Advances in Applied Mathematics 应用数学进展, 2022, 11(3), 956-965
Published Online March 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.113102

Hans汉斯

关于Polar码重量谱的一个验证

乔玉洁，杨卫华

太原理工大学，数学学院，山西 晋中

收稿日期：2022年2月9日；录用日期：2022年3月3日；发布日期：2022年3月10日

摘　要

Polar码的优势和局限性都在于其严格的结构。Polar码常用的信息位选择方式为根据串行抵消(SC)译码算法中的信道可靠度进行选择，但是这样的选择方法不适用所有的情况。在基于SC译码算法的基础上改进的列表(SCL)译码算法中，选择信息位需要考虑码重量谱和可靠度，得到的性能较好。目前，已经有很多通过改善码谱进而改善性能的方法了。为了去寻找一种通用的改善码谱的方法，我们需要刻画原码重量谱的分布规则，探索在不同情形下选择信息位的方法。在本文中，提出了一种新的行表示方法，在此基础上验证了码谱唯一的信息集的数量范围，引入容斥原理推出二元域下码重的通用公式。

关键词

Polar码，RM码，码重量谱，信息集，容斥原理

A Verification of Polar Code Weight Spectrum

Yujie Qiao, Weihua Yang

School of Mathematics, Taiyuan University of Technology, Jinzhong Shanxi

Received: Feb. 9th, 2022; accepted: Mar. 3rd, 2022; published: Mar. 10th, 2022

Abstract

The advantages and disadvantages of Polar codes lie in its strict structure. At present, the existing information set selection method is based on the reliability of Successive Cancellation (SC) decoding algorithm, which may not be suitable for other algorithms. Improved SCL (SC List) decoding based on SC decoding needs to consider reliability and code weight spectrum. Various methods to improve the spectrum have been proposed and achieved better performance. In order to find a good way to improve the spectrum, we characterize the distribution law of weight spectrum and

文章引用: 乔玉洁, 杨卫华. 关于 Polar 码重量谱的一个验证[J]. 应用数学进展, 2022, 11(3): 956-965.
DOI: 10.12677/aam.2022.113102

try to find suitable information set selection methods in different situations. In this paper, a new row representation method is proposed. On this basis, the number range of the information set of the unique code spectrum is verified, and the general formula of code weight in the binary field is derived by introducing the principle of tolerance and exclusion.

Keywords

Polar Codes, RM Codes, Code Weight Spectrum, Information Set, The Principle of Tolerance and Exclusion

1. 引言

E Arikan [1]在 2009 年发现并分析了信道联合和信道极化的现象，并据此提出了 Polar 码和其使用的 SC 译码算法。Polar 码在编码理论中作为容量可达的码字是一个很大的突破。在 5G 通信网络中，Polar 码在短码长度的应用范围上可以代替 LDPC 码。Tae 和 A. Vardy [2]针对 Polar 码的 SC 译码算法引入列表辅助验证，提出了 SCL 译码算法改善性能，并且该算法的性能在列表较大的时候可以达到最大似然(ML)译码性能。Li B [3]提出了一类新的混合码字“RM-Polar”码。这类码字通过混合 RM 码和 Polar 码构造而成，其最小汉明距离比 Polar 码的最小汉明距离大，因此性能要优于 Polar 码。为了提升 Polar 码的最小距离，建议使用 RM-Polar 码或者将 Polar 码与 CRC [4]和 PC [5]串联以显著提高性能。最近，E. Arikan [6]提出了一类新的 PAC Polar 码，通过在 RM 码之前进行卷积运算，可以提供比以前的纠错码更好的性能。Li B [7]简单证明了预变换 Polar 码的最小距离不会变小，并且提出了一种通过分类和总结级联码的特性来设计上三角预变换的构造方法。2016 年，[8]提出，Polar 码和 RM 码是很相近的，因为它们具有相同的代数结构，也就是说，他们可以组合单项式构成。特别的，这种构造提供了一种有效的方法去计算递减单项式码和 Polar 码的最小码字的数量。通过在 Polar 码编码器的中间的阶中加入交织器[9]，Chiu M C [10]提出了一类新的 Polar 码——交织 Polar 码(I-Polar 码)。假设交织器是均匀分布的，他们衍生出重量枚举函数(WEF)来计算从 I-Polar 码集中随机选择的码的误块率(BLER)的上限。在[11]中，他们修正了之前关于 Polar 码的信息位的选择方式，并且提出了基于可靠度和和行重选择的方法。通过阅读大量文献，我们发现了很多改善 Polar 码和 RM 码码谱的方法。这些方法没有改变信息位的选择，而且易于实现。

2. 预备知识

2.1. Polar 码

n 阶 Polar 码由生成矩阵 $G^{\otimes n}$ 构成，其中二元核矩阵定义为

$$G=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$$

n 表示 n 阶克罗内克积。该 Polar 码的码长为 $N=2^n$ 并且包含 K 个信息比特。

码字由 $x=G^{\otimes n}Bu$ 得到，其中 $u=\{u_1,u_2,\cdots,u_n\}^{\mathrm{T}}$， $s=\{s_1,s_2,\cdots,s_n\}^{\mathrm{T}}$ 分别表示输入的信息序列和输出的码字序列。B 表示比特逆序排列操作。由于 Polar 码的特殊结构，其可以使用 SC 译码器来进行编译码

操作，复杂度为$\mathrm{O}\left(N\log_2 N\right)$。随着码长$N$趋于无穷时，Polar码可以达到信道容量[1]。

u中的N个比特可以根据它们在信道中的可靠度分为两组，K个最可靠的比特被看作信息比特用来传递信息，剩余的$N-K$个比特作为冻结比特被设置为固定值，该固定值在编译码器两端均已知。我们用$\mathbb{K}$和$\overline{\mathbb{K}}$表示u的子集，分别包含对应信息比特和冻结比特的位置索引值。可靠度序列可以通过下列方法获得，比如，巴氏参数[1]，密度进化[12]，高斯近似[13]，遗传算法[14]，beta扩展[15]和深度学习[16]。

2.2. RM码

RM码(Reed Muller)，码长为$N=2^m$，包含$K=\sum_{i=1}^{r}C_m^r$个信息比特，最小距离为$d=2^{m-r}$。RM码的K个信息比特是根据矩阵$G^{\otimes m}$中行的重量由大到小选取的，并且将重量为2^{m-r}的行全部选入信息集。行重最大的对应的K个比特作为信息比特，剩余的作为冻结比特，固定值为“0”。我们用$\mathcal{R}\left(m,r\right)$表示RM码，汉明距离$d$，最小汉明距离$d_{\min}$。

2.3. 行的表示方法

假设一个Polar码的码长为$N=2^m,\left(m\geq 1\right)$，我们将会得到一个明确的矩阵。通过[1]的比特索引法，可以得出一个长度为$N=2^m$的向量a_1^N。我们将其第i个元素表示为$a_{b_1b_2\cdots b_m}$，其中$1\leq i\leq N$，$b_1b_2\cdots b_m$是整数$i-1$的二元表示。也就是说，$i=1+\sum_{j=1}^{m}b_j2^{m-j}$，可以看作是行的另一种表示。同样的，一个$N\times N$的矩阵$A$中的元素$A_{ij}$可以表示为$A_{b_1b_2\cdots b_m,b_1'b_2'\cdots b_m'}$，其中，$b_1b_2\cdots b_m,b_1'b_2'\cdots b_m'$分别是$i-1$和$j-1$的二元表示。然后，就可以得到$G^{\otimes m}$中的元素为$G^{\otimes m}_{b_1b_2\cdots b_m,b_1'b_2'\cdots b_m'}=\prod_{i=1}^{m}G_{b_ib_i'}=\prod_{i=1}^{m}\left(1\oplus b_i'\oplus b_ib_i'\right)$。

基于上述的分析，我们提出了一个新的行表示，关于行号i与行中“1”的位置索引值集合的双射如下：

$$f\left(i\right)=\begin{pmatrix}1&&&&\\1+2^{b_1}&&&&\\1+2^{b_2}&1+2^{b_1}+2^{b_2}&&&\\1+2^{b_3}&1+2^{b_1}+2^{b_3}&1+2^{b_2}+2^{b_3}&1+2^{b_1}+2^{b_2}+2^{b_3}&\\\vdots&\vdots&\vdots&\vdots&\end{pmatrix}$$

等号左侧的i为行号，等号右侧的集合是矩阵$G^{\otimes m}$第i行中“1”的位置索引值。例如，矩阵中的最后一行(全“1”行)的行号为$i=1+\sum_{j=1}^{m}b_j2^{m-j}$，则$f\left(i\right)$包含所有的列索引值。在剩余的行中，重量为$w=2^{m-1}$的行的二元表示与全“1”行相比缺失了一项，也就是说，对应的$f\left(i\right)$中的元素不包含缺失的项。我们将每一个$f\left(i\right)$都看作一个事件。

为了方便理解，让我们通过以下例子来解释。

例：$m=4$，

行号16，$i=1+2^0+2^1+2^2+2^3, w=2^m=16$

$$f\left(i\right)=\begin{pmatrix}1&&&&\\1+2^0&&&&\\1+2^1&1+2^0+2^1&&&\\1+2^2&1+2^0+2^2&1+2^1+2^2&1+2^0+2^1+2^2&\\1+2^3&1+2^0+2^3&1+2^1+2^3&1+2^0+2^1+2^3&\\1+2^2+2^3&1+2^0+2^2+2^3&1+2^1+2^2+2^3&1+2^0+2^1+2^2+2^3&\end{pmatrix}$$

行号 15，$i=1+2^1+2^2+2^3, w=2^{m-1}=8$

$$f(i)=\begin{pmatrix} 1 & & & \\ \sim & & & \\ 1+2^1 & \sim & & \\ 1+2^2 & \sim & 1+2^1+2^2 & \sim \\ 1+2^3 & \sim & 1+2^1+2^3 & \sim \\ 1+2^2+2^3 & \sim & 1+2^1+2^2+2^3 & \sim \end{pmatrix}$$

行号 14，$i=1+2^0+2^2+2^3, w=2^{m-1}=8$

$$f(i)=\begin{pmatrix} 1 & & & \\ 1+2^0 & & & \\ \sim & \sim & & \\ 1+2^2 & 1+2^0+2^2 & \sim & \sim \\ 1+2^3 & 1+2^0+2^3 & \sim & \sim \\ 1+2^2+2^3 & 1+2^0+2^2+2^3 & \sim & \sim \end{pmatrix}$$

…

我们可以按行重将矩阵中所有的行分为以下几组，每组中的元素都是行重固定的长度为 m 的行的二元表示。C_m^i 表示每一组元素的数量，w 表示对应的行重。

$$\begin{array}{cccccc} C_m^m, w=2^m & C_m^{m-1}, w=2^{m-1} & C_m^{m-2}, w=2^{m-2} & & C_m^1, w=2^1 & C_m^0, w=2^0 \\ & (0,1,1,\cdots,1,1,1) & (0,0,1,\cdots,1,1,1) & & (1,0,0,\cdots,0,0,0) & \\ (1,1,1,\cdots,1,1,1) & (1,0,1,\cdots,1,1,1) & (0,1,0,\cdots,1,1,1) & & (0,1,0,\cdots,0,0,0) & (0,0,0,\cdots,0,0,0) \\ & (1,1,0,\cdots,1,1,1) & (1,0,0,\cdots,1,1,1) & \cdots & (0,0,1,\cdots,0,0,0) & \\ & \vdots & \vdots & & \vdots & \\ & (1,1,1,\cdots,1,1,0) & (1,1,1,\cdots,1,0,0) & & (0,0,0,\cdots,0,0,1) & \end{array}$$

3. 码谱分析

由假设 Polar 码码长为 2^m，包含 K 个信息比特，是根据行重从大到小选取的。在 K 确定之后，如果满足 $K=\sum_{i=0}^{s} C_m^i, s\in(1,2,\cdots,m)$，码谱与 RM 码相同且信息位的选择是唯一的。如果不满足 $K=\sum_{i=0}^{s} C_m^i, s\in(1,2,\cdots,m)$，信息位的选择不唯一。那么不同的信息集产生的码谱有什么规律吗？

基于仿真结果，我们可以得到以下定理。

定理 3.1：码长为 2^m 的 Polar 码若选用 RM 码选择信息位的方式，则当 K 的范围满足 $K\in\{0,1,\cdots,C_m^0+C_m^1+1\}\cup\left\{\sum_{i=0}^{i=m-2} C_m^i-1,\cdots,\sum_{i=0}^{i=m} C_m^i\right\}\cup\left\{\sum_{i=0}^{j} C_m^i\pm 1 \middle| j=1,2,\cdots,m\right\}$ 时，可以得到唯一的重量谱。

证明：假设我们按照 RM 码的方法选择信息位，也就是说，根据行重从大到小(分组中从左到右)。如果 K 满足 $K=\sum_{i=0}^{s} C_m^i, s\in(1,2,\cdots,m)$，码谱和信息位的选择都是唯一的，与 RM 码相同。在其他情况下，K 个信息位的选择方式是不唯一的。因为会出现在相同重量的组中只选取一部分行作为信息位。我们可以定义从这个组取出的元素数量为 K_1，这些元素进行线性组合时的系数为“1”的数量为 s，码字的重量为 w_s，重量为 w_s 的码字数量为 N_s。首先，我们刻画同组内的线性组合的情况。

1) 当 $w=2^{m-1}, 0\le K_1\le C_m^{m-1}$ 时，

$$s=1, w_1=2^{m-1}, N_1=C_{K_1}^1$$

$$s=2, w_2=w_1+2^{m-1}-2*\left(\frac{w_1}{2}\right)=2^{m-1}, N_2=C_{K_1}^2$$

$$s=3, w_3=w_2+2^{m-1}-2*\left(\frac{w_2}{2}\right)=2^{m-1}, N_3=C_{K_1}^3$$

$$\vdots$$

$$s=K_1, w_{K_1}=w_{K_1-1}+2^{m-1}-2*\left(\frac{w_{K_1-1}}{2}\right)=2^{m-1}, N_{K_1}=C_{K_1}^{K_1}$$

2) 当 $w=2^{m-2}, 0\le K_1\le C_m^{m-2}$ 时，

$$s=1, w_1=2^{m-2}, N_1=C_{K_1}^1$$

$$s=2, w_2=\begin{cases}2*2^{m-2}-2*2^{m-4} & \text{缺失的项完全不同}\\ 2*2^{m-2}-2*2^{m-3} & \text{缺失的项有两项相同}\end{cases}$$

$$s=3, w_3=\begin{cases}7*2^{m-4} & \text{缺失的项完全不同}\\ 3*2^{m-3} & \text{缺失的项有两项相同}\\ 2^{m-1} & \text{缺失的项有三项相同}\\ 3*2^{m-3} & \text{缺失的项有四项相同}\end{cases}$$

$$\vdots$$

m) 当 $w=2^{m-(m-1)}=2, 0\le K_1\le C_m^1$ 时，

$$s=1, w_1=2^1, N_1=C_{K_1}^1$$

$$s=2, w_2=w_1+2^1-2*\left(\frac{w_1}{2}\right)=2, N_2=C_{K_1}^2$$

$$s=3, w_3=w_2+2^1=4, N_3=C_{K_1}^3$$

$$\vdots$$

$$s=2i-1, w_{2i-1}=2i, N_{2i-1}=C_{K_1}^{2i-1}$$

$$s=2i, w_{2i}=2i, N_{2i}=C_{K_1}^{2i}$$

$$s=2i+1, w_{2i+1}=2i+2, N_{2i}=C_{K_1}^{2i+1}$$

$$\vdots$$

$$s=K_1, w_{K_1}=\begin{cases}K_1 & s\text{是偶数}\\ K_1+1 & s\text{是奇数}\end{cases}$$

接下来，我们刻画不同组之间的线性组合的情况。我们首先解释说明 $K\in\left\{0,1,\cdots,C_m^0+C_m^1+1\right\}$ 的情况。因为选择方法的要求，全“1”行一定会被选入信息集的 K 行中。

情况 1：对于 $K=C_m^0$ 和 $K=C_m^0+C_m^1$，信息集的选择方式唯一，码重量谱自然唯一。

情况 2：对于 $C_m^0+1\le K\le C_m^0+C_m^1$，$w=2^{m-1}$ 组中有 C_m^1 行，其中的 $K-1$ 行被选择。与全“1”行相比较，被选择的行的二元表示均缺少一项。我们可以得知被选择的 K 行的线性组合满足：

$$w=\begin{cases}2^{m-1} & \text{如果全“1”行的系数为“1”}\\ 2^{m-1} & \text{如果全“1”行的系数为“1”}\end{cases}$$

在这个情形下，所得到的码字重量是相同的。在上述两种情况下，该重量所对应的数量是相同的，均为 C_m^{K-1}。如果 K 值确定，码谱唯一。

情况 3：对于 $K=C_m^0+C_m^1+1$，在 $K=C_m^0+C_m^1$ 的基础上，要从重量为 $w=2^{m-2}$ 的组中取出一行，有 $C_{C_m^2}^1$ 种取法。与全“1”行相比，被选择的行的二元表示缺失两项，这样的行有 C_m^2 个。我们可以这样考虑：首先我们固定之前的线性组合，将其看作一个码字，然后将这样的码字按照是否与新选择的行具有相同的缺失项分类。

$$w=\begin{cases}2^{m-1} & \text{如果固定的码字缺失一项，且缺失项与选择的行的缺失项完全不同}\\ 2^{m-2} & \text{如果固定的码字缺失一项，且缺失项与选择的行的缺失项有一项相同}\\ 5*2^{m-3} & \text{如果固定的码字缺失两项，且缺失项与选择的行的缺失项完全不同}\\ 2^{m-1} & \text{如果固定的码字缺失两项，且缺失项与选择的行的缺失项有一项相同}\\ 3*2^{m-2} & \text{如果固定的码字缺失两项，且缺失项与选择的行的缺失项完全相同}\\ & \vdots\end{cases}$$

很明显，因为组合排列的随机性，会出现新的重量的码字。通过行的二元表示的规则，我们可以知道从 $w=2^{m-2}$ 组中选择的每一行都会出现上述的情况。所以在这样的情况下，同样会出现这样重量的码字。最终，将会获得一个唯一的码谱。

情况 4：对于 $K=C_m^0+C_m^1+2$，也就是，在情况 3 的基础上再从 $w=2^{m-2}$ 中再选取一行。此时，我们从(2)中得知，从 $w=2^{m-2}$ 中选取的两行会根据彼此之间的关系将会形成不同的重量和码谱。同理，如果从该组中抽取更多的行，将会出现更多的组合和不同的码谱。

情况 5：对于 $K=\sum_{i=0}^{i=m-2}C_m^i-1$，我们可以在 $\sum_{i=0}^{i=m-2}C_m^i$ 得到唯一码谱的基础上考虑。因为二元域的计算特性(假设 A,B 都是二元码字，则 $A-B=A+B$)，该情况等同于在 $K=\sum_{i=0}^{i=m-2}C_m^i$ 的情况下从 $w=2^2$ 组中选择一行相加，即等效于情况 3，最终得到一个唯一的码谱。

情况 6：同理可得，$K=\left\{\sum_{i=0}^{j}C_m^i\pm1\middle|j=1,2,\cdots,m\right\}$ 和 $\sum_{i=0}^{i=m-2}C_m^i-1\le K\le\sum_{i=0}^{i=m}C_m^i$ 的情况可以按照排列组合和重量分布的对称性解释。

定理成立。

上述方法只能列出一些简单情况，我们可以应用组合数学中的容斥原理及其推论来刻画一般情况，见图 1。

定理 3.2：(容斥原理) 假设 S 是一个有限集，$A_i\subseteq S\left(i=1,2,\cdots,n,n\ge2\right)$，则

$$\begin{aligned}\left|\bigcup_{i=1}^{n}A_i\right|&=\sum_{1\le i_1\le n}\left|A_{i_1}\right|-\sum_{1\le i_1<i_2\le n}\left|A_{i_1}\cap A_{i_2}\right|+\cdots\\&\quad+\left(-1\right)^{k-1}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|+\cdots+\left(-1\right)^{n-1}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_n}\right|\\&=\sum_{k=1}^{n}\left(-1\right)^{k-1}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|\end{aligned}$$

推论 3.3：假设 S 是一个有限集，$A_i\subseteq S\left(i=1,2,\cdots,n,n\ge2\right)$，则

$$\left|S-\bigcup_{i=1}^{n}A_i\right|=\left|S\right|+\sum_{k=1}^{n}\left(-1\right)^{k}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|$$

定理 3.4：假设 S 是一个有限集，$a_1,a_2,\cdots,a_n$ 是 n 条性质。对于任意 $k\left(1\le k\le n\right)$ 个正整数，$i_1,i_2,\cdots,i_k,\left(1\le i_1<i_2<\cdots<i_k\le n\right)$，以 $N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$ 表示 S 中同时具有性质 $a_{i_1},a_{i_2},\cdots,a_{i_k}$ 的元素个数，以 $N\left(a'_{i_1}a'_{i_2},\cdots,a'_{i_n}\right)$ 表示 S 中不具有 $a_{i_1},a_{i_2},\cdots,a_{i_n}$ 中任一个性质的元素个数，则

$$N\left(a'_{i_1},a'_{i_2},\cdots,a'_{i_k}\right)=\left|S\right|+\sum_{k=1}^{n}\left(-1\right)^k\sum_{1\le i_1<i_2<\cdots<i_k\le n}N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$$

我们将上述定理应用到二元域 F_2 上，得到一个新的定理。在 F_2 上，偶数次重复的部分被消除，奇数次重复的部分被保留一份。我们将每一个事件 $f\left(i\right)$ 记为 A_i。

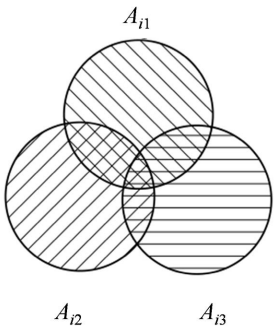

Figure 1. The graph of Inclusion and exclusion principle
图 1. 容斥原理例图

定理 3.5：假设 S 是二元域上的一个有限集，$A_i\subseteq S\left(i=1,2,\cdots,n,n\ge 2\right)$，则

$$\begin{aligned}\left|\bigcup_{i=1}^{n}A_i\right|&=\sum_{1\le i_1\le n}\left|A_{i_1}\right|-2\sum_{1\le i_1<i_2\le n}\left|A_{i_1}\cap A_{i_2}\right|+4\sum_{1\le i_1<i_2<i_3\le n}\left|A_{i_1}\cap A_{i_2}\cap A_{i_3}\right|\\&\quad-8\sum_{1\le i_1<i_2<i_3<i_4\le n}\left|A_{i_1}\cap A_{i_2}\cap A_{i_3}\cap A_{i_4}\right|+\cdots\\&\quad+\left(-1\right)^{k-1}2^{k-1}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|+\cdots\\&\quad+\left(-1\right)^{n-1}2^{n-1}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_n}\right|\\&=\sum_{k=1}^{n}\left(-2\right)^{k-1}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|\end{aligned}$$

证明：当 $n=2$ 时，

$$\left|\bigcup_{i=1}^{2}A_i\right|=\left|A_1\right|+\left|A_2\right|-2\left|A_1\cap A_2\right|$$

当 $n=3$ 时，

$$\begin{aligned}\left|\bigcup_{i=1}^{3}A_i\right|&=\left|\left(\bigcup_{i=1}^{2}A_i\right)\cup A_3\right|=\left|\bigcup_{i=1}^{2}A_i\right|+\left|A_3\right|-2\left|\left(\bigcup_{i=1}^{2}A_i\right)\cap A_3\right|\\&=\left|A_1\right|+\left|A_2\right|-2\left|A_1\cap A_2\right|+\left|A_3\right|-2\left|\left(\left|A_1\right|+\left|A_2\right|-2\left|A_1\cap A_2\right|\right)\cap A_3\right|\\&=\left|A_1\right|+\left|A_2\right|+\left|A_3\right|-2\left|A_1\cap A_2\right|-2\left|A_1\cap A_3\right|-2\left|A_2\cap A_3\right|+4\left|A_1\cap A_2\cap A_3\right|\\&=\sum_{1\le i_1\le n}\left|A_{i_1}\right|-2\sum_{1\le i_1<i_2\le n}\left|A_{i_1}\cap A_{i_2}\right|+4\sum_{1\le i_1<i_2<i_3\le n}\left|A_{i_1}\cap A_{i_2}\cap A_{i_3}\right|\end{aligned}$$

假设当$n=s(s\geq 3)$时，该结论成立。

那么当$n=s+1$时，

$$\begin{aligned}\left|\bigcup_{i=1}^{s+1}A_i\right| &= \left|\left(\bigcup_{i=1}^{s}A_i\right)\cup A_{s+1}\right| = \left|\bigcup_{i=1}^{s}A_i\right| + \left|A_{s+1}\right| - 2\left|\left(\bigcup_{i=1}^{s}A_i\right)\cap A_{s+1}\right| \\ &= \sum_{1\leq i_1\leq s+1}\left|A_{i_1}\right| + \sum_{k=2}^{s}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq s}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right| \\ &\quad + \sum_{k=1}^{s-1}(-2)^{k}\sum_{1\leq i_1<i_2<\cdots<i_k\leq s}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\cap A_{s+1}\right| \\ &\quad + (-2)^{s}\left|A_1\cap A_2\cap\cdots\cap A_s\cap A_{s+1}\right| \\ &= \sum_{1\leq i_1\leq s+1}\left|A_{i_1}\right| + \left[\sum_{k=2}^{s}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq s}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|\right. \\ &\quad \left. + \sum_{k=2}^{s}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_{k-1}\leq s}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\cap A_{s+1}\right|\right] \\ &\quad + (-2)^{s}\left|A_1\cap A_2\cap\cdots\cap A_s\cap A_{s+1}\right| \\ &= \sum_{1\leq i_1\leq s+1}\left|A_{i_1}\right| + \sum_{k=2}^{s}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq s+1}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right| \\ &\quad + (-2)^{s}\left|A_1\cap A_2\cap\cdots\cap A_s\cap A_{s+1}\right| \\ &= \sum_{k=1}^{s+1}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq s+1}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right| \\ &= \sum_{k=1}^{n}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|\end{aligned}$$

综上所述，定理成立$(n\geq 2)$。

推论 3.6：假设S是二元域上的一个有限集，$a_1,a_2,\cdots,a_n$是n条性质。对于任意$k(1\leq k\leq n)$个正整数，$i_1,i_2,\cdots,i_k,(1\leq i_1<i_2<\cdots<i_k\leq n)$，以$N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$表示$S$中同时具有性质$a_{i_1},a_{i_2},\cdots,a_{i_k}$的元素个数，以$N\left(a'_{i_1},a'_{i_2},\cdots,a'_{i_n}\right)$表示$S$中不具有$a_{i_1},a_{i_2},\cdots,a_{i_n}$中任一个性质的元素个数，则

$$N\left(a'_{i_1},a'_{i_2},\cdots,a'_{i_k}\right)=|S|+\sum_{k=1}^{n}(-2)^{k}\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$$

证明：我们将$A_i\,(i=1,2,\cdots,n)$看作S中具有性质a_i的全部元素所成之集，则$S-\sum_{i=1}^{n}A_i$表示S中不具有$a_1,a_2,\cdots,a_n$中任一个性质的全部元素所成之集，所以

$$N\left(a'_{i_1},a'_{i_2},\cdots,a'_{i_k}\right)=\left|S-\sum_{i=1}^{n}A_i\right|=|S|+\sum_{k=1}^{n}(-2)^{k-1}\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}\left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}\right|$$

因为$A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}$表示$S$中同时具有性质$a_1,a_2,\cdots,a_n$的全部元素所成之集，所以$A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k}=N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$，从而

$$N\left(a'_{i_1},a'_{i_2},\cdots,a'_{i_k}\right)=|S|+\sum_{k=1}^{n}(-2)^{k}\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}N\left(a_{i_1},a_{i_2},\cdots,a_{i_k}\right)$$

综上所述，定理成立。

这里，我们认为更好的码谱是具有更少的最小距离码字数量。那么当信息集选择不唯一的时候，什么样的信息集选择方式可以有更好的码谱呢？

通过上述定理 3.5 和 3.6，我们可以得到可能出现的码字重量及其补集。如果我们想要得到更好的码谱，我们需要选择在相同事件的条件下具有最小重量码字的数量较少的情况。也就是说，我们需要将定理 3.5 的结果进行量化，选择最小重量最少的情况所对应的选择方式。

通过图 1，如果想要码字的最小距离最大，即使得重复奇数次的部分尽可能大，重复偶数次的部分尽可能小。让我们定义一个函数为 $F=\sum_{t=1}^{t=s} f\left(i_t\right)$ 作为线性组合的结果。在 F_2 中，出现偶数次的项被消除，出现奇数次的项被保留一次。虽然不甚准确，但是可以用它来衡量得到的码字重量。因此 F 中的项越多，说明这样组合后得到的码字重量越大，即所选择的行的二元表示尽可能不同。虽然没有给出具体的结果，但逻辑具有一定的意义，因此该衡量函数将在后续工作中进行实验。

4. 总结与展望

在本文中，我们已经刻画了原 Polar 码的重量谱分布规则，给出了一些结构化改善的想法。目前大部分的码谱优化方法也可以从这个角度进行分析。已经证明 PAC-Polar 码的结构和在阶之间添加交织器可以改善码谱。我们可以利用 F 函数的计算结果来分析优化后的结果，甚至可以根据一些已知的结果来预测哪个交织器可以获得更好的码谱。我们也可以根据定理 3.5 设计阶之间的交织器。通过定理 3.5 得到某些码字的具体形式，然后通过交织器将其他码字的“1”置于已知码字的“0”位置，得到一个更大权重的码字。我们可以使用一个符合条件的线性组合以获得更好的码谱的方法，想一想，有没有可能基于这个想法来设计动态交织器？

例如 Polar 码的生成矩阵可以表示为：

$$G=\begin{bmatrix} G_1 & \\ G_2 & G_2 \end{bmatrix}$$

其中 $G_1=G_2$。

因为信息集的不同选择方式，我们定义 G 构成的码字 c_0 重量为 d，G_1 构成的码字 c_1 重量为 d_1，G_2 构成的码字 c_2 重量为 d_2，c_1 和 c_2 中共同为“1”的位置的数量为 c。如果我们想要在 G_1 中设计一个交织器，我们需要将 c_1 中的“1”尽可能放置在 c_2 中“0”的位置上，c_1 中多余的“1”可以随机放置在 c_2 中“0”的位置上。然后原始重量为 d_1+2d_2-2c 的码字，现在重量为 $d_1+2d_2-2\left(d_1+d_2-2^{m-1}\right)=2^m-d_1$，即这是可能达到的最大重量。

参考文献

[1] Arikan, E. (2009) Channel Polarization: A Method for Constructing Capacity Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory*, **55**, 3051-3073. https://doi.org/10.1109/TIT.2009.2021379

[2] Tae, I. and Vardy, A. (2012) List Decoding of Polar Codes. arXiv: 1206.0050v1.

[3] Li, B., Shen, H. and Tse, D. (2014) A RM-Polar Codes. Mathematics. arXiv:1407.5483v1.

[4] Niu, K. and Cien, K. (2012) CRC-Aided Decoding of Polar Codes. *IEEE Communications Letters*, **16**, 1668-1671. https://doi.org/10.1109/LCOMM.2012.090312.121501

[5] Zhang, H.Z., Li, R., Wang, J., Dai, S., Zhang, G., Chen, Y., *et al*. (2018) Parity-Check Polar Coding for 5G and Beyond. 2018 *IEEE International Conference on Communications*, Kansas City, 20-24 May 2018, 1-7. https://doi.org/10.1109/ICC.2018.8422462

[6] Arikan, E. (1908) From Sequential Decoding to Channel Polarization and Back again. arXiv: 1908.09594v1.

[7] Li, B., Zhang, H. and Gu, J. (2019) On Pre-Transformed Polar Codes. arXiv:1912.06359v1.

[8] Bardet, M., Dragoi, V., Otmani, A. and Tillich, J.-P. (2016) Algebraic Properties of Polar Codes from a New Polynomial Formalism. *Proc. of the IEEE Int. Symposium on Inform. Theory* (*ISIT*), Barcelona, 10-15 July 2016, 230-234. https://doi.org/10.1109/ISIT.2016.7541295

[9] Bioglio, V. and Land, I. (2018) Polar Codes with Internal Edge Permutations. 2018 *IEEE Wireless Communications and Networking Conference Workshops* (*WCNCW*), Barcelona, 15-18 April 2018, 61-66. https://doi.org/10.1109/WCNCW.2018.8369014

[10] Chiu, M.C. (2019) Interleaved Polar (I-Polar) Codes. *IEEE Transactions on Information Theory*, **66**, 2430-2442. https://doi.org/10.1109/TIT.2020.2969155

[11] Chiu, M.C. and Chen, C.Y. (2020) Design of I-Polar Codes. *IEEE Communications Letters*, **24**, 1865-1869. https://doi.org/10.1109/LCOMM.2020.2995697

[12] Tal, I. and Vardy, A. (2013) How to Construct Polar Codes. *IEEE Transactions on Information Theory*, **59**, 6562-6582. https://doi.org/10.1109/TIT.2013.2272694

[13] Trifonov, P. (2012) Efficient Design and Decoding of Polar Codes. *IEEE Transactions on Communications*, **60**, 3221-3227. https://doi.org/10.1109/TCOMM.2012.081512.110872

[14] Elkelesh, A., Ebada, M., Cammerer, S. and Ten Brink, S. (2019) Decoder Tailored Polar Code Design Using the Genetic Algorithm. *IEEE Transactions on Communications*, **67**, 4521-4534. https://doi.org/10.1109/TCOMM.2019.2908870

[15] He, G., Belfiore, J. C., Land, I., Yang, G., Liu, X., Chen, Y., Li, R., Wang, J., Ge, Y., Zhang, R. and Tong, W. (2017) Beta-Expansion: A Theoretical Framework for Fast and Recursive Construction of Polar Codes. *GLOBECOM* 2017: 2017 *IEEE Global Communications Conference*, Singapore, 4-8 December 2017, 1-6. https://doi.org/10.1109/GLOCOM.2017.8254146

[16] Ebada, M., Cammerer, S., Elkelesh, A. and Ten Brink, S. (2019) Deep Learning Based Polar Code Design. 2019 57*th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, 24-27 September 2019, 177-183. https://doi.org/10.1109/ALLERTON.2019.8919804