{n}$ be? Kasami et al. [11] gave a construction where $\alpha \geq 1-\epsilon$ and $\beta \geq 0.25$. This is recently improved by Wiman [22] to $\alpha \geq 1-\epsilon$ and $\beta \geq 0.2563$. Urbanke and Li [21] proved that when $\alpha \geq 1-\epsilon$, we have $\beta \leq 0.4921$. It is improved by Ordentlich and Shayevitz [18] to $\beta \leq 0.4798$ when $\alpha \geq 1-\epsilon$ and by Austrin et al. [3] to $\beta \leq 0.4228$ when $\alpha \geq 1-\epsilon$.

Let us discuss R_h for $h \geq 3$. The special case where all $|\mathcal{C}_i| = 2$ is studied under the name detecting matrix. Cantor and Mills [6] and Lindström [14] constructed codes with sum rate increases as $(1+o(1))\frac{\log h}{2}$ as $h \to \infty$. For the general case, Khachatrian and Martirossian [12] gave a combinatorial construction for all h. Kiviluoto and Östergård [13] gave better explicit constructions for $3 \leq h \leq 5$. For $k \geq 3$, it has been proven by Bross and Blake [5] that R_h is strictly smaller than $H(B(h, \frac{1}{2}))$.

Now let us turn to R_2^*. A B_2-code is also called a Sidon code, in analogy with Sidon sequences in number theory. Lindström [15] gave a construction of a B_2 code of rate $\frac{1}{2}$ that actually works with addition over $\mathbb{Z}/2\mathbb{Z}$. There has been several nontrivial upper bounds for R_2^*. Lindström proved in [15] that $R_2^* \leq \frac{2}{3}$, and in [16] that $R_2^* \leq 0.6$. Cohen et al. [9] improved this to $R_2^* \leq 0.5753$.

The number theoretic analogy of B_h-codes are called B_h-sequences. Any construction of B_k-sequences can be directly translated into B_k-codes with the same rate. Bose and Chowla [4], using finite fields, constructed B_h-sequences (and thus B_h-codes) with rate $\frac{1}{h}$. This rate is optimal in number theoretic setting, but known to be suboptimal in coding theoretic setting, at least for $h \geq 3$. D'yachkov and Rykov [10] proved using random coding that $R_h^* \geq \frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h}$. This is improved by Poltyrev [19] to $R_h^* \geq \frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h-1}$. As h goes to ∞, the above rates increase as $(1+o(1))\frac{\log h}{4h}$. There has been no general upper bound for R_h^* with $h \geq 3$ except for the trivial fact that $R_h^* \leq R_h$.

D'yachkov-Rykov [10] also studied what they called plans, a weaker version of

B_h-codes, which are sets $\mathcal{C} \subseteq \{0,1\}^n$ satisfying the property that for two distinct subsets $\{u_1, \ldots, u_h\}$ and $\{v_1, \ldots, v_h\}$ of $\mathcal{C}$, we have

$$u_1 + \cdots + u_h = v_1 + \cdots + v_h.$$

The currently known lower bound and upper bound of the optimal rate of plans are the same as those of B_h-codes.

Chapter 2

Preliminaries

2.1 Definitions

In this chapter we give necessary definitions and study existing constructions of B_h-codes.

Definition 2.1. Let A be an abelian group and $\mathcal{C} \subseteq A$ be a subset. We say $\mathcal{C}$ is a B_h-set (or $\mathcal{C}$ satisfies the B_h-property) if for any $a \in A$, there exists at most one multiset $\{u_1, \ldots, u_h\}$ with $u_1, \ldots, u_h \in \mathcal{C}$ such that $a = u_1 + \cdots + u_h$. In other words, if $u_1, \ldots, u_h, v_1, \ldots, v_h \in \mathcal{C}$ satisfies $u_1 + \cdots + u_h = v_1 + \cdots + v_h$, then the multisets $\{u_1, \ldots, u_h\}$ and $\{v_1, \ldots, v_h\}$ are equal.

Definition 2.2. A B_h-code is a B_h-set $\mathcal{C} \subseteq \{0,1\}^n \subseteq \mathbb{Z}^n$. The rate of a B_h-code is defined as $\frac{\log |\mathcal{C}|}{n}$.

Remark 2.3. We are most interested in the asymptotic growth of rate of B_h-codes as n goes to ∞. Therefore, when we say "there exist B_h-codes of rate f" we actually mean "there exist a family of B_h-codes $\mathcal{C}_1, \mathcal{C}_2, \cdots$ with $\mathcal{C}_i \subseteq \{0,1\}^{n_i}$ such that $n_i \to \infty$ and $\log \frac{\log |\mathcal{C}_i|}{n_i} \to f$ as $i \to \infty$."

2.2 Constructions from number theory

The only known explicit constructions of B_h-codes achieve rate $\frac{1}{h}$, and all come form number theory.

Theorem 2.4 (Bose-Chowla [4]). *Let q be a prime power and h be a positive integer. Then there exists a B_h-set $\mathcal{C} \subseteq \mathbb{Z}/(q^h-1)\mathbb{Z}$ of size q.*

Proof. Let $\alpha \in \mathbb{F}_{q^h}$ be a generator of $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$. By elementary number theory, $\deg \alpha = h$ and α is a generator of $\mathbb{F}_{q^h}^\times \simeq \mathbb{Z}/(q^h-1)\mathbb{Z}$. Let elements of $\mathbb{F}_q$ be $x_1, \ldots, x_q$. Let $d_i \in \mathbb{Z}/(q^h-1)\mathbb{Z}$ be the unique solution to $\alpha^{d_i} = \alpha + x_i$. We claim that $\mathcal{C} = \{d_1, \ldots, d_q\}$ is a B_h-set.

Suppose that we have $u_1, \ldots, u_h, v_1, \ldots, u_h$ with $1 \le u_i, v_i \le q$ $(1 \le i \le h)$ satisfying

$$d_{u_1} + \cdots + d_{u_h} = d_{v_1} + \cdots + d_{v_h}.$$

Then we have

$$\alpha^{d_{u_1}+\cdots+d_{u_h}} = \alpha^{d_{v_1}+\cdots+d_{v_h}}.$$

By definition of d_i, this means

$$(\alpha + x_{u_1}) \cdots (\alpha + x_{u_h}) = (\alpha + x_{v_1}) \cdots (\alpha + x_{v_h}).$$

Consider the polynomial

$$f(x) = (x + x_{u_1}) \cdots (x + x_{u_h}) - (x + x_{v_1}) \cdots (x + x_{v_h}).$$

Because $\deg f \le h-1$ and $f(\alpha) = 0$, we must have $f = 0$. So the multisets $\{u_1, \ldots, u_h\}$ and $\{v_1, \ldots, v_h\}$ are equal. □

Corollary 2.5. *There exist B_h-codes of rate $\frac{1}{h}$.*

Proof. Let elements of $\mathbb{Z}/(q^h-1)\mathbb{Z}$ be $0, 1, \ldots, q^h-2$. Consider the map $f : \mathbb{Z}/(q^h-1)\mathbb{Z} \to \{0,1\}^{\lceil \log_2(q^h-2) \rceil}$ which maps an integer to its binary representation. It is easy to see that f preserves the B_h-property: for any B_h-set $\mathcal{C} \subseteq \mathbb{Z}/(q^h-1)\mathbb{Z}$, its image

$f(\mathcal{C})$ is also a B_h-set. Therefore we get a B_h-set of rate $\frac{\log q}{\lceil \log(q^h-2)\rceil} = (1+o(1))\frac{1}{h}$. As $q \to \infty$ we get the desired code family. □

We present another (folklore) construction of B_h-codes which has nice geometric meaning. This construction is similar to the construction in Lindström [15] for $h = 2$.

Theorem 2.6. *Let $\mathbb{F}_q$ be a finite field with $\operatorname{char}\mathbb{F}_q > h$. Then there exists a B_h-set $\mathcal{C} \subseteq \mathbb{F}_q^h$ of size q.*

Proof. Let $\mathcal{C} = \{(x^1, x^2, \cdots, x^h) : x \in \mathbb{F}_q\}$. We claim that $\mathcal{C}$ is a B_h-set. Suppose we have $u_1, \ldots, u_h, v_1, \ldots, v_h \in \mathbb{F}_q$ such that for $i = 1, 2, \ldots, h$ we have

$$u_1^i + \cdots + u_h^i = v_1^i + \cdots + v_h^i.$$

By Newton's identities for symmetric polynomials, we see that

$$e_i(u_1, \ldots, u_h) = e_i(v_1, \ldots, v_h)$$

for $0 \le i \le h$, where e_i is the i-th elementary symmetric polynomial. So we have

$$\begin{aligned}(x+u_1)\cdots(x+u_h) &= \sum_{0\le i\le n} e_i(u_1,\ldots,u_h)x^{n-i} \\ &= \sum_{0\le i\le n} e_i(v_1,\ldots,v_h)x^{n-i} \\ &= (x+v_1)\cdots(x+v_h).\end{aligned}$$

Therefore the multisets $\{u_1, \ldots, u_h\}$ and $\{v_1, \ldots, v_h\}$ are equal. □

This construction also implies that there exist B_h-codes of rate $\frac{1}{h}$.

2.3 Random coding for B_h-code

For $h \ge 3$, the best currently known B_h-codes are all inexplicit and constructed by random coding. We review the construction and formulate the proof in a way so that it can be easily generalized to more complicated constructions.

2.3.1 D'yachkov-Rykov

Theorem 2.7 (D'yachkov-Rykov [10]). *There exist B_h-codes of rate* $\frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h}$.

Fix vector length n and number of vectors t. Let $v_1, \ldots, v_t \in \{0,1\}^n$ be iid uniformly randomly chosen. Let $\mathcal{C} = \{v_1, \ldots, v_t\}$.

Let us consider the probability that $\mathcal{C}$ is a B_h-code. Suppose $\mathcal{C}$ is not a B_h-code. Then there exist $i_1, \ldots, i_h, j_1, \ldots, j_h$ such that

$$v_{i_1} + \cdots + v_{i_h} = v_{j_1} + \cdots v_{j_h}$$

and the multisets $\{i_1, \ldots, i_h\}$ and $\{j_1, \ldots, j_h\}$ are not equal.

One immediate idea is to bound the expected number of such violations of B_h-property. If the expectation is smaller than one, then we know that there exist desired B_h-codes. However, this idea does not work, because the expectation could be large. For example, if $v_1 = v_2$, then we have $\Theta(t^{h-1})$ violations of the form

$$v_1 + v_{i_2} + \cdots + v_{i_h} = v_2 + v_{i_2} + \cdots + v_{i_h}.$$

Therefore, instead of looking at the expected number of violations, we bound the expected number of "minimal" violations, i.e., $i_1, \ldots, i_k, j_1, \ldots, j_k$ $(1 \le k \le h)$ such that

$$v_{i_1} + \cdots + v_{i_k} = v_{j_1} + \cdots v_{j_k}$$

and the multisets $\{i_1, \ldots, i_k\}$ and $\{j_1, \ldots, j_k\}$ are disjoint.

Furthermore, minimal violations with the same k can have different forms. For example, the probability that $v_1 + v_1 = v_2 + v_3$ is different from the probability that $v_1 + v_2 = v_3 + v_4$. To address this, we make the following definition.

Definition 2.8. A configuration C of shape $(k, 2)$ is a $k \times 2$ matrix of random variables $(C_{i,j})_{1 \le i \le k, 1 \le j \le 2}$ taking values in $\{0, 1\}$ with the property that

1. For each i, j, $\mathbb{P}(C_{i,j} = 0) = \mathbb{P}(C_{i,j} = 1) = \frac{1}{2}$.

2. Some (or no) variables are identified, i.e., $\mathbb{P}(C_{i,j} = C_{i',j'}) = 1$ for some i, j, i', j'. We treat identified variables as the same variable. Variables that are not identified are mutually independent.

3. No variable appears in two columns, i.e., if $\mathbb{P}(C_{i,j} = C_{i',j'}) = 1$, then $j = j'$.

Two configurations of the same shape are equivalent if they have the same law after repeatedly (1) swapping columns and (2) swapping entries in the same column. Let $\mathrm{Conf}(k, 2)$ denote the set of equivalence classes of configurations of shape $(k, 2)$. Let $\mathrm{Conf}(\leq h, 2) = \bigcup_{1 \leq k \leq h} \mathrm{Conf}(k, 2)$.

Define $d(C)$ to be the number of distinct variables in C. Define $p(C)$ to be the probability that

$$C_{1,1} + \cdots + C_{k,1} = C_{1,2} + \cdots + C_{k,2}.$$

Remark 2.9. Due to the equivalence condition, we can also define a configuration of type $(k, 2)$ as two disjoint size-k multisets of random variables. Similarly, in Definition 4.2, we can define a configuration of type (k, l) as a size-l set of size-k multisets of random variables satisfying certain properties. We choose to describe a configuration as a matrix because this is easier to present.

Example 2.10. There is one configuration of shape $(1, 2)$: $C = \begin{pmatrix} a & b \end{pmatrix}$. (We use different lowercase letters to denote distinct variables.) We have $d(C) = 2$ and $p(C) = \frac{1}{2}$.

There are three non-equivalent configurations of shape $(2, 2)$. They are

1. $C_1 = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$. $d(C_1) = 2$ and $p(C_1) = \frac{1}{2}$.

2. $C_2 = \begin{pmatrix} a & b \\ a & c \end{pmatrix}$. $d(C_2) = 3$ and $p(C_2) = \frac{1}{4}$.

3. $C_3 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $d(C_3) = 4$ and $p(C_3) = \frac{3}{8}$.

It is not hard to see that there are $\binom{p_k+1}{2}$ non-equivalent configurations of shape $(k, 2)$, where p_k is the number of partitions of k.

Now let us discuss the relationship between minimal violations and configurations. For each minimal violation $i_1, \ldots, i_k, j_1, \ldots, j_k$, we can associate it with a configuration of shape $(k, 2)$, by identifying $C_{a,1}$ and $C_{b,1}$ for $i_a = i_b$, and identifying $C_{a,2} = C_{b,2}$ for $j_a = j_b$. Simple calculation shows that for each configuration C, there are $\Theta(t^{d(C)})$ minimal violations associated with it, and for each such minimal violation, the probability that it occurs is $p(C)^n$.

Therefore the expected number of minimal violations is at most

$$c \cdot \sum_{C \in \mathrm{Conf}(\leq h,2)} t^{d(C)} p(C)^n$$

where c is a constant only depending on h. So when

$$t = c' \left(\max_{C \in \mathrm{Conf}(\leq h,2)} p(C)^{1/d(C)} \right)^{-n}$$

for some small enough constant c', the expected number of minimal violations is less than one. So the only problem remains is to determine the maximum value of $p(C)^{1/d(C)}$ for $C \in \mathrm{Conf}(\leq h, 2)$.

It turns out that the maximum value is achieved at the configuration whose all variables are distinct, i.e., $d(C) = 2h$. Let $C_{\max}(h, 2)$ denote this configuration.

We need the following lemmas.

Lemma 2.11. *Let $X = \sum_{1 \leq i \leq d} c_i X_i$ where $c_i \in \mathbb{Z}_{\geq 1}$, $X_1, \ldots, X_d$ are iid uniform random variables taking values in $\{0, 1\}$. Then*

$$\sum_{a \geq 0} \mathbb{P}(X = a)^2 \leq p(C_{\max}(d, 2)).$$

Proof. Let $Y = \sum_{1 \leq i \leq d} c_i Y_i$ where $Y_1, \ldots, Y_d$ are an independent copy of $X_1, \ldots, X_d$. Then $\sum_{a \geq 0} \mathbb{P}(X = a)^2 = \mathbb{P}(X = Y)$.

Let us consider the characteristic function. Because $X - Y$ only takes integer

values, we have

$$\begin{aligned}\mathbb{P}(X = Y) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \phi_{X-Y}(t)dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \prod_{1\le i\le d} \phi_{c_i(X_i-Y_i)}(t)dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \prod_{1\le i\le d} \phi_{X_i-Y_i}(c_i t)dt.\end{aligned}$$

Note that

$$\phi_{X_i-Y_i}(t) = \phi_{X_i}(t)\overline{\phi_{Y_i}(t)} = |\phi_{X_1}(t)|^2 \in \mathbb{R}_{\ge 0}.$$

So we can apply AM-GM and get

$$\begin{aligned}\mathbb{P}(X = Y) &\le \frac{1}{2\pi d}\sum_{1\le i\le d}\int_{-\pi}^{\pi} \phi_{X_i-Y_i}(c_i t)^d dt \\ &= \frac{1}{2\pi d}\sum_{1\le i\le d}\int_{-\pi}^{\pi} \phi_{X_i-Y_i}(t)^d dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \phi_{X_1-Y_1}(t)^d dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \phi_{X_1+\cdots+X_d-Y_1-\cdots-Y_d}(t)dt \\ &= \mathbb{P}(X_1+\cdots+X_d = Y_1+\cdots+Y_d) \\ &= p(C_{\max}(d,2)).\end{aligned}$$

□

Lemma 2.12. *The value $p(C_{\max}(d,2))^{1/(2d)}$ is monotone increasing in d.*

Proof. Let $X_1,\ldots,X_d,Y_1,\ldots,Y_d$ be iid uniform random variables taking values in $\{0,1\}$. Then

$$\begin{aligned}p(C_{\max}(d,2)) &= \mathbb{P}(X_1+\cdots+X_d = Y_1+\cdots+Y_d) \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \phi_{X_1-Y_1}(t)^d dt.\end{aligned}$$

So the lemma follows from generalized mean inequality. □

Using the lemmas we can prove the following proposition.

Proposition 2.13. *Over all configurations in* $C \in \mathrm{Conf}(\leq h, 2)$*, the configuration* $C_{\max}(h, 2)$ *gives the maximum* $p(C)^{1/d(C)}$*.*

Proof. Let $C \in \mathrm{Conf}(k, 2)$ where $1 \leq k \leq h$. For $a \in \{0, 1 \ldots, k\}$, let $p_i(a)$ $(i = 1, 2)$ denote the probability that $C_{1,i} + \cdots + C_{k,i} = a$. By Cauchy-Schwarz inequality, we have

$$p(C) = \sum_{0 \leq a \leq k} p_1(a)p_2(a) \leq \sqrt{(\sum_{0 \leq a \leq k} p_1(a)^2)(\sum_{0 \leq a \leq k} p_2(a)^2)}.$$

Let d_i $(i = 1, 2)$ denote the number of distinct variables in column i. By Lemma 2.11 and Lemma 2.12,

$$\sum_{0 \leq a \leq k} p_i(a)^2 \leq p(C_{\max}(d_i, 2)) \leq p(C_{\max}(h, 2))^{d_i/h}.$$

So we have

$$\begin{aligned} p(C) &\leq \sqrt{(\sum_{0 \leq a \leq k} p_1(a)^2)(\sum_{0 \leq a \leq k} p_2(a)^2)} \\ &\leq \sqrt{p(C_{\max}(h, 2))^{d_1/h} p(C_{\max}(h, 2))^{d_2/h}} \\ &= p(C_{\max}(h, 2))^{d(C)/(2h)}. \end{aligned}$$

In other words,

$$p(C)^{1/d(C)} \leq p(C_{\max}(h, 2))^{1/(2h)}.$$

□

Now we can prove the theorem.

Proof of Theorem 2.7. By Proposition 2.13, we have

$$t = c' p(C_{\max}(h,2))^{-n/d(C_{\max}(h,2))}$$

and the rate of code $\mathcal{C}$ is

$$\frac{\log t}{n} = (1+o(1))\frac{-\log p(C_{\max}(h,2))}{d(C_{\max}(h,2))} = (1+o(1))\frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h}.$$

As $n \to \infty$ we get the desired code family. □

2.3.2 Poltyrev

With slight modification to the proof of D'yachkov-Rykov, we can achieve Poltyrev's rate.

Theorem 2.14 (Poltyrev [19])**.** *There exist B_h-codes of rate* $\frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h-1}$.

We need a lemma of basic math.

Lemma 2.15. *If $x^{1/n} \le y^{1/m}$ where $0 \le x, y \le 1$ and $2 \le n \le m$, then $x^{1/(n-1)} \le y^{1/(m-1)}$.*

Proof. We have

$$x^{1/(n-1)} \le y^{n/(m(n-1))} \le y^{1/(m-1)}.$$

□

Proof of Theorem 2.14. We perform the same random construction as in D'yachkov-Rykov to get $\mathcal{C} = \{v_1, \ldots, v_t\} \subseteq \{0,1\}^n$. The multiset $\mathcal{C}$ may contain several minimal violations. For each minimal violation appearing in $\mathcal{C}$, we arbitrarily pick and remove one vector in this minimal violation. In this way we get a set $\mathcal{C}'$ containing no minimal violations.

If

$$t = c'\Big(\max_{C \in \mathrm{Conf}(\le h,2)} p(C)^{1/(d(C)-1)}\Big)^{-n}$$

for some small enough constant c', the expected number of minimal violations in $\mathcal{C}$ is at most $\frac{t}{2}$ and the size of $\mathcal{C}'$ is at least $\frac{t}{2}$. By Lemma 2.15 and Proposition 2.13, the configuration $C_{\max}(h,2)$ achieves the maximum $p(C)^{1/(d(C)-1)}$ over all $C \in \mathrm{Conf}(\leq h, 2)$.

So rate of the code $\mathcal{C}'$ is at least

$$\frac{\log(t/2)}{n} = (1+o(1))\frac{-\log p(C_{\max}(h,2))}{d(C_{\max}(h,2))-1} = (1+o(1))\frac{\log\left(\frac{2^{2h}}{\binom{2h}{h}}\right)}{2h-1}.$$

As $n \to \infty$ we get the desired code family. $\square$

Chapter 3

Changing distribution

In this section we discuss whether we can change the probability distribution in random constructions of D'yachkov-Rykov and Poltyrev to achieve B_h-codes of higher rate.

3.1 Rate of random coding with a general distribution

In the original random construction, $\mathcal{C} = \{v_1, \ldots, v_t\}$ where each v_i is iid uniformly randomly chosen from $\{0,1\}^n$. The strategy we consider is to divide each length-n vector v_i into blocks $v_{i,1}, v_{i,2}, \cdots, v_{i,n/n_0}$ of length n_0, where n_0 is some constant. The $v_{i,j}$'s are iid randomly chosen from a fixed distribution $\mathcal{A}$ over $\{0,1\}^{n_0}$. If $\mathcal{A}$ is the uniform distribution, then this construction reduces to the original random construction.

Definition 3.1. Let X be a discrete random variable. The collision entropy is defined as

$$H_2(X) = -\log \sum_a \mathbb{P}(X = a)^2.$$

Definition 3.2. Let X be a random variable. The n-fold sum $X^{(h)}$ is a random variable such that $X^{(h)} = X_1 + \cdots + X_h$ where X_i's are independent copies of X.

Theorem 3.3. *Fix a constant n_0 and a probability distribution $\mathcal{A}$ over $\{0,1\}^{n_0}$. Let X be a random variable with distribution $\mathcal{A}$. Then there exist B_h-codes of rate at least $\frac{H_2(X^{(h)})}{n_0(2h-1)}$.*

Similar to the proof of D'yachkov-Rykov, we need to define configurations to characterize the minimal violations.

Definition 3.4. A configuration C of shape $(k,2)$ over distribution $\mathcal{A}$ is a $k \times 2$ matrix of random variables $(C_{i,j})_{1\le i\le k, 1\le j\le 2}$ taking values in $\{0,1\}^{n_0}$ with the following properties.

1. For each i,j, $C_{i,j}$ is distributed according to $\mathcal{A}$.

2. Some (or no) variables are identified.

3. No variable appears in two columns.

Two configurations of the same shape (and over the same distribution) are equivalent if they have the same law after (1) swapping columns and (2) swapping entries in the same column. Let $\mathrm{Conf}_{\mathcal{A}}(k,2)$ denote the set of equivalence classes of configurations of shape $(k,2)$ over $\mathcal{A}$. Let $\mathrm{Conf}_{\mathcal{A}}(\le h,2) = \bigcup_{1\le k\le h} \mathrm{Conf}_{\mathcal{A}}(k,2)$.

Similar to the uniform distribution case, there is a unique configuration of shape $(h,2)$ over $\mathcal{A}$ whose all variables are distinct. Let $C_{\mathcal{A},\max}(h,2)$ denote this configuration.

We prove the following lemmas in analogy with Lemma 2.11 and Lemma 2.12.

Lemma 3.5. *Let $X = \sum_{1\le d\le c_i} X_i$ where $c_i \in \mathbb{Z}_{\ge 1}$, $X_1,\dots,X_d$ are iid and each $X_i \sim \mathcal{A}$. Then*

$$\sum_a \mathbb{P}(X=a)^2 \le p(C_{\mathcal{A},\max}(d,2)).$$

Proof. Let $Y = \sum_{1\le i\le d} c_i Y_i$ where $Y_1,\dots,Y_d$ are an independent copy of $X_1,\dots,X_d$.

Then $\sum_a \mathbb{P}(X=a)^2 = \mathbb{P}(X=Y)$. Considering the characteristic function, we have

$$\begin{aligned}\mathbb{P}(X=Y) &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \phi_{X-Y}(t)dA(t)\\ &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \prod_{1\le i\le d}\phi_{c_i(X_i-Y_i)}(t)dA(t)\\ &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \prod_{1\le i\le d}\phi_{X_i-Y_i}(c_it)dA(t).\end{aligned}$$

Note that

$$\phi_{X_i-Y_i}(t) = \phi_{X_i}(t)\overline{\phi_{Y_i}(t)} = |\phi_{X_1}(t)|^2 \in \mathbb{R}_{\ge 0}.$$

So we can apply AM-GM and get

$$\begin{aligned}\mathbb{P}(X=Y) &\le d^{-1}(2\pi)^{-n_0}\sum_{1\le i\le d}\int_{[-\pi,\pi]^{n_0}} \phi_{X_i-Y_i}(c_it)^d dA(t)\\ &= d^{-1}(2\pi)^{-n_0}\sum_{1\le i\le d}\int_{[-\pi,\pi]^{n_0}} \phi_{X_i-Y_i}(t)^d dA(t)\\ &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \phi_{X_i-Y_i}(t)^d dA(t)\\ &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \phi_{X_1+\cdots+X_d-Y_1-\cdots-Y_d}(t)dA(t)\\ &= \mathbb{P}(X_1+\cdots+X_d = Y_1+\cdots+Y_d)\\ &= p(C_{\mathcal{A},\max}(d,2)).\end{aligned}$$

□

Lemma 3.6. *The value $p(C_{\mathcal{A},\max}(d,2))^{1/(2d)}$ is monotone increasing in d.*

Proof. Let $X_1,\dots,X_d,Y_1,\dots,Y_d$ be iid random variables, each with distribution $\mathcal{A}$. Then

$$\begin{aligned}p(C_{\mathcal{A},\max}(d,2)) &= \mathbb{P}(X_1+\cdots+X_d = Y_1+\cdots+Y_d)\\ &= (2\pi)^{-n_0}\int_{[-\pi,\pi]^{n_0}} \phi_{X_i-Y_i}(t)^d dA(t).\end{aligned}$$

So the lemma follows from generalized mean inequality. □

We have the following proposition in analogy with Proposition 2.13.

Proposition 3.7. *Over all $C \in \mathrm{Conf}_{\mathcal{A}}(\leq h, 2)$, the configuration $C_{\mathcal{A},\max}(h,2)$ gives the maximum $p(C)^{1/d(C)}$.*

Proof. Let $C \in \mathrm{Conf}_{\mathcal{A}}(k,2)$ where $1 \leq k \leq h$. For $a \in \{0, 1 \ldots, k\}^{n_0}$, let $p_i(a)$ $(i = 1, 2)$ denote the probability that $C_{1,i} + \cdots + C_{k,i} = a$. By Cauchy-Schwarz inequality, we have

$$p(C) = \sum_a p_1(a)p_2(a) \leq \sqrt{(\sum_a p_1(a)^2)(\sum_a p_2(a)^2)}.$$

Let d_i $(i = 1, 2)$ denote the number of distinct variables in column i. By Lemma 3.5 and Lemma 3.6,

$$\sum_a p_i(a)^2 \leq p(C_{\mathcal{A},\max}(d_i, 2)) \leq p(C_{\mathcal{A},\max}(h,2))^{d_i/h}.$$

So we have

$$\begin{aligned} p(C) &\leq \sqrt{(\sum_a p_1(a)^2)(\sum_a p_2(a)^2)} \\ &\leq \sqrt{p(C_{\mathcal{A},\max}(h,2))^{d_1/h} p(C_{\mathcal{A},\max}(h,2))^{d_2/h}} \\ &= p(C_{\mathcal{A},\max}(h,2))^{d(C)/(2h)}. \end{aligned}$$

In other words,

$$p(C)^{1/d(C)} \leq p(C_{\mathcal{A},\max}(h,2))^{1/(2h)}.$$

□

Now we prove the theorem.

Proof of Theorem 3.3. Similar to proof of Theorem 2.7, we consider the minimal vi-

olations, $i_1, \ldots, i_k, j_1, \ldots, j_k$ $(1 \le k \le h)$ such that

$$v_{i_1} + \cdots + v_{i_k} = v_{j_1} + \cdots + v_{j_k}$$

and the multisets $\{i_1, \ldots, i_k\}$, $\{j_1, \ldots, j_k\}$ are disjoint. For each minimal violation we can associate it with a configuration of shape $(k, 2)$ over $\mathcal{A}$. For each configuration $C \in \mathrm{Conf}_{\mathcal{A}}(\le h, 2)$, there are $\Theta(t^{d(C)})$ minimal violations associated with it, and for each such minimal violation, the probability that it occurs is $p(C)^n$.

Therefore the expected number of minimal violations is at most

$$c \cdot \sum_{C \in \mathrm{Conf}_{\mathcal{A}}(\le h, 2)} t^{d(C)} p(C)^{n/n_0}$$

where c is a constant only depending on h. So when

$$t = c'\big(\max_{C \in \mathrm{Conf}_{\mathcal{A}}(\le h, 2)} p(C)^{1/(d(C)-1)}\big)^{-n/n_0}$$

for some small enough constant c', the expected number of minimal violations is at most $\frac{t}{2}$. So if we remove one vector for each minimal violation, we would get a B_h-code $\mathcal{C}'$ of size at least $\frac{t}{2}$.

By Proposition 3.7 and Lemma 2.15, we have

$$t = c' p(C_{\mathcal{A},\max}(h, 2))^{-n/(n_0(d(C_{\mathcal{A},\max}(h,2))-1))}$$

and the rate of code $\mathcal{C}'$ is

$$\frac{\log(t/2)}{n} = (1 + o(1)) \frac{-\log p(C_{\mathcal{A},\max}(h, 2))}{n_0(d(C_{\mathcal{A},\max}(h, 2)) - 1)} = (1 + o(1)) \frac{H_2(X^{(h)})}{n_0(2h - 1)}$$

where $X^{(h)} = X_1 + \cdots + X_h$ and X_i's are iid random variables with distribution $\mathcal{A}$.

As $n \to \infty$ we get the desired code family.

□

3.2 A conjecture on collision entropy

In light of Theorem 3.3, if we can find distribution $\mathcal{A}$ with

$$\frac{H_2(X^{(h)})}{n_0} > \log\left(\frac{2^{2h}}{\binom{2h}{h}}\right),$$

then we achieve B_h-codes with higher rate. We were not able to find such a distribution and consequently propose the following conjecture.

Conjecture 3.8. For any distribution $\mathcal{A}$ over $\{0,1\}^{n_0}$, we have

$$\frac{H_2(X^{(h)})}{n_0} \leq \log\left(\frac{2^{2h}}{\binom{2h}{h}}\right).$$

Some partial results on this conjecture is discussed in Chapter 5.

Chapter 4

Random coding for $B_h[g]$-code

In this chapter we study the performance of random coding on list-decoding versions of B_h-codes. The primary version we consider is the $B_h[g]$-code.

4.1 Rate of random coding

Definition 4.1. A $B_h[g]$-code is a set $\mathcal{C} \subseteq \{0,1\}^n$ satisfying the property that for any $a \in \{0,1,\ldots,h\}^n$, there exists at most g multisets $\{u_1,\ldots,u_h\}$ such that $a = u_1 + \cdots + u_h$. Note that a $B_h[1]$-code is exactly the same as a B_h-code. The rate of a $B_h[g]$-code is defined as $\frac{\log|\mathcal{C}|}{n}$.

We would like to apply random coding. Therefore it is important to keep track of the minimal violations. The following definition should not come as a surprise.

Definition 4.2. A configuration C of shape (k,l) is a $k \times l$ matrix of random variables $(C_{i,j})_{1\le i\le k, 1\le j\le l}$ taking values in $\{0,1\}$ with the property that

1. For each i,j, $\mathbb{P}(C_{i,j}=0) = \mathbb{P}(C_{i,j}=1) = \frac{1}{2}$.
2. Some (or no) variables are identified, i.e., $\mathbb{P}(C_{i,j} = C_{i',j'}) = 1$ for some i,j,i',j'. We treat identified variables as the same variable. Variables that are not identified are mutually independent.
3. No variable appears in all columns.

4. For two different columns, the multiset of variables in this column are different.

Two configurations of the same shape are equivalent if they have the same law after repeatedly (1) swapping columns and (2) swapping entries in the same column. Let $\mathrm{Conf}(k,l)$ denote the set of equivalence classes of configurations of shape (k,l). Let $\mathrm{Conf}(\leq h,l) = \bigcup_{1\leq k\leq h} \mathrm{Conf}(k,l)$.

Define $d(C)$ to be the number of distinct variables in C. Define $p(C)$ to be the probability that $C_{1,j} + \cdots + C_{k,j}$ are equal for $1 \leq j \leq l$.

Example 4.3. There are seven non-equivalent configurations of shape $(2,3)$. They are

1. $C_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$. $d(C_1) = 3$ and $p(C_1) = \frac{1}{4}$.
2. $C_2 = \begin{pmatrix} a & b & c \\ a & b & d \end{pmatrix}$. $d(C_2) = 4$ and $p(C_2) = \frac{1}{8}$.
3. $C_3 = \begin{pmatrix} a & b & d \\ a & c & e \end{pmatrix}$. $d(C_3) = 5$ and $p(C_3) = \frac{1}{16}$.
4. $C_4 = \begin{pmatrix} a & c & e \\ b & d & f \end{pmatrix}$. $d(C_4) = 6$ and $p(C_4) = \frac{5}{32}$.
5. $C_5 = \begin{pmatrix} a & a & b \\ b & c & c \end{pmatrix}$. $d(C_5) = 3$ and $p(C_5) = \frac{1}{4}$.
6. $C_6 = \begin{pmatrix} a & a & b \\ b & c & d \end{pmatrix}$. $d(C_6) = 4$ and $p(C_6) = \frac{1}{4}$.
7. $C_7 = \begin{pmatrix} a & a & d \\ b & c & e \end{pmatrix}$. $d(C_7) = 5$ and $p(C_7) = \frac{3}{16}$.

Matrix $\begin{pmatrix} a & a & a \\ b & c & d \end{pmatrix}$ is not a valid configuration because it violates property 3. Matrix $\begin{pmatrix} a & a & c \\ b & b & d \end{pmatrix}$ is not a valid configuration because it violates property 4.

Theorem 4.4. *There exist $B_h[g]$-codes of rate at least*

$$\min_{C \in \mathrm{Conf}(\leq h, g+1)} \frac{-\log p(C)}{d(C)-1}.$$

Proof. A violation of the $B_h[g]$-property is a matrix $(x_{i,j})_{1 \leq i \leq h, 1 \leq j \leq g+1}$ where $1 \leq x_{i,j} \leq t$, no two columns have the same multisets of variables, and the column sums

$$v_{x_{1,j}} + \cdots + v_{x_{h,j}}$$

are equal for all j. A violation can be non-minimal in the sense that there are numbers appearing in all columns. Therefore the minimal violations we consider are matrices $(x_{i,j})_{1 \leq i \leq k, 1 \leq j \leq g+1}$ where $1 \leq k \leq h$, $1 \leq x_{i,j} \leq t$, no two columns have the same multisets of variables and the column sums

$$v_{x_{1,j}} + \cdots + v_{x_{k,j}}$$

are equal for all j.

For each minimal violation, we can associate to it a configuration of shape $(k, g+1)$. For each configuration $C \in \mathrm{Conf}(\leq h, g+1)$, the number of minimal violations associated to it is $\Theta(t^{d(C)})$, and each such minimal violation appears with probability $p(C)^n$. So the expected number of minimal violations is at most

$$c \cdot \sum_{C \in \mathrm{Conf}(\leq h, g+1)} t^{d(C)} p(C)^n$$

where c is some constant depending only on h and g. So when

$$t = c' \left(\max_{C \in \mathrm{Conf}(\leq h, g+1)} p(C)^{1/(d(C)-1)} \right)^{-n}$$

for some small enough constant c', the expected number of violations is no more than $\frac{t}{2}$. Then we can remove one vector for each minimal violation, and get a $B_h[g]$-code $\mathcal{C}'$ of size at least $\frac{t}{2}$.

The rate of code $\mathcal{C}'$ is

$$\frac{\log(t/2)}{n} = (1+o(1)) \min_{C \in \mathrm{Conf}(\leq h, g+1)} \frac{-\log p(C)}{d(C)-1}.$$

As $n \to \infty$ we get the desired code family. □

4.2 Suboptimality of the all-distinct configuration

Let $C_{\max}(h, g+1)$ denote the configuration where all variables are distinct. In analogy with Proposition 2.13 and Proposition 3.7, one may guess that the maximum value of $p(C)^{1/(d(C)-1)}$ is achieved at $C_{\max}(h, g+1)$. Unfortunately, this turns out to be not true.

Proposition 4.5. *There exist g and h such that the configuration $C_{\max}(h, g+1)$ does not give the maximum $p(C)^{1/(d(C)-1)}$ over all $C \in \mathrm{Conf}(\leq h, g+1)$.*

Proof. Let C be the following configuration.

$$\begin{pmatrix} a_1 & c_2 & c_3 & \cdots & c_{g+1} \\ a_2 & b_2 & b_2 & \cdots & b_2 \\ a_3 & b_3 & b_3 & \cdots & b_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_h & b_h & b_h & \cdots & b_h \end{pmatrix}$$

where different variables denote distinct random variables. Clearly $d(C) = 2h-1+g$. Column sums are all equal if and only if

$$a_1 + \cdots + a_h = c_2 + b_2 + \cdots + b_h$$

and

$$c_2 = c_3 = \cdots = c_{g+1}.$$

So

$$\begin{aligned} p(C) &= \mathbb{P}(a_1 + \cdots + a_h = c_2 + b_2 + \cdots + b_h)\mathbb{P}(c_2 = c_3 = \cdots = c_{g+1}) \\ &= 2^{-2h}\binom{2h}{h}2^{-(g-1)} \\ &= \binom{2h}{h}2^{-(2h+g-1)}. \end{aligned}$$

So

$$p(C)^{1/(d(C)-1)} = (2^{-(2h+g-1)}\binom{2h}{h})^{1/(2h-1+g-1)}.$$

Take $g = 2$ and $h = 100$. Numerical computations shows that

$$p(C)^{1/(d(C)-1)} \approx 0.982312$$

and

$$p(C_{\max}(h, g+1))^{1/(d(C_{\max}(h,g+1))-1)} \approx 0.981414.$$

□

Remark 4.6. By Lemma 2.15, the proposition implies that there exist g and h such that the configuration $C_{\max}(h, g+1)$ does not give the maximum $p(C)^{1/d(C)}$ over all $C \in \mathrm{Conf}(\leq h, g+1)$.

Numerical computation suggests that for fixed $g \geq 2$, the all-distinct configuration $C_{\max}(h, g+1)$ is suboptimal for all h large enough.

4.3 Separable configurations

Proposition 4.5 shows that the rate of random coding construction for $B_h[g]$-codes is much more complicated than that for B_h-codes. On the other hand, for configurations with nice properties, analogies of Proposition 2.13 and Proposition 3.7 may hold.

Definition 4.7. We say a configuration is separable if no variable appears in two or more columns. Let $\mathrm{SConf}(k,l)$ denote the set of separable configurations of shape (k,l). Let $\mathrm{SConf}(\leq h,l) = \bigcup_{1\leq k\leq h} \mathrm{SConf}(k,l)$.

Proposition 4.8. *Fix h to be an even number. Over all separable configurations $C \in \mathrm{SConf}(\leq h, g+1)$, the configuration $C_{\max}(h,g+1)$ gives the maximum $p(C)^{1/d(C)}$.*

We first prove some lemmas. The proofs of them are more difficult than the previous ones.

Lemma 4.9. *Let $X = \sum_{1\leq i\leq d} c_i X_i$ where $c_i \in \mathbb{Z}_{\geq 1}$, $X_1, \ldots, X_d$ are iid uniform random variables taking values in $\{0,1\}$. Then*

$$\sum_{a\geq 0} \mathbb{P}(X=a)^{g+1} \leq p(C_{\max}(d, g+1)).$$

Before proving this lemma, let us have some discussions about symmetric decreasing rearrangement and majorization.

Definition 4.10. Let $(p_a)_{a\geq 0}$ be a sequence of non-negative numbers with only finitely-many nonzero entries. Let $(T(p)_a)_{a\geq 0}$ be the sorted version of p in decreasing order.

For two sequences p and q, if we have

$$\sum_{0\leq i\leq n} T(p)_i \leq \sum_{0\leq i\leq n} T(q)_i,$$

for all n, we say p is majorized by q, written as $p \preceq q$.

Let $(S(p)_a)_{a\geq 0}$ be as follows:

$$\cdots \quad T(p)_4 \quad T(p)_2 \quad T(p)_0 \quad T(p)_1 \quad T(p)_3 \quad T(p)_5 \quad \cdots$$

(with zeros on the left removed). We say $S(p)$ is the symmetric decreasing rearrangement of p.

For a nonzero integer c, define the sequence $C_c(p) = (p_a + p_{a-c})_{a\geq 0}$, where $p_i = 0$ for $i < 0$.

Lemma 4.11. *Let $(p_a)_{a\geq 0}$ be a sequence of non-negative numbers with only finitely-many nonzero entries. Let c be a nonzero integer. Then $C_c(p) \preceq C_1(S(p))$.*

Proof. Let $q = T(p)$. Simple calculation shows that

$$\sum_{0\leq i\leq n} T(C_1(S(p)))_i = \sum_{0\leq i\leq n-1} q_i + \sum_{0\leq i\leq n+1} q_i.$$

We know that $\sum_{0\leq i\leq n} T(C_c(p))_i$ is sum of $2n+2$ terms of q, where each q_i appears at most twice. So if

$$\sum_{0\leq i\leq n} T(C_1(S(p)))_i < \sum_{0\leq i\leq n} T(C_c(q))_i,$$

then

$$\sum_{0\leq i\leq n} T(C_c(p))_i = 2\sum_{0\leq i\leq n} q_i$$

and $q_n > q_{n+1}$.

Consider the largest $(n+1)$ terms of $C_c(p)$. Each p_i appearing in these terms appears twice. Let a be the largest number such that p_a appears in the largest $(n+1)$ terms of $C_c(p)$. Then p_{a-c} and p_{a+c} must both appear. Because $c \neq 0$, this contradicts the maximality of a. □

Lemma 4.12. *If $p \preceq q$, then $C_1(S(p)) \preceq C_1(S(q))$.*

Proof. WLOG assume that p and q are sorted in decreasing order. Then for all $n \geq 1$, we have

$$\begin{aligned}\sum_{0\leq i\leq n} T(C_1(S(p)))_i &= \sum_{0\leq i\leq n-1} p_i + \sum_{0\leq i\leq n+1} p_i \\ &\leq \sum_{0\leq i\leq n-1} q_i + \sum_{0\leq i\leq n+1} q_i \\ &= \sum_{0\leq i\leq n} T(C_1(S(q)))_i.\end{aligned}$$

□

Proof of Lemma 4.9. Let $Y = Y_1 + \cdots + Y_d$ where Y_i's are independent copies of X_i's. Let $p(Y)$ denote the sequence $(p(Y)_a)_{a\geq 0}$ where $p(Y)_a = \mathbb{P}(Y = a)$. Similarly define $p(X)$. The sequences $p(X)$ and $p(Y)$ each contain at most 2^d nonzero numbers. The function $f((p_a)_{a\geq 0}) = \sum_a p_a^{g+1}$ is Schur-convex. So we only need to prove that $p(X) \preceq p(Y)$. We prove this by induction on d.

Base case: When $d = 0$, $p(X) = p(Y)$.

Induction step: Suppose the result for $d-1$ variables is true. Let

$$X' = \sum_{1\leq i\leq d-1} c_i X_i$$

and

$$Y' = \sum_{1\leq i\leq d-1} Y_i.$$

By induction hypothesis, $p(X') \preceq p(Y')$. By Lemma 4.11 and Lemma 4.12, we have

$$\begin{aligned} p(X) = \frac{1}{2}C_c(p(X')) &\preceq \frac{1}{2}C_1(S(p(X'))) \\ &\preceq \frac{1}{2}C_1(S(p(Y'))) = \frac{1}{2}C_1(p(Y')) = p(Y). \end{aligned}$$

□

Lemma 4.13. *Fix $g \in \mathbb{Z}_{\geq 1}$. Suppose $d \leq h$ and h is even. Then we have*

$$p(C_{\max}(d, g+1))^{1/(d(g+1))} \leq p(C_{\max}(h, g+1))^{1/(h(g+1))}.$$

Proof.

$$p(C_{\max}(d, g+1))^{1/(d(g+1))} = \frac{1}{2}\Big(\sum_{0\leq i\leq d} \binom{d}{i}^{g+1}\Big)^{1/(d(g+1))}.$$

The sum $\sum_{0\leq i\leq d} \binom{d}{i}^{g+1}$ is the constant coefficient of

$$(1+z_1)^d \cdots (1+z_g)^d (1+(z_1\cdots z_g)^{-1})^d.$$

So by Cauchy's integral formula, we have

$$\sum_{0\le i\le d}\binom{d}{i}^{g+1} = (2\pi i)^{-g}\oint\cdots\oint(1+z_1)^d\cdots(1+z_g)^d \cdot(1+(z_1\cdots z_g)^{-1})^d(z_1^{-1}dz_1\cdots z_g^{-1}dz_g)$$

where the integrals are taken along the unit circles in the complex plane. Perform substitution $z_j=\exp(2it_j)$. We get

$$\sum_{0\le i\le d}\binom{d}{i}^{g+1} = 2^{(g+1)d}\pi^{-g} \cdot\int\cdots\int(\cos t_1\cdots\cos t_g\cos(t_1+\cdots+t_g))^d dt_1\cdots dt_g$$

where the integrals are taken over $[-\frac{\pi}{2},\frac{\pi}{2}]$. Therefore

$$\begin{aligned}
&p(C_{\max}(d,g+1))^{1/(d(g+1))}\\
&=(\pi^{-g}\cdot\int\cdots\int(\cos t_1\cdots\cos t_g\cos(t_1+\cdots+t_g))^d dt_1\cdots dt_g)^{1/(d(g+1))}\\
&\le(\pi^{-g}\cdot\int\cdots\int|\cos t_1\cdots\cos t_g\cos(t_1+\cdots+t_g)|^d dt_1\cdots dt_g)^{1/(d(g+1))}\\
&\le(\pi^{-g}\cdot\int\cdots\int|\cos t_1\cdots\cos t_g\cos(t_1+\cdots+t_g)|^h dt_1\cdots dt_g)^{1/(h(g+1))}\\
&=(\pi^{-g}\cdot\int\cdots\int(\cos t_1\cdots\cos t_g\cos(t_1+\cdots+t_g))^h dt_1\cdots dt_g)^{1/(h(g+1))}\\
&=p(C_{\max}(h,g+1))^{1/(h(g+1))}.
\end{aligned}$$

(Third step is generalized mean inequality. Fourth step uses that h is even.) □

Remark 4.14. Numerical computation suggests that for fixed g, the value $p(C_{\max}(d,g+1))^{1/(d(g+1))}$ is monotone increasing in d. If this is indeed true, we can remove the hypothesis that h is even in Proposition 4.8.

Proof of Proposition 4.8. Let $C\in\mathrm{SConf}(k,2)$ where $1\le k\le h$. For $a\in\{0,1,\ldots,k\}$, let $p_i(a)$ $(1\le i\le g+1)$ denote the probability that $C_{1,i}+\cdots+C_{k,i}=a$. By Hölder's

inequality, we have

$$\begin{aligned} p(C) &= \sum_{0\le a\le k} p_1(a)p_2(a)\cdots p_{g+1}(a) \\ &\le \prod_{1\le i\le g+1} (\sum_{0\le a\le k} p_i(a)^{g+1})^{1/(g+1)}. \end{aligned}$$

Let d_i $(1 \le i \le g+1)$ denote the number of distinct variables in column i. By Lemma 4.9 and Lemma 4.13,

$$\sum_{0\le a\le k} p_i(a)^{g+1} \le p(C_{\max}(d_i, g+1)) \le p(C_{\max}(h, g+1))^{d_i/h}.$$

So we have

$$\begin{aligned} p(C) &\le \prod_{1\le i\le g+1} (\sum_{0\le a\le k} p_i(a)^{g+1})^{1/(g+1)} \\ &\le \prod_{1\le i\le g+1} p(C_{\max}(h, g+1))^{d_i/(h(g+1))} \\ &= p(C_{\max}(h, g+1))^{d(C)/(h(g+1))}. \end{aligned}$$

In other words,

$$p(C)^{1/d(C)} \le p(C_{\max}(h, g+1))^{1/(h(g+1))}.$$

□

4.4 Another kind of list-decoding

There is another natural list-decoding version of B_h-codes, which is more closely related to the number of distinct elements in configurations.

Definition 4.15. A $B_h^{\#}[d]$-code is a set $\mathcal{C} \subseteq \{0,1\}^n$ satisfying the property that for any $a \in \{0, 1, \ldots, h\}^n$, there exists a subset $S \subseteq \mathcal{C}$ of size at most d such that if $u_1 + \cdots + u_h = a$, $u_i \in \mathcal{C}$ for $1 \le i \le h$, then $u_i \in S$ for $1 \le i \le h$.

Note that this definition is only meaningful when $d \geq h$. Let us apply random coding to this problem. Considering the minimal violations, we have the following definition.

Definition 4.16. Define $\mathrm{Conf}^{\#}(\leq h)[d]$ as the set of configurations C of shape (k, l) where $1 \leq k \leq h$, $l \geq 2$, $d(C) \geq d + 1 - h + k$, and such that removing any column from C will make the number of distinct variables less than or equal to $d - h + k$.

Proposition 4.17. *The set* $\mathrm{Conf}^{\#}(\leq h)[d]$ *is finite.*

Proof. Let $C \in \mathrm{Conf}^{\#}(\leq h)[d]$. Because every column has at most h distinct variables, the last condition implies that $d(C) \leq d+k$. Now we fix $d(C)$. For each column, there are a finite number of possible choices. Because C is a valid configuration, no two columns are the same. Therefore the number of columns is bounded by a finite number. So the number of possible C's is finite. □

Theorem 4.18. *There exist* $B_h^{\#}[d]$*-codes of rate at least*

$$\min_{C \in \mathrm{Conf}^{\#}(\leq h)[d]} \frac{-\log p(C)}{d(C) - 1}.$$

Proof. A violation of the $B_h^{\#}[d]$-property is a matrix $(x_{i,j})_{1 \leq i \leq h, 1 \leq j \leq l}$ with $l \geq 2$ such that the column sums $x_{1,j} + \cdots + x_{h,j}$ are equal for $1 \leq j \leq l$, and the set $\{x_{i,j}, 1 \leq i \leq h, 1 \leq j \leq l\}$ has cardinality at least $d + 1$. A violation can be non-minimal in the sense that (1) some variables appear in all columns, or (2) we can remove some columns so that the number of distinct $x_{i,j}$'s is still larger than d. Also, note that removing one occurrence in each column for a variable that appears in all columns will decrease the number of distinct entries by at most one. So the restriction on the number of distinct entries is weaker for minimal violations with fewer rows.

Therefore a minimal violation is a matrix $(x_{i,j})_{1 \leq i \leq k, 1 \leq j \leq l}$ with $1 \leq k \leq h$, $l \geq 2$ such that the column sums $x_{1,j} + \cdots + x_{k,j}$ are equal for $1 \leq j \leq l$, the set of $x_{i,j}$'s has cardinality at least $d+1-h+k$, and removing any column will make the matrix have at most $d - h + k$ distinct entries.

For each minimal violation, we can associate to it a configuration in $\mathrm{Conf}^{\#}(\leq h)[d]$. For each such configuration C, there are $\Theta(t^{d(C)})$ minimal violations associated to it, and each such minimal violation appears with probability $p(C)^n$. So the expected number of minimal violations is at most

$$c \cdot \sum_{C \in \mathrm{Conf}^{\#}(\leq h)[d]} t^{d(C)} p(C)^n$$

where c is some constant depending only on h and d. So whn

$$t = c' \left(\max_{C \in \mathrm{Conf}^{\#}(\leq h)[d]} p(C)^{1/(d(C)-1)} \right)^{-n}$$

for some small enough constant c', the expected number of violations is no more than $\frac{t}{2}$. Then we can remove one vector for each minimal violation, and get a $B_h^{\#}[d]$-code $\mathcal{C}'$ of size at least $\frac{t}{2}$. The rate of code $\mathcal{C}'$ is

$$\frac{\log(t/2)}{n} = (1 + o(1)) \min_{C \in \mathrm{Conf}^{\#}(\leq h)[d]} \frac{-\log p(C)}{d(C) - 1}.$$

As $n \to \infty$ we get the desired code family. □

Chapter 5

Some problems about Rényi entropy

In this chapter we study several problems about maximizing Rényi entropy that arises in the study of communication over adder MAC.

We first define Rényi entropy, a natural generalization of Shannon entropy.

Definition 5.1. Let X be a discrete random variable. The Rényi entropy of order α ($\alpha \geq 0, \alpha \neq 1$) is defined as

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_a \mathbb{P}(X = a)^\alpha.$$

The Rényi entropy of order 1 is

$$H_1(X) = \lim_{\alpha \to 1} H_\alpha(X) = -\sum_a \mathbb{P}(X = a) \log \mathbb{P}(X = a) = H(X)$$

where $H(X)$ is Shannon entropy. The Rényi entropy of order ∞ (also called min-entropy) is

$$H_\infty(X) = \lim_{\alpha \to \infty} H_\alpha(X) = -\log \max_a \mathbb{P}(X = a).$$

Remark 5.2. The Rényi entropy of order 2 is collision entropy (Definition 3.1).

In this chapter, the kind of problems we study is the following. Fix a set A inside some ambient abelian group and fix a non-negative real number α. We would like

to determine the maximum $H_\alpha(X+X)$ where X is a random variable taking value in A (where $X+X$ is understood as sum of two independent copies of X). We are also interested in the maximum $H_\alpha(X+Y)$ where X and Y are independent random variables taking value in A, and X and Y need not have the same distribution.

5.1 Addition in $\{0,1\}^n$

The setting most related to adder MAC is $A = \{0,1\}^n \subseteq \mathbb{Z}^n$. Ajjanagadde and Polyanskiy [2] made the following conjecture arising from studying noisy communication over adder MAC with finite block length.

Conjecture 5.3 (Ajjanagadde-Polyanskiy [2])**.** For $0 \leq \alpha \leq 1$, the Rényi entropy $H_\alpha(X+Y)$ is maximized at the uniform distribution.

In their conjecture, the distribution of X and Y can be different. We consider the same-distribution version and thus it makes sense to generalize Conjecture 3.8 to the following.

Conjecture 5.4. For $0 \leq \alpha \leq 2$ and $h \geq 2$, the Rényi entropy $H_\alpha(X^{(h)})$ is maximized at the uniform distribution. In particular, for $0 \leq \alpha \leq 2$, the Rényi entropy $H_\alpha(X+X)$ is maximized at the uniform distribution.

Remark 5.5. The general conjecture is true for $\alpha = 0$ trivially and for $\alpha = 1$ by subadditivity of Shannon entropy. The case $\alpha = 2$ is Conjecture 3.8.

We discuss some partial results for the case $h = 2$.

Proposition 5.6. *For $\alpha > 2$, there exists n such that the uniform distribution over $\{0,1\}^n$ does not maximize $H_\alpha(X+X)$.*

Proof. For $x \in \{0,1\}^n$, denote $\mathbb{P}(X = x)$ as p_x. For $z \in \{0,1,2\}^n$, define $c_z = \sum_{x+y=z} p_x p_y$. Define $f(p) = \sum_z c_z^\alpha$. Then $H_\alpha(X+X) = \frac{1}{1-\alpha} \log f(p)$. Let p° denote the uniform distribution over $\{0,1\}^n$. We claim that the uniform distribution does not minimize $f(p)$.

It is easy to see that for $z = \{0,1,2\}^n$, we have

$$c_z|_{p^\circ} = 2^{-2n} 2^{\#_1(z)}$$

where $c_z|_{p^\circ}$ denote c_z for the uniform distribution, and $\#_1(z)$ denote the number of i's $(1 \le i \le n)$ with $z_i = 1$.

Let us compute the first derivatives. For $x \in \{0,1\}^n$ and $z = x + y \in \{0,1,2\}^n$ with $y \in \{0,1\}^n$, we have

$$\frac{\partial c_z^\alpha}{\partial p_x} = 2\alpha c_z^{\alpha-1} p_y.$$

So

$$\frac{\partial f(p)}{\partial p_x} = \sum_y 2\alpha c_{x+y}^{\alpha-1} p_y.$$

By symmetry of f, the first derivatives $\frac{\partial f(p)}{\partial p_x}|_{p^\circ}$ are the same for all $x \in \{0,1\}^n$. So we need to check second derivatives.

It is easily computed that

$$\frac{\partial^2 c_z^\alpha}{\partial p_x \partial p_y} = 4\alpha(\alpha-1) c_z^{\alpha-2} p_{z-y} p_{z-x}$$

for $z \neq x + y$ with $z - x, z - y \in \{0,1\}^n$ and

$$\frac{\partial^2 c_z^\alpha}{\partial p_x \partial p_y} = 4\alpha(\alpha-1) c_z^{\alpha-2} p_{z-y} p_{z-x} + 2\alpha c_z^{\alpha-1}$$

for $z = x + y$.

Define $d(x,y)$ to be Hamming distance between x and y. For fixed x and y, there are $2^{n-d(x,y)}$ different z's such that $z - x, z - y \in \{0,1\}^n$. (For i such that $x_i \neq y_i$, we must have $z_i = 1$; for i such that $x_i = y_i$, we have $z_i = i$ or $i + 1$.) Among these z's,

$\binom{n-d(x,y)}{w}$ of them have $\#_1(z) = d(x,y) + w$. Therefore

$$\begin{aligned}\frac{\partial^2 f(p)}{\partial p_x \partial p_y}|_{p^\circ} &= 4\alpha(\alpha-1) \sum_{0\le w\le n-d(x,y)} \binom{n-d(x,y)}{w} (2^{d(x,y)+w}2^{-2n})^{\alpha-2}2^{-2n} \\ &\quad + 2\alpha(2^{d(x,y)}2^{-2n})^{\alpha-1} \\ &= 4\alpha(\alpha-1)(4+2^\alpha)^{n-d(x,y)}2^{\alpha d(x,y)-2\alpha n} + 2\alpha(2^{d(x,y)}2^{-2n})^{\alpha-1}.\end{aligned}$$

Let A be an $2^n \times 2^n$ matrix indexed by $\{0,1\}^n$ with

$$A_{x,y} = \frac{\partial^2 f(p)}{\partial p_x \partial p_y}|_{p^\circ}.$$

We claim that there exists a length-2^n vector v with $\sum_x v_x = 0$ and $v^t A v < 0$. Let v be such that $v_x = (-1)^{\#_1(x)}$. Then we have

$$\begin{aligned}v^t A v &= \sum_{x,y\in\{0,1\}^n} (-1)^{d(x,y)} A_{x,y} \\ &= 2^n \sum_{0\le d\le n} \binom{n}{d} (-1)^d (4\alpha(\alpha-1)(4+2^\alpha)^{n-d}2^{\alpha d-2\alpha n} + 2\alpha(2^d 2^{-2n})^{\alpha-1}) \\ &= 2^{1+2n-2\alpha n}((2-2^\alpha)^n + 2^{n+1}(\alpha-1))\alpha.\end{aligned}$$

If $\alpha > 2$ and n is a large enough odd number, the above value is negative. So $f(p^\circ + \epsilon v) < f(p^\circ)$ for $\epsilon > 0$ small enough. □

Proposition 5.7. *For $0 \le \alpha \le 2$, the uniform distribution over $\{0,1\}^n$ is a local maximum of $H_\alpha(X+X)$.*

Proof. The cases $\alpha = 0$ and $\alpha = 1$ follow from Remark 5.5. Now assume $\alpha \ne 0, 1$. Follow notations p_x, c_z, p°, f, A in proof of Proposition 5.6.

We prove that p° is a local maximum of $f(p)$ for $0 < \alpha < 1$ and a local minimum of $f(p)$ for $1 < \alpha < 2$. By proof of Proposition 5.6, the first derivatives $\frac{\partial f(p)}{\partial p_x}|_{p^\circ}$ are the same for all $x \in \{0,1\}^n$, and

$$\frac{\partial^2 f(p)}{\partial p_x \partial p_y}|_{p^\circ} = 4\alpha(\alpha-1)(4+2^\alpha)^{n-d(x,y)}2^{\alpha d(x,y)-2\alpha n} + 2\alpha(2^{d(x,y)}2^{-2n})^{\alpha-1}.$$

Note that $\mathbb{1}$ is an eigenvector of A. Let $\mathbb{1}^\perp$ denote the vector space of vectors v orthogonal to $\mathbb{1}$, i.e., $v^t\mathbb{1} = 0$. Clearly A acts on $\mathbb{1}^\perp$.

We prove that matrix A is positive definite (resp. negative definite) on $\mathbb{1}^\perp$ for $1 < \alpha < 2$ (resp. $0 < \alpha < 1$). Let $v \in \mathbb{1}^\perp$ be an eigenvector of A with eigenvalue λ. Note that $A_{x,y}$ only depends on $d(x, y)$, so A possesses a lot of symmetry. Let $g_i : \{0,1\}^n \to \{0,1\}^n$ $(1 \le i \le n)$ be the map that flips the i-th coordinate. Then $g_i^{-1} A g_i = A$. Therefore $g_i v$ is also an eigenvector of A with eigenvalue λ.

We repeatedly perform the following: Choose a coordinate i such that $v \neq g_i v$ and $v + g_i v \neq 0$, and replace v with $v + g_i v$. This process ends in at most n turns, and when it ends, the vector v satisfies the property that for each coordinate i, either $v = g_i v$ or $v = -g_i v$.

Suppose there are m-coordinates i with $v = -g_i v$. Because $v \in \mathbb{1}^\perp$, $m \neq 0$. WLOG assume that for $i = 1, \ldots, m$, $v = -g_i v$. By multiplying by a nonzero constant, we can assume that

$$v_x = (-1)^{x_1 + \cdots + x_m}.$$

Then we can compute

$$\begin{aligned} v^t A v &= \sum_{x,y \in \{0,1\}^n} (-1)^{d(x,y)} A_{x,y} \\ &= 2^{2n-m} \sum_{0 \le d \le m} \binom{m}{d} (-1)^d (4\alpha(\alpha-1)(4+2^\alpha)^{n-d} 2^{\alpha d - 2\alpha n} + 2\alpha(2^d 2^{-2n})^{\alpha-1}) \\ &= 2^{1-m+4n-2\alpha n} \alpha((1-2^{\alpha-1})^m + (1+2^{\alpha-2})^{n-m}(2\alpha-2)). \end{aligned}$$

So it remains to study the function

$$g_\alpha(n, m) = (1-2^{\alpha-1})^m + (1+2^{\alpha-2})^{n-m}(2\alpha-2).$$

When $1 < \alpha < 2$, we have

$$\begin{aligned} g_\alpha(n,m) &\geq g_\alpha(m,m) = (1-2^{\alpha-1})^m + 2\alpha - 2 \\ &\geq 2\alpha - 2 - |1-2^{\alpha-1}| = 2\alpha - 1 - 2^{\alpha-1} =: h(\alpha). \end{aligned}$$

When $0 < \alpha < 1$, we have

$$\begin{aligned} g_\alpha(n,m) &\leq g_\alpha(m,m) = (1-2^{\alpha-1})^m + 2\alpha - 2 \\ &\leq 2\alpha - 2 + |1-2^{\alpha-1}| = 2\alpha - 1 - 2^{\alpha-1} = h(\alpha). \end{aligned}$$

It remains to show that $h(\alpha) < 0$ for $0 < \alpha < 1$ and $h(\alpha) > 0$ for $1 < \alpha < 2$. This follows from $h(1) = 0$ and

$$h'(\alpha) = 2 - 2^{\alpha-1} \log_e 2 > 0$$

on the interval $[0, 2]$. □

5.2 Addition in a Sidon set

In Section 5.1, the additive structure of $\{0,1\}^n$ can be thought of as a source of complexity of the problem. Therefore it is natural to consider addition over a set with minimal additive structure, such as Sidon sets (B_2-sets in Definition 2.1) in some ambient abelian group. Ganesh Ajjanagadde, in private communication, made the following conjecture.

Conjecture 5.8. If A is a Sidon set, then the $H(X+Y)$ achieves its maximum at uniform distribution.

We consider the same-distribution version with Rényi entropy, and prove the following results.

Proposition 5.9. *Let α_* be the unique root of the equation*

$$2^\alpha \alpha - 4\alpha + 2 = 0$$

in range $[1.1, 2]$ (with approximate value $\alpha_* \approx 1.29856$). For $0 \le \alpha \le \alpha_*$, if A is a Sidon set, then the Rényi entropy $H_\alpha(X + X)$ achieves its maximum at uniform distribution.

Proof. The case $\alpha = 0$ is obvious. We first prove the case $\alpha = 1$. For $x \in A$, we denote $P(X = x)$ as p_x. We have

$$-H(X + X) = \sum_x p_x^2 \log(p_x^2) + \sum_{x<y} 2p_x p_y \log(2p_x p_y)$$

where $<$ is an arbitrary total order on $\{0, 1\}^n$. Let $f(p) = -H(X + X)$. Our goal is to minimize $f(p)$. Let us compute the first derivative.

$$\begin{aligned}
\frac{\partial f(p)}{\partial p_x} &= 2p_x \log e + 2p_x \log(p_x^2) + \sum_{y \neq x} (2p_y \log e + 2p_y \log(2p_x p_y)) \\
&= 2 \log e - 2p_x + \sum_{y \in A} 2p_y \log(2p_x p_y) \\
&= 2 \log e - 2p_x + 2 + 2 \log p_x + 2 \sum_{y \in A} p_y \log(p_y) \\
&= 2 \log e - 2p_x + 2 + 2 \log p_x - 2H(X).
\end{aligned}$$

The function $-2p_x + 2 \log p_x$ is monotone increasing in $p_x \in [0, 1]$. Therefore if there exists $x, y \in A$ such that $p_x < p_y$, then we can make the transform $p_x \mapsto p_x + \epsilon$, $p_y \mapsto p_y - \epsilon$ for some small $\epsilon > 0$ so that $f(p)$ decreases. So a local minimum point of $f(p)$ must be the uniform distribution.

Now we consider the case $\alpha \neq 1$. Let

$$f(p) = \sum_x p_x^{2\alpha} + \sum_{x<y} (2p_x p_y)^\alpha.$$

Then $H_\alpha(p) = \frac{1}{1-\alpha} f(p)$. We would like to maximize $f(p)$ when $0 < \alpha < 1$ and

minimize $f(p)$ when $1 < \alpha < \alpha_*$. Let us compute the first derivative.

$$\begin{aligned}\frac{\partial f(p)}{\partial p_x} &= 2\alpha p_x^{2\alpha-1} + \sum_{y\neq x} \alpha 2^\alpha p_y^\alpha p_x^{\alpha-1} \\ &= \alpha p_x^{\alpha-1}(2p_x^\alpha + \sum_{y\neq x} 2^\alpha p_y^\alpha) \\ &= \alpha p_x^{\alpha-1}((2-2^\alpha)p_x^\alpha + \sum_{y\in A} 2^\alpha p_y^\alpha).\end{aligned}$$

Let $B = \sum_{y\in A} 2^\alpha p_y^\alpha$. Then clearly $B \geq 2^\alpha p_x^\alpha$. If we view B as a constant, then

$$\begin{aligned}&\frac{\partial}{\partial p_x}(\alpha p_x^{\alpha-1}((2-2^\alpha)p_x^\alpha + B)) \\ &= \alpha p_x^{\alpha-2}(B(\alpha-1) - (2^\alpha-2)(2\alpha-1)p_x^\alpha).\end{aligned}$$

Using $B \geq 2^\alpha p_x^\alpha$, we see that

$$\alpha p_x^{\alpha-1}((2-2^\alpha)p_x^\alpha + B)$$

is monotone increasing in p_x when $1 < \alpha < \alpha_*$, and is monotone decreasing in p_x when $0 < \alpha < 1$. Therefore if there are $p_x < p_y$, we can make transform $p_x \mapsto p_x + \epsilon$, $p_y \mapsto p_y - \epsilon$ for some small $\epsilon > 0$ so that $f(p)$ decreases (when $1 < \alpha < \alpha_*$) or increases (when $0 < \alpha < 1$). So a local maximum point of $H_\alpha(X+X)$ must be the uniform distribution. □

Proposition 5.10. *Let α^* be the unique root of the equation*

$$2^\alpha - 4\alpha + 2 = 0$$

in range $[3,4]$ (with approximate value $\alpha^* \approx 3.65986$). For $\alpha > \alpha^*$, for some Sidon set A, the Rényi entropy $H_\alpha(X+X)$ does not achieve its maximum at uniform distribution.

Proof. Let $A = \{0,1\}$ be a Sidon set with two elements. Let $p = \mathbb{P}(X=1)$. Then

$1-p=\mathbb{P}(X=0)$. Let

$$f(p)=p^{2\alpha}+(2p(1-p))^{\alpha}+(1-p)^{2\alpha}.$$

Then $H_\alpha(X+X)=\frac{1}{1-\alpha}\log f(p)$. For $\alpha>\alpha^*$, maximizing $H_\alpha(X+X)$ is equivalent to minimizing $f(p)$.

Simple calculation shows that $f'(\frac{1}{2})=0$ and

$$f''(\frac{1}{2})=-2^{3-2\alpha}(2^\alpha-4\alpha+2)\alpha.$$

When $\alpha>\alpha^*$, we have $f''(\frac{1}{2})<0$, and thus $p=\frac{1}{2}$ is not a local minimum of f. $\square$

Bibliography

[1] R. Ahlswede and V. B. Balakirsky. Construction of uniquely decodable codes for the two-user binary adder channel. *IEEE Transactions on Information Theory*, 45(1):326–330, 1999.

[2] G. Ajjanagadde and Y. Polyanskiy. Adder MAC and estimates for Rényi entropy. In *53rd Annual Allerton Conference on Communication, Control, and Computing*, pages 434–441. IEEE, 2015.

[3] P. Austrin, P. Kaski, M. Koivisto, and J. Nederlof. Sharper upper bounds for unbalanced uniquely decodeable code pairs. *IEEE Transactions on Information Theory*, 2017.

[4] R. C. Bose and S. Chowla. Theorems in the additive theory of numbers. *Commentarii Mathematici Helvetici*, 37(1):141–147, 1962.

[5] S. I. Bross and I. F. Blake. Upper bound for uniquely decodable codes in a binary input n-user adder channel. *IEEE Transactions on Information Theory*, 44(1):334–340, 1998.

[6] D. G. Cantor and W. H. Mills. Determination of a subset from certain combinatorial properties. *Canad. J. Math*, 18:42–48, 1966.

[7] P. A. B. M. Coebergh van den Braak. Constructions and an existence result of uniquely decodable codepairs for the two-access binary adder channel. *EUT report. WSK, Dept. of Mathematics and Computing Science*, 1983.

[8] P. A. B. M. Coebergh van den Braak and H. C. A. van Tilborg. A family of good uniquely decodable code pairs for the two-access binary adder channel. *IEEE Transactions on Information Theory*, 31(1):3–9, 1985.

[9] G. Cohen, S. Litsyn, and G. Zémor. Binary B_2-sequences: a new upper bound. *Journal of Combinatorial Theory, Series A*, 94(1):152–155, 2001.

[10] A. G. D'yachkov and V. V. Rykov. On a coding model for a multiple-access adder channel. *Problemy Peredachi Informatsii*, 17(2):26–38, 1981.

[11] T. Kasami, S. Lin, V. Wei, and S. Yamamura. Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel. *IEEE Transactions on Information Theory*, 29(1):114–130, 1983.

[12] G. H. Khachatrian and S. S. Martirossian. Code construction for the t-user noiseless adder channel. *IEEE Transactions on Information Theory*, 44(5):1953–1957, 1998.

[13] L. Kiviluoto and P. R. J. Östergård. New uniquely decodable codes for the t-user binary adder channel with $3 \leq t \leq 5$. *IEEE transactions on information theory*, 53(3):1219–1220, 2007.

[14] B. Lindström. On a combinatorial problem in number theory. *Canad. Math. Bull*, 8(4):477–490, 1965.

[15] B. Lindström. Determination of two vectors from the sum. *Journal of Combinatorial Theory*, 6(4):402–407, 1969.

[16] B. Lindström. On b2-sequences of vectors. *Journal of number Theory*, 4(3):261–265, 1972.

[17] M. Mattas and P. R. J. Östergård. A new bound for the zero-error capacity region of the two-user binary adder channel. *IEEE transactions on information theory*, 51(9):3289–3291, 2005.

[18] O. Ordentlich and O. Shayevitz. An upper bound on the sizes of multiset-union-free families. *SIAM Journal on Discrete Mathematics*, 30(2):1032–1045, 2016.

[19] G. S. Poltyrev. Improved upper bound on the probability of decoding error for codes of complex structure. *Problemy Peredachi Informatsii*, 23(4):5–18, 1987.

[20] Y. Polyanskiy and Y. Wu. Lecture notes on information theory. 2017. `http://people.lids.mit.edu/yp/homepage/data/itlectures_v5.pdf`.

[21] R. Urbanke and Q. Li. The zero-error capacity region of the 2-user synchronous bac is strictly smaller than its shannon capacity region. In *Information Theory Workshop*, page 61. IEEE, 1998.

[22] M. Wiman. Improved constructions of unbalanced uniquely decodable code pairs, 2017.