arXiv:2304.02913v1 [cs.IT] 6 Apr 2023

非链环类上的可逆循环码与可逆补循环码

NIKITA JAIN、SUCHETA DUTT 和 RANJEET S EHMI

Abstract. 本文建立了任意长度的循环码在非链环 $Z_4+\nu Z_4$ for $\nu^2 \in \{0, 1, \nu, 2\nu, 3\nu, 2+\nu、\ 2+3\nu、\ 3+2\nu\}$ 上的循环码成为可逆循环码的充要条件。此外，还确定了这些非链环上的循环码成为可逆互补循环码的必要且充分条件。最后还给出了这些环上可逆循环码和可逆互补循环码的一些示例。

1. Introduction

在代数编码理论中，循环码类是码的重要类别之一。继 Calderbank等人的重要工作之后，循环码在环上的研究得到了广泛开展，其中引入了格雷映射，以表明一些非线性二元码可以被视为环上 Z_4的线性码的二元图像。 [1]

可逆码是一类重要的码，在 DNA 计算和检索系统中发挥着作用。J. Massey 首先引入了域上的可逆码 [2]。Abualrub 和 Siap 给出了判定 Z_4 上奇数长度循环码为可逆循环码的充要条件 [3]。H. Islam 和 O. Parkash 给出了判定 Z_{p^k} 上长度为 n 且与 p 互素的循环码为可逆码的条件 [4]。J. Kaur 等人研究了伽罗瓦环上的可逆循环码 [5]。Srinivasulu 和 Bhaintwal 得出了有限链环 $F_4+\nu F_4$、$\nu^2=0$ 上任意长度可逆循环码的结构 [6]。J. Liu 和 H. Liu 确定了环 $F_4+\nu F_4+\nu^2 F_4$、$\nu^3=0$ 上任意长度可逆循环码的结构 [7]。O. Parkash 等人给出了判定 $F_q+\nu F_q+\cdots+\nu^{k-1}F_q$、$\nu^k=0$ 和$k\geq 2$ 上的循环码为任意长度可逆循环码的条件 [8, 9]。S. Pattanayak、A. Kumar 建立了判定非链环 $Z_4+\nu Z_4$、$\nu^2=0$ 上奇数长度循环码为可逆循环码的充要条件 [10]；H. Dinh 等人则给出了非链环 $Z_4+\nu Z_4$、$\nu^2=1$ 上的相关条件 [11]。

由于在基于 DNA 的计算中有着广泛的应用，许多研究者也对可逆补循环码进行了深入研究。关于不同环 [12, 13, 14, 15] 上的可逆补循环码，已有大量文献。循环码成为

Key words and phrases. 循环码、可逆、补码。NIKITA JAIN 谨向印度科学与工业研究委员会（CSIR）致谢，感谢其提供研究资助。

伽罗瓦环上的可逆补循环码的充要条件已由 J.Kaur 等人给出 [15]。S. Pattanayak、A.Kumar [10] 已确立非链环 $Z_4+\nu Z_4, \nu^2=0$上奇数长度循环码成为可逆补循环码的充要条件；H. Dinh 等人 [11]则给出了非链环$Z_4+\nu Z_4$, $\nu^2=1$ 上的相关充要条件。

本文结构安排如下：第 2 节回顾一些基本定义。第 3 节给出了在环 $Z_4+\nu Z_4$ for $\nu^2\in\{0,\nu,2\nu,3\nu,1,3+2\nu,2+\nu,2+3\nu\}$ 上，循环码成为可逆循环码的充分必要条件。第 4 节确定了在环 $Z_4+\nu Z_4$ for $\nu^2\in\{0,\nu,2\nu,3\nu,1,3+2\nu,2+\nu,2+3\nu\}$ 上，循环码成为可逆补循环码的充分必要条件。

2. 预备知识

设 R 是一个有限含幺交换环。如果环 R 的所有理想在包含关系下构成一条链，则称 R 为链环；否则称 R 为非链环。长度为 n 的 R 上的线性码 C 是 R^n 的一个 R-子模，其元素称为 C 的码字。对于码字 $(s_0, s1, \cdots, s_{n-1}) \in C$，如果 $(s_{n-1}, s0, \cdots, s_{n-2}) \in C$，则称 C 为 R 上长度为 n 的循环码。码字 $s=(s_0, s1, \cdots, s_{n-1})$ 可由其多项式表示 $s(z)=s_0+s_1z+\cdots+s_{n-1}z^{n-1}$ 表示，而 R 上的循环码 C 可视为商环 $R[z]/\langle z^n-1\rangle$. 的一个理想。如果对于 C 中的每个 $s=(s_0, s1, \cdots, s_{n-1})$，码字 $s^r=(s_{n-1}, s_{n-2}, \cdots, s_0)$ 也属于 C，则称线性码 C 为可逆码。次数为 $k\le n-1$ 的多项式 $g(z)$ 的 $g^*(z)=z^kg(z^{-1})$ 定义为其倒数多项式。当且仅当 $g^*(z)=g(z)$ 时，多项式 $g(z)$ 称为自倒数多项式。

在以下引理中，我们回顾一些继续进行所需的结果。

引理 2.1. [5] 设 C 是 R 上由 $g_1(z)\ g_2(z)\ \cdots, g_k(z)$ 生成的循环码。那么 C 是可逆循环码，当且仅当 $g_i^*(z)\in C$ 对于 $1\le i\le k$。

引理 2.2. [5] 设 $g_1(z)\ g_2(z)$ 是 $R[z]$ 中任意两个多项式，且 deg $g_1(z)\ge$deg $g_2(z)$。则

(i) $\big(g_1(z)+g_2(z)\big)^*=g_1^*(z)+z^ig_2^*(z)$, 其中 $i=$deg $g_1(z)-$ deg $g_2(z)$,
(ii) $\big(g_1(z)g_2(z)\big)^*=g_1^*(z)g_2^*(z)$ 】【。

引理2.3. [16] 设 $C=\langle g(z)+2p(z)\ 2a(z)\rangle$ 是一个长度为 n、定义在Z_4上的循环码，其中 $g(z)$ $p(z)$ 和 $a(z)$ 是满足以下条件的二元多项式： $a(z)|g(z)|z^n-1$，且 $p(z)=0$ 或 $a(z)|p(z)\left(\frac{z^n-1}{g\ z}()\right)$，其中 deg $a(z)>$ deg $p(z)$。那么，C 是 Z_4 上的可逆循环码，当且仅当

(a) $g(z)$和 $a(z)$ 是自反互易的，(b) $a(z)|(z^\lambda p^*(z)-p(z))$，其中 $\lambda=$ deg $g(z)-$ deg $p(z)>0$。

环 $Z_4+\nu Z_4$、 $\nu^2\in Z_4+\nu Z_4$ 是环 Z_4 的扩展，Adel Alahmadi 等人 [17]已将其分类为链环和非链环。他们证明，对于 $\nu^2\in\{2,3,1+\nu,3+\nu,1+2\nu,2+2\nu$、$1+3\nu$、 $3+3\nu\}$， $Z_4+\nu Z_4$是链环；对于 $\nu^2\in\{0,\nu,2\nu,3\nu,1,3+2\nu,2+\nu,2+3\nu\}$.，则是非链环。本文中，我们将非链环 $Z_4+\nu Z_4$、 $\nu^2=\theta$ 记为 R_θ，其中 $\theta\in S$，且 $S=\{0,\nu,2\nu,3\nu,1,3+2\nu,2+\nu,2+3\nu\}$.。其完整结构为

N. Jain 等人[18]已建立了 R_θ, $\theta \in S$ 上任意长度的循环码。为求完整起见，我们回顾所需的结果。

设 C_θ 是 R_θ, $\theta \in S$ 上长度为 n 的循环码。定义 $\phi_\theta: R_\theta \to Z_4$ as$\phi_\theta(x) = x(\text{mod } k_\theta)$, 其中 $x \in R_\theta$,

$$k_\theta = \begin{cases} \nu & ;\theta \in \{0, \nu, 2\nu, 3\nu\}, \\ 1+\nu & ;\theta \in \{1, 3+2\nu\}, \\ 2+\nu & ;\theta \in \{2+\nu, 2+3\nu\}. \end{cases}$$

映射 ϕ_θ 可自然扩展为映射 $\phi_\theta: C_\theta \to Z_4[z]/\langle z^n-1\rangle$ as$\phi_\theta\left(s_0 + s_1 z + \cdots + s_{n-1} z^{n-1}\right) = \phi_\theta(s_0) + \phi_\theta(s_1)z + \cdots + \phi_\theta(s_{n-1})z^{n-1}$. 然后，$\phi_\theta$ 的核以及 C_θ 的挠子定义为 $ker_\theta = \{a(z) \in C_\theta$，使得 $\phi_\theta(a(z)) = 0\}$，以及 Tor(C_θ)=$\{b(z) \in \frac{Z_4[z]}{\langle z^n-1\rangle}: k_\theta b(z) \in C_\theta\}$。

引理 2.4. [18] 设 C_θ 是任意长度为 n 的环 $R_\theta, \theta \in S$上的循环码。那么C_θ 由多项式 $g_{\theta_1}(z)$ $g_{\theta_2}(z)$ $g_{\theta_3}(z)$唯一生成，
$g_{\theta_4}(z)$，其中 $g_{\theta_1}(z) = g_{11}(z) + 2g_{12}(z) + k_\theta g_{13}(z) + 2k_\theta g_{14}(z)$，$g_{\theta_2}(z) = 2g_{22}(z) + k_\theta g_{23}(z) + 2k_\theta g_{24}(z)$，$g_{\theta_3}(z) = k_\theta g_{33}(z) + 2k_\theta g_{34}(z)$，$g_{\theta_4}(z) = 2k_\theta g_{44}(z)$，使得多项式 $g_{ij}(z)$ 属于 $Z_2[z]/\langle z^n-1\rangle$，其中 $1 \le i \le 4$、$i \le j \le 4$，并满足条件

$$g_{22}(z) | g_{11}(z) | z^n - 1,\ g_{44}(z) | g_{33}(z) | z^n - 1,$$
$$g_{22}(z) | g_{12}(z)\frac{z^n-1}{g_{11}(z)},\ g_{44}(z) | g_{34}(z)\frac{z^n-1}{g_{33}(z)}.$$

此外，对于 $1 \le i \le 3$，要么 $g_{ij}(z) = 0$ or deg $g_{ij}(z) <$ deg $g_{jj}(z)$，$i < j \le 4$. 进一步，$\phi_\theta(C_\theta) = \langle g_{11}(z) + 2g_{12}(z)\ 2g_{22}(z)\rangle$ 并且 $ker_\theta = k_\theta\langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$.

3. Reversible cyclic codes over R_θ

本节中，我们证明了 $R_\theta, \theta \in S$ 上可逆循环码的挠子码是 Z_4. 上的可逆循环码。此外，我们得到了循环码 C_θ 成为 $R_\theta, \theta \in S$ 上可逆循环码的充要条件。

定理 3.1. 设 $C_\theta = \langle g_{\theta_1}(z)\, g_{\theta_2}(z)\, g_{\theta_3}(z)\, g_{\theta_4}(z)\rangle$ 是环 $R_\theta, \theta \in S$ 上任意长度 n 的可逆循环码，其中 $g_{\theta_1}(z) = g_{11}(z)+2g_{12}(z)+k_\theta g_{13}(z)+2k_\theta g_{14}(z)$，$g_{\theta_2}(z) = 2g_{22}(z) + k_\theta g_{23}(z) + 2k_\theta g_{24}(z)$，$g_{\theta_3}(z) = k_\theta g_{33}(z) + 2k_\theta g_{34}(z)$，$g_{\theta_4}(z) = 2k_\theta g_{44}(z)$，使得多项式 $g_{ij}(z)$ 属于 $Z_2[z]/\langle z^n-1\rangle$，其中 $1 \le i \le 4$，$i \le j \le 4$.。那么 Tor(C_θ) $= \langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$ 是 Z_4. 上的可逆循环码

证明。$C_\theta = \langle g_{\theta_1}(z)\, g_{\theta_2}(z)\, g_{\theta_3}(z)\, g_{\theta_4}(z)\rangle$ 是环 $R_\theta, \theta \in S$ 上任意长度 n 的可逆循环码。根据引理 2.4，我们有 $ker_\theta = k_\theta\langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$. 因此，Tor($C_\theta$) $= \langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$。由于 $k_\theta(g_{33}(z) + 2g_{34}(z)) \in C_\theta$，且 C_θ 是可逆的，因此，根据引理 2.1，$k_\theta(g_{33}(z) + 2g_{34}(z))^* \in C_\theta$。由此可得，$(g_{33}(z) + 2g_{34}(z))^* \in$ Tor(C_θ)。同理，$(2g_{44}(z))^* \in$ Tor(C_θ)。因此，根据引理 2.1，Tor(C_θ) $= \langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$ 是 Z_4 上的可逆循环码。□

下面的引理易于证明。

引理 3.2. 设 C_θ 是长度为 n 的 R_θ, $\theta \in S$ 上的可逆循环码。那么$\phi_\theta(C_\theta)$ 是 Z_4. 上的可逆循环码

以下定理给出了任意长度 n 的循环码 C_θ 在 R_θ 上成为可逆循环码的充分必要条件。

定理 3.3. 设 $C_\theta = \langle g_{\theta_1}(z)\, g_{\theta_2}(z)\, g_{\theta_3}(z)\, g_{\theta_4}(z)\rangle$ 是长度任意的 n 上的循环码，其中环 R_θ, $\theta \in S$, 且 $g_{\theta_1}(z) = g_{11}(z) + 2g_{12}(z) + k_\theta g_{13}(z) + 2k_\theta g_{14}(z)$, $g_{\theta_2}(z) = 2g_{22}(z) + k_\theta g_{23}(z) + 2k_\theta g_{24}(z)$, $g_{\theta_3}(z) = k_\theta g_{33}(z) + 2k_\theta g_{34}(z)$, $g_{\theta_4}(z) = 2k_\theta g_{44}(z)$, 使得多项式 $g_{ij}(z)$ 属于 $Z_2[z]/\langle z^n - 1\rangle$，对 $1 \le i \le 4, i \le j \le 4$. 也有，要么 $g_{ij}(z) = 0$，要么对 $1 \le i \le 3, i < j \le 4.$，$\deg g_{ij}(z) < \deg g_{jj}(z)$。令 $g_1(z) = g_{13}(z) + 2g_{14}(z)$, $g_2(z) = g_{23}(z) + 2g_{24}(z) \in Z_4[z].$。那么，当且仅当 C_θ 是环 R_θ 上的可逆循环码时， hәрбий

(i) $g_{ii}(z)\ 1 \le i \le 4$均为自反多项式，(ii) $g_{44}(z)|z^\alpha g_{34}^*(z) - g_{34}(z)$，其中 $\alpha = \deg g_{33}(z) - \deg g_{34}(z) > 0$, (iii) $2(z^\beta g_{12}^*(z) - g_{12}(z)) + k_\theta(z^\gamma g_1^*(z) - g_1(z)) \in C_\theta$，其中 $\beta = \deg g_{11}(z) - \deg g_{12}(z) > 0$ 且 $\gamma = \deg g_{11}(z) - \deg g_1(z) > 0$, (iv) $z^\delta g_2^*(z) - g_2(z) \in \mathrm{Tor}(C_\theta)$，其中 $\delta = \deg g_{22}(z) - \deg g_2(z) \ge 0.$

证明。首先，设 C_θ 是 R_θ上长度为 n 的可逆循环码。由引理 2.4 和引理 3.2 可得 $\phi_\theta(C_\theta) = \langle g_{11}(z) + 2g_{12}(z)\ 2g_{22}(z)\rangle$是 Z_4上的可逆循环码。此外，由定理 3.1 可知，$\mathrm{Tor}(C_\theta) = \langle g_{33}(z) + 2g_{34}(z)\ 2g_{44}(z)\rangle$是 Z_4上的可逆循环码。由引理 2.3 可得，$g_{11}(z)\ g_{22}(z)\ g_{33}(z)$ 和 $g_{44}(z)$ 是自反多项式，且 $g_{44}(z)|z^\alpha g_{34}^*(z) - g_{34}(z)$，其中 $\alpha = \deg g_{33}(z) - \deg g_{34}(z) > 0.$。这证明了条件 (i) 和 (ii)。由于 C_θ 是可逆的，利用引理 2.1、引理 2.2 以及 $g_{11}(z)$ 的自反性，可得 $(g_{11}(z)+2g_{12}(z)+k_\theta g_1(z))^* = g_{11}^*(z) + 2z^\beta g_{12}^*(z) + k_\theta z^\gamma g_1^*(z) = g_{11}(z) + 2z^\beta g_{12}^*(z) + k_\theta z^\gamma g_1^*(z) \in C_\theta$，其中 $\beta = \deg g_{11}(z) - \deg g_{12}(z) > 0$且 $\gamma = \deg g_{11}(z) - \deg g_1(z) > 0$。这意味着，

$$g_{11}(z) + 2z^\beta g_{12}^*(z) + k_\theta z^\gamma g_1^*(z) = A(z)\big(g_{11}(z) + 2g_{12}(z) + k_\theta g_1(z)\big) + B(z)\big(2g_{22}(z) + k_\theta g_2(z)\big) + k_\theta C(z)\big(g_{33}(z) + 2g_{34}(z)\big) + k_\theta D(z)\big(2g_{44}(z)\big) \tag{3.1}$$

对于某些 $A(z)\ B(z)\ C(z)\ D(z) \in R_\theta[z]$。将方程 (3.1) 两边分别乘以 $2k_\theta$for $\theta \in \{0, 1, 2\nu, 3 + 2\nu\}$ 和 $2(k_\theta - 1)$（ $\theta \in \{\nu, 3\nu, 2 + \nu, 2 + 3\nu\}$），我们得到

$$\begin{cases} 2k_\theta g_{11}(z) = 2k_\theta A(z) g_{11}(z) & \text{for } \theta \in \{0, 1, 2\nu, 3 + 2\nu\} \\ 2(k_\theta - 1) g_{11}(z) = 2(k_\theta - 1) A(z) g_{11}(z) & \text{for } \theta \in \{\nu, 3\nu, 2 + \nu, 2 + 3\nu\} \end{cases} \tag{3.2}$$

比较方程(3.2)两边的次数，我们发现 $A(z)$是常数。进一步观察到 $A(z) = 1 + 2a + k_\theta b$, 其中 $a \in Z_2$ 和$b \in Z_4$.将 $A(z)$ 的值代入方程 (3.1)，得到，$2z^\beta g_{12}^*(z) + k_\theta z^\gamma g_1^*(z) = 2g_{12}(z) + k_\theta g_1(z) + (2a + k_\theta b)\big(g_{11}(z) + 2g_{12}(z) + k_\theta g_1(z)\big) + B(z)\big(2g_{22}(z) + k_\theta g_2(z)\big) + k_\theta C(z)\big(g_{33}(z) + 2g_{34}(z)\big) + k_\theta D(z)\big(2g_{44}(z)\big)$，这意味着 $2\big(z^\beta g_{12}^*(z) - g_{12}(z)\big) + k_\theta\big(z^\gamma g_1^*(z) - g_1(z)\big) = (2a + k_\theta b)\big(g_{11}(z) + 2g_{12}(z) + k_\theta g_1(z)\big) + B(z)\big(2g_{22}(z) + k_\theta g_2(z)\big) + k_\theta C(z)\big(g_{33}(z) + 2g_{34}(z)\big) + k_\theta D(z)\big(2g_{44}(z)\big) \in C_\theta$·由此可得 $2\big(z^\beta g_{12}^*(z) - g_{12}(z)\big) + k_\theta\big(z^\gamma g_1^*(z) - g_1(z)\big) \in C_\theta$，这证明了条件$(iii)$。由于 C_θ是可逆的，利用引理2.1、引理2.2以及 $g_{22}(z)$ 的自反性，我们有$\big(2g_{22}(z) + k_\theta g_2(z)\big)^* = 2g_{22}^*(z) + k_\theta z^\delta g_2^*(z) = 2g_{22}(z) + k_\theta z^\delta g_2^*(z) \in C_\theta$，其中 $\delta =$次数

$g_{22}(z)-\deg g_2(z) \geq 0$。这意味着 $2g_{22}(z)+k_\theta g_2(z)+k_\theta\left(z^\delta g_2^*(z)-g_2(z)\right) \in C_\theta \cdot$ 由于 $2g_{22}(z)+k_\theta g_2(z) \in C_\theta$，可得 $k_\theta\left(z^\delta g_2^*(z)-g_2(z)\right) \in C_\theta$。因此，$z^\delta g_2^*(z)-g_2(z) \in \operatorname{Tor}(C_\theta)$。

反过来，假设所有条件（i）-（iv）均成立。为了证明 C_θ 是 R_θ 上的可逆循环码，根据引理 2.1，只需证明（$g_{11}(z)+2g_{12}(z)+k_\theta g_1(z)$）*，（$2g_{22}(z)+k_\theta g_2(z)$）*、$k_\theta$（$g_{33}(z)+2g_{34}(z)$）*以及 $2k_\theta$（$g_{44}(z)$）* $\in C_\theta \cdot$。利用引理 2.2 和条件（i），有（$g_{11}(z)+2g_{12}(z)+k_\theta g_1(z)$）* $=g_{11}^*(z)+2z^\beta g_{12}^*(z)+k_\theta z^\gamma g_1^*(z)=(g_{11}(z)+2g_{12}(z)+k_\theta g_1(z))+2(z^\beta g_{12}^*(z)-g_{12}(z))+k_\theta(z^\gamma g_1^*(z)-g_1(z))$，根据条件（$iii$），它属于 C_θ。再次利用引理 2.2 和条件（i），有（$2g_{22}(z)+k_\theta g_2(z)$）* $=2g_{22}^*(z)+k_\theta z^\delta g_2^*(z)=(2g_{22}(z)+k_\theta g_2(z))+k_\theta(z^\delta g_2^*(z)-g_2(z))$，根据条件（$iv$），它属于 C_θ。类似地，利用引理 2.2、条件（i）和（ii），有 $k_\theta(g_{33}(z)+2g_{34}(z))^*=k_\theta(g_{33}^*(z)+2z^\alpha g_{34}^*(z))=k_\theta(g_{33}(z)+2g_{34}(z))+2k_\theta(z^\alpha g_{34}^*(z)-g_{34}(z))=k_\theta(g_{33}(z)+2g_{34}(z))+2k_\theta s(z)g_{44}(z)$，其中某个 $s(z) \in Z_4[z].$。显然，它属于 $C_\theta \cdot$。最后，$2k_\theta(g_{44}(z))^*=2k_\theta g_{44}(z)$ 根据条件（i）属于 C_θ. □

以下示例说明了我们的结果。

例 3.4。设 $C_\theta=\langle z^3+z^2+z+1,\ 2(z^2+1)+2\nu, \nu(z^2+1)\ 2\nu(z+1)\rangle$ 是环 R_θ 上长度为 4 的循环码，其中 $\theta=2\nu.$。这里 $g_{11}(z)=z^3+z^2+z+1, g_{22}(z)=z^2+1, g_{33}(z)=z^2+1, g_{44}(z)=z+1, g_{12}(z)=0, g_{34}(z)=0,\ g_1(z)=0,\ g_2(z)=2.$。于是我们有，

(i) $g_{11}^*(z)=1+z+z^2+z^3, g_{22}^*(z)=1+z^2, g_{33}^*(z)=1+z^2, g_{44}^*(z)=1+z.$因此，$g_{ii}^*(z)=g_{ii}(z)$ 对于 $1 \leq i \leq 4.$(ii) 由于 $\alpha=2$ 且 $g_{34}(z)=0$，这意味着 $g_{44}(z)|z^2 g_{34}^*(z)-g_{34}(z)$。(iii) 由于 $\beta=\gamma=3$ 且 $g_{12}(z)=g_1(z)=0$，这意味着 $2\left(z^3 g_{12}^*(z)-g_{12}(z)\right)+\nu\left(z^3 g_1^*(z)-g_1(z)\right)=0 \in C_\theta \cdot$(iv) 由于 $\delta=2$ 且 $g_2^*(z)=2$，因此 $z^2 g_2^*(z)-g_2(z)=2z^2-2=(z-1)\left(2(z+1)\right) \in \operatorname{Tor}(C_\theta)$。

因此，C_θ 是一个可逆循环码，因为它满足定理 3.3 的所有条件。

例 3.5. 设 $C_\theta=\langle z^4+z^3+z+1, 2(z^2+z+1)+(2+\nu)(z^2+z+1), (2+\nu)(z^4+z^3+z+1), 2(2+\nu)(z^2+z+1)\rangle$ 是一个长度为 6 的循环码，定义在环 R_θ 上，其中 $\theta=2+\nu.$ Here $g_{11}(z)=z^4+z^3+z+1, g_{22}(z)=z^2+z+1, g_{33}(z)=z^4+z^3+z+1, g_{44}(z)=z^2+z+1, g_{12}(z)=0, g_{34}(z)=0, g_1(z)=0, g_2(z)=z^2+z+1.$ 我们有，

(i) $g_{11}^*(z)=1+z+z^3+z^4, g_{22}^*(z)=1+z+z^2, g_{33}^*(z)=1+z+z^3+z^4, g_{44}^*(z)=1+z+z^2.$ 因此，$g_{ii}^*(z)=g_{ii}(z)$ 对于 $1 \leq i \leq 4.$(ii) 由于 $\alpha=4$ 和 $g_{34}(z)=0$，这意味着 $g_{44}(z)|z^4 g_{34}^*(z)-g_{34}(z)$。(iii) 由于 $\beta=\gamma=4, g_{12}(z)=g_1(z)=0$，我们看到 $2\left(z^4 g_{12}^*(z)-g_{12}(z)\right)+(2+\nu)\left(z^4 g_1^*(z)-g_1(z)\right)=0 \in C_\theta \cdot$(iv) 由于 $\delta=0$ 和 $g_2^*(z)=z^2+z+1$，因此我们有 $z^0 g_2^*(z)-g_2(z)=0 \in \operatorname{Tor}(C_\theta)$。

因此，C_θ 满足定理 3.3 的所有条件。因此，C_θ 是一个可逆循环码。

例3.6. 设$C_\theta=\langle z^3+z^2+z+1+(1+\nu), 2(z^2+1), (1+\nu)(z-1), 2(1+\nu)\rangle$是一个长度为 4的循环码，定义在环$R_\theta$ 上，对于 $\theta=3+2\nu.$ 此处 $g_{11}(z)=z^3+$

$z^2+z+1, g_{22}(z) = z^2+1, g_{33}(z) = z-1, g_{44}(z) = 1, g_{12}(z) = 0, g_{34}(z) = 0$, $g_1(z) = 1$, $g_2(z) = 0$. 我们有,

(i) $g_{11}^*(z) = 1+z+z^2+z^3, g_{22}^*(z) = 1+z^2, g_{33}^*(z) = 1+z, g_{44}^*(z) = 1$. 因此, $g_{ii}^*(z) = g_{ii}(z)$ 对于 $1 \le i \le 4$.(ii) 由于 $\alpha = 1$ 且 $g_{34}(z) = 0$, 这意味着 $g_{44}(z) | z g_{34}^*(z) - g_{34}(z)$。(iii) 由于 $\beta = \gamma = 3, g_{12}(z) = 0$ 且 $g_1(z) = 1$, 我们看到 $2\left(z^3 g_{12}^*(z) - g_{12}(z)\right) + (1+\nu)\left(z^3 g_1^*(z) - g_1(z)\right) = (1+\nu)(z^3-1) = (z^2+z+1)\left((1+\nu)(z-1)\right) \in C_\theta$.(iv) 由于 $\delta = 2$ 且 $g_2^*(z) = 0$, 因此 $z^2 g_2^*(z) - g_2(z) = 0 \in \mathrm{Tor}(C_\theta)$.

因此, C_θ 满足定理 3.3 的所有条件。因此, C_θ 是一个可逆循环码。

例 3.7. 设$C_\theta = \langle z^3+z^2+z+1+\nu(z+3), 2(z^2+1)+2\nu, \nu(z^2+1)\ 2\nu(z+1)\rangle$是环$R_\theta$ 上的长度为 4 的循环码, 其中 $\theta = 2\nu$. 这里 $g_{11}(z) = z^3+z^2+z+1, g_{22}(z) = z^2+1$, $g_{33}(z) = z^2+1, g_{44}(z) = z+1, g_{12}(z) = 0, g_{34}(z) = 0, g_1(z) = z+3, g_2(z) = 2$. 我们有,

(i) $g_{11}^*(z) = 1+z+z^2+z^3$, $g_{22}^*(z) = 1+z^2$, $g_{33}^*(z) = 1+z^2$, $g_{44}^*(z) = 1+z$.因此, $g_{ii}^*(z) = g_{ii}(z)$ 对于 $1 \le i \le 4$.(ii) 由于 $\alpha = 2$ 且 $g_{34}(z) = 0$, 这意味着 $g_{44}(z) | z^2 g_{34}^*(z) - g_{34}(z)$。(iii) 由于 $\beta = 3, \gamma = 2, g_{12}(z) = 0$ 且 $g_1(z) = z+3$, 这意味着$2\left(z^3 g_{12}^*(z) - g_{12}(z)\right) + \nu\left(z^2 g_1^*(z) - g_1(z)\right) = \nu(3z^3+z^2+3z+1) = (3z+1)\left(\nu(z^2+1)\right) \in C_\theta$.(iv) 由于 $\delta = 2$ 且 $g_2^*(z) = 2$, 因此 $z^2 g_2^*(z) - g_2(z) = 2z^2+2 = 2\left(z^2+1\right) \in \mathrm{Tor}(C_\theta)$。

因此, C_θ 满足定理 3.3 的所有条件。因此, C_θ 是一个可逆循环码。

例 3.8。设 $C_\theta = \langle z^5+z^4+z^3+z^2+z+1+\nu(z^4+z^2+1), 2(z+1)+\nu(z+1)\ \nu(z^5+z^4+z^3+z^2+z+1)\ 2\nu\rangle$ 是环 R_θ 上的一个长度为 6 的循环码, 其中$\theta = \nu$. 有 $g_{11}(z) = z^5+z^4+z^3+z^2+z+1, g_{22}(z) = z+1, g_{33}(z) = z^5+z^4+z^3z^2+z+1$, $g_{44}(z) = 1, g_{12}(z) = 0, g_{34}(z) = 0, g_1(z) = z^4+z^2+1, g_2(z) = z+1$。我们有,

(i) $g_{11}^*(z) = z^5+z^4+z^3+z^2+z+1$, $g_{22}^*(z) = 1+z$, $g_{33}^*(z) = z^5+z^4+z^3+z^2+z+1$, $g_{44}^*(z) = 1$.因此, $g_{ii}^*(z) = g_{ii}(z)$, 对于 $1 \le i \le 4$.(ii) 由于 $\alpha = 2$ 且 $g_{34}(z) = 0$, 这意味着 $g_{44}(z) | z^2 g_{34}^*(z) - g_{34}(z)$。(iii) 由于 $\beta = 5, \gamma = 1, g_{12}(z) = 0$ 且 $g_1(z) = z^4+z^2+1$, 这意味着$2\left(z^5 g_{12}^*(z) - g_{12}(z)\right) + \nu\left(z g_1^*(z) - g_1(z)\right) = \nu(z^5+3z^4+z^3+3z^2+z+3) = \nu\left(z^5+z^4+z^3+z^2+z+1\right) + 2\nu(z^4+z^2+1) \in C_\theta$.(iv) 由于 $\delta = 0$ 且 $g_2^*(z) = z+1$, 因此 $z^0 g_2^*(z) - g_2(z) = 0 \in \mathrm{Tor}(C_\theta)$。

因此, C_θ 满足定理 3.3 的所有条件。因此, C_θ 是一个可逆循环码。

例 3.9. 设 $C_\theta = \langle z^5+z^4+z^3+z^2+z+1+\nu(z^2+z+1) + 2\nu z, 2(z^4+z^2+1)\ \nu(z^3+3)\ 2\nu(z^2+z+1)\rangle$ 是环 R_θ 上长度为 6 的循环码, 其中 $\theta = 0$. 。这里 $g_{11}(z) = z^5+z^4+z^3+z^2+z+1, g_{22}(z) = z^4+z^2+1, g_{33}(z) = z^3+3, g_{44}(z) = z^2+z+1, g_{12}(z) = 0, g_{34}(z) = 0, g_1(z) = z^2+3z+1, g_2(z) = 0$。显然, $g_{33}^*(z) = 3z^3+1 \neq g_{33}(z)$, 这违反了定理 3.3 的条件（$i$）。因此, C_θ 不是可逆循环码。

4. Reversible complement cyclic codes over R_θ上的可逆互补循环码

本节将给出环 $R_\theta, \theta \in S$ 上任意长度的循环码成为可逆补循环码的充要条件。为此，我们将采用 J. Kaur 等人 [15] 给出的有限交换环上元素补元的广义概念。

定义 4.1. [15] 对于元素 $a \in R_\theta$，$\overline{a}$ 若 $a + u_\theta \overline{a} = t_\theta$，则称其为 a 关于 u_θ 和 t_θ 的互补元，其中 u_θ 是 R_θ 中的单位元，t_θ 是 R_θ 中的任意元素，满足 $u_\theta^2 = 1$ 和 $u_\theta t_\theta = t_\theta$.。我们将 a 关于 u_θ 和 t_θ 的互补元记为 $(\overline{a})_{(u_\theta, t_\theta)}$.

定义 4.2. 设 C_θ 是 R_θ 上长度为 n 的循环码。若对于任意 $(s_0, s_1, \cdots, s_{n-1}) \in C_\theta$，均有 $(s_{n-1})_{(u_\theta,t_\theta)}$、$(s_{n-2})_{(u_\theta,t_\theta)}$ $\cdots$ 和 $(s_0)_{(u_\theta,t_\theta)}\big) \in \overline{C}_\theta$，则称其为 $(u_\theta, \overline{t_\theta})$ 可逆互补循环码。

定义 4.3. 对于次数为 $k \le n-1$ 的多项式 $s(z)$，其反向多项式 1
为 $s^r(z) = z^{n-k-1} s^*(z)$。

定义 4.4. 码字 $(s_0, s_1, \cdots, s_{n-1})$ 的多项式表示 $s(z)$ 的 (u_θ, t_θ) 反向补多项式是元素 $\big((s_{n-1})_{(u_\theta,t_\theta)}, (s_{n-2})_{(u_\theta,t_\theta)} \cdots, (s_0)_{(u_\theta,t_\theta)}\big)$. 的多项式表示。我们将记作 $(s^r(z))_{(u_\theta,t_\theta)}$.

由补的定义可直接得到以下引理。

引理 4.5. 对任意 $r_1, r_2, r_3 \in R_\theta$，有

(1) $\left(\overline{(\overline{r_1})_{(u_\theta,t_\theta)}}\right)_{(u_\theta,t_\theta)} = r_1$.
(2) $(\overline{r_1 + r_2})_{(u_\theta,t_\theta)} = (\overline{r_1})_{(u_\theta,t_\theta)} + (\overline{r_2})_{(u_\theta,t_\theta)} + 3u_\theta^{-1} t_\theta$.
(3) $(\overline{r_1 + t_\theta r_2})_{(u_\theta,t_\theta)} = (\overline{r_1})_{(u_\theta,t_\theta)} + 3u_\theta^{-1} t_\theta r_2$.
(4) $u_\theta (\overline{r_1})_{(u_\theta,t_\theta)} + 3t_\theta = 3r_1$.
(5) $(\overline{r_1 + r_2 + r_3})_{(u_\theta,t_\theta)} = (\overline{r_1})_{(u_\theta,t_\theta)} + (\overline{r_2})_{(u_\theta,t_\theta)} + (\overline{r_3})_{(u_\theta,t_\theta)} + 2u_\theta^{-1} t_\theta$.

以下定理给出了任意长度n、定义在 R_θ 上的循环码 C_θ 成为 (u_θ, t_θ) 可逆补循环码的充要条件。

定理 4.6. 设 $u_\theta, t_\theta \in R_\theta$，且 u_θ 是一个单位。R_θ 上长度为 n 的循环码 C_θ 是一个 (u_θ, t_θ) 可逆补循环码，当且仅当 C_θ 是一个可逆循环码，且 $(0^r(z))_{(u_\theta,t_\theta)} \in C_\theta$.

证明。首先，假设 C_θ 是长度为 n 、定义在 R_θ 上的可逆循环码，并且 $(0^r(z))_{(u_\theta,t_\theta)} \in \overline{C_\theta}$.。令 $s(z) = s_0 + s_1 z + \cdots + s_k z^k$；$0 \le k \le n-1$ 为 C_θ. 中的任意多项式。由于 C_θ 是可逆循环码，因此 $s^r(z) = z^{n-k-1} s^*(z) = s_k z^{n-k-1} + s_{k-1} z^{n-k} + \cdots + s_0 z^{n-1} \in C_\theta$.。此外 $(0^r(z))_{(u_\theta,t_\theta)} \in C_\theta$.。于是，$(0^r(z))_{(u_\theta,t_\theta)} - u_\theta^{-1} s^r(z) \in C_\theta$.。此外，

$$
\begin{aligned}
&(\overline{0^r(z)})_{(u_\theta,t_\theta)} - u_\theta^{-1} s^r(z) = u_\theta^{-1} t_\theta (1 + z + z^2 + \cdots + z^{n-1}) - u_\theta^{-1}(s_k z^{n-k-1} + \\
&s_{k-1} z^{n-k} + \cdots + s_0 z^{n-1}) = u_\theta^{-1} t_\theta (1 + z + z^2 + \cdots + z^{n-k-2}) + \big(u_\theta^{-1}(t_\theta - s_k) \\
&z^{n-k-1} + u_\theta^{-1}(t_\theta - s_{k-1}) z^{n-k} + \cdots + u_\theta^{-1}(t_\theta - s_0) z^{n-1}\big) = u_\theta^{-1} t_\theta (1 + z + z^2 + \\
&\cdots + z^{n-k-2}) + \big((\overline{s}_k)_{(u_\theta,t_\theta)} z^{n-k-1} + (\overline{s}_{k-1})_{(u_\theta,t_\theta)} z^{n-k} + \cdots + (\overline{s}_0)_{(u_\theta,t_\theta)} z^{n-1}\big) \\
&= (\overline{s^r(z)})_{(u_\theta,t_\theta)},
\end{aligned}
$$

也就是说，对于 C_θ中的每个多项式 $s(z)\ \overline{\in}$，$(s^r(z))_{(u_\theta,t_\theta)}\ \in C_\theta\cdot$。因此，$C_\theta$是一个 (u_θ, t_θ) 可逆补循环码。

反之，假设 C_θ 是一个 (u_θ, t_θ) 可逆补循环码。令 $s(z) = s_0 + s_1 z + \cdots + s_k z^k$; $0 \le k \le n-1$为 C_θ中的任意多项式。由于 C_θ是一个 (u_θ, t_θ) 可逆补循环码，因此 $(s^r(z))_{(u_\theta,t_\theta)} \in C_\theta$·特别地，$(0^r(z))_{(u_\theta,t_\theta)} \in C_\theta\cdot$因此，$(0^r(z))_{(u_\theta,t_\theta)} - (s^r(z))_{(u_\theta,t_\theta)} = u_\theta^{-1} s^r(z) = u_\theta^{-1} z^{n-k-1} s^*(z) \in C_\theta\cdot$ 由此可得，$s^*(z) \in C_\theta$，C_θ 为循环码。因此，C_θ 是 R_θ. □上的可逆循环码。

在下表中，我们检查了示例 3.4—示例 3.9 中的循环码，判断对于某些 u_θ 和 t_θ.的取值，它们是否为（u_θ， t_θ）可逆互补循环码。

序号	循环码 C_θ	θ	可逆	(u_θ, t_θ)	可逆互补-ment
1	$\langle z^3 + z^2 + z + 1, 2(z^2 + 1) + 2\nu, \nu(z^2 + 1)\ 2\nu(z + 1)\rangle$	2ν	Yes	所有可能的取值	Yes
2	$\langle z^4 + z^3 + z + 1, 2(z^2 + z + 1) + (2 + \nu)(z^2 + z + 1), (2 + \nu)(z^4 + z^3 + z + 1),\ 2(2 + \nu)(z^2 + z + 1)\rangle$	$2 + \nu$	Yes	$(1,\ 2 + \nu)$	Yes
3	$\langle z^4 + z^3 + z + 1,\ 2(z^2 + z + 1) + (2 + \nu)(z^2 + z + 1),\ (2 + \nu)(z^4 + z^3 + z + 1),\ 2(2 + \nu)(z^2 + z + 1)\rangle$	$2 + \nu$	Yes	$(1 + 2\nu,\ 2\nu)$	No
4	$\langle z^3 + z^2 + z + 1 + (1 + \nu), 2(z^2 + 1), (1 + \nu)(z - 1), 2(1 + \nu)\rangle$	$3 + 2\nu$	Yes	$(3 + 2\nu, 2)$	Yes
5	$\langle z^3 + z^2 + z + 1 + (1 + \nu), 2(z^2 + 1), (1 + \nu)(z - 1), 2(1 + \nu)\rangle$	$3 + 2\nu$	Yes	$(3, 2 + 2\nu)$	No
6	$\langle z^3 + z^2 + z + 1 + \nu(z + 3), 2(z^2 + 1) + 2\nu, \nu(z^2 + 1)\ 2\nu(z + 1)\rangle$	2ν	Yes	$(1, \nu)$	Yes
7	$\langle z^3 + z^2 + z + 1 + \nu(z + 3), 2(z^2 + 1) + 2\nu, \nu(z^2 + 1)\ 2\nu(z + 1)\rangle$	2ν	Yes	$(1, 3 + \nu)$	No
8	$\langle z^5 + z^4 + z^3 + z^2 + z + 1 + \nu(z^4 + z^2 + 1), 2(z + 1) + \nu(z + 1)\ \nu(z^5 + z^4 + z^3 + z^2 + z + 1)\ 2\nu\rangle$	ν	Yes	$(1, \nu)$	Yes
9	$\langle z^5 + z^4 + z^3 + z^2 + z + 1 + \nu(z^4 + z^2 + 1), 2(z + 1) + \nu(z + 1)\ \nu(z^5 + z^4 + z^3 + z^2 + z + 1)\ 2\nu\rangle$	ν	Yes	$(1 + 2\nu, 2\nu)$	No
10	$\langle z^5 + z^4 + z^3 + z^2 + z + 1 + \nu(z^2 + z + 1) + 2\nu z,\ 2(z^4 + z^2 + 1)\ \nu(z^3 + 3)\ 2\nu(z^2 + z + 1)\rangle$	0	No	所有可能的值	No

5. Conclusion

本文建立了环 $Z_4 + \nu Z_4$ 上任意长度的循环码成为可逆循环码的充分必要条件，适用于 $Z_4 + \nu Z_4$ 为非链环的 ν^2 值。此外，还给出了.....的条件。

在这些环上的循环码成为可逆补循环码的必要且充分条件已经确定。

References

[1] A. Hammons, A. Kumar, A. Calderbank, 《Kerdock、Preparata、Goethals 及相关码的 $\mathbf{Z_4}$ 线性》, 《IEEE 信息论汇刊》40(2)（1994）301-319。https://doi.org/10.1109/18.312154。[2] J.L.Massey, 《可逆码》, 《信息与控制》7（1964）369-380。[3] T. Abualrub, I. Siap, 《 Z_4上的可逆循环码》, 《澳大利亚组合杂志》38（2007）195-205。[4] H. Islam, O. Parkash, 《 Z_p^k上的可逆循环码构造》, 《离散数学科学与密码学杂志》（2021）1-14。[5] J.Kaur, 《伽罗瓦环上的循环码》, 博士论文，PEC 理工大学（2017）。[6] Srinivasulu B, M. Bhaintwal, 《 $F_4 + uF_4$ 上的可逆循环码及其在 DNA 码中的应用》, 信息技术与电气工程国际会议（ICITEE）（2015）。[7] J.Liu, H. Liu, 《环 $F_4[u]/\langle u^3\rangle$上的 DNA 码》, IEEE 4（2016）。[8] O. Parkash, S. Patel, S. Yadav, 《某些有限环上的可逆循环码及其在 DNA 码中的应用》, 《计算与应用数学》（2021）。[9] O. Parkash, S. Patel, P. Sharma, 《一类链环上的可逆循环码及其在 DNA 码中的应用》, 《国际信息与编码理论杂志》（2022）。[10] S. Pattanayak, A.Singh, 《环 $Z_4 + uZ_4$上的循环 DNA 码》, arXiv:1508.02015vl [cs.IT]（2015）。[11] H. Dinh, A. kumar, S. Pattanayak, S. Sriboonchitta, 《基于删除距离的环 $Z_4[u]/\langle u^2 - 1\rangle$ 上的循环 DNA 码构造》, 《理论计算机科学》773（2019）27-42。[12] T.Abualrub, A.Ghrayeb, X.Zeng, 《用于 DNA 计算的 GF(4) 上循环码构造》, 《富兰克林研究所杂志》343（2006）448-457。[13] K. Guenda, T.A. Gulliver, 《用于 DNA 计算的 $F_2 + vF_2$ 上循环码构造》, 《应用代数与工程通信计算》 24(6) （ 2013 ） 445-459。[14] A. Bayram, E.S. Oztas, I.Siap, 《 $F_4 + vF_4$ 上的码及其若干 DNA 应用》, 《设计、码与密码学》80（2016）379-393。[15] J. Kaur, R. Sehmi S. Dutt, 《伽罗瓦环上的可逆互补循环码及其在 DNA 码中的应用》, 《离散应用数学》（2020）。[16] O. Parkash, S. Patel, S. Yadav, 《某些有限环上的可逆循环码及其在 DNA 码中的应用》, 《计算与应用数学》40:242（2021）。[17] A.Alahmadi, K. G. Benerjee, S. Deb, M.K. Gupta, arxiv: 2110.09089vl [cs.IT]（2021）[18] N.Jain, S. Dutt, R. Sehmi, 《一类非链环上循环码的结构与秩》, arXiv:2303.07800 [cs.IT]（2023）。

Punjab Engineering College (Deemed to be University), Chandigarh
Email address: nikitajain.phd19appsc@pec.edu.in

Punjab Engineering College (Deemed to be University), Chandigarh
Email address: sucheta@pec.edu.in

Punjab Engineering College (Deemed to be University), Chandigarh
Email address: rsehmi@pec.edu.in