作为内循环码与外极化类和 Reed-Muller 类码级联的极化调整卷积（PAC）码

MohsenMoradi，*IEEE* 会员

arXiv:2304.01463v2 [cs.IT] 2 Aug 2023

摘要

极化调整卷积（PAC）码是一类新的线性分组码，在短码长区间内，其性能接近理论界限。这类码结合了极化编码和卷积编码。本研究表明，PAC码等价于一类新码，由内循环码和外极化类及 Reed-Muller 类码构成。我们利用循环码的性质，证明 PAC码在最小距离方面优于极化类和 Reed-Muller 类码。

索引词

PAC码、循环码、极化编码、信道编码、最小距离。

一、引言

最近提出的极化调整卷积（PAC）码是一类线性码，在短分组长度下可逼近理论极限 [2]。本文建立了 PAC 码与循环码之间的关系，并证明 PAC 码可视为由内循环移位码和外极化码串接而成。我们还研究了 PAC 码的重量分布。利用循环移位矩阵，我们为 [3], 的一项结果给出了新的证明。该结果指出，PAC 码的最小距离 $d_{\min}$ 大于或等于类极化码和 Reed-Muller（RM）码的最小距离 $d_{\min}$ 。

本文基于 [1, 第 6]章。作者任职于土耳其安卡拉 TR-06800 比尔肯特大学电气与电子工程系（电子邮箱：moradi@ee.bilkent.edu.tr）。

我们在研究中使用循环码，受到 [4], 的工作的启发。该工作针对实际应用，基于 $N/4$ 次循环移位设计并分析了极化码的一个特定置换集合，其中 N 是码块 [5] 的长度。在本研究中，我们将这一代数结果推广到 m 次循环移位（适用于 $1 \leq m \leq N$），给出显式证明，并展示这些发现如何应用于 PAC 码。在 [3], 中，他们还证明，将$\mathbf{g}_i$（i阶行 $F^{\otimes n}$，其中 $1 \leq i < N$，而 $F^{\otimes n}$ 是 $F = [\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}]$的 n 次克罗内克幂，且 $n =$ 为 $\log_2 N$）与其下方的一些行相加（我们将其表示为$\mathbf{g}_i$），所得结果的重量大于或等于$\mathbf{g}_i$ 的重量。我们将这一结果加以推广，并证明$\mathbf{g}_i$ 的奇数个顺时针循环移位之和，其重量也大于或等于 $\mathbf{g}_i$ 的重量。此外，我们证明，矩阵 $F^{\otimes n}$ 的一行与其下方一行相加，等于该行的若干顺时针循环移位之和，并据此证明，PAC 码的 $d_{\min}$ 大于或等于类极化码和类 RM 码的 $d_{\min}$。线性码的重量分布决定最大似然（ML）译码的性能，在高信噪比（SNR）下尤其可以用并集界进行准确估计。这意味着，在纠错性能方面，PAC 码优于类极化码和类 RM 码。以下简要概述本研究的主要贡献。

- 我们提出了一类新的编码方案，它与 PAC码等价，由循环码作为内码、极化码和类 RM 码作为外码构成。
- 我们证明，对于极化码和类 Reed-Muller 码的生成矩阵中的任意一行，将其与其下方若干行相加后，再进行奇数次顺时针循环移位，不会降低该行的重量。
- 利用循环码显著的内在代数结构，我们证明，就最小距离而言，PAC码优于极化码和类 RM 码。
- 我们证明，极化码和类 RM 码生成矩阵中的任意一行与其下方任意一行相加，结果等于该行经过若干次顺时针循环移位所得的结果。

本文中，向量以粗体表示，运算在二元域 $\mathbb{F}_2$上进行。对于向量 $\mathbf{c} = (c_1, c_2, \cdots, c_N)$，使用记号 $\mathbf{c}^i$ 表示 $(c_1, \cdots, c_i)$，使用记号 $\mathbf{c}_i^j$ 表示 $(c_i, \cdots, c_j)$。对于向量 $\mathbf{c}$，$(\mathbf{c})_i$ 表示其第 i 个元素c_i。向量 $\mathbf{c} = (c_1, c_2, \cdots, c_N)$ 的多项式表示记为 $\mathbf{c}(x) = c_1 + c_2 x + \cdots + c_N x^{N-1}$。

本文其余部分安排如下。第二节简要回顾 PAC码。

第三节证明，PAC码可视为由内循环移位码和外极化码和RM类码串接而成。最后，第四节总结全文。

II. PAC 编码

图 1 展示了 PAC 编码方案的框图。PAC码由参数 (N， K， $\mathcal{A}$， T) 指定，其中 N($N = 2^n$ 和 $n \in \mathbb{N}$) 是码字的分组长度，K 是数据字的长度， $\mathcal{A}$ 称为数据索引集， T 是上三角托普利兹矩阵。数据索引集 $\mathcal{A}$ 定义了 PAC码的码率配置（数据插入）模块，该模块将长度为 K 的数据字 $\mathbf{d}$ 映射为长度为 N 的数据承载向量 $\mathbf{v}$ ，满足$\mathbf{v}_{\mathcal{A}} =\mathbf{d}$且$\mathbf{v}_{\mathcal{A}^c} = \mathbf{0}$。该向量作为由矩阵 T定义的卷积编码器的输入，其中

$$T = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_m & 0 & \cdots & 0 \\ 0 & c_0 & c_1 & c_2 & \cdots & c_m & & \vdots \\ 0 & 0 & c_0 & c_1 & \ddots & \cdots & c_m & \vdots \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 & c_0 & c_1 & c_2 \\ \vdots & & & & 0 & 0 & c_0 & c_1 \\ \vdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & c_0 \end{bmatrix},$$

且可由连接多项式 $\mathbf{c}(x) = c_m x^m + \cdots + c_1 x + c_0$表示，满足 $c_0 = c_m = 1$。对于 PAC码，需要基于极化截止速率构造集合 $\mathcal{A}$ ，以实现低复杂度的树搜索算法 [6], [7]。卷积编码器的输出为$\mathbf{u} = \mathbf{v}T$。随后，对卷积编码器的输出应用单速率极化变换（极化映射器），得到$\mathbf{x} = \mathbf{u}F^{\otimes n}$ ，从而获得 PAC码字。请注意，我们为码率配置单独设置了一个模块，并且信息比特的选择可以基于极化码、RM码或任何其他任意码率配置（称为类极化码和类 RM 码）。

在接收端，树搜索算法借助度量计算器 [8]生成对$\mathbf{v}$ 的估计$\mathbf{v}$ 。最后，从$\mathbf{v}$中提取数据字的估计。

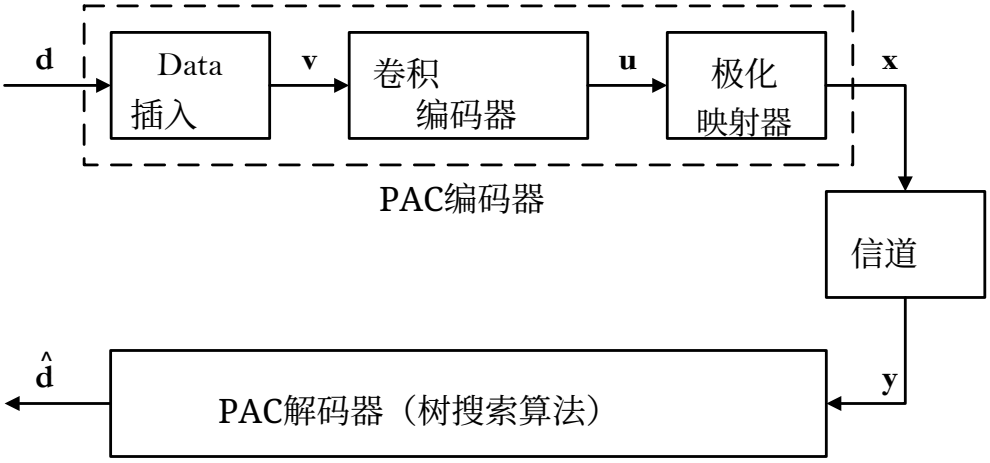

图 1. PAC编码方案。

例 1. 考虑一个 *PAC(8,3)*码，其码块长度 N 为 *8*，数据比特 K 的长度为 *3*。极化映射矩阵为

$$F^{\otimes 3}=\begin{bmatrix}1&0&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&1&1&1&0&0&0&0\\1&0&0&0&1&0&0&0\\1&1&0&0&1&1&0&0\\1&0&1&0&1&0&1&0\\1&1&1&1&1&1&1&1\end{bmatrix}.$$

令连接多项式为 $\mathbf{c}(x)=x^6+x^5+x^3+1$（八进制形式为 *151*）。因此，卷积编码器矩阵为

$$T=\begin{bmatrix}1&1&0&1&0&0&1&0\\0&1&1&0&1&0&0&1\\0&0&1&1&0&1&0&0\\0&0&0&1&1&0&1&0\\0&0&0&0&1&1&0&1\\0&0&0&0&0&1&1&0\\0&0&0&0&0&0&1&1\\0&0&0&0&0&0&0&1\end{bmatrix}.$$

假设数据索引集为 $\mathcal{A}=\{4,7,8\}$。数据插入模块将数据向量 $\mathbf{d}=(d_1,d_2,d_3)$ 插入向量 $\mathbf{v}=(v_1,v_2,\cdots,v_8)$ 中，使得 $\mathbf{v}=(0,0,0,d_1,0,0,d_2,d_3)$。卷积编码器模块根据向量 $\mathbf{v}$ 生成向量 $\mathbf{u}=\mathbf{v}T$。最后，计算极化变换$\mathbf{x}=\mathbf{u}F^{\otimes 3}$，完成编码过程。

III. PAC码 V. 极化码

设 $\mathbf{g}_i$为矩阵 $G_n \triangleq F^{\otimes n}$的第 i行，其中 $1 \leq i \leq N$。$\mathbf{g}_i$的权重为 $w(\mathbf{g}_i)=2^{\sum_{m=1}^{n} i_m}$，其中 $i_n i_{n-1}\cdots i_1=\sum_{m=1}^{n} i_m 2^{m-1}$是索引 $i-1$ [9]的比特索引表示。设 C_N^j为顺时针循环移位矩阵，在 j处移位。$\mathbf{g}_i C_N^j=(g_{i,1},g_{i,2},\cdots,g_{i,N})C_N^j=(g_{i,N-j+1},g_{i,N-j+2},\cdots g_{i,N},\cdots,g_{i,N-j})$。在多项式表示中，这等价于

$$x^j \mathbf{g_i}(x)=g_{i,N-j+1}+g_{i,N-j+2}x+\cdots g_{i,N}x^{j-1}+\cdots+g_{i,N-j}x^{N-1} \mod x^N-1, \quad (1)$$

其中 $\mathbf{g_i}(x)=g_{i,1}+g_{i,2}x+\cdots+g_{i,N}x^{N-1}$。

示例 2。 设 $N=8$、$j=3$ 和 $i=6$。

$$C_8^3=\begin{bmatrix}0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\end{bmatrix}, \quad G_3=\begin{bmatrix}1&0&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&1&1&1&0&0&0&0\\1&0&0&0&1&0&0&0\\1&1&0&0&1&1&0&0\\1&0&1&0&1&0&1&0\\1&1&1&1&1&1&1&1\end{bmatrix}.$$

对于 $\mathbf{g}_6=(1,1,0,0,1,1,0,0)$,

$$\mathbf{g}_6 C_8^3=(1,0,0,1,1,0,0,1).$$

对于任意非零二进制向量 $\mathbf{u}=(0,\cdots,0,1,u_{i+1},u_{i+2},u_N)$，其中第一个 1 位于其第 i 个位置，$\mathbf{u}G_n=\mathbf{g}_i\oplus u_{i+1}\mathbf{g}_{i+1}+\cdots\oplus u_N\mathbf{g}_N$。我们使用 $\mathbf{g}_i$ 记号表示向量$\mathbf{g}_i$ 与其下方指定的其他行之和。

在下面的命题中，我们证明，对矩阵 G_n 中任意一行添加奇数次顺时针循环移位，并在该行下方添加若干行（即，对于矩阵的第 i 行，$\mathbf{g}_i$ ）

不会降低该行的重量。在证明中，我们将生成矩阵 G_{n+1} 分为上部和下部，即 $G_{n+1} = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$，

使得 H_1 和 H_2 的行分别可以表示为 $(\mathbf{h}_i, \mathbf{0})$ 和 $(\mathbf{h}_k, \mathbf{h}_k)$，其中 $\mathbf{h}_i$ 和 $\mathbf{h}_k$ 都是矩阵 G_n 的行。

命题 1。 对于任意向量 $(u_{i+1}, u_{i+2}, \cdots, u_N) \in \{0,1\}^{N-i}$ 以及任意奇数 l =1、3、5、$\cdots$，

$$w\left(\underline{\mathbf{g}}_i \sum C_N^l\right) \geq w(\mathbf{g}_i), \tag{2}$$

其中 $1 \leq i \leq N$、$\underline{\mathbf{g}}_i = \mathbf{g}_i \oplus u_{i+1}\mathbf{g}_{i+1} + \cdots \oplus u_N\mathbf{g}_N$，并且在模 N 的意义下，存在奇数个互不相同的循环移位。

证明。 利用关于 n 的归纳法进行证明。对于 $n = 1$，该陈述显然成立。根据归纳法，假设该陈述对于 n成立。我们希望证明，对于 G_{n+1} 的任意行 $\mathbf{g}_i$ ，

$$w\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right) \geq w(\mathbf{g}_i), \tag{3}$$

其中 $1 \leq i \leq 2N$。根据行索引 i 是否大于 N，我们将证明分为两种情况。

情况 1： $i > N$。

在这种情况下，我们可以将向量 $\mathbf{g}_i$ 写成（$\underline{\mathbf{h}}^{i-N}, _\mathbf{h}^{i-N}$），其中 $\mathbf{h}_{i-N}$是矩阵 G_n的第（$i-N$）行。因此，

$$\begin{aligned} w\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right) &= w\left((\underline{\mathbf{h}}_{i-N}, \underline{\mathbf{h}}_{i-N}) \sum C_{2N}^l\right) \\ &= w\left(\underline{\mathbf{h}}_{i-N} \sum C_N^l, \underline{\mathbf{h}}_{i-N} \sum C_N^l\right) \\ &= 2w\left(\underline{\mathbf{h}}_{i-N} \sum C_N^l\right) \geq 2w(\mathbf{h}_{i-N}) \\ &= w(\mathbf{h}_{i-N}, \mathbf{h}_{i-N}) = w(\mathbf{g}_i), \end{aligned} \tag{4}$$

其中，不等式由归纳法得到。注意，在第三个等式中，经过偶数次移位后（l 和 $l+N$）有可能相等，此时不等式仍然成立。

情形 2： $i \leq N$。

在这种情况下，矩阵 G_{n+1} 的第 i 行可写为 $\mathbf{g}_i = (\mathbf{h}, \mathbf{0})$，满足 $\mathbf{h}$ 是矩阵 G_n的第 i 行。我们有

$$\underline{\mathbf{g}}_i = (\underline{\mathbf{h}}, \mathbf{0}) \oplus (\underline{\mathbf{y}}, \underline{\mathbf{y}}), \tag{5}$$

其中（ $\mathbf{y}$，$\mathbf{y}$) 是零向量，或者是矩阵 G_{n+1} 的第 j 行，满足 $j > N$。我们有

$$\begin{aligned}\underline{\mathbf{g}}_i \sum C_{2N}^l &= (\underline{\mathbf{h}}, \mathbf{0}) \sum C_{2N}^l \oplus (\underline{\mathbf{y}}, \underline{\mathbf{y}}) \sum C_{2N}^l \\ &= (\underline{\mathbf{h}}, \mathbf{0}) \sum C_{2N}^l \oplus \left(\underline{\mathbf{y}} \sum C_N^l, \underline{\mathbf{y}} \sum C_N^l\right).\end{aligned} \tag{6}$$

假设 $\gamma \triangleq \left(\underline{\mathbf{y}} \sum C_N^l\right)_k$。另外，注意第 k 位

$$\left(\underline{\mathbf{h}} \sum C_N^l\right)_k = \underbrace{\left((\underline{\mathbf{h}}, \mathbf{0}) \sum C_{2N}^l\right)_k}_{\alpha} \oplus \underbrace{\left((\underline{\mathbf{h}}, \mathbf{0}) \sum C_{2N}^l\right)_{k+N}}_{\beta} \tag{7}$$

等于 1，当 (α, β) =(1,0) 或 (α, β) =(0, 1) 时，因此有以下四种情况之一：

If $\gamma = 0$ and $(\alpha, \beta) = (0, 1)$, then $\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right)_{k+N} = 1$.
If $\gamma = 1$ and $(\alpha, \beta) = (0, 1)$, then $\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right)_k = 1$.
If $\gamma = 0$ and $(\alpha, \beta) = (1, 0)$, then $\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right)_k = 1$.
If $\gamma = 1$ and $(\alpha, \beta) = (1, 0)$, then $\left(\underline{\mathbf{g}}_i \sum C_{2N}^l\right)_{k+N} = 1$.

So,

$$w(\underline{\mathbf{g}}_i \sum C_{2N}^l) \geq w(\underline{\mathbf{h}} \sum C_N^l) \geq w(\mathbf{h}) = w(\mathbf{g}_i), \tag{8}$$

最后一个不等式由归纳法得出。 □

以下引理有助于证明定理 1。

引理 1。 对于 $1 \leq m \leq N-1$和 $1 \leq k \leq N$，如果 $k + m > N$，

$$\mathbf{g}_k = \mathbf{g}_k \sum_{\substack{1 \leq l \leq N-1 \\ g_{m+1,l+1}=1}}^{s.t.} C_N^l, \tag{9}$$

其中，$\mathbf{g}_k$ 和 $\mathbf{g}_{m+1}$ 分别是矩阵 G_n 的第 k 行和第 $(m+1)$ 行。

例 *3.* 对于 $n = 3$、$k = 6$ 和 $m = 3$，有 $m + k = 9 > N$。因此，对于 g_k =*(1, 1, 0, 0, 1, 1, 0, 0)* 和 g_{m+1} =*(1, 1, 1, 1, 0, 0, 0, 0)*，有 $g_k = g_k(C^1 \oplus C^2 \oplus C^3)$。

证明。 证明采用归纳法。假设引理 1 对 n成立，并证明其对 $n+1$情形也成立。根据 k 是否大于 N，我们将证明分为两种情况。

情况 1： $k > N$。

矩阵 G_{n+1}的第 k 行可写为 $\mathbf{g}_k = (\mathbf{h}_{k-N},\ \mathbf{h}_{k-N})$，其中 $\mathbf{h}_{k-N}$是矩阵 G_n的第 $(k-N)$ 行。若 $k+m>2N$，则 $k+m-N>N$，根据归纳法可得

$$\mathbf{h}_{k-N} = \mathbf{h}_{k-N} \sum_{\substack{1\le l\le N-1 \ \text{s.t.} \\ h_{m+1,l+1}=1}} C_N^l. \tag{10}$$

由此可得

$$\begin{aligned}
&\mathbf{g}_k \sum_{\substack{1\le l\le 2N-1 \ \text{s.t.} \\ g_{m+1,l+1}=1}} C_{2N}^l \\
&= (\mathbf{h}_{k-N}, \mathbf{h}_{k-N}) \sum_{\substack{1\le l\le 2N-1 \ \text{s.t.} \\ g_{m+1,l+1}=1}} C_{2N}^l \\
&= (\mathbf{h}_{k-N} \sum_{\substack{1\le l\le N-1 \ \text{s.t.} \\ h_{m+1,l+1}=1}} C_N^l, \mathbf{h}_{k-N} \sum_{\substack{1\le l\le N-1 \ \text{s.t.} \\ h_{m+1,l+1}=1}} C_N^l) \\
&= (\mathbf{h}_{k-N}, \mathbf{h}_{k-N}) = \mathbf{g}_k.
\end{aligned} \tag{11}$$

情况 2： $k \le N$。

假设 $\mathbf{g}_k = (\mathbf{h}_k,\ \mathbf{0})$ 是矩阵 G_{n+1} 和 $k+m>2N$ 的第 k 行，其中 $\mathbf{h}_k$ 是矩阵 G_n 的第 k 行。由于 $k \le N$，我们可以将 m 写为 $m = j+N$，使得 $j < N$。由 $j+N+k>2N$，我们有 $j+k>N$，根据归纳法可得

$$\mathbf{h}_k = \mathbf{h}_k \sum_{\substack{1\le l\le N-1 \ \text{s.t.} \\ h_{j+1,l+1}=1}} C_N^l. \tag{12}$$

另外请注意，对于任意长度为 N 且满足 $1 \le l \le N-1$ 的向量 $\mathbf{x}$，我们有

$$(\mathbf{x}, 0)(C_{2N}^l \oplus C_{2N}^{l+N}) = (\mathbf{x}C_N^l, \mathbf{x}C_N^l). \tag{13}$$

例如，对于 $N=8$ 和 $l=3$,

$$\begin{aligned}
&(\mathbf{x}, 0)(C_{2N}^l \oplus C_{2N}^{l+N}) \\
&= (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, 0,0,0,0,0,0,0,0) C_{16}^3 \\
&+ (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, 0,0,0,0,0,0,0,0) C_{16}^{11} \\
&= (0,0,0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, 0,0,0,0,0) \\
&+ (x_6, x_7, x_8, 0,0,0,0,0,0,0,0, x_1, x_2, x_3, x_4, x_5) \\
&= (x_6, x_7, x_8, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_1, x_2, x_3, x_4, x_5) \\
&= (\mathbf{x}C_N^l, \mathbf{x}C_N^l).
\end{aligned}$$

因此，我们有

$$\begin{aligned}\mathbf{g}_k \sum_{\substack{1\le l\le 2N-1 \text{ s.t.}\\ g_{m+1,l+1}=1}} C_{2N}^l &= (\mathbf{h}_k, \mathbf{0}) \sum_{\substack{1\le l\le N-1 \text{ s.t.}\\ (h_{j+1,l+1}, h_{j+1,l+1})=(1,1)}} C_{2N}^l \\ &= (\mathbf{h}_k \sum_{\substack{1\le l\le N-1 \text{ s.t.}\\ h_{j+1,l+1}=1}} C_N^l, \mathbf{h}_k \sum_{\substack{1\le l\le N-1 \text{ s.t.}\\ h_{j+1,l+1}=1}} C_N^l) \\ &= (\mathbf{h}_k, \mathbf{h}_k) = \mathbf{g}_k,\end{aligned} \tag{14}$$

其中，第二个等式由式 (13) 得出，第三个等式由归纳法得出。 □

定义一个 $N \times N$ 上三角双对角矩阵 D_N 如下:

$$D_N \triangleq \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & & \vdots \\ \vdots & 0 & \ddots & \ddots & \\ & \vdots & & 1 & 1 \\ 0 & 0 & \dots & & 1 \end{bmatrix}, \tag{15}$$

该矩阵是一个上三角托普利兹矩阵，其主对角线和上对角线元素均为 1（其第一行的第一个和第二个位置为 1），其余所有元素均为零。

我们还将矩阵 D_N^m 定义为一个上三角托普利兹矩阵，其第一行的第一个位置和第 ($m+1$) 个位置为 1，其中 $1 \le m \le N-1$；并将 D_N^0 定义为单位矩阵。

下面的定理描述了矩阵 D_N^m 与顺时针循环移位矩阵 C_N^l之间的关系。注意，当 $m = 0$时，该关系显然成立；两个矩阵分别乘以 G_n 后均为单位矩阵。

定理 1。对于任意 $m \le N-1$,

$$D_N^m G_n = G_n \sum_{\substack{1\le l\le N-1 \ s.t.\\ g_{m+1,l+1}=1}} C_N^l. \tag{16}$$

这等价于说，如果 $i = k + m \le N$，那么

$$\mathbf{g}_k \oplus \mathbf{g}_i = \mathbf{g}_k \sum_{\substack{1\le l\le N-1 \ s.t.\\ g_{i-k+1,l+1}=1}} C_N^l, \tag{17}$$

且如果 $k + m > N$，那么

$$\mathbf{g}_k = \mathbf{g}_k \sum_{\substack{1\le l\le N-1 \ s.t.\\ g_{m+1,l+1}=1}} C_N^l \tag{18}$$

例 4。对于 $n=2$,

$$G_n=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{bmatrix}, D^2=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{bmatrix},$$

$$C^2=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix},$$

$$D^2G_n=G_nC^2=\begin{bmatrix}0&0&1&0\\0&0&1&1\\1&0&1&0\\1&1&1&1\end{bmatrix}. \tag{19}$$

例 5. 对于 $n=2$,

$$G_n=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{bmatrix},\ D^3=\begin{bmatrix}1&0&0&1\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},$$

$$C^1=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix},\ C^2=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix},\ C^3=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix},$$

$$D^3G_n=G_n(C^1\oplus C^2\oplus C^3)=\begin{bmatrix}0&1&1&1\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{bmatrix}. \tag{20}$$

证明。引理 1 证明了等式 (18)，我们给出 $i=k+m\le N$ 情况的证明。证明采用归纳法，并假设 (17) 对于 G_n成立；然后证明它对于 G_{n+1} 也成立。对此，我们有 $i=k+m\le 2N$。根据取值不同，我们将证明分为 6 种情况：

i和 k。第一种情况是 $k > N$，第二种情况是 i， $k \leq N$，其余四种情况是 $k \leq N$ 和 $i > N$。

情形 1： $k > N$。

我们有

$$\mathbf{g}_k \oplus \mathbf{g}_i = (\mathbf{h}_{k-N} \oplus \mathbf{h}_{i-N}, \mathbf{h}_{k-N} \oplus \mathbf{h}_{i-N}), \tag{21}$$

其中，$\mathbf{h}_{k-N}$和$\mathbf{h}_{i-N}$分别是矩阵 G_N的第（$k-N$）行和第（$i-N$）行。根据归纳法，我们有

$$\begin{aligned}
&\mathbf{g}_k \oplus \mathbf{g}_i = (\mathbf{h}_{k-N} \oplus \mathbf{h}_{i-N}, \mathbf{h}_{k-N} \oplus \mathbf{h}_{i-N}) \\
&= (\mathbf{h}_{k-N} \sum_{\substack{1 \leq l \leq N-1 \ \text{s.t.} \\ h_{i-k+1,l+1}=1}} C_N^l, \mathbf{h}_{k-N} \sum_{\substack{1 \leq l \leq N-1 \ \text{s.t.} \\ h_{i-k+1,l+1}=1}} C_N^l) \\
&= (\mathbf{h}_{k-N}, \mathbf{h}_{k-N}) \sum_{\substack{1 \leq l \leq 2N-1 \ \text{s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^l \\
&= \mathbf{g}_k \sum_{\substack{1 \leq l \leq 2N-1 \ \text{s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^l.
\end{aligned} \tag{22}$$

例如，对于 $N = 8$、 $k = 12$ 和 $i = 15$，矩阵 G_4 的第 12 行和第 15 行为

$$\mathbf{g}_{12} = (\mathbf{h}_4, \mathbf{h}_4) = (1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0),$$

$$\mathbf{g}_{15} = (\mathbf{h}_7, \mathbf{h}_7) = (1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0).$$

由 $i - k + 1 = 4$可知，我们有

$$\mathbf{g}_{12} \oplus \mathbf{g}_{15} = \mathbf{g}_{12}(C_{16}^1 \oplus C_{16}^2 \oplus C_{16}^3).$$

情形 2： $k \leq N$ 和 $i \leq N$。

矩阵 G_{n+1} 的第 k 行和第 i 行分别可写为 $\mathbf{g}_k = (\mathbf{h}_k, \mathbf{0})$ 和 $\mathbf{g}_i = (\mathbf{h}_i, \mathbf{0})$，其中 $\mathbf{h}_k$ 和 $\mathbf{h}_i$ 是矩阵 G_n 中对应的行。根据归纳法，我们有

$$\mathbf{h}_k \oplus \mathbf{h}_i = \mathbf{h}_k \sum_{\substack{1 \leq l \leq N-1 \ \text{s.t.} \\ h_{i-k+1,l+1}=1}} C_N^l. \tag{23}$$

注意，$\mathbf{h}_k$ 的最后一个 1 位于第 k 个位置，而基于向量 $\mathbf{h}_{i-k+1}$ 进行移位，可以将该 1 移至第 $i-k$ 个位置。因此，向量 $\mathbf{h}_k$ 的最后一个 1 可以移至第 i 个位置，该位置小于或等于 N。由此可得

$$\begin{aligned}\mathbf{g}_k \oplus \mathbf{g}_i &= (\mathbf{h}_k, \mathbf{0}) \oplus (\mathbf{h}_i, \mathbf{0}) = (\mathbf{h}_k \oplus \mathbf{h}_i, \mathbf{0}) \\ &= (\mathbf{h}_k \sum_{\substack{1\le l\le N-1 \text{ s.t.} \\ h_{i-k+1,l+1}=1}} C_N^l, \mathbf{0}) \\ &= (\mathbf{h}_k, \mathbf{0}) \sum_{\substack{1\le l\le 2N-1 \text{ s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^l = \mathbf{g}_k \sum_{\substack{1\le l\le 2N-1 \text{ s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^l,\end{aligned} \tag{24}$$

wher第三个等式由归纳法得出，第四个等式由上述讨论得出 .

例如 ，对于 $N=8$、 $k=2$ 和 $i=8$，矩阵 G_4 的第 2 行和第 8 行为

$$\mathbf{g}_2 = (\mathbf{h}_2, \mathbf{0}) = (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0),$$

$$\mathbf{g}_8 = (\mathbf{h}_8, \mathbf{0}) = (1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0).$$

由已知 $i-k+1=7$，可得

$$\mathbf{g}_2 \oplus \mathbf{g}_8 = \mathbf{g}_2(C_{16}^2 \oplus C_{16}^4 \oplus C_{16}^6).$$

情况 3： $k \le N$， $i = j+N$ 且 $j \ge k$。

矩阵 G_{n+1} 的第 k 行、第 j 行和第 i 行分别为 $\mathbf{g}_k = (\mathbf{h}_k, \mathbf{0})$、$\mathbf{g}_j = (\mathbf{h}_j, \mathbf{0})$ 和 $\mathbf{g}_i = (\mathbf{h}_j, \mathbf{h}_j)$，其中 $\mathbf{h}_k$ 和 $\mathbf{h}_j$ 是矩阵 G_n 中对应的行。根据归纳法，以矩阵 G_n 的第 $r = j-k+1$ 行为基础进行移位，可得

$$\mathbf{h}_k \oplus \mathbf{h}_j = \mathbf{h}_k \sum_{\substack{1\le l\le N-1 \text{ s.t.} \\ h_{j-k+1,l+1}=1}} C_N^l. \tag{25}$$

请注意，这些移位是根据向量 $\mathbf{h}_r$中位置大于或等于 2 的项进行的，我们将其表示为 $(\times, h_{r,2}, h_{r,3}, \cdots, h_{r,N})$。一般而言，我们称基于向量 $(\times, h_{r,2}, h_{r,3}, \cdots, h_{r,N})$ 对向量 $\mathbf{h}_k$ 进行移位后得到 $\mathbf{h}_k \oplus \mathbf{h}_j$，这是公式 (25) 的一种替代表达方式。

注意，根据情况 2，我们知道，将 $\mathbf{h}_k$ 按行 $j-k+1$移位时，$\mathbf{h}_k$ 中的最后一个 1 元素最多会移至第 N 个位置。由此可知，根据 $(\times, h_{r,2}, h_{r,3}, \cdots, h_{r,N}, 0)$ 对 $(\mathbf{h}_k, 0)$ 进行移位，结果为 $(\mathbf{h}_k \oplus \mathbf{h}_j, 0)$。类似地，根据 $(0, \times, h_{r,2}, h_{r,3}, \cdots, h_{r,N})$ 对第 k 行 $(\mathbf{h}_k, 0)$ 进行移位，结果为 $(0, \mathbf{h}_k \oplus \mathbf{h}_j)$。另外，注意，根据一个仅在第 $(N+1)$ 个位置上为 1 的向量，对向量 $(x_1, x_2, \cdots x_N, 0)$ 进行移位，结果为 $(0, x_1, x_2, \cdots x_N)$，即

$$(x_1, x_2, \cdots x_N, \mathbf{0}) C_{2N}^N = (\mathbf{0}, x_1, x_2, \cdots x_N). \tag{26}$$

因此，根据向量对第 k 行 $(\mathbf{h}_k, \mathbf{0})$ 进行移位

$$(\times, h_{r,2}, h_{r,3}, \cdots, h_{r,N}, 1, h_{r,2}, h_{r,3}, \cdots, h_{r,N})$$

得到（$\mathbf{h}_k \oplus \mathbf{h}_j$，$\mathbf{h}_k \oplus$（$\mathbf{h}_k \oplus \mathbf{h}_j$））＝（$\mathbf{h}_k \oplus \mathbf{h}_j$，$\mathbf{h}_j$）。这意味着

$$\begin{aligned}
&\mathbf{g}_k \sum_{\substack{1\le l\le 2N-1 \text{ s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^{l} \\
&= (\mathbf{h}_k, \mathbf{0}) \sum_{\substack{1\le l\le 2N-1 \text{ s.t.} \\ g_{i-k+1,l+1}=1}} C_{2N}^{l} \\
&= (\mathbf{h}_k \oplus \mathbf{h}_j, \mathbf{0}) \oplus (\mathbf{0}, \mathbf{h}_k) \oplus (\mathbf{0}, \mathbf{h}_k \oplus \mathbf{h}_j) \\
&= (\mathbf{h}_k \oplus \mathbf{h}_j, \mathbf{h}_j) = \mathbf{g}_k \oplus \mathbf{g}_i.
\end{aligned} \tag{27}$$

例如，对于 $N = 8$、$k = 7$ 和 $i = 16$，矩阵 G_4 的第 7 行和第 16 行为

$$\mathbf{g}_7 = (\mathbf{h}_7, \mathbf{0}) = (1,0,1,0,1,0,1,0,0,0,0,0,0,0,0,0),$$

$$\mathbf{g}_{16} = (\mathbf{h}_8, \mathbf{h}_8) = (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1).$$

由于 $j = 8$ 和 $j - k + 1 = 2$，移位基于（×、h_2、2、⋯、h_2、8、1、h_2、2、⋯、h_2、8）＝（×、1、0、0、0、0、0、0、1、1、0、0、0、0、0、0）。因此

$$\mathbf{g}_7 \oplus \mathbf{g}_{16} = \mathbf{g}_7(C_{16}^{1} \oplus C_{16}^{8} \oplus C_{16}^{9}).$$

情况 4： $k \le N$、$i = j + N$、$j \le k$ 和 $j > N/2$。

我们有 $N/2 < k \le N$ 和 $N + N/2 < i$。矩阵 G_{n+1} 的第 k 行和第 i 行分别可写为 $\mathbf{g}_k = (\mathbf{h}_k, 0) = (\mathbf{x}, \mathbf{x}, 0, 0)$ 和 $\mathbf{g}_i = (\mathbf{h}_j, \mathbf{h}_j) = (\mathbf{y}, \mathbf{y}, \mathbf{y}, \mathbf{y})$，其中 $\mathbf{h}_k$ 和 $\mathbf{h}_j$ 是矩阵 G_N 中对应的行，而 $\mathbf{x}$ 和 $\mathbf{y}$ 是矩阵 $G_{N/2}$ 中对应的行。

我们有

$$\mathbf{h}_{k-N/2} \oplus \mathbf{h}_j = (\mathbf{x}, \mathbf{0}) \oplus (\mathbf{y}, \mathbf{y}) = (\mathbf{x} \oplus \mathbf{y}, \mathbf{y}), \tag{28}$$

并由归纳法可得

$$(\mathbf{x} \oplus \mathbf{y}, \mathbf{y}) = (\mathbf{x}, \mathbf{0}) \sum_{\substack{1\le l\le N-1 \text{ s.t.} \\ h_{j-k+N/2+1,l+1}=1}} C_{N}^{l}. \tag{29}$$

注意到 $j - k + N/2 + 1 \le N/2$。因此 $\mathbf{g}^{j-k+N/2+1} = (\mathbf{r}, \mathbf{0}, \mathbf{0}, \mathbf{0})$，其中 $\mathbf{r}$ 是矩阵$G_{N/2}$的一行。这样，$i - k + 1 = (j - k + N/2 + 1) + N/2$ 且 $\mathbf{g}_{i-k+1} = (\mathbf{r}, \mathbf{r}, \mathbf{0}, \mathbf{0})$。

由（29）可知，将 (x, 0, 0, 0) 移位 $(\times, r_2, \cdots, r_{N/2}, 0, 0, 0)$ 后得到 (x ⊕ y, y, 0, 0)。此外，将 (x, 0, 0, 0) 移位 $(0, 1, r_2, \cdots, r_{N/2}, 0, 0)$ 后得到 (0, x⊕(x⊕y), y, 0) ＝(0, y, y, 0)。

同样，将 $(\mathbf{0},\mathbf{x},\mathbf{0},\mathbf{0})$ 移位 $(\times,r_2,\cdots,r_{N/2},\mathbf{0},\mathbf{0},\mathbf{0})$ 后，也得到 $(\mathbf{0},\mathbf{x}\oplus\mathbf{y},\mathbf{y},\mathbf{0})$。

最后，将 (0, x, 0, 0) 按 $(0,1,r_2,\cdots,r_{N/2},0,0)$ 移位，得到 (0, 0, x $\oplus$(x $\oplus$y), y) =(0, 0, y, y)。综合考虑这四次移位，(x, x, 0, 0) 的移位为

$$(\times,r_2,\cdots,r_{N/2},1,r_2,\cdots,r_{N/2},\mathbf{0},\mathbf{0})$$

为 *(x $\oplus$y, y, 0, 0) $\oplus$(0, y, y, 0) $\oplus$(0, x $\oplus$y, y,0) $\oplus$(0, 0, y, y) =(x $\oplus$y, x $\oplus$y,y,y)*。因此，我们得出

$$\begin{aligned}\mathbf{g}_k\sum_{\substack{1\le l\le 2N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}&=(\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0})\sum_{\substack{1\le l\le 2N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}\\&=(\mathbf{x}\oplus\mathbf{y},\mathbf{x}\oplus\mathbf{y},\mathbf{y},\mathbf{y})\\&=(\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0})\oplus(\mathbf{y},\mathbf{y},\mathbf{y},\mathbf{y})=\mathbf{g}_k\oplus\mathbf{g}_i.\end{aligned}\tag{30}$$

例如，对于 $N=8$、 $k=8$ 和 $i=15$，矩阵 G_4 的第 8 行和第 15 行为

$$\begin{aligned}\mathbf{g}_8&=(\mathbf{h}_8,\mathbf{0})=(\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0})\\&=(1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0),\\\mathbf{g}_{15}&=(\mathbf{h}_7,\mathbf{h}_7)=(\mathbf{y},\mathbf{y},\mathbf{y},\mathbf{y})\\&=(1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0).\end{aligned}$$

由于 $i-k+1=8$，移位基于向量 $\mathbf{g}_{i-k+1}=(\times,r_2,\cdots,r_{N/2},1,r_2,\cdots,r_{N/2},0,0)$ =(×, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)。因此 $\mathbf{g}_8\oplus\mathbf{g}_{15}=\mathbf{g}_8(C^1\oplus C^2\oplus\cdots\oplus C^7)$。

情形 5： $k\le N$、 $i=j+N$、 $j\le k$、 $1\le j\le N/2$ 和 $k>N/2$。

我们有 $N<i\le N+N/2$ 和 $1\le i-k+1\le N$。矩阵G_{n+1}的第 k 行和第 i 行分别可写为 $\mathbf{g}_k=(\mathbf{h}_k,0)=(\mathbf{x},\mathbf{x},0,0)$ 和 $\mathbf{g}_i=(\mathbf{h}_j,\mathbf{h}_j)=(\mathbf{y},0,\mathbf{y},0)$，其中 $\mathbf{h}_k$ 和 $\mathbf{h}_j$ 是矩阵 G_N 的相应行，而 x 和 y 是矩阵 $G_{N/2}$ 的相应行。此外，$\mathbf{h}_{k-N/2}=(\mathbf{x},0)$ 和 $\mathbf{h}_{i-N/2}=(\mathbf{y},\mathbf{y})$。根据归纳法，我们有

$$\begin{aligned}(\mathbf{x},\mathbf{0})\sum_{\substack{1\le l\le N-1\ \text{s.t.}\\ h_{i-k+1,l+1}=1}}C_N^l&=\mathbf{h}_{k-N/2}\sum_{\substack{1\le l\le N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_N^l\\&=\mathbf{h}_{k-N/2}\oplus\mathbf{h}_{i-N/2}=(\mathbf{x}\oplus\mathbf{y},\mathbf{y}).\end{aligned}\tag{31}$$

由于 $i-k+1\le N$，$\mathbf{g}_{i-k+1}=(\mathbf{r},\ \mathbf{0})$。

由 (31) 可知，将 $(\mathbf{x},\ \mathbf{0},\ \mathbf{0},\ 0)$ 按 $(\times,\ r_2,\ \cdots,\ r_N,\ 0)$ 移位后，得到 $(\mathbf{x}\oplus\mathbf{y},\ \mathbf{y},\ \mathbf{0},\ 0)$。

此外，将（$\mathbf{0},\mathbf{x},\mathbf{0},0$）移位（$\times,r_2,\cdots,r_N,\mathbf{0}$）后得到（$\mathbf{0},\mathbf{x}\oplus\mathbf{y},\mathbf{y},\mathbf{0}$）。

综合考虑这两次移位，将（$\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0}$）移位（$\times,r_2,\cdots,r_N,\mathbf{0}$）后得到（$\mathbf{x}\oplus\mathbf{y},\mathbf{y}\oplus(\mathbf{x}\oplus\mathbf{y}),\mathbf{y},\mathbf{0}$）$=$（$\mathbf{x}\oplus\mathbf{y},\mathbf{x},\mathbf{y},\mathbf{0}$）。因此我们得出结论：

$$\begin{aligned}\mathbf{g}_k\sum_{\substack{1\le l\le 2N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}&=(\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0})\sum_{\substack{1\le l\le N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}\\&=(\mathbf{x}\oplus\mathbf{y},\mathbf{x},\mathbf{y},\mathbf{0})\\&=(\mathbf{x},\mathbf{x},\mathbf{0},\mathbf{0})\oplus(\mathbf{y},\mathbf{0},\mathbf{y},\mathbf{0})=\mathbf{g}_k\oplus\mathbf{g}_i.\end{aligned}\tag{32}$$

情况 6： $k\le N$, $i=j+N$, $j\le k$，以及 $1\le j\le N/2$ 和 $k\le N/2$。

我们有 $N<i\le N+N/2$ 和 $N/2<i-k+1\le N$。矩阵 G_{n+1} 的第 k 行和第 i 行分别可写为 $\mathbf{g}_k=(\mathbf{h}_k,\mathbf{0})=(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})$ 和 $\mathbf{g}_i=(\mathbf{h}_j,\mathbf{h}_j)=(\mathbf{y},\mathbf{0},\mathbf{y},\mathbf{0})$，其中 $\mathbf{h}_k$ 和 $\mathbf{h}_j$ 是矩阵 G_N 中对应的行，而 $\mathbf{x}$ 和 $\mathbf{y}$ 是矩阵 $G_{N/2}$ 中对应的行。此外，$\mathbf{h}_k=(\mathbf{x},\mathbf{0})$ 和 $\mathbf{h}^{i-N/2}=(\mathbf{y},\mathbf{y})$。由归纳法可得

$$\begin{aligned}(\mathbf{x},\mathbf{0})\sum_{\substack{1\le l\le N-1\ \text{s.t.}\\ h_{i-N/2-k+1,l+1}=1}}C_{N}^{l}&=\mathbf{h}_k\sum_{\substack{1\le l\le N-1\ \text{s.t.}\\ h_{i-N/2-k+1,l+1}=1}}C_{N}^{l}\\&=\mathbf{h}_k\oplus\mathbf{h}_{i-N/2}=(\mathbf{x}\oplus\mathbf{y},\mathbf{y}).\end{aligned}\tag{33}$$

注意到 $1<i-N/2-k+1\le N/2$ 和 $N/2<i-k+1\le N$。因此 $\mathbf{g}_{i-k+1}=(\mathbf{r},\ \mathbf{r},\ \mathbf{0},\ \mathbf{0})$。

根据（33），将 $(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})$ 移位 $\mathbf{g}^{i-N/2-k+1}=(\times,r_2,\cdots,r_{N/2},\mathbf{0},\mathbf{0},\mathbf{0})$ 后得到 $(\mathbf{x}\oplus\mathbf{y},\mathbf{y},\mathbf{0},\mathbf{0})$。

同样地，将 $(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})$ 移位 $(\mathbf{0},\mathbf{1},r_2,\cdots,r_{N/2},\mathbf{0},\mathbf{0})$ 后得到 $(\mathbf{0},\mathbf{x}\oplus(\mathbf{x}\oplus\mathbf{y}),\mathbf{y},\mathbf{0})$。

将这两次移位结合起来，$(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})$ 的移位为

$$(\times,r_2,\cdots,r_{N/2},1,r_2,\cdots,r_{N/2},\mathbf{0},\mathbf{0})$$

为 $(\mathbf{x}\oplus\mathbf{y},\ \mathbf{0},\ \mathbf{y},\ \mathbf{0})$。

因此我们得出

$$\begin{aligned}\mathbf{g}_k\sum_{\substack{1\le l\le 2N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}&=(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})\sum_{\substack{1\le l\le 2N-1\ \text{s.t.}\\ g_{i-k+1,l+1}=1}}C_{2N}^{l}\\&=(\mathbf{x}\oplus\mathbf{y},\mathbf{0},\mathbf{y},\mathbf{0})\\&=(\mathbf{x},\mathbf{0},\mathbf{0},\mathbf{0})\oplus(\mathbf{y},\mathbf{0},\mathbf{y},\mathbf{0})=\mathbf{g}_k\oplus\mathbf{g}_i.\end{aligned}\tag{34}$$

□

假设矩阵 T_N 是一个 $N\times N$ 上三角托普利兹矩阵，且矩阵沿每条对角线的元素都相同。我们可以看到，对于某些 m 的取值，$T_N=\sum_m D_N^m$ 成立；根据定理 1，对于某些 l 的取值，$D_N^m G_n=G_n\sum_l C_N^l$ 成立。

例 6. 假设 $N = 8$。对于多项式 $\mathbf{c}(x) = x^6 + x^4 + x^3 + x + 1$ （八进制形式为 *133*），卷积编码器矩阵如下：

$$T_8 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

此外，

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

注意，$T_8 G_3 = \left(D_8^0 + D_8^2 + D_8^3 + D_8^5 + D_8^6\right) G_3$。此外，

$$\begin{aligned} D_8^0 G_3 &= G_3 C_3^0, \\ D_8^2 G_3 &= G_3 \sum_{\substack{1 \le l \le 7 \ \ s.t. \\ g_{3,l+1}=1}} C_8^l = G_3 C_8^2, \\ D_8^3 G_3 &= G_3 \sum_{\substack{1 \le l \le 7 \ \ s.t. \\ g_{4,l+1}=1}} C_8^l = G_3 \left(C_8^1 + C_8^2 + C_8^3\right), \\ D_8^5 G_3 &= G_3 \sum_{\substack{1 \le l \le 7 \ \ s.t. \\ g_{6,l+1}=1}} C_8^l = G_3 \left(C_8^1 + C_8^4 + C_8^5\right), \\ D_8^6 G_3 &= G_3 \sum_{\substack{1 \le l \le 7 \ \ s.t. \\ g_{7,l+1}=1}} C_8^l = G_3 \left(C_8^2 + C_8^4 + C_8^4\right). \end{aligned}$$

因此，$T_8 G_3 = \left(D_8^0 + D_8^2 + D_8^3 + D_8^5 + D_8^6\right) G_3 = G_3 \left(C_8^0 + C_8^2 + C_8^3 + C_8^5 + C_8^6\right)$。

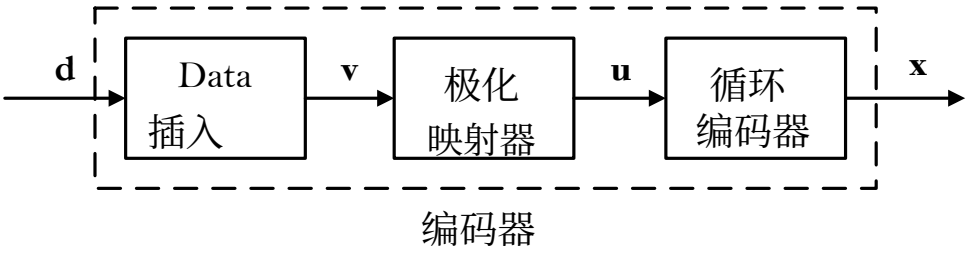

图 2. 所提出的编码方案等价于采用循环内码和极化类 RM 外码的 PAC 码。

因此，对于数据字**v**，

$$\mathbf{v}T_N G_n = \mathbf{v}\sum_m D_N^m G_n = \mathbf{v}G_n \sum_s C_N^s, \tag{35}$$

其中，第二个等式由定理 1 得出。图 2 展示了我们所提出编码方案的框图，该方案等价于采用循环码作为内码、极化码和类 RM 码作为外码的 PAC 编码。

假设数据向量 **v** 的第一个 1 出现在第 i 个位置，即 $\mathbf{v}G_n = \mathbf{g}_i$，其中 $\underline{\mathbf{g}}_i$ 是矩阵 G_n 的第 i 行。由 (35) 可得

$$w(\mathbf{v}T_N G_n) = w(\mathbf{v}G_n \sum_s C_N^s) = w(\underline{\mathbf{g}}_i \sum_s C_N^s) \geq w(\mathbf{g}_i), \tag{36}$$

其中，不等式由命题 1 得出。注意到，极化码的 $d_{\min}$ 是 $G_{N,\mathcal{A}}$ 的最小行重量，这证明 PAC 码的 $d_{\min}$ 大于或等于极化类 RM 码的 $d_{\min}$。

尽管该证明并不能保证 PAC 码的最小距离严格优于极化码和类 RM 码，但仿真结果表明，选择适当的卷积码可以显著改善 PAC 码的重量枚举。图 3 比较了 PAC(128,29) 码和 RM(128, 29) 码的帧错误率（FER）与译码复杂度。我们对 PAC 码也采用 RM 码的码率配置，连接多项式为 $\mathbf{c}(x) = x^{10} + x^9 + x^7 + x^3 + 1$ (3211（八进制形式）。复杂度以每个译码比特的平均访问次数（ANV）衡量 [8]。两种码的复杂度相同，但该图表明，在纠错性能方面，PAC 码优于 RM 码。两种码的最小距离均为 32。然而，对于 RM(128,29) 码，重量等于最小距离的码字有 10668 个；而对于 PAC(128,29) 码，这一数量降至 324 个。

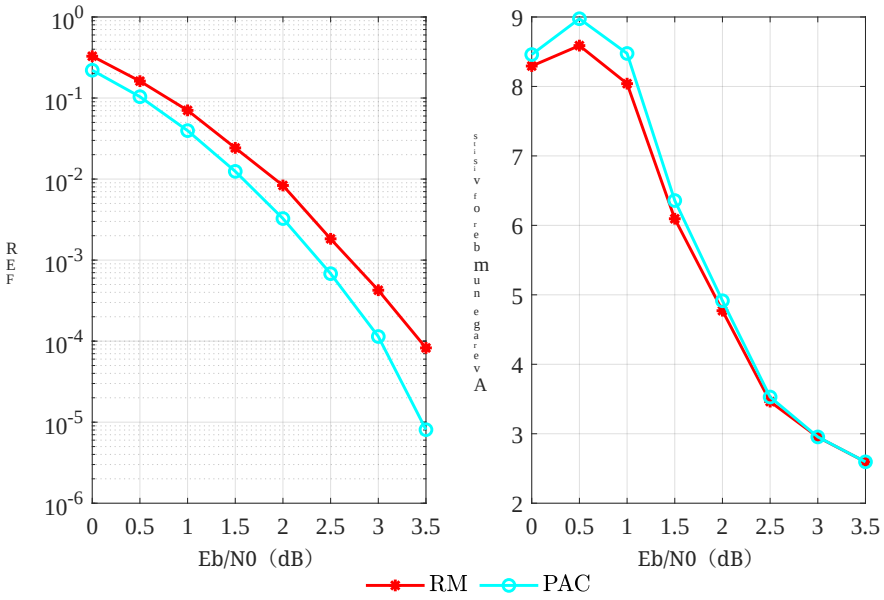

图3. PAC码与RM码的费诺译码器性能比较。

IV. 结论

文献中已对循环移位码进行了广泛研究，将其与 PAC 码、RM 码和极化码联系起来，为改进这些码的分析开辟了新的研究方向。我们证明，PAC 码等价于一类级联码，其内码为循环码，外码为极化码和类 RM 码。我们研究了 PAC 码的最小距离，旨在以新的方式证明 PAC 码在重量分布方面优于极化码和类 RM 码。我们证明，对极化码和类 Reed-Muller 码的生成矩阵中任意一行及其下方若干行构成的部分，进行奇数次顺时针循环移位不会降低该行的重量。基于这一结果，我们证明 PAC 码的最小距离大于或等于极化码和 RM 码的最小距离。

参考文献

[1] M. Moradi，《极化调整卷积（PAC）码的性能与计算分析》，博士论文，比尔肯特大学，2022年。[2] E. Arıkan，《从序贯译码到信道极化，再回到序贯译码》，*arXiv* 预印本 *arXiv:1908.09594*，2019年。[3] B. Li、H. Zhang 和 J. Gu，《关于预变换极化码》，*arXiv* 预印本 *arXiv:1912.06359*，2019年。

[4] H. Luo、G. Zhang、A. Maevskiy、V. Gritsenko、Y. Zhou、Y. Chen、R. Li、Y. Ge、J. Wang 和 J. Wang，《置换极化码的分析与应用》，载于*2018*年 *IEEE* 全球通信大会（*GLOBECOM*）。IEEE，2018年，第1–5页。[5] H. Luo、G. Zhang、J. Wang、R. Li、Y. HuangFu、H. Zhang、Y. Chen 和 J. Wang，《极化码传输方法及装置》，载于美国专利申请。IEEE，2020年，申请号16/673,581。[6] M. Moradi 和 A. Mozammel，《基于蒙特卡洛的极化调整卷积（PAC）码构造》，*arXiv* 预印本 *arXiv:2106.08118*，2021年。[7] M. Moradi，《猜测在极化调整卷积（PAC）码序贯译码中的应用》，*IEEE*通信汇刊，2023年。[8] ——，《关于极化调整卷积（PAC）码的序贯译码度量函数》，*IEEE*通信汇刊，第69卷，第12期，第7913–7922页，2021年。[9] E. Arıkan，《信道极化：一种为对称二进制输入无记忆信道构造容量可达码的方法》，*IEEE*信息论汇刊，第55卷，第7期，第3051–3073页，2009年。