Doob图中的准循环完美码与伽罗瓦环的特殊划分

¨Minjia Shi、Xiaoxiao Li、Denis S. Krotov、Ferruh Ozbudak

arXiv:2305.02735v1 [math.CO] 4 May 2023

摘要——伽罗瓦环 GR(4^{Δ}) 是剩余类环$Z_4[x]/(h(x))$，其中 $h(x)$ 是一个次数为 Δ 、定义在 Z_4上的基本本原多项式。对于任意大于 1 的奇数 Δ ，我们将 GR(4^{Δ})\{0} 划分为类型为 $\{a, b, -a-b, -a, -b, a+b\}$ 的 6 元子集和类型为 $\{c, -c, 2c\}$ 的 3 元子集，使得该划分在 GR(4^{Δ}) 中 Teichmüller 集合的非零元素所对应的乘法作用下保持不变；此外，当 Δ 不是 3 的倍数时，该划分也在 GR(4^{Δ}) 的自同构群作用下保持不变。

作为推论，这意味着在 $D((2^{\Delta}-1)(2^{\Delta}-2)/6, 2^{\Delta}-1)$ 中存在指标为 $(2^{\Delta}-1)$ 的准循环加性 1- 完美码，其中 $D(m, n)$ 是 onZ^{2m+n} 上的 Doob度量方案。

索引词——Doob图、伽罗瓦环、1-完美码、准循环码。

I. 引言

THE 研究Doob图中的码的动机在于关联方案在编码理论中的应用[3]。Doob图中的码可用于具有二维或复值调制的信道中的信息传输。事实上，这些码是Eisenstein–Jacobi整数上的码的特殊情形，参见例如 [5], [12]。从距离正则图的角度来看，与Doob图相关联的方案的代数参数与四元汉明方案的相同。Doob图的顶点可被视为混合由艾森斯坦–雅可比整数环的商环（模 4 和模 2）中的元素构成的字母表，参见例如 [8]。

Doob图 $D(m, n)$ 是由m 个 Shrikhande 图 Sh 与 n 个具有 4 个顶点的完全图 K_4 作笛卡尔积得到的。Shrikhande 图是定义在 $\mathbb{Z}_4^2$ 上、连接集为{±(0,1) ± (1,0) ±(1,1)} 的凯莱图，当且仅当两个顶点之差属于该连接集时，这两个顶点相邻。我们理论中的完全图 K_4 是定义在 $\mathbb{Z}_4$ 或 $\mathbb{Z}_2^2$ 上的凯莱图。若图中每个顶点到且仅到一个码顶点的距离不超过 1，则称该图的顶点集中的一个集合为 1-完美码。

Koolen 和 Munemasa 在 [7]，开创了 Doob图中完美码的研究，并构造了直径为 5 的两个 Doob图中的 1-完美码：$D(1, 3)$ 和 $D(2, 1)$。在 [8]，中，线性1-完美码得到了刻画；若一个码是模 GR(4^2)^m ×GF(2^2)^n 的子模（该模自然地与 $D(n, m)$ 的顶点集相关联），则称其为线性码；当且仅当.....时，这类码可以构造。

$$n = \frac{4^{\gamma+\delta}-1}{3}, \qquad m = \frac{4^{\gamma+2\delta}-4^{\gamma+\delta}}{6} \tag{1}$$

对于某些整数 $\gamma \geq 0$ 和 $\delta > 0$ （情形 $\delta = 0$ 也有意义，但它对应于 4 元字母表上的汉明图 $D(0, n) = H(n, 4)$）。然而，1-完美码存在的球堆积必要条件仅要求图的顶点数 $16^m \cdot 4^n$ 能被半径为1的球的基数 $1+6m+3n$整除。满足这一条件的参数族远比满足（1）的参数族宽。例如，直径为 21 的全部 10 个 Doob图， $D(1, 19)$、 $D(2, 17)$、...、 $D(10, 1)$，其半径为1的球大小均为 64，且 64 整除 4^{21}, ；但其中只有一个图 $D(8, 5)$ 满足限制条件（1）。正如 [10],所示，球堆积分整条件足以保证 Doob图中存在非受限1-完美码，其中“非受限”意为不假定该码具有任何代数结构。受通过代数构造覆盖比线性码参数更多的参数这一可能性启发，文献 [8]提出了加性码的概念。Doob图 $D(m, n)$继承了模 $\mathbb{Z}_4^{2m+n''} \times \mathbb{Z}_2^{2n'}$ 的结构，其中 $n = n' + n''$；若一个码在加法下封闭，或者等价地说，是该模的子模，则称其为加性码。必要条件

$$2m + n' + n'' = \frac{2^{\Gamma+2\Delta}-1}{3}, \quad 3n' + n'' = 2^{\Gamma+\Delta}-1,$$
$$0 \leq n'' \leq 2^{\Delta}-1, \quad n'' \neq 1, \quad \Gamma \geq 0, \quad \Delta \geq 2 \tag{2}$$

这是发表于《IEEE信息论汇刊》的论文经同行评审后接受的版本，https://doi.org/10.1109/TIT.2023.3272566 © 2023年 IEEE。允许个人使用，但转载/再分发须获得 IEEE 许可。

本研究得到国家自然科学基金（12071001）资助。D.S. Krotov 的工作是在索博列夫数学研究所国家合同（项目 FWNF- 2022-0017）框架内完成的。

Minjia Shi 任职于安徽大学智能计算与信号处理重点实验室（教育部）、数学科学学院，中国合肥，邮编 230601；中国科学院信息工程研究所信息安全国家重点实验室，北京，邮编 100093。

Xiaoxiao Li 任职于安徽大学数学科学学院，中国合肥，邮编 230601。

Denis S. Krotov 任职于索博列夫数学研究所，地址：俄罗斯新西伯利亚 Akademika Koptyuga 大道 4 号，邮编 630090（电子邮箱：krotov@math.nsc.ru）。

¨Ferruh Ozbudak 任职于土耳其伊斯坦布尔 34956 的萨班哲大学工程与自然科学学院，以及土耳其安卡拉 06800 的中东技术大学（电子邮箱：ferruh.ozbudak@sabanciuniv.edu）。

在 [8], 中给出，并构造了首批实例；而 [13] 中的构造覆盖了满足（2）的 Doob图 $D(m, n'+n'')$的整个三参数族。除了解决 Doob图中加性1-完美码存在性问题的递归构造外，文献 [8], [13]还描述了三个优美的码。它们位于以下图中

$$D\Big((2^{\Delta}-1)\cdot\frac{2^{\Delta}-2}{6},\ 0+(2^{\Delta}-1)\Big) \tag{3}$$

其参数为 $\Delta=3$、5、7，并具有阶为 $2^{\Delta}-1$ 的拟循环置换自同构。本文的主要目标是将这些拟循环加性 1-完美码推广到任意奇数 Δ 的情形。

下面说明参数 (3) 为何特殊。加性 1-完美码 C 是 $\mathbb{Z}_4^{2m+n''}\times\mathbb{Z}_2^{2n'}$ 的子模，商模 $Q=(\mathbb{Z}_4^{2m+n''}\times\mathbb{Z}_2^{2n'})/C$ 与 $\mathbb{Z}_4^{\Delta}\times\mathbb{Z}_2^{\Gamma}$ 同构。当 $\Gamma=0$ 时，它是一个自由模。在这种情况下，Q 可以与伽罗瓦环 GR(4^{Δ}) 联系起来，而 C 可能具有阶为 $2^{\Delta}-1$ 的坐标置换自同构，该自同构对应于 GR(4^{Δ}) 中 Teichmüller集合的非零元素所产生的乘法。只有当每种类型的坐标数 m、n'、n'' 都能被 $2^{\Delta}-1$ 整除时，这种情况才可能发生；这立即推出 $n'=0$，并得到 (3) 中所示的参数。

让我们考虑本研究的几个动机。首先，循环码和拟循环码具有重要的理论和实际意义，因为它们能够以紧凑的方式表示码，并由此构建可在硬件中高效实现的编码和解码算法。混合字母表中的码在实践中似乎很少使用。然而，“汉明”坐标所属的最后一组的数量为 n''，相对于“Shrikhande”坐标的数量 m 而言较小；将一个1-完美码在所有这些 n'' 个坐标上缩短，可以使其成为 $D(m,0)$ 中的非混合码。该码虽然不再是完美码，但仍然非常接近最优码。我们还提及 [1] 的一项研究结果，该结果指出，在李氏度量下，混合 $\mathbb{Z}_2\mathbb{Z}_4$ 字母表上的循环1-完美码并不存在，只有一个例外。考虑到混合 $\mathbb{Z}_2\mathbb{Z}_4$ 字母表上的码与 Doob 度量下的码之间存在某些相似性，我们可以推测，Doob图中几乎不存在循环1-完美码，而拟循环结构是可能达到的最佳结构。

其次，我们所考虑的可加码与 $\mathbb{Z}_4$上的模的一个非常有趣的划分类有关。为了在 $D(m, n'+n'')$中构造加性 1-完美码的校验矩阵，需要将 $\mathbb{Z}_4^{\Delta}\times\mathbb{F}_2^{\Gamma}$的非零元素划分为 m 个 $\{\pm a, \pm b, \pm(a+b)\}$型六元组、$n''$ 个 $\{a, 2a, -a\}$型三元组，以及 n' 个$\{2a, 2b, 2a+2b\}$ 型三元组（在我们当前的研究中，最后一组为空）。在 $m=n''=\Delta=0$的情形下，这类划分是扩张的特例；扩张在离散几何中得到了广泛研究，参见例如 [6]。对于所有可容许的参数集合（m、n'、n''），所需的划分已在 [13], 中通过三种组合递归构造得到。如果我们希望构造具有相应划分、且该划分在GR(4^{Δ})中Teichmüller集合的乘法作用下保持不变的准循环完美码，那么这种技术便无从使用。因此，我们采用完全不同的代数技术来证明具有这一良好性质的划分的存在性（此外，在 $\Delta\not\equiv 0$ 模 3 的情形下，我们的划分还在GR(4^{Δ})的自同构群作用下保持不变）。需要注意的是，预先规定一个自同构群——通常基于与环境空间相关联的域或环中的乘法——是通过计算寻找不同组合结构的一种有效方法，参见例如 [2], ，其中介绍了首个已知子空间斯坦纳结构的发现过程。在我们的研究中，我们也从计算求解较小情形入手，但最终找到了本文所 प्रस्तुत的理论方法。

最后，正如 [7], 所指出的，参数与 1-完美码的参数对偶的码是单纯形码，也称为紧 2-设计；在适当定义内积和对偶图后（详情见 [9]），Doob图中的加性 1-完美码与加性单纯形码相对应。此外，这种对偶性保留了置换自同构，这意味着我们也构造了拟循环单纯形码。

本文结构如下。下一节汇总后续各节所需的背景知识。第三节构造伽罗瓦环的特殊划分。第四节给出本文的主要结果：一种在 Doob图中构造拟循环1-完美码的方法。第五节总结全文。

II. 背景材料

本节将介绍以下三个方面的一些预备结果。

A. 伽罗瓦环

设 Δ 为奇数。若 $h(x)$ 是一个次数为 Δ 、以 $\mathbb{Z}_4$ 为系数环的基本本原多项式，且 ξ 是 $h(x)$ 的一个根，则剩余类环 $\mathbb{Z}_4[x]/(h(x))$ 中的任意元素都可以写成 $h_0+h_1\xi+\cdots+h_{\Delta-1}\xi^{\Delta-1}$，也可以看作是 $\mathbb{Z}_4$ 上的向量（$h_0, h_1, \ldots, h_{\Delta-1}$）。环 $\mathbb{Z}_4[x]/(h(x))$ 称为含有 4^{Δ} 个元素的伽罗瓦环，记作 GR(4^{Δ})。Teichmüller集合 $\mathcal{T}=\{0,1,\xi,\xi^2,\ldots,\xi^{2^{\Delta}-2}\}$ 是剩余域 $\mathbb{F}_{2^{\Delta}}\simeq$ GR(4^{Δ})/2GR(4^{Δ}) 的代表元集合。已知，GR(4^{Δ}) $=\mathcal{T}\oplus 2\mathcal{T}$（GR($4^{\Delta}$) 的 2-进分解），并且伽罗瓦环的单位群为 GR(4^{Δ})$^*=\mathcal{T}^*\oplus 2\mathcal{T}$，其中 $\mathcal{T}^*=\mathcal{T}\setminus\{0\}$。下面这个关于 $\mathcal{T}$ 中元素之和的公式很有用。

引理 1（山田公式，参见例如 [14, 推论 6.9]）。若c_1、$c_2\in\mathcal{T}$，且 $c_1+c_2=a+2b$、a、$b\in\mathcal{T}$，则

$$a=c_1+c_2+2(c_1c_2)^{1/2}, b=(c_1c_2)^{1/2},$$

其中，$(c_1c_2)^{1/2}$ 表示 $\mathcal{T}$ 中满足 $((c_1c_2)^{1/2})^2=c_1c_2$ 的唯一元素。

我们知道，环同态的核

$$\overline{\ }:\mathbb{Z}_4[x]\to\mathbb{Z}_2[x]$$
$$\overline{h_0+h_1x+\cdots+h_nx^n}=\overline{h}_0+\overline{h}_1x+\cdots+\overline{h}_nx^n$$

是理想 $2\mathbb{Z}_4[x]$ ，而 $(h(x))$ 在下的像为 $(\overline{h}(x))$。因此，¯环同态诱导出一个环同态

$$\overline{\ }: \mathbb{Z}_4[\xi] \to \mathbb{Z}_2[\overline{\xi}]$$
$$\overline{h_0 + h_1\xi + \cdots + h_{\Delta-1}\xi^{\Delta-1}} = \overline{h}_0 + \overline{h}_1\overline{\xi} + \cdots + \overline{h}_{\Delta-1}\overline{\xi}^{\Delta-1},$$

其中， $\overline{\xi}$ 是 ξ的像。实际上， $\overline{\xi}$ 是$(\overline{h}(x))$的一个根，并且 $\mathbb{Z}_2[\overline{\xi}] = \mathbb{F}_{2^\Delta}$。

GR(4^Δ)上的广义 Frobenius 映射定义为

$$f : \mathrm{GR}(4^\Delta) \to \mathrm{GR}(4^\Delta), \quad c = a + 2b \mapsto f(c) = a^2 + 2b^2,$$

其中， a、 $b \in \mathcal{T}$是 GR(4^Δ)的环自同构。此外，如果 σ 是 GR(4^Δ)的环自同构，那么对于某些l、 $0 \le l \le \Delta - 1$， $\sigma = f^l$，例如参见 [14, 第 6]章。

B. 迹映射

对于$u \in \mathbb{F}_{2^\Delta}$， u 在 $\mathbb{F}_2$ 上的迹 $\mathrm{Tr}^{\mathbb{F}_{2^\Delta}/\mathbb{F}_2}(u)$定义为

$$\mathrm{Tr}_{\mathbb{F}_{2^\Delta}/\mathbb{F}_2}(u) = u + u^2 + \cdots + u^{2^{\Delta-1}}.$$

$\mathrm{Tr}^{\mathbb{F}_{2^\Delta}/\mathbb{F}_2}(u)$是 u 的绝对迹，简记为 $\mathrm{Tr}(u)$。

以下引理对于证明我们的主要定理至关重要。

引理 2. 若 $y_1, y_2 \in \mathbb{F}_{2^\Delta}$ 且 $\mathrm{Tr}(y_1) = \mathrm{Tr}(y_2)$，则 $\mathrm{Tr}(y_1y_2) = 0$ 或 $\mathrm{Tr}((y_1+1)(y_2+1)) = 0$。

证明. 直接计算可得 $\mathrm{Tr}((y_1+1)(y_2+1)) = \mathrm{Tr}(y_1y_2) + \mathrm{Tr}(y_1 + y_2) + \mathrm{Tr}(1) = \mathrm{Tr}(y_1y_2) + 1$。 □

下一个事实是一个著名结果——希尔伯特定理 90（参见第 75] 页的 [11, 注 3）的特例。对于我们所考虑的这一特例，我们给出一个简单的证明。

引理 3. 若 $a \in \mathbb{F}_{2^\Delta}$，则方程

$$x^2 + x = a \tag{4}$$

在 $\mathbb{F}_{2^\Delta}$ 中有两个解，当 $\mathrm{Tr}(a) = 0$ ；而当 $\mathrm{Tr}(a) = 1$ 时，在 $\mathbb{F}_{2^\Delta}$ 中无解。

证明。根据以下两个观察，结论显而易见。

(i) 对于 $\mathbb{F}_{2^\Delta}$ 中的每个元素 x_0， x_0 和 $x_0 + 1$ 都是方程 (4) 的解，且 $a = x_0(x_0 + 1)$。另一方面，二次方程至多有两个解。这意味着对于 a 的 $2^\Delta/2$ 个值，方程 (4) 有解。(ii) 若 x_0 是方程 (4) 的一个解，则 $\mathrm{Tr}(a) = \mathrm{Tr}(x_0) + \mathrm{Tr}(x_0^2) = \mathrm{Tr}(x_0) + \mathrm{Tr}(x_0) = 0$。

□

C. Doob图中的加性1-完美码

用 $D(m, n)$ 表示由 m 个 Shrikhande 图 Sh 的笛卡尔积 $\mathrm{Sh}^m \times K^n$ 和 n 个完全四顶点图的笛卡尔积构成的图。若 $m > 0$，则称 $D(m, n)$ 为 Doob图。（情形 $m = 0$ 对应于汉明图 $H(n, 4) = D(0, n)$）。

Shrikhande 图 Sh 是加法群 $\mathbb{Z}_4^{2+}$ 的凯莱图，其底层群为 $\mathbb{Z}_4^2$ ，连接集为 $S = \{01, 30, 33, 03, 10, 11\}$。取 $\mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n$ 中的 $(2m + 2n)$ 元组 $(x_1, \ldots, x_{2m}, z_1, \ldots, z_n)$ 作为 $D(m, n)$ 的顶点集。若码 $C \subset \mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n$ 对加法封闭，则称其为加性码。加性码必然对乘以 $\mathbb{Z}_4$ 的元素封闭。因此，它实际上是 $\mathbb{Z}_4^{2m+n}$ 的一个子模。

注 1. 在 [8], 中，可加码被定义为一个更一般的类别：最后的若干 n 个坐标取值来自 $\mathbb{Z}_2^2$。然而，正如引言中所述，在我们当前的研究中，这类坐标并不存在。

Doob图 $D(m, n)$中的1-完美码是$\mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n$ 的一个子集 C，它是一个独立集，并且 $\mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n \setminus C$ 中的每个顶点都恰好与 C中的一个顶点相邻。

设 $(A|A')$ 是一个行来自 $\mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n$ 的矩阵。如果 : ( ) ，则称其为码 C D m $n' + n''$ C =in (,) 的校验矩阵。$\{c \in \mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n \quad A|A''\ c^T = \overline{0}^T\}$

引理 4（[13, 引理 1]）。设 $(A|A'')$ 是 $\mathbb{Z}_4^{2m} \times \mathbb{Z}_4^n$ 中加性码 C 的校验矩阵。记 $(A|A'')$ 的第 i 列为 a_i，并用 Q 表示所有 a_i、 $1 \le i \le 2m+n$ 的线性张成。当且仅当以下集合构成 $Q\backslash\{\overline{0}^T\}$ 的一个划分时，码 C 是 $D(m, n)$ 中的 1-完美码：

(I) 六元集合

$$\{\pm a_{2i-1}, \pm a_{2i}, \pm(a_{2i-1} + a_{2i})\}, \quad i = 1, \ldots, m,$$

(II) 三元集合

$$\{a_j, 2a_i, -a_j\}, \quad j = 2m + 1, \ldots, 2m + n.$$

一般而言， Q 是某些 Δ和 Γ对应的 $\mathbb{Z}_4^\Delta \times \mathbb{Z}_2^\Gamma$ 型模，但我们关注的是 $\Gamma = 0$的情形，并为方便起见，假设 $Q = \mathrm{GR}(4^\Delta)$。我们的目标是将GR$(4^\Delta)\backslash\{0^\Delta\}$ 划分为(I)型和(II)型集合，使该划分在 ξ的乘法下保持不变。令 $a_j = \xi^j$， $j = 2m+1, \ldots, 2m+n$，于是形如ξ^j、 $2\xi^j$和 $3\xi^j = -\xi^j$ 的元素都由(II)型集合覆盖。接着，GR(4^Δ)中剩余的元素必须由(I)型集合覆盖。

III. GR(4^Δ)的划分

设 $\mathcal{R} = \mathrm{GR}(4^\Delta)$。 $\mathcal{R}$ 中的每个元素都可以唯一表示为 $A = X + 2Y$，其中 X、 $Y \in \mathcal{T}$。若 $A \notin \mathcal{T} \cup 2\mathcal{T}$，则对于某个唯一的 i 和 $\{0, \ldots, 2^\Delta - 2\}$ 中的 j，有 $A = \xi^i(1 + 2\xi^j)$。它们分别记作 $i(A)$ 和 $j(A)$。设 $C_i = \{i \cdot 2^j$ 模 $2^\Delta - 1 : 0 \le j \le \Delta - 1\}$、 $0 \le i \le 2^\Delta - 2$。对于每个 i，集合 C_i 称为模 $2^\Delta - 1$ 的 2-循环陪集。显然，

$C_i = C_j$ 或 $C_i \cap C_j = \emptyset$，对任意 i、j 均成立。用 Cos 表示除 $\{0\}$ 外所有 2-循环陪集构成的集合；用 Cos(s) 表示集合$\{\mathcal{A} \in$ Cos: $|\mathcal{A}| = s\}$；用 N_s 表示其基数。

引理 5. 对于每个 A, B，它们来自 $\mathcal{R}\backslash(\mathcal{T} \cup 2\mathcal{T} \cup 3\mathcal{T})$,

(i) 若 $j(A) = j(B)$，则 $j(-A) = j(-B)$；(ii) $j(A)$ 和 $j(-A)$（$j(B)$ 和 $j(-B)$）属于 Cos 中不同的陪集；(iii) 若 $j(A)$ 和 $j(B)$ 属于同一陪集，则 $j(-A)$ 和$j(-B)$ 属于同一陪集。

证明. 不失一般性，设 $A = 1+2\xi^{j(A)}$ and$B = \xi^{i(B)}($ $1 + 2\xi^{j(B)})$。我们有

$$\begin{aligned}\xi^{i(-B)}(1 + 2\xi^{j(-B)}) - B &= B + 2B \\ &= \xi^{i(B)}\big(1 + 2(1 + \xi^{j(B)})\big) \quad (5) \\ &= \xi^{i(B)}\big(1 + 2\xi^{j}\big),\end{aligned}$$

对某个 j。因此，$j = j(-B)$ 和 $i(B) = i(-B)$。类似地，$i(A) = i(-A) = 0$。

(i) 若 $j(A) = j(B)$，则 $B = \xi^{i(B)}A$，这意味着 $-B = -\xi^{i(B)}A$, $-B = \xi^{i(-B)}(-A)$，且 $j(-B) = j(-A)$。

(ii) 由 (5) 可知，$2(1 + \xi^{j(B)}) = 2\xi^{j(-B)}$。因此，$1+\overline{\xi}^{j(B)} = \overline{\xi}^{j(-B)}$，且 $1 + \mathrm{Tr}(\overline{\xi}^{j(B)}) = \mathrm{Tr}(\overline{\xi}^{j(-B)})$。另一方面，对于所有 s，$\mathrm{Tr}(\overline{\xi}^{j(B)}) = \mathrm{Tr}(\overline{\xi}^{2^s j}{}_{(B)})$。因此，不存在 s 使得 $j(B) \equiv 2^s j(-B) \bmod 2^\Delta - 1$，这就证明了 $j(\pm B)$ 的结论 (ii)。对于 $j(\pm A)$，证明类似。

(iii) 如果 $j(A)$ 和 $j(B)$ 属于同一个陪集，那么存在某个 s，使得 $\overline{\xi}^{j(B)} = \overline{\xi}^{2^s j}{}_{(A)}$。由此可得

$$\begin{aligned}\overline{\xi}^{j(-B)} &= 1 + \overline{\xi}^{j(B)} = 1^{2^s} + \big(\overline{\xi}^{j(A)}\big)^{2^s} \\ &= \big(1 + \overline{\xi}^{j(A)}\big)^{2^s} = \big(\overline{\xi}^{j(-A)}\big)^{2^s} = \overline{\xi}^{2^s j(-A)},\end{aligned}$$

这意味着 $j(-A)$ 和 $j(-B)$ 也属于同一个陪集。

□

引理 5 在 Cos 中的陪集上建立了一个匹配。对于陪集 $\mathcal{A}$，与 $\mathcal{A}$ 匹配的陪集记作 $-\mathcal{A}$。记号 $\pm\mathcal{A}$ 表示 $\mathcal{A}$ 和 $-\mathcal{A}$ 的并集。

命题 1. 对于每个正整数 Δ 和每个整数 $s > 2$, $N_s \cdot s$ 的值都能被 3 整除。

证明. 假设 a 是循环群 $\mathbb{Z}^+_{2^\Delta-1}$ 中一个大小为 s 的 2-循环陪集的元素。根据定义，我们有

$$2^s a \equiv a \bmod 2^\Delta - 1, \tag{6}$$

其中，s 是使 (6) 成立的最小正整数。由于显然有 $2^\Delta a \equiv a \bmod 2^\Delta - 1$，我们看到 s 整除 Δ。特别地，2^s-1 整除 $2^\Delta-1$。接下来，(6) 意味着对于某个 A，$(2^s-1)a = A(2^\Delta-1)$。因此，$a = A\cdot\frac{2^\Delta-1}{2^s-1}$，且 a 是 $\frac{2^\Delta-1}{2^s-1}$ 的倍数。我们得出如下结论：

(*) 每个大小为 s 的陪集都包含在群 $\mathbb{Z}^+_{2^\Delta-1}$ 的 $\frac{2^\Delta-1}{2^s-1}\mathbb{Z}^+_{2^\Delta-1}$ 子群中，该子群的阶为 2^s-1。

利用 (*)，通过对 Δ 进行归纳，可以轻松证明该命题。归纳基础为 $\Delta = 1$ 和 $\Delta = 2$，此时不存在满足 $s > 2$ 和 $N_s > 0$ 的 s。假设 $\Delta > 2$。由 (*) 和归纳假设，我们得到：

(**) 如果 $2 < s < \Delta$，那么 $N_s \cdot s$ 能被 3 整除。

还需证明 $N_\Delta \cdot \Delta$ 能被 3 整除。我们由显然的 $2^\Delta - 1 = |\mathbb{Z}^+_{2^\Delta-1}| = \sum_{s\le\Delta} N_s \cdot s$ 推出这一点：

$$\begin{aligned}N_\Delta \cdot \Delta &= 2^\Delta - 1 - \sum_{s<\Delta} N_s \cdot s \\ &= \big(2^\Delta - 1 - N_1 \cdot 1 - N_2 \cdot 2\big) - \sum_{s:\,2<s<\Delta} N_s \cdot s.\end{aligned}$$

由于偶数 Δ 时 $N_1 = 1, N_2 = 1$，而奇数 Δ 时 $N_2 = 0$，括号中的表达式能被 3 整除。根据 (**)，其余部分也能被 3 整除。因此，$N_\Delta \cdot \Delta$ 能被 3 整除，归纳证明完成。

□

定理 1. 假设 Δ 和 s 是奇正整数，且 s 整除 Δ, $s > 2$, 并且 s 不能被 3 整除。在 $\mathcal{R}\backslash(\mathcal{T} \cup 2\mathcal{T} \cup 3\mathcal{T})$ 中，存在 $A_1, B_1, \ldots, A_k, B_k$，其中 $k = N_s/6$，使得 $j(A_i)$、$j(B_i)$、$j(-A_i - B_i)$、$j(-A_i)$、$j(-B_i)$、$j(A_i + B_i)$、$i = 1, \ldots, k$ 表示 Cos 中大小为 s 的所有陪集；特别地，对于每个 $i = 1, \ldots, k$，有$|C_{j(A_i)}| = |C_{j(B_i)}| = |C_{j(-A_i-B_i)}| = |C_{j(-A_i)}| = |C_{j(-B_i)}| = |C_{j(A_i+B_i)}| = s$。

证明。由于 s 不能被 3 整除，根据命题 1，Cos(s) 的大小 N_s 能被 3 整除。根据引理 5 的情形（ii），如果 $\mathcal{A} \in$ Cos(s)，那么 $-\mathcal{A} \in$ Cos(s)，即 N_s 能被 2 整除。因此，N_s 能被 6 整除。

由引理 5 可知，只需证明以下命题：

(*) 对于给定的任意三个陪集 $\mathcal{A}, \mathcal{B}, \mathcal{C} \in$Cos($s$)，使得 $\pm\mathcal{A} \ne \pm\mathcal{B} \ne \pm\mathcal{C} \ne \pm\mathcal{A}$，存在 A 和 B 属于 $\mathcal{R}\backslash(\mathcal{T} \cup 2\mathcal{T} \cup 3\mathcal{T})$，使得

$$j(A) \in \mathcal{A}, \quad j(B) \in \pm\mathcal{B}, \quad j(A + B) \in \pm\mathcal{C}.$$

我们现在假设 $i(A) = 1$，不失一般性，固定 $j(A)$ 在 $\mathcal{A}$、$j(B)$ 在 $\mathcal{B}$ 以及 j' 在 $\mathcal{C}$ 中的任意取值，并尝试求出使得 $j(A + B) = j'$ 成立的 $i(B)$ 的值。分别将 $\xi^{j(A)}$、$\xi^{i(B)}$、$\xi^{j(B)}$、$\xi^{j'}$ 记为 α、x、β、γ；特别地，

$$A = 1 + 2\alpha \quad \text{and} \quad B = x(1 + 2\beta).$$

由山田公式（引理 1），我们得到

$$A + B = (1 + x + 2\sqrt{x})(1 + 2\gamma), \tag{7}$$

其中 $(1 + x + 2\sqrt{x}) \in \mathcal{T}$. 请记住，我们希望找到 x。展开后，（7）变为

$$2(1 + x)\gamma = 2(\alpha + x\beta + \sqrt{x}),$$

这等价于

$$(1+\overline{x})\overline{\gamma}=\overline{\alpha}+\overline{x}\overline{\beta}+\sqrt{\overline{x}}.$$

将两边同时乘以 $\overline{\beta}+\overline{\gamma}$，并记 $T=(\overline{\beta}+\overline{\gamma})\sqrt{\overline{x}}$，我们将其改写为

$$T^2+T+(\overline{\alpha}+\overline{\gamma})(\overline{\beta}+\overline{\gamma})=0 \tag{8}$$

（注意，根据假设，$\overline{\beta}+\overline{\gamma}\neq 0$ 因为 $j(B)$ 和 j' 属于不同的陪集。）现在我们考虑两种情形。

情形1。假设 $\mathrm{Tr}\big((\overline{\alpha}+\overline{\gamma})(\overline{\beta}+\overline{\gamma})\big)=0$。根据引理 3，方程（8）存在一个非零解 T。由 T，我们得到$\overline{x}=T^2/(\overline{\beta}+\overline{\gamma})^2$, x，以及 $i(B)=\log_{\overline{\xi}}\overline{x}=\log_{\xi}x$。由（7）可知，$j(A+B)=j'$，这正是所需的，并且 (*) 成立，其中

$$j(A)\in\mathcal{A},\quad j(B)\in\mathcal{B},\quad j(A+B)\in\mathcal{C}.$$

情形2。假设 $\mathrm{Tr}\big((\overline{\alpha}+\overline{\gamma})(\overline{\beta}+\overline{\gamma})\big)=1$。根据 $\mathrm{Tr}(\overline{\alpha}+\overline{\gamma})$ 和 $\mathrm{Tr}(\overline{\beta}+\overline{\gamma})$ 的取值，以下至少有一个成立：

$$\mathrm{Tr}\big((\overline{\alpha}+\overline{\gamma})(\overline{\beta}+\overline{\gamma}+1)\big)=0, \tag{9}$$

$$\mathrm{Tr}\big((\overline{\alpha}+\overline{\gamma}+1)(\overline{\beta}+\overline{\gamma})\big)=0, \tag{10}$$

$$\mathrm{Tr}\big((\overline{\alpha}+\overline{\gamma}+1)(\overline{\beta}+\overline{\gamma}+1)\big)=0. \tag{11}$$

在子情形（11）中，将 $\overline{\gamma}$ 替换为 $\overline{\gamma}+1$（这会将 j' 改为 $\log_{\overline{\xi}}(\overline{\xi}^{j'}+1)$ 并将其移至 $-\mathcal{C}$），即可使方程（8）有解，并证明 (*) 成立，其中

$$j(A)\in\mathcal{A},\quad j(B)\in\mathcal{B},\quad j(A+B)\in-\mathcal{C}.$$

在子情形（9）中，将 $\overline{\beta}$ 替换为 $\overline{\beta}+1$（这会改变 $j(B)$ 的选择，并将其移至 $-\mathcal{B}$），可使方程有解，并证明 (*)，其中

$$j(A)\in\mathcal{A},\quad j(B)\in-\mathcal{B},\quad j(A+B)\in\mathcal{C}.$$

子情形（10）可用类似方法解决：同时将 $\overline{\beta}$ 替换为 $\overline{\beta}+1$，并将 $\overline{\gamma}$ 替换为 $\overline{\gamma}+1$。 □

定理 2. 若 s 可被 3 整除，则对任意大小为 s 的 Cos 中的陪集 $\mathcal{A}$，存在 A、$B\in\mathcal{R}$，使得 $j(-A-B)=2^{\delta}j(B)=2^{2\delta}j(A)$ 或 $j(A+B)=2^{\delta}j(B)=2^{2\delta}j(A)$，其中$\delta=s/3$ 且 $j(A)=j\in\mathcal{A}$。

证明。当 s 能被 3 整除时，对于 Cos 中一个大小为 s 的给定陪集 $\mathcal{A}$，我们需要证明存在 $j\in\mathcal{A}$ 和 $x_2\in\mathcal{T}$，使得 $A=1+2y$、$B=x_2(1+2y^{2^{\delta}})$，且 $A+B=u_0(1+2y^{2^{2\delta}})$ 或 $-A-B=u_0(1+2y^{2^{2\delta}})$，其中 $y=\xi^j$ 和 $u_0=1+x_2+2\sqrt{x_2}$ 来自山田公式（引理 1）。与定理 1 中前面的讨论类似，我们需要证明存在 $j\in\mathcal{A}$ 和 $\overline{y}=\overline{\xi}^j\in F_{2^{\Delta}}$，使得

$$\mathrm{Tr}\big((\overline{y}^{2^{\delta}}+\overline{y}^{2^{2\delta}})(\overline{y}+\overline{y}^{2^{2\delta}})\big)=0\quad\text{or}$$
$$\mathrm{Tr}\big((\overline{y}^{2^{\delta}}+1+\overline{y}^{2^{2\delta}})(\overline{y}+1+\overline{y}^{2^{2\delta}})\big)=0.$$

根据引理 2，

$$\begin{aligned}&\mathrm{Tr}\big((\overline{y}^{2^{\delta}}+1+\overline{y}^{2^{2\delta}})(\overline{y}+1+\overline{y}^{2^{2\delta}})\big)\\&=\mathrm{Tr}\big((\overline{y}^{2^{\delta}}+\overline{y}^{2^{2\delta}})(\overline{y}+\overline{y}^{2^{2\delta}})+(\overline{y}^{2^{\delta}}+\overline{y}^{2^{2\delta}})+(\overline{y}+\overline{y}^{2^{2\delta}})+1\big)\\&=\mathrm{Tr}\big((\overline{y}^{2^{\delta}}+\overline{y}^{2^{2\delta}})(\overline{y}+\overline{y}^{2^{2\delta}})\big)+1.\end{aligned}$$

因此，上述方程中至少有一个成立。 □

本节的主要结果如下定理所示。

定理 3. 对每个奇数 Δ，$\mathcal{R}\backslash\{0\}$都存在一个划分，由 $2^{\Delta}-1$ 个形如 $\{a,2a,3a\}$ 的三元组以及 $\frac{(2^{\Delta}-1)(2^{\Delta}-2)}{6}$ 个形如 $\{\pm a,\pm b,\pm(a+b)\}$ 的六元组组成，使得该划分在乘以 ξ 的作用下保持不变；若 $\Delta\not\equiv 0 \bmod 3$，则在 GR($4^{\Delta}$) 的自同构作用下也保持不变。

证明。容易看出，$(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})\backslash\{0\}$ 可以划分为 $2^{\Delta}-1$ 个三元组 $\{\xi^i,2\xi^i,3\xi^i\}$, $i=0,\ldots,2^{\Delta}-2$，且该划分在乘以 ξ后保持不变。

接下来需要将 $\mathcal{R}\backslash(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})$划分为$(2^{\Delta}-1)(2^{\Delta}-2)$个所需形式的/6 六元组。我们先证明以下结论：

(*) *There are* $(2^{\Delta}-2)/6$ *pairs* (A,B), $A,B\in\mathcal{R}\backslash(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})$ *such that every* j *in* $\{1,\ldots,2^{\Delta}-2\}$ *is uniquely represented as* $j(A)$, $j(B)$, $j(-A-B)$, $j(-A)$, $j(-B)$, *or* $j(A+B)$ *for one of these pairs.*

为证明(*)，我们将集合 $\{1,\ldots,2^{\Delta}-2\}$ 划分为集合 $\bigcup_{\mathcal{A}\in\mathrm{Cos}(s)}\mathcal{A}$，并针对每个 s 构造 $N_s\cdot s/6$ 对，以同(*)中相同的意义覆盖相应集合。此步骤分为两个子情形，取决于3是否整除 s。

(i) 若 $s>1$ 不能被3整除，则存在 $N_s\cdot s/6$对(A,B)，$A,B\in\mathcal{R}\backslash(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})$，使得$\bigcup_{\mathcal{A}\in\mathrm{Cos}(s)}\mathcal{A}$ 中的每个j 都能唯一表示为 $j(A)$、$j(B)$、$j(-A-B)$、$j(-A)$、$j(-B)$或 $j(A+B)$，其中某一对取自这些对。

- （i）的证明。根据定理 1，存在 $A_1,B_1,\ldots,A_k,B_k$，其中 $k=N_s/6$，使得 $j(A_i)$、$j(B_i)$、$j(-A_i-B_i)$、$j(-A_i)$、$j(-B_i)$、$j(A_i+B_i)$、$i=1,\ldots,k$ 表示 Cos(s) 中的所有陪集。换言之，$\bigcup_{\mathcal{A}\in\mathrm{Cos}(s)}\mathcal{A}$可以分解为如下集合 $\pm\mathcal{A}_i\cup\pm\mathcal{B}_i\cup\pm\mathcal{C}_i$，其中 $i=1,\ldots,k$。不失一般性，设 $j(A_i)\in\mathcal{A}_i$、$j(B_i)\in\mathcal{B}_i$且 $j(A_i+B_i)\in\mathcal{C}_i$，其中 $i=1,\ldots,k$。设 f 为第 II-A 节中定义的 GR(4^{Δ}) 的自同构。记 $f^l(A_i)$、$f^l(B_i)$ 为 $A(l)_i$，$B(l)_i$，其中$l=0,1,2,\ldots,s-1$。由于 f^l是同态，我们有

$$j(A_i^{(l)})=2^l j(A_i),\quad j(B_i^{(l)})=2^l j(B_i),\quad\text{and}$$
$$j(A_i^{(l)}+B_i^{(l)})=j((A_i+B_i)^{(l)})=2^l j(A_i+B_i).$$

容易看出

$$\begin{aligned} 2^l j(A_i) &\in \mathcal{A}_i, & 2^l j(-A_i) &\in -\mathcal{A}_i,\\ 2^l j(B_i) &\in \mathcal{B}_i, & 2^l j(-B_i) &\in -\mathcal{B}_i,\\ 2^l j(A_i+B_i) &\in \mathcal{C}_i, & 2^l j(-A_i-B_i) &\in -\mathcal{C}_i. \end{aligned}$$

更确切地说,

$$\begin{aligned} \mathcal{A}_i &= \{2^l j(A_i)\}_l, & -\mathcal{A}_i &= \{2^l j(-A_i)\}_l,\\ \mathcal{B}_i &= \{2^l j(B_i)\}_l, & -\mathcal{B}_i &= \{2^l j(-B_i)\}_l,\\ \mathcal{C}_i &= \{2^l j(A_i+B_i)\}_l, & -\mathcal{C}_i &= \{2^l j(-A_i-B_i)\}_l \end{aligned}$$

其中包含 $l=0$、1、2、.....、$s-1$。不难发现, $\bigcup_{\mathcal{A}\in \mathrm{Cos}(s)\mathcal{A}}$ 可以表示为

$$\bigcup_{i=1}^{k}\bigcup_{l=0}^{s-1}\Big\{ j\big(A_i^{(l)}\big),\ j\big(B_i^{(l)}\big),\ j\big(A_i^{(l)}+B_i^{(l)}\big),\\ j\big(-A_i^{(l)}\big),\ j\big(-B_i^{(l)}\big),\ j\big(-A_i^{(l)}-B_i^{(l)}\big)\Big\}.$$

因此, 这些满足 $1\le i\le k$、 $0\le l\le s-1$ 的配对 $(A_i^{(l)},\ B_i^{(l)})$ 满足 (i) 的结论。

(ii) 如果 s 能被 3 整除, 那么对于每个属于 Cos(s) 的 $\mathcal{A}$, 都存在 $s/3$ 对 (A,B)、 $A,B\in\mathcal{R}\backslash(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})$, 使得每个 $\pm\mathcal{A}$ 中的 j 都能唯一表示为这些对中的一对所对应的 $j(A)$、 $j(B)$、$j(-A-B)$、 $j(-A)$、 $j(-B)$ 或 $j(A+B)$。

(ii) 的证明。由定理 2, 对于任意 $\mathcal{A}\in$Cos(s), 存在 $A,B\in\mathcal{R}$ 使得

$$j(-A-B)=2^\delta j(B)=2^{2\delta}j(A) \tag{12}$$

$$\text{or}\quad j(A+B)=2^\delta j(B)=2^{2\delta}j(A), \tag{13}$$

其中 $\delta=s/3$ 和 $j(A)=j\in\mathcal{A}$。我们假设 (12) 成立 ((13) 的情形类似)。令 f 为 II-A 节中定义的 GR(4^Δ) 的自同构。记 $f^l(A)$ 为 $A^{(l)}$, 其中 $l=0,1,2,\ldots,s-1$。由于 f^l 是同态, 我们有

$$\begin{aligned} j(A^{(l)}) &= 2^l j(A), & j(-A^{(l)}) &= 2^l j(-A),\\ j(B^{(l)}) &= 2^{\delta+l} j(A), & j(-B^{(l)}) &= 2^{\delta+l} j(-A),\\ j(-A^{(l)}-B^{(l)}) &= 2^{2\delta+l} j(A), & & \end{aligned}$$

$$\text{and}\quad j(A^{(l)}+B^{(l)})=2^{2\delta+l}j(-A).$$

对于这样的 A, 我们有

$$\begin{aligned} \mathcal{A} &= \{2^l j(A): 0\le l\le s-1\}\\ &= \bigcup_{i=0,1,2}\big\{2^{l+i\delta}j(A): 0\le l\le \delta-1\big\}, \end{aligned}$$

以及 (另见引理 5)

$$\begin{aligned} -\mathcal{A} &= \{2^l j(-A): 0\le l\le s-1\}\\ &= \bigcup_{i=0,1,2}\big\{2^{l+i\delta}j(-A): 0\le l\le \delta-1\big\}. \end{aligned}$$

现在很容易看出

$$\mathcal{A}=\bigcup_{0\le l\le\delta-1}\big\{j(A^{(l)}), j(B^{(l)}), j(-A^{(l)}-B^{(l)})\big\},$$

and

$$-\mathcal{A}=\bigcup_{0\le l\le\delta-1}\big\{j(-A^{(l)}), j(-B^{(l)}), j(A^{(l)}+B^{(l)})\big\}.$$

因此, 满足 $0\le l\le\delta-1$ 的数对 $(A^{(l)},B^{(l)})$ 满足 (ii) 的结论。

由于 $\{1,\ldots,2^\Delta-2\}$ 被划分为 (i) 和 (ii) 中考虑的集合, (*) 的证明完成。接着, 对于这样的 $(2^\Delta-2)/6$ 个数对 (A,B), 数对 (xA,xB) 也可以进行相同的操作, 其中 $x\in\mathcal{T}\setminus\{0\}$。因此,

$$\big\{\pm xA_i,\ \pm xB_i,\ \pm x(A_i+B_i)\big\}_{1\le i\le(2^\Delta-2)/6,\ x\in\mathcal{T}\setminus\{0\}}$$

与 $\mathcal{R}\backslash(\mathcal{T}\cup 2\mathcal{T}\cup 3\mathcal{T})$ 一致。接下来只需指出以下事实, 它们保证了所构造划分所需的对称性。首先, $\mathcal{T}\setminus\{0\}$ 在乘以 ξ 后保持不变。其次, 若 $s>1$ 不能被 3 整除, 则所有非空的 Cos(s) 都属于情形 (i), 且根据该情形中的构造, 所得划分在环自同构下保持不变。最后, 若 s 能被 3 整除, 则 Cos(s) 中的每个 $\pm\mathcal{A}$ 都属于情形 (ii), 该情形在环自同构下也保持不变。

□

IV. 准循环 1-完美码

根据引理 4, 上一节中构造的划分对应于 ( ) , ( )) 中的一个 1 $D\big(\ 2^\Delta-1\ \frac{2^\Delta-2}{6}\ \ 2^\Delta-$ - 1 完美码。校验矩阵的列集合在乘以 ξ 后保持不变, 而该乘法在坐标上诱导出一个置换, 其由阶为 $(2^\Delta-1)$ 的循环组成。

推论 1. 设 Δ 为奇数。设 ξ 是任意一个次数为 Δ、定义在 $\mathbb{Z}_4$上的基本本原不可约多项式的根。设 H是由 $(2^\Delta-1)_{(2^\Delta-2)\,6}$对列向量 (a,b) 组成的、定义在 $\mathbb{Z}_4$上的 $\Delta\times\frac{2^{2\Delta}-1}{3}$矩阵; 其中左侧部分的 $\{\pm a,\pm b,\pm(a+b)\}$ 是定理 3 中的六元组, 右侧部分为 $2^\Delta-1$ 列 ξ^i, $0\le i\le 2^\Delta-2$。以下结论成立:

- 由校验矩阵 H 定义的码 C 是 $D\big((2^\Delta-1)\frac{2^\Delta-2}{6}$ 中的 1- 完美码, $(2^\Delta-1)\big)$;
- 将每一列乘以 ξ 所对应的坐标置换是该码的一个自同构;
- 如果 Δ 不能被 3 整除, 那么对应于 GR(4^Δ) 的环自同构的坐标置换。

以下命题的证明与[13, 第 4 节4]中的证明相同。我们省略完整证明, 仅说明其思路。区分这些码的不变量是: 三个非零位置均位于码字右半部分的重量 3 码字的数量。每个加性 1-完美码在 $D\big((2^\Delta-1)\frac{2^\Delta-2}{6}$、 $0+(2^\Delta-1)\big)$ 中都有 $(2^\Delta-1)(2^\Delta-2)/6$

个阶为 2 的此类码字。拟循环码没有阶为 4 的此类码字，而在 [13, 第 4 节4] 中递归构造的码则有。

命题2。 $D\big((2^{\Delta}-1)\frac{2^{\Delta}-2}{6}$、$0+(2^{\Delta}-1)\big)$ 中上文构造的每个码，都不等价于在 *[13,* 第3节。*3],* 中使用相应参数构造的任何码。

五、结论性 remarks

本文展示了如何在Doob图中构造加性1-完美码，使其在阶为 $2^{\Delta}-1$的坐标拟循环置换下保持不变。如果 Δ 不能被3整除，则推论 1中的校验矩阵的列集在阶为 Δ的环自同构下也保持不变。这保证了该码具有比推论 1中所声明的更高的对称性。例如，由于5与 2^5-1 互质，D(155, 31)中的码具有阶为 $155 = 5\cdot(2^5-1)$的置换自同构，该自同构分别对两组坐标进行循环置换。按照 [1]的意义，这样的码可以称为循环码。在$D\big((2^{\Delta}-1)\frac{2^{\Delta}-2}{6}$、$(2^{\Delta}-1)\big)$ 中构造循环1-完美码且参数为 $\Delta \geq 7$ 的问题仍未解决。

另一个有趣的方向是进一步研究 $\mathbb{Z}_4$ 上的模的划分，例如我们在第三节中构造的划分，探究它们在离散几何中的地位，将其推广到其他环，并寻求其在编码理论中的应用。注意，如 [4], 所示，非素有限域上的加性1-完美码与扩张有关，这种关系类似于 Doob图中的完美码与本文所研究的 GR(4^{Δ})划分之间的关系。扩张是被广泛研究的对象 [6], ，我们认为，对有限环进行不同的推广（包括本文所研究的推广）值得关注。

参考文献

[1] J. Borges、C. Fern´andez-C´ordoba，《恰好存在一个 Z_2Z_4-循环1-完美码》，Des. Codes Cryptogr.，第85卷，第3期，第557–566页，2017年。[2] M. Braun、T. Etzion、P. R. J. ¨Osterg˚ard、A. Vardy、A. Wassermann，《Steiner系统的 q类比的存在性》，Forum Math. Pi，第4卷，e7号，第1–14页，2016年。[3] P. Delsarte，《编码理论关联方案的代数方法》，Philips Res. Rep.增刊第10卷。N.V. Philips' Gloeilampenfabrieken，埃因霍温，1973年。[4] M. Herzog、J. Sch¨onheim，《线性与非线性单错纠正完美混合码》，Inf. Control，第18卷，第4期，第364–368页，1971年。[5] K. Huber，《艾森斯坦–雅可比整数上的码》。载于《有限域：理论、应用与算法》（美国内华达州拉斯维加斯，1993年），Contemp. Math.第168卷，第165–179页，美国罗德岛州普罗维登斯，1994年。美国数学学会。[6] N. L. Johnson，《扩张与平行类的组合学》，Pure Appl. Math.（博卡拉顿）第295卷。CRC出版社，美国佛罗里达州博卡拉顿，2010年。[7] J. H. Koolen、A. Munemasa，《Doob图中的紧2-设计与完美1-码》，J. Stat. Plann. Inference，第86卷，第2期，第505–513页，2000年。[8] D. S. Krotov，《Doob图中的完美码》，Des. Codes Cryptogr.，第80卷，第1期，第91–102页，2016年。[9] D. S. Krotov，《关于 Doob方案中的对偶码》，载于 IEEE信息论国际研讨会，法国巴黎，2019年7月7–12日，第1917–1921页。IEEE，2019年。[10] D. S. Krotov，《Doob图中完美码的存在性》，IEEE Trans. Inf. Theory，第66卷，第3期，第1423–1427页，2020年。[11] R. Lidl、H. Niederreiter，《有限域》，Encycl. Math. Appl.第20卷。剑桥大学出版社，英国剑桥，1997年。[12] C. Mart´ınez、E. Stafford、R. Beivide、E. M. Gabidulin，《用 Eisenstein–Jacobi图建模六边形星座》，Probl. Inf. Transm.，第44卷，第1期，第1–11页，2008年。译自 Probl. Peredachi Inf.第44卷，第1期，第3–14页，2008年。[13] M. Shi、D. Huang、D. S. Krotov，《Doob图中的加性完美码》，Des. Codes Cryptography，第87卷，第8期，第1857–1869页，2019年。[14] Z. X. Wan，《四元码》，Series on Applied Mathematics第8卷。World Scientific，1997年。