arXiv:2301.00753v1 [cs.IT] 2 Jan 2023

加性循环码的多项式表示与新的量子码

REZA DASTBASTEH 和 KHALIL SHIVJI

Abstract. 我们给出了关于 $\mathbb{F}_{p^2}$ 上加性循环码的多项式表示。借助这一表示，每个加性循环码都可以唯一地用至多两个生成多项式表示。我们确定了所有不同加性循环码的生成多项式。我们还将利用 $\mathbb{F}_p$ 上的线性循环码，为加性循环码给出最小距离下界。我们对 $\mathbb{F}_{p^2}$ 上所有辛自对偶、自正交和近自正交加性循环码进行了分类。最后，我们将量子构造应用于自正交和近自正交加性循环码，给出了十个打破纪录的二元量子码，定义在 $\mathbb{F}_4$ 上。

关键词：加性循环码、量子码、自正交码、自对偶码

1. Introduction

量子纠错码，或简称量子码，用于量子计算，以保护量子信息免受噪声（退相干）造成的损坏。量子码的一般框架见[9, 13]。本文中， $\mathbb{F}_{p^2}$ 表示含有 p^2个元素的有限域，其中 p 为素数。将 $\mathbb{F}_p$ 上的量子码参数记为k ，该码将 n 个逻辑量子比特编码为 d 个物理量子比特，且最小距离为 $[[n, k, d]]_p$。量子稳定子码是一个重要的量子码族，其许多性质与经典分组码相似。具体而言，量子稳定子码由关于某种辛内积自正交的加法码构造而成。文献 [18]给出了基于各种经典码构造量子稳定子码的若干方法。对量子稳定子码原始定义的一种有趣改动，是放宽其自正交约束[5, 19]。这种方法使我们能够利用不一定自正交的 $\mathbb{F}_4$上的加法码构造优良量子码。此前，这一改动已应用于从不同族的线性码构造新的量子码[6, 10, 20]。

加性循环码因其丰富的代数性质以及在量子码构造中的应用而备受关注。文献中已有多项研究，致力于对具有不同应用的加性循环码进行分类 [1, 4, 7, 16, 17, 21], ，也关注它们与准循环码等其他分组码族之间的联系 [15]。在[16], 中，利用 $\mathbb{F}_4$的某些有限域扩张，引入了 $\mathbb{F}_4$ 上加性循环码的典范分解。该分解被用于确定相对于迹内积的 $\mathbb{F}_4$ 上的自正交和自对偶加性循环码。在 [3], 中证明，长度为 n 的 $\mathbb{F}_4$ 上的每个加性循环码，都可以由 $\mathbb{F}_4[x]/\langle x^n - 1\rangle$ 中至多两个多项式及其循环移位的 $\mathbb{F}_2$-张成空间生成。此外，文中还给出了此类码相对于迹内积自正交的判据。 [1]中还提出了一种针对加性循环码子类——扭曲码——的有趣构造。该构造类似于线性循环码的构造方式。尽管扭曲码具有许多有用性质，但并非所有加性循环码都能用加性扭曲码理论来描述。

在本研究中，我们首先给出所有 $\mathbb{F}_p$上的 $\mathbb{F}_{p^2}$-加性循环码的一种规范表示，且至多使用两个生成多项式。与[16]的规范表示相比，我们的表示在计算上更加友好。借助这一表示，我们利用 $\mathbb{F}_p$上的线性循环码的最小距离，给出 $\mathbb{F}_{p^2}$ 上加性循环码的最小距离下界。此外，我们为 $\mathbb{F}_{p^2}$上的每个加性循环码提供一组唯一的生成多项式。我们将利用这种生成多项式表示，刻画相对于辛内积的所有自正交和自对偶加性循环码。我们还确定给定的 $\mathbb{F}_{p^2}$上加性循环码的辛对偶的生成多项式，并且仅利用各加性循环码的生成多项式计算其近似自正交性。这使我们能够应用 [5, 19]中提出的近自正交量子码构造。具体而言，将上述量子构造应用于近自正交加性循环码后，我们给出了十一种创纪录的二元量子码。此外，将次级构造应用于我们新构造的量子码，还能得到更多创纪录的二元码。值得注意的是，利用相同长度的自正交加性循环码无法构造出这类新量子码。

本文组织结构如下。第2 节简要回顾本文所用的基本术语。第3 节给出 $\mathbb{F}_{p^2}$上加性循环码的规范表示。事实上，我们采用模论方法，利用 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$中的多项式表示对每个加性循环码进行分解。第4节计算每个加性循环码的辛对偶。我们给出关于辛内积的加性循环码为自正交、自对偶或近似自正交的充要条件。最后，在第5节中，我们给出所构造的破纪录量子码的参数。

2. 预备知识

设 ω 是 $\mathbb{F}_{p^2}$的本原元。那么集合 $\{1,\omega\}$ 构成了 $\mathbb{F}_{p^2}$ 关于 $\mathbb{F}_p$的一组基。设 $a+b\omega$ 和 $a'+b'\omega\in\mathbb{F}_{p^2}^n$，其中 a、a'、b、$b'\in\mathbb{F}_p^n$。$a+b\omega$ 和 $a'+b'\omega$ 的辛内积定义为

$$\langle a+b\omega, a'+b'\omega\rangle_s = a'\cdot b - a\cdot b'. \tag{2.1}$$

称一个 $\mathbb{F}_p$线性子空间 $C\subseteq\mathbb{F}_{p^2}^n$ 为长度为 n 的 $\mathbb{F}_{p^2}$上的加法码。我们用 $\dim^{\mathbb{F}_p}(C)$ 表示 $\mathbb{F}_{p^2}$ 上加法码 C 的$\mathbb{F}_p$维数。设 $C\subseteq\mathbb{F}_{p^2}^n$ 是 $\mathbb{F}_{p^2}$ 上的一个加法码，且 $\dim^{\mathbb{F}_p}(C)=k$。则称 C 为一个（n，p^k）码。集合

$$C^{\perp_s}=\{x\in\mathbb{F}_{p^2}^n : \langle x,y\rangle_s=0 \text{ for all } y\in C\}.$$

称为的辛对偶，C。容易看出，$C^{\perp_s}$ 是一个（n，p^{2n-k}）上的加法码。码 C 称为自正交（自对偶），如果 $C\subseteq C^{\perp_s}$（若 $C=C^{\perp_s}$则称为自对偶）。对于每个 $x\in\mathbb{F}_{p^2}^n$，我们用 wt(x) 表示x的非零坐标数。此外，加法码 C 中非零向量的最小重量记为d（C）。量子稳定子码与经典加法码之间的联系最初由 Calderbank、Rains、Shor 和 Sloane[3] 以及 Gottesman[11]各自独立提出。下面给出这一联系的非二元版本。

定理 2.1. [18, 推论 16] 设 C 是定义在 $\mathbb{F}_{p^2}$ 上的一个 (n,p^{n-k}) 加法码。若 C 是辛自正交的，则存在一个 $[[n,k,d]]_p$ 量子稳定子码，其中 $d=\min\{\mathrm{wt}(x): x\in C_s^{\perp}\setminus C\}$ 若 $k>0$，且 $d=\min\{\mathrm{wt}(x): x\in C\}$ 若 $k=0$。

定理 2.1 中的量子码称为 纯 当 $d=d(C^{\perp_s})$。量子码有若干种次级构造。以下简要列举其中一些构造。

定理 2.2。 [18, 第 XV 节] 设 C 是一个 $[[n,k,d]]_p$ 量子码。

(1) 若 $k>0$，则存在一个 $[[n+1,k,d]]_p$ 量子码。(2) 若 C 是纯的，且 $n,d\geq 2$，则存在一个 $[[n-1,k+1,d-1]]_p$ 纯量子码。(3) 若 $k>1$，则存在一个 $[[n,k-1,d]]_p$ 量子码。

3. Additive cyclic codes over $\mathbb{F}_{p^2}$

在本节中，我们假设 n 是一个正整数，满足 $(n,p)=1$ 且$\mathbb{F}_{p^2}=\{\alpha+\beta\omega:\ \alpha,\beta\in\mathbb{F}_p\}$，其中 ω 是$\mathbb{F}_p$上的一个二次不可约多项式的根。本节中，我们给出域$\mathbb{F}_{p^2}$上加性循环码的规范表示。特别地，我们用至多两个生成多项式给出 $\mathbb{F}_{p^2}$ 上每个加性循环码的唯一表示。此外，我们确定 $\mathbb{F}_{p^2}$上所有不同加性循环码的生成多项式。特别地， $\mathbb{F}_p^2$ 上的每个加性循环码都是由其生成多项式的循环移位线性组合而成。这种表示也适用于加性循环码的实际计算，尤其是使用 Magma 计算机代数系统 [2]。更具体地说，Magma 中有一个内置函数，可根据给定的两个生成多项式构造生成的加性循环码。本节末尾，我们利用 $\mathbb{F}_p$上线性循环码的最小距离，给出 $\mathbb{F}_{p^2}$ 上加性循环码最小距离的下界。

定义 3.1. 若对于每个 $(a_0,a_1,\ldots,a_{n-1})\in C$，向量 $(a_{n-1},a_0,\ldots,a_{n-2})$ 也是 C 的码字，则称 $\mathbb{F}_p$-子空间 $C\subseteq\mathbb{F}_{p^2}^n$ 为一个长度为 n 、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码。

本节将频繁用到以下模论概念；更多详情可参见例如 [8, 第 12] 章。设 R 为主理想整环，M 为一个R-模。 M 的湮灭子是 R 的一个理想，定义为 $\{r\in R:\ rm=0$ ，对任意 $m\in M\}$ 均成立。若存在 $0\neq r\in R$ 使得 $rm=0$，则称元素 $m\in M$ 为挠元。若模 M 的所有元素都是挠元，则称该模为挠模。以下定理称为模的主分解定理，在我们对加性循环码的表示中发挥着重要作用。

定理 3.2。[8, 第 12 章，定理 7] 设 R 是一个主理想整环， M 是一个挠$_nR$-模，其湮灭子为 $\langle a\rangle\neq 0$。设 $a=u\prod p_i^{a_i}$，其中 u 是单位，且对每个 $1\leq i\leq n$， p_i 都是一个素$_{i=1}$元。于是，我们可以将 M 分解为其子模的直和，形式如下:

$$M=\bigoplus_{i=1}^{n}N_i, \tag{3.1}$$

其中 $N_i=\{x\in M:$ 对每个 $1\leq i\leq n,\ xp_i^{a_i}=0\}$ 。

每个元素（a_0， a_1，...， a_{n-1}） $\in\mathbb{F}_{p^2}^n$ 都可以唯一地表示为 $\mathbb{F}_{p^2}[x]/\langle x^n-_{n-1}1\rangle$ 中的一个多项式，形式为 $\sum a_ix^i$。容易验证，在这种对应关系下，长度为 n 的 $\mathbb{F}_{p^2}$ 上的加法$_{i=0}$循环码是 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$的一个 $\mathbb{F}_p[x]$-子模。

记号 3.3。设 f和 $g\in\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$。本文余下部分将固定使用以下记号。

(1) 由 f 在 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$ 中生成的理想记作 $\langle f\rangle_{\mathbb{F}_{p^2}[x]}$。等价地，它是由多项式 f 生成的 $\mathbb{F}_{p^2}[x]$-子模 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$ 。

(2) 由多项式 g 生成的 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$ 的 $\mathbb{F}_p[x]$-子模记作 $\langle g\rangle_{\mathbb{F}_p[x]}$。

直接计算可得，$\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$ 作为 $\mathbb{F}_p[x]$-s模的湮灭子是理想 $\langle x^n-1\rangle$。此外，我们可以将 x^n-1 在 $\mathbb{F}_p[x]$ 上分解为 $x^n-1=\prod_{i=1} f_i(x)$，其中每个 $f_i(x$都是与模 p的 n-分圆陪集对应的不可约多项式。接下来，我们将定理3.2 应用于 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle$。容易看出

$$\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle=\bigoplus_{i=1}^{s} N_i, \tag{3.2}$$

其中 $N_i=\langle (x^n-1)/f_i(x)\rangle_{\mathbb{F}_{p^2}[x]}$ 对每个 $1\le i\le s$ 均成立。我们称 $\mathbb{F}_{p^2}$ 上非零长度的 n 加性循环码 C 是不可约的，若对于任意加性循环码 $D\subseteq C$，都有 $D=\{0\}$ 或 $D=C$。下一个引理表明，每个 N_i 都可以分解为两个不可约加性循环码的直和。我们确定了 N_i 中所有不可约加性循环码的生成多项式，并给出关于每个 N_i 中加性循环码的其他有用信息。

引理 3.4. 设 $f(x)$ 是 $\mathbb{F}_p[x]$ 上 x^n-1 的一个不可约因子，且 $\deg(f)=k$ and $N=\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_{p^2}[x]}$。

(1) 设 $0\neq r(x)\in N$，则集合 $L=\{r(x)\ xr(x)\ldots,x^{k-1}r(x)\}$ 构成 $\langle r(x)\rangle_{\mathbb{F}_p[x]}$ 作为 $\mathbb{F}_p$ 向量空间的一组基。(2) 设 $0\neq C\subsetneq N$ 是一个加性循环码。码 C 的 $\mathbb{F}_p$- 维数为 k，且对于任意 $0\neq r(x)\in C$，都有 $C=\langle r(x)\rangle_{\mathbb{F}_p[x]}$。(3) 加性循环码 N 可分解为

$$N=\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}\oplus\langle \omega((x^n-1)/f(x))\rangle_{\mathbb{F}_p[x]}.$$

此外，$\dim^{\mathbb{F}_p}(N)=2k$，且 N 是 $\mathbb{F}_{p^2}$ 上的线性空间。

(4) N 中不可约加性循环码的数量为 2^k+1。特别地，以下集合给出了这类加性循环码的所有不同生成多项式。

$$A=\{\big((x^n-1)/f(x)\big)\big(\omega+g(x)\big):g(x)\in\mathbb{F}_p[x],\deg(g(x))<k\}\cup\{(x^n-1)/f(x)\}. \tag{3.3}$$

证明。(1) 显然 $L\subseteq\langle r(x)\rangle_{\mathbb{F}_p[x]}$。反设 L 在 $\mathbb{F}_p$上线性相关。因此，我们可以找到一个次数小于 k 的多项式 $0\neq s(x)\in\mathbb{F}_p[x]$，使得 $r(x)s(x)\equiv 0\pmod{x^n-1}$。由于 $(x^n-1)/f(x)\mid r(x)$，且 $f(x)$ 不可约，我们得出 $f(x)\mid s(x)$。然而，这与 $\deg(s(x))<k$ 矛盾。这说明 L在 $\mathbb{F}_p$ 上线性无关。注意，集合 $L\cup\{x^k r(x)\}$ 在 $\mathbb{F}_p$上线性相关，因为这个新集合生成 $f(x)r(x)\equiv 0\pmod{x^n-1}$。同理，可以证明，对于 $k<i<n-1$，$\{x^i r(x)\}$ 可以表示为 $\mathbb{F}_p$上 L 中元素的线性组合。因此，L 构成了 $\langle r(x)\rangle_{\mathbb{F}_p[x]}$ 的一组基。

(2) 设 $0\neq r(x)\in C$。反设 $\langle r(x)\rangle_{\mathbb{F}_p[x]}\subsetneq C$。那么存在一个多项式 $s(x)\in C$，使得 $s(x)\notin\langle r(x)\rangle_{\mathbb{F}_p[x]}$。注意，$\langle r(x)\rangle_{\mathbb{F}_p[x]}\cap\langle s(x)\rangle_{\mathbb{F}_p[x]}=\{0\}$，否则，根据（1），对于交中的任意多项式 $a(x)$，我们有

$$\langle r(x)\rangle_{\mathbb{F}_p[x]}=\langle a(x)\rangle_{\mathbb{F}_p[x]}=\langle s(x)\rangle_{\mathbb{F}_p[x]},$$

这就产生了矛盾。因此 $C=\langle r(x)\rangle_{\mathbb{F}_p[x]}$，且其在 $\mathbb{F}_p$ 上的维数为 k。

(3) 很容易看出 $\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}\cap\langle \omega((x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}=\{0\}$ 且

$$N=\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}\oplus\langle \omega((x^n-1)/f(x))\rangle_{\mathbb{F}_p[x]}.$$

因此， N 在 $\mathbb{F}_p$ 上的维数为 $2k$ 。其线性性质可直接由其生成多项式的结构得出。

(4) 为了找到一个维数为 k 的加性循环码（其维数为 $\mathbb{F}_p$），我们需要选择一个非零多项式 $r(x) \in N$ 作为其生成元。此外， $\langle r(x)\rangle_{\mathbb{F}_p[x]}$ 中任意非零元素都会生成同一个码。因此， N 内恰有 $\frac{2^{2k}-1}{2^k-1} = 2^k+1$ 个由单个非零生成元生成的加性循环码。

设 C_1 和 C_2 是 N 中两个维数为 k 的加性循环码。如果 $C_1 \cap C_2 \neq \{0\}$，则根据第 (1) 部分有 $C_1 = C_2$。等价地，如果 $C_1 + C_2 = N$，则 $C_1 \cap C_2 = \{0\}$。现在我们证明集合 A 中的不同元素生成不同的码。设 $g(x) \in \mathbb{F}_p[x]$，使得 $\deg(g(x)) < k$。显然，加性循环码 $C_1 = \langle (x^n-1)/f(x), ((x^n-1)/f(x))(g(x)+\omega)\rangle_{\mathbb{F}_p[x]}$ 包含 $(x^n-1)/f(x)$ 和 $\omega(x^n-1)/f(x)$。因此 $C_1 = N$。所以 $\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}$ 和 $\langle ((x^n-1)/f(x))(g(x)+\omega)\rangle_{\mathbb{F}_p[x]}$ 是不同的加性循环码。

设 $g_1(x)$ 和 $g_2(x) \in \mathbb{F}_p[x]$ 是两个次数小于 k 的不同多项式。码 $C = \langle ((x^n-1)/f(x))(\omega + g_1(x)), ((x^n-1)/f(x))(\omega+g_2(x))\rangle_{\mathbb{F}_p[x]}$ 包含 $(x^n-1)/f(x)$ 和 $\omega(x^n-1)/f(x)$。这主要是因为

$$\langle \big((x^n-1)/f(x)\big)(g_1(x)-g_2(x))\rangle_{\mathbb{F}_p[x]} = \langle (x^n-1)/f(x)\rangle_{\mathbb{F}_p[x]}.$$

因此 $C = N$。这意味着加性循环码 $\langle ((x^n-1)/f(x))(\omega+g_1(x))\rangle_{\mathbb{F}_p[x]}$ 和 $\langle ((x^n-1)/f(x))(\omega+g_2(x))\rangle_{\mathbb{F}_p[x]}$ 是不同的。这证明集合 A 包含 N 内所有不同的不可约加性循环码的生成元。□

正如引理 3.4 的第 (1) 部分所述， $\langle (x^n-1)/f(x)\rangle_{\mathbb{F}_{p^2}[x]}$ 内的每个加性循环码都可以有多个不同的生成多项式。通过下面的评注，我们为 N 内的每个加性循环码固定一种规范表示。

注 3.5. 对于每个加法码 $0 \neq C \subsetneq \langle (x^n-1)/f(x)\rangle_{\mathbb{F}_{p^2}[x]}$，我们固定其在集合 A（见 (3.3)）中的生成多项式，并将其称为 C 的“生成多项式”。类似地，加性循环码 $C' = \langle (x^n-1)/f(x)\rangle_{\mathbb{F}_{p^2}[x]}$ 可由多项式 $(x^n-1)/f(x)$ 和 $\omega((x^n-1)/f(x))$ 生成。我们称它们为 C' 的“生成多项式”。

这种表示有助于在 N 中唯一确定每个加法循环码，并避免对同一个码重复考虑。接下来，我们利用引理 3.4 的结果来刻画 s 所有长度为 n 的加法循环码，它们定义在 $\mathbb{F}_{p^2}$ 上。回顾 $x^n-1 = \prod_{i=1}^{s} f_i(x)$，其中 $f_i(x)$ 是在 $\mathbb{F}_p[x]$ 上对每个 $1 \le i \le s$ 均成立的不可约多项式，且 $N_i = \langle (x^n-1)/f_i(x)\rangle_{\mathbb{F}_{p^2}[x]}$。

定理 3.6. 设 C 是一个长度为 n 的 $\mathbb{F}_{p^2}$ 上的加性循环码。则

(i) 我们可以将码 C 分解为 $C = \bigoplus_{i=1}^{s} C_i$，其中每个 C_i 都是 N_i 内的加性循环码。

(ii) 我们有 $C = \langle g(x) + \omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]}$，其中

(a) $g(x) + \omega k(x) = \sum_{i=1}^{s} g_i(x) + \omega k_i(x)$，

(b) $h(x) = \sum_{i=1}^{s} h_i(x)$，

(c) 并且 C_i 具有生成多项式 $g_i(x) + \omega k_i(x)$ 和 $\omega h_i(x)$，其选取方式如注 3.5 所述。

(iii) $\dim_{\mathbb{F}_p}(C) = \sum_{i=1}^{s}(\deg(f_i) \times$非零生成元的数量 $C_i)$。

证明。 (i) 正如我们在（3.2）中提到的，以下分解成立

$$\mathbb{F}_{p^2}[x]/\langle x^n - 1\rangle = \bigoplus_{i=1}^{s} N_i.$$

因此，我们可以将 C 表示为 $C = \bigoplus_{i=1}^{s} C_i$，其中每个 C_i 都是 N_i中的一个加性循环码。

(ii) 我们证明 $\langle g(x) + \omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]}$ 相同。首先注意到 $g(x) + \omega k(x)\ \omega h(x) \in C$，因此 $\langle g(x) + \omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]} \subseteq C$。设$1 \le i \le s$ 为一个固定整数。由于 $\big((x^n-1)/f_i(x)\big) \mid g_i(x)\ k_i(x)\ h_i(x)$，并且

$$\big((x^n-1)/f_i(x)\big)g_j(x) \equiv \big((x^n-1)/f_i(x)\big)k_j(x) \equiv \big((x^n-1)/f_i(x)\big)h_j(x) \equiv 0 \pmod{x^n-1}$$

对于任意 $j \neq i$，我们有

$$\big((x^n-1)/f_i(x)\big)\big(g(x)+\omega k(x)\big) \equiv \big((x^n-1)/f_i(x)\big)\big(g_i(x)+\omega k_i(x)\big) \pmod{x^n-1}$$

and

$$\big((x^n-1)/f_i(x)\big)\omega h(x) \equiv \big((x^n-1)/f_i(x)\big)\omega h_i(x) \pmod{x^n-1}.$$

此外，我们有

$$C_i = \langle g_i(x) + \omega k_i(x)\ \omega h_i(x)\rangle_{\mathbb{F}_p[x]} = \langle \big((x^n-1)/f_i(x)\big)\big(g(x)+\omega k(x)\big), \big((x^n-1)/f_i(x)\big)\omega h(x)\rangle_{\mathbb{F}_p[x]}.$$

Thus

$$C_i \subseteq \langle g(x) + \omega k(x), \omega h(x)\rangle_{\mathbb{F}_p[x]}.$$

这表明 $\bigoplus_{i=1}^{s} C_i \subseteq \langle g(x) + \omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]}$，从而完成证明。

（iii）注意到 $\dim_{\mathbb{F}_p}(C) = \sum_{i=1}^{s}\dim_{\mathbb{F}_p}(C_i)$。此外，根据引理 3.4，$\dim_{\mathbb{F}_p}(C_i) = 0$，$k_i$，或者$2k_i$ 若 $C_i = 0$，C_i 由一个生成多项式生成，或者 C_i 具有两个生成多项式，分别成立。将这些事实与（i）部分的结果结合起来，即完成证明。□

通过下面的推论，我们刻画了所有长度为 n 的域 $\mathbb{F}_{p^2}$ 上的不可约加性循环码。

命题 3.7. 设 C 是长度为 n、定义在 $\mathbb{F}_{p^2}$上的加性循环码。那么，当且仅当存在某个 $0 \neq r(x) \in N_i$ 和 $1 \le i \le s$，使得 $C = \langle r(x)\rangle_{\mathbb{F}_p[x]}$，$C$ 才是不可约的。此外，共有 $\sum_{i=1}^{s}(2^{\deg(f_i)} + 1)$个不同的不可约加性循环码。

证明。令 $C = \langle r(x)\rangle_{\mathbb{F}_p[x]}$，其中 $0 \neq r(x) \in N_i$ 且 $1 \le i \le s$。引理 3.4 第 (1) 部分的结果表明 C 是不可约的。反过来，设 C 是一个不可约加性循环码。那么根据定理 3.6 的第 (i) 部分，我们有 $C = \bigoplus C_i$。由于 C 是不可约的，因此对于某个 $1 \le j \le s$，有 $C = C_j$。此外，由于根据引理 3.4 第 (3) 部分，N_j 不可约，我们得出对于某个 $0 \neq r(x) \in N_j$，有 $C = \langle r(x)\rangle_{\mathbb{F}_p[x]}$。

在每个 N_i 中，都有 $2^{\deg(f_i)}+1$ 个不同的单生成元加性循环码。因此s不可约码的总数为 $\sum_{i=1}(2^{\deg(f_i)}+1)$ 。□

注 3.8. 从此以后，我们总是用定理 $g(x)+\omega k(x)$ 和 $\omega h(x)$ 的第（ii）部分中引入的生成多项式来表示每个加性循环码 3。6。此外，这些多项式的生成方式是唯一的，因此每个加性循环码都有唯一的一组生成元。

从现在起，我们将 $\mathbb{F}_{p^2}$-线性循环码简称为线性循环码。设 $C=\langle g(x)+\omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]}$ 是 $\mathbb{F}_{p^2}$ 上长度为 n 的加性循环码。注意，定理 3.6 和引理 3.4 的第 (3) 部分表明， C 是线性的，当且仅当 $g(x)=h(x)$ 且 $k(x)=0$。因此，线性循环码很容易与非线性循环码区分开来。

接下来，我们利用 $\mathbb{F}_p$ 上的线性循环码，为加法循环码给出一个最小距离界。一般而言，线性码的最小距离计算比加性码更快。因此，以下结果可以加快加法循环码的最小距离计算。我们用 $d(C)$ 表示码 C 的最小距离。

定理 3.9. 设 $C=\langle g(x)+\omega k(x)\ \omega h(x)\rangle_{\mathbb{F}_p[x]}$ 是 $\mathbb{F}_{p^2}$ 上长度为 n 的加法循环码。设 $G(x)=\frac{x^n-1}{\text{与 gcd}(x^n-1,g}(x))$，并设 $S(x)$ 是由 $k(x)$ 生成的长度为 n 的线性循环码与由 $h(x)$ 生成的线性循环码在 $\mathbb{F}_p$ 上的交的生成多项式。假设 D_1、 D_2、 D_3 和 D_3 分别是 $\mathbb{F}_p$ 上由 $g(x)$、$\gcd(k(x)\ h(x))$、$\gcd(G(x)k(x)\ h(x))$ 以及 $\frac{g(x)S(x)}{\gcd(x^n-1,k(x))}$ 生成的长度为 n 的线性循环码。那么

$$\min\{d(D_3),d(D_4),\max\{d(D_1),d(D_2)\}\}\le d(C). \tag{3.4}$$

证明。码 C 中可能出现的码字只有以下三种。

$$T_1=\{a(x)\in C:\ 0\neq a(x)\in\mathbb{F}_p[x]\},$$
$$T_2=\{\omega b(x)\in C:\ 0\neq b(x)\in\mathbb{F}_p[x]\},$$
$$T_3=\{a(x)+\omega b(x)\in C:\ 0\neq a(x),0\neq b(x)\in\mathbb{F}_p[x]\}.$$

我们通过考察这些集合中各自的最小距离，来界定 C 的最小距离。设 $f(x)\in T_1$。那么，对于某个 $a_1(x)$ $b_1(x)\in\mathbb{F}_p[x]$，可将其写为 $f(x)=a_1(x)(g(x)+\omega k(x))+b_1(x)\omega h(x)$。因此， $f(x)=a_1(x)g(x)$，且 $a_1(x)k(x)+b_1(x)h(x)\equiv 0\pmod{x^n-1}$。这意味着 $a_1(x)k(x)$ 是由 $S(x)$ 生成的、长度为 n 的 $\mathbb{F}_p$ 上线性循环码的元素。因此，$\frac{S(x)}{\gcd(x^n-1,k(x))}\mid a_1(x)$。换言之， $f(x)=a(x)g(x)\in D_4$。

接下来，设 $\omega f_1(x)\in T_2$。那么，对于某个 $a_1(x)$ $b_1(x)\in\mathbb{F}_p[x]$，有 $\omega f_1(x)=a_1(x)(g(x)+\omega k(x))+b_1(x)\omega h(x)$。于是，$a_1(x)g(x)\equiv 0\pmod{x^n-1}$，或者等价地， $G(x)\mid a_1(x)$。这意味着 $f_1(x)=a_1(x)k(x)+b_1(x)h(x)$。因此， $f_1(x)\in D_3$。

最后，令 $a(x)+\omega b(x)\in T_3$。则对于某个 $l(x)$ $m(x)\in\mathbb{F}_p[x]$，有 $a(x)+\omega b(x)=l(x)(g(x)+\omega k(x))+m(x)\omega h(x)$。因此， $a(x)\in D_1$ 且 $b(x)\in D_2$。这意味着 $\text{wt}(a(x)+\omega b(x))\ge\max\{d(D_1)\ d(D_2)\}$。□

注意，如果 $D_i=0$ 对于任意值 $1\le i\le 4$，那么我们只需在（3.4）的最小距离下界中舍弃此码。例如，如果 $D_1=0$，那么（3.4）的最小距离下界变为

$$\min\{d(D_3),d(D_4),d(D_2)\}\le d(C).$$

以下推论将这一结果修改为适用于加性循环码的形式，而加性循环码只由一个生成元生成。在这一结果中，循环码 C_i 是从 D_i 经

将 $h(x)$ 替换为 0，应用定理 3。9 得到 $1 \leq i \leq 3$。然而，码 C_4 则是通过考虑一个更直接的观察以不同方式得到的。

推论 3.10. 设 $C = \langle g(x) + \omega k(x) \rangle_{\mathbb{F}_p[x]}$ 是一个定义在 $\mathbb{F}_{p^2}$ 上、长度为 n 的加性循环码。设C_1、C_2、C_3 和 C_4 是定义在 $\mathbb{F}_p$ 上、长度为 n 的线性循环码，分别由多项式 $g(x)$、$k(x)$、$\frac{x^n-1}{\text{最大公因式}(x^n-1,\ g(x))}k(x)$ 和 $\frac{x^n-1}{\text{最大公因式}(x^n-1,\ k(x))}g(x)$生成。则

$$\min\{d(C_3), d(C_4), \max\{d(C_1), d(C_2)\}\} \leq d(C). \tag{3.5}$$

证明。 如上所述，码 C_i 都是在码的结构中应用条件 $h(x) = 0$后得到的 D_i，其中 $1 \leq i \leq 3$ 见定理 3.9。由于定理 D_4 中的码3.9 用于界定集合的最小重量

$$T_1 = \{a(x) \in C : \ 0 \neq a(x) \in \mathbb{F}_p[x]\},$$

在此证明中，我们直接计算 T_1 的最小重量。设 $f(x) \in T_1$。那么我们可以将其写为 $f(x) = a(x)(g(x) + \omega k(x))$，其中某个 $a(x) \in \mathbb{F}_p[x]$。因此 $f(x) = a(x)g(x)$ 且 $a(x)k(x) \equiv 0$(模 $x^n - 1$)。这意味着 $\frac{x^n-1}{\text{最大公因式}(x^n-1,k(x))}$ 最大公因式$(x^n-1,k(x))$ $\mid a(x)$。因此 $\frac{x^n-1}{\text{最大公因式}(x^n-1,k(x))}g(x) \mid a(x)$，并且有 $f(x) \in C_4$。□

接下来，我们考虑上述最小距离界在线性循环码上的限制，这些码的生成多项式为 $g(x) + \omega k(x)$ 和 $h(x)$，其中 $k(x) = 0$。

推论 3.11. 设 $C = \langle g(x)\ \omega h(x) \rangle_{\mathbb{F}_p[x]}$ 是长度为 n 、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码。设 E_1 和 E_2 分别是由多项式 $g(x)$ 和 $h(x)$ 生成的、定义在 $\mathbb{F}_p$ 上的长度为 n 的线性循环码。那么

$$\min\{d(E_1), d(E_2)\} \leq d(C). \tag{3.6}$$

证明。将条件 $k(x) = 0$ 应用于定理 3。9 可得 $D_1 = D_4 = E_1$ 且$D_2 = D_3 = E_2$。现在，根据定理 3。9的最小距离界即可得到结论。□

4. Symplectic inner product and dual of additive cyclic codes

本节中，我们确定给定的定义在 $\mathbb{F}_{p^2}$上的加性循环码的辛对偶的生成多项式。此外，我们给出所有自正交码和自对偶码的生成多项式。我们还衡量给定的加性循环码与辛自正交的接近程度。回顾一下，p 是一个素数，且 n 是与 p互素的正整数。此外，$\mathbb{F}_{p^2}$ 中的元素表示为 $\mathbb{F}_{p^2} = \{\alpha + \beta\omega : \ \alpha,\ \beta \in \mathbb{F}_p\}$，其中 ω 是定义在 $\mathbb{F}_p$ 上的二次不可约多项式的一个根。回顾一下，在（2.1）中，我们定义了 $\mathbb{F}^n{}_2$中两个元素的辛内积。我们类似地定义两个多项式的辛内积。在

particular, for $c(x) = \sum_{i=0}^{n-1}(a_i + \omega b_i)x^i$ and $c'(x) = \sum_{i=0}^{n-1}(a'_i + \omega b'_i)x^i \in \mathbb{F}_{p^2}[x]/\langle x^n - 1\rangle$, we define

$$c(x) * c'(x) = \sum_{i=0}^{n-1}(a_i b'_i - a'_i b_i).$$

这里我们对辛内积采用不同的记号，以区分作为不同对象的向量和多项式。

注 4.1. 设 $c(x) = g_1(x) + \omega g_2(x)$ 和 $c'(x) = g'_1(x) + \omega g'_2(x)$ 是 $\mathbb{F}_{p^2}[x]/\langle x^n - 1\rangle$ 的两个多项式，其中 $g_1(x)$ $g_2(x)$ $g'_1(x)$ $g'_2(x) \in \mathbb{F}_p[x]/\langle x^n - 1\rangle$。那么 $c(x) * c'(x)$ 是 $g_1(x)g'_2(x^{-1}) - g_2(x)g'_1(x^{-1})$ 的常数项（mod $x^n - 1$）。类似的论证表明，$c(x) * x^i c'(x)$ 是 $g_1(x)g'_2(x^{-1}) - g_2(x)g'_1(x^{-1})$ 中 x^i 的系数（mod $x^n - 1$）。因此，如果

$g_1(x)g_2'(x^{-1}) - g_2(x)g_1'(x^{-1}) \equiv 0 \pmod{x^n-1}$，那么由 $c'(x)$ 生成的码包含于由 $c(x)$ 生成的码的辛对偶中。我们在本节中会频繁使用这一性质。

容易验证，加性循环码 C 在 $\mathbb{F}_{p^2}$ 上的辛对偶也是 $\mathbb{F}_{p^2}$上的加性循环码。回顾定理 3.6 的 (ii) 部分， $\mathbb{F}_{p^2}$ 上的每个长度为 n 的加性循环码都可以唯一表示为 $C = \langle g_1(x) + \omega g_2(x)\ h(x)\rangle_{\mathbb{F}_p[x]}$，其中 $g_1(x)\ g_2(x)\ h(x) \in \mathbb{F}_p[x]/\langle x^n-1\rangle$。下一个定理给出了加性循环码自正交性的判据。证明与 [3, 定理 14 的 c 部分]非常相似。

定理 4.2。设 $C = \langle g_1(x) + \omega g_2(x)\ h(x)\rangle_{\mathbb{F}_p[x]}$ 是 $\mathbb{F}_{p^2}$上的长度为 n 的加性循环码。当且仅当满足以下条件时，码 C 是自正交的:

(1) $g_2(x)h(x^{-1}) \equiv 0$ (模 x^n-1)，(2) $g_1(x)g_2$

$(x^{-1}) \equiv g_2(x)g_1(x^{-1})$ (模 x^n-1)。

证明。 $\Rightarrow$: 假设 C 是自正交的。对于每个 $0 \le i \le n-1$，$g_1(x)+\omega g_2(x)$ 与 $x^i h(x)$ 的内积等于 x^i 在 $-g_2(x)h(x^{-1})$ 中的系数（模 x^n-1）。由于 C是自正交的，我们有 $g_2(x)h(x^{-1})$ $\equiv 0$ (模 x^n-1)。此外， $\big(x^i(g_1(x) + \omega g_2(x))\big) * \big(g_1(x) + \omega g_2(x)\big)$ 是 x^i 在 $g_1(x)g_2(x^{-1}) - g_2(x)$ $g_1(x^{-1})$ 中的系数（模 x^n-1）。因此，对于每个$0 \le i \le n-1$， x^i 在 $g_1(x)g_2(x^{-1}) - g_2(x)g_1$ (x^{-1}) (模 x^n-1) 中的系数为零。因此$g_1(x)g_2(x^{-1}) \equiv g_2(x)g_1(x^{-1})$ (模 x^n-1)。

$\Leftarrow$: 反过来，由 $g_1(x)g_2(x^{-1}) \equiv g_2(x)g_1(x^{-1})$（mod x^n-1）可知， $\langle g_1(x) + \omega g_2(x)$ $\rangle_{\mathbb{F}_p[x]}$ 中的所有向量都是自正交的。此外，由于 $g_2(x)h(x^{-1}) \equiv 0$(mod x^n-1)，我们得出 $h($ $x)$ 与 $g_1(x) + \omega g_2(x)$ 的所有循环移位都正交。最后，对于每个 $0 \le i \le n-1$，都有 $h(x) * x^i h$ $(x) = 0$。因此， $\langle g_1(x) + \omega g_2(x)\ h(x)\rangle_{\mathbb{F}_p[x]}$ 是一个辛自正交码。□

$_s$回顾一下， $x^n - 1 = \prod f_i(x)$，其中每个 $f_i(x)$ 都是 $\mathbb{F}_p[x]$ 上的不可约多项式。$_{i=1s}$此外，正如我们先前在 (3.2) 中提到的，我们有 $\mathbb{F}_{p^2}[x]/\langle x^n-1\rangle = \bigoplus N_i$，其中 $N_i =_{i=1}\langle($ $x^n-1)/f_i(x)\rangle_{\mathbb{F}_{p^2}[x]}$。令 α 为有限域扩张 $\mathbb{F}_p$ 中的一个本原 n 次单位根。对于每个 $1 \le i \le s$，我们按如下方式将模 n 的 p-分圆陪集记为 Z_i : $f_i(x) = \prod(x-\alpha^i)$。这在集合 N_i 与所有模 n 的 $_{a\in Z_i}p$-分圆陪集之间建立了一一对应关系。本节的首要目标是求给定加性循环码的辛对偶。为实现这一目标，我们需要一些预备结果。在下一个引理中，我们求出每个 N_i 的辛对偶。

$_s$引理 4.3。设 $1 \le i \le s$ 和 $C = N_i$。则 $C^{\perp_s} = \bigoplus N_k$，其中 $Z_j = -Z_i$。

$_{k=1k\neq j}$

证明。首先注意，根据引理 3.4 的第 (3) 部分，我们有 $C = \langle(x^n-1)/f_i(x)\ \omega((x^n-1)/f_i(x))\rangle_{\mathbb{F}_p[x]}$。若 $Z_k \neq -Z_i$，则 $f_i(x) \mid (x^n-1)/f_k(x^{-1})$，且 $f_k(x) \mid (x^n-1)/f_i(x^{-1})$。因此我们有

- $\big((x^n-1)/f_i(x)\big)\big((x^n-1)/f_k(x^{-1})\big) \equiv 0 \pmod{x^n-1}$ and
- $\big((x^n-1)/f_k(x)\big)\big((x^n-1)/f_i(x^{-1})\big) \equiv 0 \pmod{x^n-1}$.

因此，根据s的定义， N_i 中的每个元素与 N_k 中的每个元素的辛内积均为零。这证明了 $\bigoplus N_k \subseteq C^{\perp_s}$。注意， N_i 和 N_j 的维数均为 $\mathbb{F}_p$-维数$_{k=1k\neq j}$2 deg(f_i)。现在，由 dim$^{\mathbb{F}_p}$(C) + dim$^{\mathbb{F}_p}$($C^{\perp_s}$) $= 2n$ 以及 dim$^{\mathbb{F}_p}$(C) $= 2\deg(f_i)$ 这些事实可得另一个包含关系。□

接下来，我们求出 N_i for $1 \leq i \leq s$ 中每个不可约加性循环码的辛对偶。

引理 4.4. 设 $C \subsetneq N_i$ 是某个 $1 \leq i \leq s$ 的非零加性循环码。那么

$$C^{\perp_s} = (\bigoplus_{\substack{k=1\\k\neq j}}^{s} N_k) \bigoplus \langle g_1(x) + \omega g_2(x)\rangle_{\mathbb{F}_p[x]}, \tag{4.1}$$

其中 $Z_j = -Z_i$ 且

$$g_1(x) + \omega g_2(x) = \begin{cases} ((x^n-1)/f_j(x))(s(x^{-1}) + \omega) & if\ C = \langle \big((x^n-1)/f_i(x)\big)\big(\omega + s(x)\big)\rangle_{\mathbb{F}_p[x]} \\ (x^n-1)/f_j(x) & if\ C = \langle (x^n-1)/f_i(x)\rangle_{\mathbb{F}_p[x]} \end{cases}.$$

$_s$证明。 由引理 4.3，可知 $\bigoplus N_k \subseteq C^{\perp_s}$。注意 dim$^{\mathbb{F}_p}$($\langle g_1(x)+\omega g_2(x)\rangle_{\mathbb{F}_p[x]}$) $=_{k=1k\neq j}$ dim$^{\mathbb{F}_p}$(C)。因此，只需证明 C 与 $g_1(x) + \omega g_2(x)$ 及其所有循环移位正交。我们分两步证明后一个结论。首先，设 $C = \langle \big((x^n-1)/f_i(x)\big)\big(\omega+s(x)\big)\rangle_{\mathbb{F}_p[x]}$，其中 $s(x) \in \mathbb{F}_p[x]$。为证明码 C 与 $\langle g_1(x) + \omega g_2(x)\rangle_{\mathbb{F}_p[x]}$ 正交，我们应用注 4.1。特别地，

$$\begin{aligned}\big((x^n-1)/f_i(x)\big)s(x)g_2(x^{-1}) - \big((x^n-1)/f_i(x)\big)g_1(x^{-1}) &\equiv \big((x^n-1)/f_i(x)\big)s(x)\big((x^n-1)/f_i(x)\big) \\ &\quad - \big((x^n-1)/f_i(x)\big)\big((x^n-1)/f_i(x)\big)s(x) \equiv 0 \pmod{x^n-1}.\end{aligned}$$

接下来，假设 $C = \langle (x^n-1)/f_i(x)\rangle_{\mathbb{F}_p[x]}$。那么

$$\begin{aligned}\big((x^n-1)/f_i(x)\big)g_2(x^{-1}) - \big((x^n-1)/f_i(x)\big)g_1(x^{-1}) &\equiv \big((x^n-1)/f_i(x)\big)0 - 0\big((x^n-1)/f_j(x)\big)s(x) \\ &\equiv 0 \pmod{x^n-1}.\end{aligned}$$

这表明码 C 与由 $g_1(x)+\omega g_2(x)$ 生成的加性循环码正交，并完成了证明。□

注意，正如我们在引理 4.4 中所示，当 $C = \langle \big((x^n-1)/f_i(x)\big)\big(\omega + s(x)\big)\rangle_{\mathbb{F}_p[x]}$ 时，其辛内积包含码 $C' = \langle (x^n-1)/f_j(x))(s(x^{-1}) + \omega)\rangle_{\mathbb{F}_p[x]}$。码 C' 不属于引理 3.4 第 (4) 部分给出的形式之一。为了使用引理 3.4 第 (4) 部分引入的标准记号表示码 C'，我们选择其生成元为 $g(x) = (x^n-1)/f_j(x))(t(x) + \omega$，其中 $t(x) \equiv s(x^{-1})$（模 $f_j(x)$）。现在很容易看出， $g(x)$ 属于引理 3.4 第 (4) 部分引入的集合 A，且 $C' = \langle (x^n-1)/f_j(x))(t(x) + \omega)\rangle_{\mathbb{F}_p[x]}$。

接下来，我们结合前两个引理的结果以及定理 3的结果6 ，确定任意加性循环码的辛对偶的生成多项式。

定理 4.5. 设 C 是长度为 n 、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码，使得 $C = \bigoplus_{i=1}^{s} C_i$，其中对每个 $1 \leq i \leq s$，C_i 都是 N_i 中的加性循环码。 那么 $C^{\perp_s} = \langle \sum_{i=1}^{s} g_i(x) + s\omega k_i(x) \sum \omega h_i(x) \rangle_{\mathbb{F}_p[x]}$，其中对每个 $1 \leq i \leq s$，我们有 $Z_j = -Z_i$ 和 $i=1$

- $g_i(x) = k_i(x) = h_i(x) = 0$ 若 $C_j = N_j$,
- $g_i(x) = h_i(x) = (x^n - 1)/f_i(x)$，且 $k_i(x) = 0$ 若 $C_j = 0$,
- $g_i(x) + \omega k_i(x) = \big((x^n - 1)/f_i(x)\big)\big(\omega + t_i(x)\big)$ 且 $h_i(x) = 0$ 若 $C_j = \langle \big((x^n - 1)/f_j(x)\big)\big(\omega + s_j(x)\big)\rangle_{\mathbb{F}_p[x]}$ 且 $t_i(x) \equiv s_j(x^{-1})$（模 $f_j(x)$），
- $g_i(x) = (x^n - 1)/f_i(x)$，且 $k_i(x) = h_i(x) = 0$ 若 $C_j = \langle (x^n - 1)/f_j(x) \rangle_{\mathbb{F}_p[x]}$。

证明。 我们应用引理 4。3 和 4。4 来证明该命题。若 $C_j = N_j$，则 $C^{\perp_s} \cap N_i = \{0\}$根据引理 4。3。此外，根据同一引理，若 $C_j = 0$，则 $N_i \subseteq C^{\perp_s}$。这证明了前两条。最后，引理4。4 意味着

- $\langle \big((x^n - 1)/f_i(x)\big)\big(\omega + t_i(x)\big)\rangle_{\mathbb{F}_p[x]} \subseteq C^{\perp_s}$ if $C_j = \langle \big((x^n - 1)/f_j(x)\big)\big(\omega + s_j(x)\big)\rangle_{\mathbb{F}_p[x]}$, and
- $\langle (x^n - 1)/f_i(x) \rangle_{\mathbb{F}_p[x]} \subseteq C^{\perp_s}$ if $C_j = \langle (x^n - 1)/f_i(x) \rangle_{\mathbb{F}_p[x]}$.

这证明了最后两条的结论。 □

为了确定 $\mathbb{F}_{p^2}$ 上的自正交和自对偶加性循环码，我们需要更多关于 $x^n - 1$ 在 $\mathbb{F}_p$ 上的不可约因子的信息。设 $Z_1, Z_2, \ldots, Z_r$ 和 $Z'_1, -Z'_1, \ldots, Z'_t, -Z'_t$ 是模 n 的所有 p-分圆陪集，其中 $Z_i = -Z_i$ 且 $r + 2t = s$。每个 Z_i 都对应一个不可约多项式 $f_i(x)$，而 $(Z'_j, -Z'_j)$ 对应于 $\mathbb{F}_p$ 上的一对不可约多项式 $(f_{j1}(x)\ f_{j2}(x))$。因此，我们可以将 $x^n - 1$ 的不可约分解重写为

$$x^n - 1 = \prod_{i=1}^{r} f_i(x) \prod_{j=1}^{t} f_{j1}(x) f_{j2}(x).$$

在接下来的结果中，我们使用上述分圆陪集表示法。接下来，我们对 $\mathbb{F}_{p^2}$ 上的自正交和自对偶加性码进行分类。

定理 4.6. 设 C 是一个长度为 n 的 $\mathbb{F}_{p^2}$ 上的加性循环码，且 $C = \bigoplus_{i=1} C_i$，其中C_i 对每个 $1 \leq i \leq s$ 都是 N_i 内的一个加性循环码。那么，当且仅当以下条件成立时，C 是辛自正交的：

(1) 对所有 $1 \leq k \leq r$，以下条件中恰有一个成立。(a) $C_k = 0$。(b) $C_k = \langle ((x^n - 1)/f_k(x))(s(x) + \omega)\rangle_{\mathbb{F}_p[x]}$，其中 $f_k \mid s(x^{-1}) - s(x)$。(c) $C_k = \langle (x^n - 1)/f_k(x) \rangle_{\mathbb{F}_p[x]}$。

(2) 对于所有 $1 \leq j \leq t$，以下条件恰有一个成立。
   (a) $C_{j1} = 0$ *or* $C_{j2} = 0$.
   (b) $C_{j1} = \langle ((x^n - 1)/f_{j1}(x))(s(x) + \omega)\rangle_{\mathbb{F}_p[x]}$ *and* $C_{j2} = \langle ((x^n - 1)/f_{j2}(x))(s(x^{-1}) + \omega)\rangle_{\mathbb{F}_p[x]}$.
   (c) $C_{j1} = \langle (x^n - 1)/f_{j1}(x) \rangle_{\mathbb{F}_p[x]}$ *and* $C_{j2} = \langle (x^n - 1)/f_{j2}(x) \rangle_{\mathbb{F}_p[x]}$.

证明。首先，设 $1 \le k \le r$。由引理 4.3，若 $C_k = N_k$，则 $C^{\perp_s} \cap N_k = \{0\}$。因此 C_k 不可能有两个生成多项式。此外，由引理 4.4，若 $0 \neq C_k = \langle((x^n-1)/f_k(x))(s(x)+\omega)\rangle_{\mathbb{F}_p[x]}$，则 $\langle((x^n-1)/f_k(x))(s(x^{-1})+\omega)\rangle_{\mathbb{F}_p[x]} \subseteq C^{\perp_s}$。因此，$C_k$ 是自正交的，当且仅当

$$C_k = \langle((x^n-1)/f_k(x))(s(x)+\omega)\rangle_{\mathbb{F}_p[x]} = \langle((x^n-1)/f_k(x))(s(x^{-1})+\omega)\rangle_{\mathbb{F}_p[x]}.$$

注意，上述等式成立当且仅当 $f_k \mid s(x^{-1}) - s(x)$。因此，$C_k$ 是自正交的当且仅当第 (1) 部分中的某个条件成立。

接下来，设 $1 \le j \le t$。根据引理 4.3，若 $C_{j1} = N_{j1}$，则 $C^{\perp_s} \cap N_{j2} = \{0\}$。因此，如果 C_{j1} 或C_{j2} 有两个生成多项式，则另一个码应为零。此外，同一引理表明，若 $C_{j1} = 0$ 或 $C_{j2} = 0$，则 $C_{j1} + C_{j2}$ 是自正交的。因此，我们只需考虑 C_{j1} 和 C_{j2} 均恰有一个非零生成元的情形。根据引理 4.4，若$C_{j1} = \langle((x^n-1)/f_{j1}(x))(s(x)+\omega)\rangle_{\mathbb{F}_p[x]}$，则

$$C^{\perp_s} \cap N_{j2} = \langle((x^n-1)/f_{j2}(x))(s(x^{-1})+\omega)\rangle_{\mathbb{F}_p[x]}.$$

在这种情况下，码 $C_{j1} \oplus C_{j2}$ 是自正交的，当且仅当条件 (2)(b) 成立。通过应用引理4。4. □

接下来，我们利用上述条件刻画 $\mathbb{F}_{p^2}$ 上所有的辛自对偶加性循环码。

$_s$推论 4.7. 设 C 是一个长度为 n、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码，满足 $C = \bigoplus C_i$，其中对于每个 $1 \le i \le s$，$_{i=1}C_i$ 是 N_i 内的一个加性循环码。那么，C 是辛自对偶的，当且仅当

(1) 对所有 $1 \le k \le r$，以下条件恰有一个成立。(a) $C_k = \langle((x^n-1)/f_k(x))(s(x)+\omega)\rangle_{\mathbb{F}_p[x]}$，其中 $f_k \mid s(x^{-1}) - s(x)$。(b) $C_k = \langle(x^n-1)/f_k(x)\rangle_{\mathbb{F}_p[x]}$。(2) 对所有 $1 \le j \le t$，以下条件恰有一个成立。

(a) $C_{j1} = 0$ *and* $C_{j2} = N_{j2}$.
(b) $C_{j2} = 0$ *and* $C_{j1} = N_{j1}$.
(c) $C_{j1} = \langle((x^n-1)/f_{j1}(x))(s(x)+\omega)\rangle_{\mathbb{F}_p[x]}$ *and* $C_{j2} = \langle((x^n-1)/f_{j2}(x))(s(x^{-1})+\omega)\rangle_{\mathbb{F}_p[x]}$.
(d) $C_{j1} = \langle(x^n-1)/f_{j1}(x)\rangle_{\mathbb{F}_p[x]}$ *and* $C_{j2} = \langle(x^n-1)/f_{j2}(x)\rangle_{\mathbb{F}_p[x]}$.

证明。注意，所有定义在 $\mathbb{F}_{p^2}$ 上的自对偶加性循环码都满足定理4。6 的条件，且具有最大维数。因此，将最大性质代入定理 4。6 的条件即可轻易得出该结果。□

我们的下一个目标是计算所有加性循环码的参数 $e = \dim_{\mathbb{F}_p}(C) - \dim_{\mathbb{F}_p}(C \cap C^{\perp_s})$。参数 e 决定了加性循环码 C 距离自正交有多近。该参数在我们将在下一节应用的量子构造中起着重要作用。

$_s$定理 4.8。设 C 是一个长度为 n、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码，满足 $C = \bigoplus C_i$，其中$_{i=1}$
C_i 对于每个 $1 \le i \le s$，N_i 内的一个加性循环码。令

(1) $B_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_{t_1}\} \subseteq \{1, 2, \ldots, r\}$ 使得 $C_{\alpha_l} = N_{\alpha_l}$ 对所有 $1 \le l \le t_1$成立，(2) $B_2 = \{\beta_1, \beta_2, \ldots, \beta_{t_2}\} \subseteq \{1, 2, \ldots, r\}$ 使得 $C_{\beta_l} = \langle((x^n-1)/f_{\beta_l}(x))(^{s_{\beta_l}}(x)+\omega)\rangle_{\mathbb{F}_p[x]}$且 $f_{\beta_l} \nmid s_{\beta_l}(x^{-1}) -\, ^{s_{\beta_l}}(x)$ 对所有 $1 \le l \le t_2$成立，

(3) $B_3 = \{\gamma_1, \gamma_2, \ldots, \gamma_{t_3}\} \subseteq \{1, 2, \ldots, t\}$ 使得 $C_{\gamma_l 1}$ 和 $C_{\gamma_l 2}$ 中一个由两个多项式生成，另一个只有一个生成多项式，对所有 $1 \le l \le t_3$ 成立，(4) $B_4 = \{\kappa_1, \kappa_2, \ldots, \kappa_{t_4}\} \subseteq \{1, 2, \ldots, t\}$ 使得 $C_{\kappa_l 1}$ 和 $C_{\kappa_l 2}$ 均由两个多项式生成，对所有 $1 \le l \le t_4$ 成立，(5) $B_5 = \{\sigma_1, \sigma_2, \ldots, \sigma_{t_5}\} \subseteq \{1, 2, \ldots, t\}$ 使得 $C_{\sigma_l 1}$ 和 $C_{\sigma_l 2}$ 均由一个多项式生成，对所有 $1 \le l \le t_5$ 成立，且 (a) 若 $C_{\sigma_l 1} = \langle((x^n-1)/f_{\sigma_l 1}(x))(s_{\sigma_l}(x)+\omega)\rangle_{\mathbb{F}_p[x]}$，则 $C_{\sigma_l 2} \neq \langle((x^n-1)/f_{\sigma_l 2}(x))(s_{\sigma_l}(x^{-1}) + \omega)\rangle_{\mathbb{F}_p[x]}$. (b) 若 $C_{\sigma_l 1} = \langle(x^n-1)/f_{\sigma_l 1}(x)\rangle_{\mathbb{F}_p[x]}$，则 $C_{\sigma_l 2} \neq \langle(x^n-1)/f_{\sigma_l 2}(x)\rangle_{\mathbb{F}_p[x]}$。

Then

$$e = \dim_{\mathbb{F}_p}(C) - \dim_{\mathbb{F}_p}(C \cap C^{\perp_s}) = \sum_{l=1}^{t_1} 2|Z_{\alpha_l}| + \sum_{l=1}^{t_2} |Z_{\beta_l}| + \sum_{l=1}^{t_3} 2|Z_{\gamma_l}| + \sum_{l=1}^{t_4} 4|Z_{\kappa_l}| + \sum_{l=1}^{t_5} 2|Z_{\sigma_l}|. \quad (4.2)$$

证明。 根据定理 4。6，加性循环码不是辛自正交的充要条件是至少有一个集合 $B_1 - B_5$ 非空。接下来，我们分别考虑情形 (1)–(5)。

(1) 设 $j \in B_1$。在这种情况下，$C^{\perp_s} \cap C_j = \{0\}$，这意味着 $\dim^{\mathbb{F}_p}(C_j) - \dim^{\mathbb{F}_p}(C_j \cap C^{\perp_s}) = 2|Z_j|$。 (2) 设 $j \in B_2$。在这种情况下，$C^{\perp_s} \cap C_j = \{0\}$，这意味着 $\dim^{\mathbb{F}_p}(C_j) - \dim^{\mathbb{F}_p}(C_j \cap C^{\perp_s}) = |Z_j|$。 (3) 设 $j \in B_3$。不失一般性，假设 $C_{j1} = N_{j1}$，且 C_{j2} 是 N_{j2}的一个不可约子码。在这种情况下，交 $C^{\perp_s} \cap (C_{j1} \oplus C_{j2})$ 是 N_{j1}的一个不可约子码，这意味着 $\dim^{\mathbb{F}_p}(C_j) - \dim^{\mathbb{F}_p}((C_{j1} \oplus C_{j2}) \cap C^{\perp_s}) = 3|Z_j| - |Z_j| = 2|Z_j|$。 (4) 设 $j \in B_4$。在这种情况下，$C^{\perp_s} \cap (C_{j1} \oplus C_{j2}) = \{0\}$，这意味着 $\dim^{\mathbb{F}_p}(C_j) - \dim^{\mathbb{F}_p}((C_{j1} \oplus C_{j2}) \cap C^{\perp_s}) = 4|Z_j|$。 (5) 设 $j \in B_5$。在 (a) 和 (b) 两部分中，$C^{\perp_s} \cap (C_{j1} \oplus C_{j2}) = \{0\}$，这意味着 $\dim^{\mathbb{F}_p}(C_j) - \dim^{\mathbb{F}_p}((C_{j1} \oplus C_{j2}) \cap C^{\perp_s}) = 2|Z_j|$。

现在，结合上述观察即可得到该结果。

□

注意，对于 C_i 且 $\deg(f_i(x)) = 1$ 的情形，定理 4.8 的情形 (2) 不会发生。此外，对于每个 $1 \le i \le r$，分圆陪集 Z_i 要么是单元素集，要么其大小为偶数。这主要是因为对于每个 $0 \neq a \in Z_i$，若 $a \equiv -a \pmod n$，则 $n \mid 2a$，这意味着 n 为偶数。因此，在此情形下 $p \neq 2$ （我们假设 $\gcd(n, p) = 1$）且 $Z_i = \{a\}$。所以，若 Z_i 满足定理 4.8 的情形 (2) 且 $|Z_i| > 1$，则对任意 $a \in Z_i$，都有 $-a \in Z_i$ 且 $-a \neq a \pmod n$。这意味着 $|Z_i|$ 是偶整数。根据这一事实以及公式 (4.2)，加性循环码的近似自正交参数 e 总是偶整数。接下来，我们对 e 取值较小的加性循环码进行分类。首先，我们需要以下预备结果。

引理 4.9. 设 p 为素数，并且对于某个正数 n，n 与 p 的最大公因式为 $= 1$。

(i) 如果 $\gcd(n, p-1) = d$，那么模 n 有 d 个 p-分圆陪集是单元素陪集，并且它们的陪集首均为 $\{k\frac{n}{d} : 0 \le k \le d-1\}$。(ii) 如果 $\gcd(n, p-1) = d$ 且 $\gcd(n, p^2-1) = d'$，那么模 n 有 $\frac{d'-d}{2}$ 个大小为二的分圆陪集。

证明。(i) 证明很容易由以下事实得出：$\{a\}$ 是单元素陪集，当且仅当 $a \equiv pa$（模 n），或者等价地，当且仅当 $a(p-1) \equiv 0$（模 n）。根据初等数论，如果 $\gcd(n, p-1) = d$，那么后一个方程有 d 个解，其形式为 $\{k\frac{n}{d} : 0 \le k \le d-1\}$。

(ii) 模 n 的包含 a 的 p-分圆陪集的大小为二，当且仅当 $a \equiv p^2 a$ (模 n) 且 $a \not\equiv pa$ (模 n)。因此，通过求解 $a \equiv p^2 a$ (模 n)，我们得到 d' 个大小为二的陪集候选。此外，每个单元素分圆陪集都由后一方程的一个解构成。还要注意，包含 a 和 pa 的大小为二的 p-分圆陪集，在前面的讨论中被计算了两次。因此，不同的陪集共有 $\frac{d'-d}{2}$ 个。□

例如，对于奇数 n，模 n 的唯一单元素 p-分圆陪集是 $\{0\}$，当 $p = 2$ 或 $p = 3$ 时。如果 n 为偶数，则 $\{\frac{n}{2}\}$ 和 $\{0\}$ 是 $p = 3$ 的仅有的单元素分圆陪集。下一个定理将对所有满足 $e = 2$ 的加性循环码进行分类。注意，若加性循环码是辛自正交的，则会出现 $e = 0$ 这一情形，而该情形已在定理4中得到刻画。6。

定理 4.10. 设 $C = \bigoplus_{i=1}^{s} C_i$ 是长度为 n、定义在 $\mathbb{F}_{p^2}$ 上的加性循环码。那么

$$e = \dim_{\mathbb{F}_p}(C) - \dim_{\mathbb{F}_p}(C \cap C^{\perp_s}) = 2$$

当且仅当所有 C_i 均满足定理 4.6 的条件，但其中一个除外，该项对应于

(1) 一个单元素陪集，且满足定理 (1) 的条件 4.8，(2) 一个大小为二的陪集，且满足定理 (2) 的条件 4.8。

证明。 考虑公式 (4.2)，并考虑定理 4.8的所有条件，即可得出该结果。□

下一节给出的许多破纪录量子码都具有 $e = 2$。一般而言，所有加性循环码的总数可能非常庞大。因此，对 e 值进行分类，有助于大幅缩小搜索具有良好参数的量子码时的搜索范围。

5. New binary quantum codes

本节首先回顾一种由加性码构造二元量子码的方法，该方法不要求满足定理 2.1中的辛自正交条件。随后，我们将此方法应用于若干个定义在 $\mathbb{F}_4$ 上的近自正交加性循环码，并构造新的二元量子码。在本节余下部分，我们展示由$\mathbb{F}_4 = \{0, 1, \omega, \omega+1\}$构成的四元域，其中 $\omega^2 = \omega + 1$。

定理 5.1。 [5, 推论 3.3。7],[19] 设 C 是一个定义在 $(n, 2^k)$ 上的加法码 $\mathbb{F}_4$ 且

$$r = \frac{2n - k - \dim_{\mathbb{F}_p}(C \cap C^{\perp_s})}{2}$$

则存在一个参数为 $[[n+r, k-n+r, d]]_2$ 的二元量子码，其中

$$d \ge \min\{d(C), d(C + C^{\perp_s}) + 1\}.$$

请注意，我们在定理 4.8 的计算中利用了定理 5.1的结果。特别是，定理 5.1 中的值 r 为 $\frac{\dim^{\mathbb{F}_p}(C^{\perp_s}) - \dim^{\mathbb{F}_p}(C \cap C^{\perp_s})}{2}$，其中分子衡量码 $C^{\perp_s}$的~~近似自正交性。接下来~~，我们简要介绍两个新的二元量子码。表 1 中给出的其余新二元量子码也可以用类似的方法构造。

例 5.2。设 $n = 21$和 $C = \langle g(x)+\omega k(x)\rangle_{\mathbb{F}_2[x]}$是 $\mathbb{F}_4$上的一个加性循环码，其中

$$g(x) = x^{20} + x^{17} + x^{15} + x^{13} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

and

$$k(x) = x^{19} + x^{18} + x^{17} + x^{16} + x^{14} + x^{10} + x^5 + x^4 + x^3 + x^2 + x + 1.$$

该码 C 是一个 $(21, 2^{20})$ 加法码。此外，我们利用定理4.8 的结果进行计算，得到 C 的近似自正交参数为 $e = 2$。此外，

$$7 = \min\{d(C^{\perp_s}), d(C + C^{\perp_s}) + 1\}.$$

因此，将定理5.1 的构造应用于码 $C^{\perp_s}$，得到一个新的量子码，其参数为 $[[22, 2, 7]]_2$。与此前已知的具有相同长度和维数、最小距离为 6 的最佳量子码相比，它的最小距离更大。

例 5.3。设 $n = 35$和 $C = \langle g(x)+\omega k(x)\rangle_{\mathbb{F}_2[x]}$是 $\mathbb{F}_4$上的一个加性循环码，其中 e

$$g(x) = x^{33} + x^{29} + x^{28} + x^{24} + x^{19} + x^{18} + x^{15} + x^{13} + x^{12} + x^{11} + x^6 + x^4 + x + 1$$

and

$$k(x) = x^{34} + x^{33} + x^{31} + x^{30} + x^{29} + x^{27} + x^{25} + x^{23} + x^{22} + x^{20} + x^{19} + x^{18} + x^{15} + x^{12} + x^8 + x^3 + x.$$

该码 C 的参数为 $(35, 2^{20})$，它是定义在 $\mathbb{F}_4$上的加性循环码。此外，定理4.8 的结果表明，C 的近似自正交参数为 $e = 4$。此外，

$$6 = \min\{d(C^{\perp_s}), d(C + C^{\perp_s}) + 1\}.$$

因此，将定理5.1 中的构造应用于码 $C^{\perp_s}$，可得到一个破纪录量子码，其参数为 $[[37, 17, 6]]_2$。此前已知的具有相同参数的最佳二元量子码的最小距离为 5。

一般而言，为了应用定理5.1给出的量子构造，我们着眼于近似自正交参数 $e \leq 4$较小的加性循环码。因为当 e 值较小时，更有可能得到新的量子码。在表1中，我们列出了新二元量子码的参数。表中，我们从一个定义在 C 上的加性循环码 $\mathbb{F}_4$ 开始，计算其近似自正交性。然后，将定理5.1中的量子构造应用于码 $C^{\perp_s}$。相应量子码的参数列于第四列。此外，表格最后一列给出了此前具有相同长度和维数的量子码的最小距离。此前的最小距离取自 Grassl 码表 [12]。表 1 中的加性循环码的生成多项式列于表2。

另请注意，将定理 2.2 中介绍的次级构造应用于表 1 中的新码，可以得到更多破纪录量子码。特别是，仅这些新$[[52, 24, 8]]_2$ 量子码就能得到以下新的量子码：

$$[[52, 21, 8]]_2, [[52, 22, 8]]_2, [[52, 23, 8]]_2, [[53, 21, 8]]_2, [[53, 22, 8]]_2, [[53, 23, 8]]_2, [[53, 24, 8]]_2.$$

大约在我们开展研究的同时，[14] 的作者独立地通过利用准循环码与加性循环码之间的联系，发现了若干新的二元量子码。特别是，我们新得到的三个量子码，即 $[[45, 6, 10]], [[45, 45, 10, 9]]$, 和 $[[51, 8, 11]]$,也属于 [14]中的新量子码。

Acknowledgement

作者谨向 Petr Lisoněk 和 Markus Grassl 致谢，感谢他们进行了许多有趣的讨论并提出了宝贵意见。

No	长度	e 值	参数	先前的距离
1	$n = 21$	2	$[[22, 2, \mathbf{7}]]_2$	6
2	$n = 35$	4	$[[37, 17, \mathbf{6}]]_2$	5
3	$n = 45$	0	$[[45, 6, \mathbf{10}]]_2$	9
4	$n = 45$	0	$[[45, 10, \mathbf{9}]]_2$	8
5	$n = 51$	0	$[[51, 8, \mathbf{11}]]_2$	10
6	$n = 51$	2	$[[52, 16, \mathbf{10}]]_2$	9
7	$n = 51$	2	$[[52, 24, \mathbf{8}]]_2$	7
8	$n = 63$	2	$[[64, 33, \mathbf{8}]]_2$	7
9	$n = 63$	2	$[[64, 34, \mathbf{8}]]_2$	7
10	$n = 63$	2	$[[64, 35, \mathbf{8}]]_2$	7

TABLE 1. 新二元量子码的参数。

REFERENCES

[1] J. Bierbrauer 和 Y. Edel。量子扭曲码。 *Journal of Combinatorial Designs*, 8(3):174–188, 2000。[2] W. Bosma、J. Cannon 和 C. Playoust。Magma 代数系统 I：用户语言。 *Journal of Symbolic Computation* 24 3 4 235 265, 1997 , (-): – 。[3] A. R. Calderbank、E. M. Rains、P. Shor 和 N. J. Sloane。基于 GF(4) 上的码实现量子纠错。 *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998。[4] Y. Cao 和 Y. Gao。 $\mathbb{F}_{q^l}$上的重复根循环 $\mathbb{F}_q$线性码。 *Finite Fields Appl.*, 31:202–227, 2015。[5] R. Dastbasteh。 *Quantum stabilizer codes*。硕士论文，萨班哲大学，2017。[6] R. Dastbasteh 和 P. Lisonek。基于 $\mathbb{F}_4$ *arXiv preprint arXiv:2211.00891* 2022 上的自对偶码构造新量子码。, 。[7] B. K. Dey 和 B. S. Rajan。基于 F q 的线性循环码：离散傅里叶变换方法。 *Designs, Codes and Cryptography*, 34 1 89 116, 2005 ( ): – 。[8] D. S. Dummit 和 R. M. Foote。 *Abstract algebra*, 第3卷。Wiley Hoboken，2004。[9] M. F. Ezerman。量子纠错码。载于 W. C. Huffman、J.-L. Kim 和 P. Sol´e 编，*Concise* {chapter }。 *encyclopedia of coding theory* Chapman and Hall/CRC，{ }。[10] M. F. Ezerman、S. Ling、B. ¨Ozkaya 和 P. Sol´e。由 $\mathbb{F}_4$ 和$\mathbb{F}_9$上的准循环码构造优良稳定子码。载于 *2019 IEEE International Symposium on Information Theory (ISIT)*, 第2898–2902页。IEEE，2019。[11] D. Gottesman。达到量子汉明界的量子纠错码类。 *Physical Review A* 54 3 1862, 1996 , ( ): 。[12] M. Grassl。编码表：各种类型编码参数的界。http://www.codetables.de/。[13] M. Grassl。代数量子码：连接量子力学与离散数学。*Math. Comput. Syst. Theory* 6 4 243 259, 2021 *Int. J. Comput.* , ( ): – 。[14] C. Guan、R. Li 和 Z. Ma。辛自正交准循环码。 *arXiv preprint arXiv:2212.14225*, 2022。[15] C. G ¨ uneri、F. ¨ Ozdemir 和 P. Sole。论准循环码的加法循环结构。, ( ): – 。[16] W. C. Huffman。 $\mathbb{F}_4$上的加法循环码。 *Adv. Math. Commun.*, 1(4):427–459, 2007。[17] W. C. Huffman。 $\mathbb{F}_4$上的加法循环码。 *Adv. Math. Commun.*, 2(3):309–343, 2008。[18] A. Ketkar、A. Klappenecker、S. Kumar 和 P. K. Sarvepalli。有限域上的非二元稳定子码。*IEEE transactions on information theory*, 52(11):4892–4914, 2006。[19] P. Lisonˇek 和 V. Singh。量子码构造。在挪威 Loen 举行的第三届布尔函数及其应用国际研讨会上报告。https://people.uib.no/chunlei.li/workshops/BFA2018/Slides/Lisonek.pdf，2018。[20] P. Lisonˇek 和 V. Singh。由近似自正交四元线性码构造量子码。 *Designs Codes and Cryptography* 73 2 417 424, 2014 *Designs Codes* , , ( ): – 。[21] K. Samei 和 S. Mahmoudi。循环R加法码。 *Discrete Mathematics*, 340(7):1657–1668, 2017。

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BC, CANADA
Email address: rdastbas@sfu.ca, kh411@protonmail.com

No	定理中的生成多项式 3.6 （II）部分
1	g(x) $= x^{20}+x^{17}+x^{15}+x^{13}+x^{11}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+1$ k(x) $= x^{19}+x^{18}+x^{17}+x^{16}+x^{14}+x^{10}+x^{5}+x^{4}+x^{3}+x^{2}+x+1$ h(x) $= 0$
2	g(x) $= x^{33}+x^{29}+x^{28}+x^{24}+x^{19}+x^{18}+x^{15}+x^{13}+x^{12}+x^{11}+x^{6}+x^{4}+x+1$ k(x) $= x^{34}+x^{33}+x^{31}+x^{30}+x^{29}+x^{27}+x^{25}+x^{23}+x^{22}+x^{20}+x^{19}+x^{18}+x^{15}+x^{12}+x^{8}+x^{3}+x$ h(x)=0
3	g(x) $= x^{44}+x^{43}+x^{41}+x^{40}+x^{39}+x^{38}+x^{34}+x^{33}+x^{30}+x^{26}+x^{24}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{11}+x^{9}+x^{5}+x^{3}+1$ k(x) $= x^{43}+x^{42}+x^{41}+x^{40}+x^{36}+x^{33}+x^{32}+x^{31}+x^{30}+x^{28}+x^{26}+x^{25}+x^{17}+x^{16}+x^{15}+x^{13}+x^{11}+x^{10}+x^{2}+x$ h(x) $= 0$
4	g(x) $= x^{44}+x^{43}+x^{40}+x^{38}+x^{37}+x^{34}+x^{31}+x^{27}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{14}+x^{12}+x^{7}+x^{6}+x^{5}+x^{3}+x+1$ k(x) $= x^{44}+x^{41}+x^{40}+x^{37}+x^{36}+x^{35}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26}+x^{25}+x^{22}+x^{20}+x^{15}+x^{14}+x^{12}+x^{11}+x^{10}+x^{7}+x^{5}$ h(x) $= 0$
5	g(x) $= x^{50}+x^{49}+x^{48}+x^{46}+x^{45}+x^{43}+x^{42}+x^{41}+x^{40}+x^{37}+x^{36}+x^{35}+x^{30}+x^{29}+x^{28}+x^{26}+x^{23}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{9}+x^{7}+x^{6}+x$ k(x) $= x^{50}+x^{47}+x^{44}+x^{43}+x^{42}+x^{41}+x^{40}+x^{38}+x^{36}+x^{35}+x^{33}+x^{32}+x^{28}+x^{26}+x^{24}+x^{21}+x^{20}+x^{16}+x^{14}+x^{12}+x^{9}+x^{8}+x^{7}+x+1$ h(x)=0
6	g(x) $= x^{48}+x^{40}+x^{37}+x^{36}+x^{33}+x^{31}+x^{30}+x^{24}+x^{23}+x^{21}+x^{19}+x^{15}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}+x^{4}+x^{3}+x+1$ k(x) $= x^{41}+x^{40}+x^{36}+x^{35}+x^{34}+x^{33}+x^{30}+x^{29}+x^{27}+x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{16}+x^{13}+x^{12}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x$ h(x) $= x^{50}+x^{49}+x^{48}+x^{47}+x^{46}+x^{45}+x^{44}+x^{41}+x^{40}+x^{39}+x^{33}+x^{31}+x^{30}+x^{28}+x^{25}+x^{22}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{9}+x^{5}+x^{4}$
7	g(x) $= x^{49}+x^{48}+x^{46}+x^{44}+x^{43}+x^{41}+x^{38}+x^{37}+x^{36}+x^{33}+x^{32}+x^{31}+x^{30}+x^{29}+x^{27}+x^{25}+x^{21}+x^{20}+x^{18}+x^{17}+x^{15}+x^{11}+x^{10}+x^{7}+x^{2}$ k(x) $= x^{43}+x^{42}+x^{41}+x^{40}+x^{38}+x^{37}+x^{33}+x^{32}+x^{30}+x^{26}+x^{24}+x^{22}+x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{9}+x^{5}+x^{4}+x^{2}+1$ h(x) $= x^{50}+x^{49}+x^{48}+x^{47}+x^{46}+x^{45}+x^{44}+x^{43}+x^{42}+x^{41}+x^{40}+x^{39}+x^{38}+x^{37}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1$
8	g(x) $= x^{61}+x^{60}+x^{59}+x^{57}+x^{56}+x^{53}+x^{52}+x^{51}+x^{42}+x^{41}+x^{38}+x^{36}+x^{34}+x^{32}+x^{31}+x^{28}+x^{27}+x^{26}+x^{24}+x^{20}+x^{19}+x^{16}+x^{14}+x^{13}+x^{12}+x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x$ k(x) $= x^{61}+x^{59}+x^{57}+x^{56}+x^{55}+x^{54}+x^{52}+x^{51}+x^{50}+x^{49}+x^{47}+x^{44}+x^{37}+x^{36}+x^{35}+x^{33}+x^{32}+x^{31}+x^{29}+x^{28}+x^{27}+x^{26}+x^{24}+x^{22}+x^{21}+x^{16}+x^{8}+x^{5}+x^{3}+x^{2}$ h(x) $= x^{62}+x^{61}+x^{60}+x^{59}+x^{58}+x^{51}+x^{49}+x^{47}+x^{44}+x^{43}+x^{40}+x^{36}+x^{33}+x^{31}+x^{30}+x^{28}+x^{27}+x^{23}+x^{22}+x^{21}+x^{19}+x^{14}+x^{13}+x^{11}+x^{9}+x^{8}+x^{7}+x^{4}+x^{3}+x^{2}+x$
9	g(x) $= x^{60}+x^{59}+x^{58}+x^{55}+x^{54}+x^{53}+x^{52}+x^{51}+x^{48}+x^{47}+x^{45}+x^{44}+x^{40}+x^{38}+x^{37}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{24}+x^{23}+x^{22}+x^{21}+x^{15}+x^{13}+x^{10}+x^{9}+x^{7}+x^{6}+x^{3}+x+1$ k(x) $= x^{62}+x^{59}+x^{56}+x^{55}+x^{54}+x^{53}+x^{49}+x^{47}+x^{46}+x^{42}+x^{41}+x^{40}+x^{37}+x^{35}+x^{33}+x^{31}+x^{29}+x^{28}+x^{27}+x^{24}+x^{20}+x^{19}+x^{16}+x^{15}+x^{14}+x^{7}+x^{4}+x^{2}+x$ h(x) $= 0$
10	g(x) $= x^{61}+x^{60}+x^{59}+x^{58}+x^{57}+x^{53}+x^{52}+x^{49}+x^{44}+x^{41}+x^{38}+x^{37}+x^{36}+x^{35}+x^{34}+x^{32}+x^{31}+x^{30}+x^{27}+x^{26}+x^{24}+x^{23}+x^{21}+x^{20}+x^{19}+x^{13}+x^{12}+x^{11}+x^{8}+x^{6}+x^{5}+x^{4}+x^{3}+x+1$ k(x) $= x^{60}+x^{58}+x^{57}+x^{56}+x^{52}+x^{48}+x^{47}+x^{46}+x^{44}+x^{42}+x^{40}+x^{39}+x^{38}+x^{36}+x^{35}+x^{34}+x^{32}+x^{31}+x^{30}+x^{26}+x^{25}+x^{24}+x^{22}+x^{19}+x^{18}+x^{17}+x^{13}+x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+1$ h(x) $= x^{62}+x^{61}+x^{60}+x^{59}+x^{58}+x^{51}+x^{49}+x^{47}+x^{44}+x^{43}+x^{40}+x^{36}+x^{33}+x^{31}+x^{30}+x^{28}+x^{27}+x^{23}+x^{22}+x^{21}+x^{19}+x^{14}+x^{13}+x^{11}+x^{9}+x^{8}+x^{7}+x^{4}+x^{3}+x^{2}+x$

TABLE 2. 表1中加法循环码的生成多项式