有限域上常循环厄密特对偶包含码及其应用

朱士信　　黄　山*　　李　锦
(合肥工业大学数学学院　合肥　230601)

摘　要：该文研究了有限域 $\mathrm{GF}\left(q^2\right)$ 上长度为 $\left(q^{2m}-1\right)\Big/\left(q^2-1\right)$ 的常循环码。给出一类常循环码是厄米特对偶包含码的一个充要条件，并确定了这类常循环厄米特对偶包含码的参数。利用厄米特构造，得到了比量子 BCH 码参数更好的量子纠错码。

关键词：量子码；厄米特构造；常循环码；分圆陪集
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2018)05-1072-07
DOI: 10.11999/JEIT170735

Constacyclic Hermitian Dual-containing Codes over Finite Fields and Their Application

ZHU Shixin　　HUANG Shan　　LI Jin
(*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230601, *China*)

Abstract: In this paper, constacyclic codes over the finite field $\mathrm{GF}\left(q^2\right)$ of length $\left(q^{2m}-1\right)\Big/\left(q^2-1\right)$ are studied. A sufficient and necessary condition for a class of constacyclic codes to be Hermitian dual-containing codes is given, and the parameters of this class of constacyclic codes are determined. Using Hermitian construction, the obtained quantum codes, are better than the parameters of quantum BCH codes.

Key words: Quantum codes; Hermitian construction; Constacyclic codes; Cyclotomic cosets

1　引言

与经典的纠错码理论相似，量子纠错码理论研究的一个核心问题是：构造与寻求最大可能极小距离的量子纠错码。文献[1,2]将复杂的物理量态转化为数学模型，给出量子纠错码和经典纠错码的联系。厄米特构造[1]作为量子码的一个重要构造方法被广泛应用，其关键点在于构造参数较好的厄米特对偶包含码。BCH 码是一类重要的线性码，它的一个显著特点是可以控制其纠错能力。2007 年，Aly 等人[3]利用 BCH 码构造量子码，给出狭义 BCH 码是厄米特对偶包含码的充分条件。Ma 等人[4]给出有限域 $\mathrm{GF}\left(q^2\right)$ 上长度为 $\left(q^{2m}-1\right)\Big/\left(q^2-1\right)$ 的 BCH 码是厄米特对偶包含码的一个充要条件，并且通过厄米特构造，得到了一系列量子码。此后，量子 BCH 码和量子循环码得到广泛研究[5–8]。

常循环码是循环码的推广，它既继承了循环码的良好性能，同时又具有若干新的特性。Guardia[9]定义了常循环 BCH 码，并由此获得了参数较好的量子码。2004 年，Lin[10]利用常循环码构造了具有较好参数的二元量子码。2013 年，Kai 等人[11]研究了两类负循环对偶包含码，与循环对偶包含码相比，负循环对偶包含码的参数更好，从而获得了参数较好的量子码。Xu 等人[12]研究了一类四元对偶包含码，并获得了一些新参数的量子码。最近，Yuan 等人[13]研究了有限域 $\mathrm{GF}\left(q^2\right)$ 上一类常循环量子码，与文献[3]中的量子 BCH 码比较，在相同设计距离下，他们构造的量子码具有更好的参数。文献[14,15]研究了两类常循环对偶码，同样，与文献[3]的构造相比，获得了新参数的量子码。

本文研究了 $\mathrm{GF}\left(q^2\right)$ 上长度为 $\left(q^{2m}-1\right)\Big/\left(q^2-1\right)$ 的常循环厄米特对偶包含码，给出了一类常循环码是厄米特对偶包含码的一个充分必要条件，并确定了这类常循环厄米特对偶包含码的参数。利用厄米特构造，获得了一系列量子码。在相同设计距离下，将其与文献[3]和文献[4]中的量子 BCH 码进行比较，发现本文构造的量子码具有较好的参数。

收稿日期：2017-07-20；改回日期：2018-01-10；网络出版：2018-03-14
*通信作者：黄山　huangshan5197@163.com
基金项目：国家自然科学基金(61772168, 61572168)，安徽省自然科学基金(1508085SQA198, 1708085QA01)
Foundation Items: The National Natural Science Foundation of China (61772168, 61572168), The Natural Science Found of Anhui Province (1508085SQA198, 1708085QA01)

2　基础知识

设 $\mathrm{GF}\left(q^2\right)$ 是一个 q^2 元有限域。对任意正整数 n，$\mathrm{GF}\left(q^2\right)^n$ 表示 $\mathrm{GF}\left(q^2\right)$ 上 n 维行向量空间。$\mathrm{GF}\left(q^2\right)^n$ 的任意一个非空线性子空间 C 称作一个 q^2 元线性码，n 叫该码的码长，C 中的向量称作码字。码字的 Hamming 重量定义为非零分量的个数，而码字 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 之间的 Hamming 距离定义为它们相异位的个数。码 C 的最小距离定义为不同码字之间 Hamming 距离的最小值。显然，线性码的最小距离等于非零码字的 Hamming 重量的最小值。通常，将维数为 k，最小距离为 d 的 q^2 元线性码记作 $[n,k,d]_{q^2}$。设 $\lambda \in \mathrm{GF}\left(q^2\right)^*$，$\lambda$-常循环移位 τ_λ 定义为 $\tau_\lambda\left(c_0,c_1,\cdots,c_{n-1}\right)=\left(\lambda c_{n-1},c_0,\cdots,c_{n-2}\right)$，其中 $(c_0,c_1,\cdots,c_{n-1}) \in \mathrm{GF}\left(q^2\right)^n$。设 C 是一个 $[n,k,d]_{q^2}$ 线性码，如果 $\tau_\lambda(C)=C$，则 C 为 $\mathrm{GF}\left(q^2\right)$ 上长度为 n 的 λ-常循环码。通常，将码字 $(c_0,c_1,\cdots,c_{n-1})$ 与其多项式表示 $c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 等同，因此，在同构的观点下，码 C 是 $\mathrm{GF}\left(q^2\right)$ 上长度为 n 的 λ-常循环码当且仅当 C 是商环 $R=\mathrm{GF}\left(q^2\right)[x]\Big/\left\langle x^n-\lambda\right\rangle$ 的理想。因为商环 R 是主理想环，所以 $\mathrm{GF}\left(q^2\right)$ 上长度为 n 的 λ-常循环码 $C=\left\langle g(x)\right\rangle$，其中 $g(x)$ 是 $x^n-\lambda$ 的首一因子，$g(x)$ 称为码 C 的生成多项式。

设 λ 的乘法阶为 r 且 $\gcd(n,q)=1$，则在 $\mathrm{GF}\left(q^2\right)$ 的某一个扩域中存在一个 rn-次本原单位根 ζ 使得 $\zeta^n=\lambda$。因此，$x^n-\lambda$ 的零点恰好是 ζ^{1+rj}，其中 $0 \le j \le n-1$。记 $\Omega=\{1+rj: 0 \le j \le n-1\}$，对任意 $i \in \Omega$，q^2-模 rn 的分圆陪集定义为 $\mathcal{C}_i=\left\{i,iq^2,\cdots,iq^{2(\ell_i-1)}\right\}$，其中 ℓ_i 是使得 $iq^{2\ell_i} \equiv i \pmod{rn}$ 的最小正整数，分圆陪集 $\mathcal{C}_i$ 中最小的元素称为陪集首。设 $C=\left\langle g(x)\right\rangle$ 是 $\mathrm{GF}\left(q^2\right)$ 上长度为 n 的 λ-常循环码，则 $g(x)$ 的零点指数集合 $Z=\{j: g(\zeta^j)=0\}$ 称为码 C 的定义集。由定义知 $Z \subseteq \Omega$ 且 Z 是一些 q^2-分圆陪集的并。如果 λ-常循环码 C 的定义集 $Z=\bigcup_{i=0}^{\delta-2}\mathcal{C}_{1+ri}$，则称 C 是设计距离为 δ 的 λ-常循环 BCH 码，并记作 C_δ。

对于 $\mathrm{GF}\left(q^2\right)^n$ 中的向量 $\boldsymbol{x}=\left(x_0,x_1,\cdots,x_{n-1}\right)$ 和 $\boldsymbol{y}=\left(y_0,y_1,\cdots,y_{n-1}\right)$，定义它们的厄米特内积为 $(\boldsymbol{x},\boldsymbol{y})_h=\sum_{i=0}^{n-1}x_iy_i^q$。码 C 的厄米特对偶码定义为 $C^{\perp_h}=\left\{\boldsymbol{y} \in \mathrm{GF}\left(q^2\right)^n: (\boldsymbol{x},\boldsymbol{y})_h=0,\forall \boldsymbol{x} \in C\right\}$。如果 $C^{\perp_h} \subseteq C$，称 C 为厄米特对偶包含码。利用厄米特对偶包含码，可以构造量子码。

引理 1[1](厄米特构造)　设 C 是一个 $[n,k,d]_{q^2}$ 线性码，如果 $C^{\perp_h} \subseteq C$，则存在参数为 $[[n,2k-n,d]]_q$ 的量子码。

由引理 1，构造量子码关键在于构造厄米特对偶包含码。关于 $\mathrm{GF}\left(q^2\right)$ 上的 λ-常循环码是厄米特对偶包含码，有如下判别方法。

引理 2[13]　设 $\lambda \in \mathrm{GF}\left(q^2\right)^*$ 且 $\mathrm{ord}(\lambda)=r$。设 $n \ge 2$ 且 $\gcd(n,q)=1$。设 C 是 $\mathrm{GF}\left(q^2\right)$ 上长度为 n 的 λ-常循环码且定义集为 Z。则 C 为厄米特对偶包含码当且仅当 $Z \cap Z^{-q}=\varnothing$，其中 $Z^{-q}=\{-qz: z \in Z\}$。

引理 3[16](常循环 BCH 界)　设 C_δ 是 $\mathrm{GF}\left(q^2\right)$ 上长度为 n，设计距离为 δ 的 λ-常循环 BCH 码，则码 C_δ 的最小距离 $d \ge \delta$。

3　厄米特对偶包含 λ-常循环码 C_δ 的最大设计距离

设 ω 是 $\mathrm{GF}\left(q^2\right)$ 的一个本原元，令 $\lambda=\omega^{q-1}$，则 $\mathrm{ord}(\lambda)=q+1$。设 $n=\left(q^{2m}-1\right)\Big/\left(q^2-1\right)$，其中 $m \ge 2$。定义 $Z_\delta=\bigcup_{i=0}^{\delta-2}\mathcal{C}_{1+(q+1)i}$，其中 $\delta \ge 2$，$\mathcal{C}_{1+(q+1)i}$ 为 q^2-模 $(q+1)n$ 包含 $1+(q+1)i$ 的分圆陪集。设 C_δ 是 $\mathrm{GF}\left(q^2\right)$ 上长度为 n，定义集为 Z_δ 的 λ-常循环 BCH 码。下面，确定 C_δ 是厄米特对偶包含码的最大设计距离。

引理 4　λ-常循环 BCH 码 C_δ 是厄米特对偶包含码当且仅当 $2 \le \delta \le \dfrac{q^{2\lfloor m/2\rfloor+1}-q}{q^2-1}+1$。

证明　令 $\overline{\delta}=\dfrac{q^{2\lfloor m/2\rfloor+1}-q}{q^2-1}+1$，设 $Z_{\overline{\delta}} \cap Z_{\overline{\delta}}^{-q} \ne \varnothing$，则存在整数 $0 \le k,\ l \le \overline{\delta}-2$ 使得 $1+(q+1)k \equiv -[1+(q+1)l]q^{2j+1} \pmod{(q+1)n}$，其中 $0 \le j \le m-1$。由于 $1+(q+1)l \equiv -[1+(q+1)k]q^{2(m-j-1)+1} \cdot(\mathrm{mod}(q+1)n)$，所以，可以假定 $0 \le j \le \lfloor (m-1)/2 \rfloor$ 且

$$[1+(q+1)k]+[1+(q+1)l]q^{2j+1} \equiv 0(\mathrm{mod}(q+1)n) \quad (1)$$

此时，

$$\begin{aligned}1 &< [1+(q+1)k]+[1+(q+1)l]q^{2j+1}\\ &\le \left[1+(q+1)\left(\overline{\delta}-2\right)\right]\left(q^{2\lfloor (m-1)/2\rfloor+1}+1\right)\\ &= \frac{q^{2m}+q^{2\lfloor m/2\rfloor+1}-q^{2\lfloor (m-1)/2\rfloor+3}-q^2}{q-1} < (q+1)n\end{aligned}$$

这与式(1)矛盾。因此 $Z_{\bar{\delta}} \cap Z_{\bar{\delta}}^{-q} = \varnothing$。由引理 2, $C_{\bar{\delta}}^{\perp_h} \subseteq C_{\bar{\delta}}$。因为，当 $\delta_1 \le \delta_2$ 时， $C_{\delta_1}^{\perp_h} \subseteq C_{\delta_2}^{\perp_h}$。故对任意的 $\delta \le \bar{\delta}$ ， $C_{\delta}^{\perp_h} \subseteq C_{\bar{\delta}}^{\perp_h} \subseteq C_{\bar{\delta}} \subseteq C_{\delta}$ 。另一方面，$-\left[1 + (q+1)\left(\bar{\delta}-1\right)\right] q^{2\lfloor (m-1)/2 \rfloor + 1} \equiv \dfrac{q^{2\lfloor (m-1)/2 \rfloor + 1} - 1}{q-1}$ $\cdot (\mathrm{mod}(q+1)n)$。注意到 $\dfrac{q^{2\lfloor (m-1)/2 \rfloor + 1} - 1}{q-1} = 1 + (q+1)$ $\cdot \dfrac{q^{2\lfloor (m-1)/2 \rfloor + 1} - q}{q^2 - 1} \le 1 + (q+1)\left(\bar{\delta}-1\right)$， 故 $\bar{\delta} - 1 \in Z_{\bar{\delta}+1}$ $\cap Z_{\bar{\delta}+1}^{-q}$。即 $\bar{\delta}$ 是使得 $Z_{\delta} \cap Z_{\delta}^{-q} = \varnothing$ 成立的最大整数。由引理 2, $\bar{\delta}$ 是使得 C_{δ} 为厄米特对偶包含码的最大设计距离。 证毕

下面确定 λ-常循环 BCH 码 C_{δ} 的维数。由定义

$$\dim\left(C_{\delta}\right) = n - \left|Z_{\delta}\right| \tag{2}$$

因为，$1 + (q+1)i \equiv 0 \left(\mathrm{mod}\, q^2\right)$，则存在 $0 \le i' < i$ 使得 $\mathcal{C}_{1+(q+1)i'} = \mathcal{C}_{1+(q+1)i}$ 。所以，假设 $i \not\equiv q-1$ $\cdot \left(\mathrm{mod}\, q^2\right)$。我们以 $\bar{a}$ 表示使得 $\bar{a} \equiv a (\mathrm{mod}(q+1)n)$ 成立的最小非负整数，其中 a 为正整数。

引理 5 设 $m \ge 3$ 为奇数。如果 $0 \le i \le \dfrac{q^m - q}{q^2 - 1} - 1$ 且 $i \not\equiv q-1 \left(\mathrm{mod}\, q^2\right)$， 则 $1 + (q+1)i$ 是 q^2 - 模 $(q+1)n$ 的分圆陪集 $\mathcal{C}_{1+(q+1)i}$ 的陪集首，并且 $\left|\mathcal{C}_{1+(q+1)i}\right| = m$。

证明 设 $m' = (m-1)/2$。下面，证明对任意的 $1 \le \tau \le m-1$, $\overline{[1+(q+1)i]q^{2\tau}} > 1 + (q+1)i$。

当 $1 \le \tau \le m'$ 时，$[1+(q+1)i]q^{2\tau} < (q+1)n$。因此，$\overline{[1+(q+1)i]q^{2\tau}} = [1+(q+1)i]q^{2\tau} > 1 + (q+1)i$。

当 $m'+1 \le \tau \le m-2$ 时，设 $1 + (q+1)i$ 的 q^2-adic 展开为 $\sum_{j=0}^{m'} i_j q^{2j}$，其中 $0 \le i_j \le q^2 - 1$，则

$$[1+(q+1)i]q^{2\tau} \equiv \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-1-\tau} i_j q^{2(\tau+j)} \ (\mathrm{mod}(q+1)n)$$

设 $i_{m-1-\tau} = (q+1)b + a$，其中 $0 \le a \le q$，则

$$[1+(q+1)i]q^{2\tau} \equiv aq^{2m-2} + \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} - (q+1)b \cdot \sum_{j=0}^{m-2} q^{2j} \ (\mathrm{mod}\ (q+1)n)$$

(1)如果 $a = 0$ 和 $b = 0$，则

$$\overline{[1+(q+1)i]q^{2\tau}} = \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} \ge q^{2\tau} > 1 + (q+1)i$$

(2)如果 $a \ge 1$，则

$$\overline{[1+(q+1)i]q^{2\tau}} = aq^{2m-2} + \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} - (q+1)b \sum_{j=0}^{m-2} q^{2j} > q^{m+1} + 1 > 1 + (q+1)i$$

(3)如果 $a = 0$ 和 $b > 0$，分如下两种情况进行讨论。如果 $i_0 = i_1 = \cdots = i_{m-2-\tau} = (q+1)b$, $\overline{[1+(q+1)i]q^{2\tau}} = (q+1)n + \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} - (q+1)b$ $\cdot \sum_{j=0}^{\tau-1} q^{2j}$ 从而推出 $\overline{[1+(q+1)i]q^{2\tau}} > 1 + (q+1)i$。如果存在 v 使得 $i_v \ne (q+1)b$，并设 κ 是这样的整数中的最大值。当 $i_{\kappa} < (q+1)b$，则

$$\overline{[1+(q+1)i]q^{2\tau}} = (q+1)n + \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{\kappa} i_j q^{2(\tau+j)} - (q+1)b \sum_{j=0}^{\tau+\kappa} q^{2j} > q^{2\tau} + 1 > 1 + (q+1)i$$

即，$\overline{[1+(q+1)i]q^{2\tau}} > 1 + (q+1)i$。当 $i_{\kappa} > (q+1)b$，

$$\overline{[1+(q+1)i]q^{2\tau}} = \sum_{j=0}^{\tau-m'-1} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{\kappa} i_j q^{2(\tau+j)} - (q+1)b \sum_{j=0}^{\tau+\kappa} q^{2j} \ge q^{2\tau} \ge q^{m+1} > 1 + (q+1)i$$

当 $\tau = m-1$ 时，证明与 $m'+1 \le \tau \le m-2$ 类似，故略去。综上所述，对任意整数 $1 \le \tau \le m-1$, $\overline{[1+(q+1)i]q^{2\tau}} > 1 + (q+1)i$。 证毕

引理 6 设 $m \ge 3$ 为奇数。如果 $2 \le \delta \le \dfrac{q^m - q}{q^2 - 1} + 1$，则 λ-常循环 BCH 码 C_{δ} 的维数 $\dim\left(C_{\delta}\right) = n - m\left(\delta - 2 - \left\lfloor (\delta - q - 1)q^{-2} \right\rfloor\right)$。

证明 记 $\Lambda = \{i : 0 \le i \le \delta - 2, i \not\equiv q-1 (\mathrm{mod}\, q^2)\}$，由引理 5 得，当 $i \in \Lambda$, $1 + (q+1)i$ 都是陪集首。所以 $\left|Z_{\delta}\right| = \sum_{i \in \Lambda} \left|\mathcal{C}_{1+(q+1)i}\right| = m|\Lambda|$ 。因为， $|\Lambda| = \delta - 2 - \left\lfloor (\delta - q - 1)q^{-2} \right\rfloor$。由式 (2) 推出， $\dim\left(C_{\delta}\right) = n - m\left(\delta - 2 - \left\lfloor (\delta - q - 1)q^{-2} \right\rfloor\right)$。 证毕

由引理 1，引理 3 和引理 6，可以构造如下参数的量子码。

定理 1　设 $m \ge 3$ 为奇数且 $2 \le \delta \le \dfrac{q^m - q}{q^2 - 1} + 1$，则存在参数为 $[[n,k,\ge \delta]]_q$ 的量子码，其中，

$$k = n - 2m\left(\delta - 2 - \left\lfloor (\delta - q - 1)q^{-2} \right\rfloor\right)$$

下面将定理 1 中构造的量子码与文献[3]和文献[4]中的量子 BCH 进行比较，发现定理 1 中的量子码有较好的参数。

例 1　设 $m \ge 3$ 为奇数且 $2 \le \delta \le \dfrac{q^m - q}{q^2 - 1} + 1$。设 $\delta - 1 = \delta_0 q^2 + \delta_1$，其中 $0 \le \delta_1 \le q^2 - 1$。由文献[3]和文献[4]知，存在参数为

$$\left[\left[n,\ n - 2m\left[\delta_0\left(q^2 - 1\right) + \delta_1\right], \ge \delta\right]\right]_q \tag{3}$$

的量子 BCH 码。由定理 1，存在参数为

$$\left[\left[n, n - 2m\left[\delta_0\left(q^2 - 1\right) + \delta_1\right] + 2m\theta,\ \ge \delta\right]\right]_q \tag{4}$$

的量子码，如果 $\delta_1 \ge q$，$\theta = 1$；如果 $\delta_1 < q$，$\theta = 0$。比较式(3)和式(4)，发现在相同设计距离下，定理 1 构造的量子码比量子 BCH 码具有更大的维数。

引理 7　设 $m \ge 2$ 为偶数。如果 $0 \le i \le \dfrac{q^{m+1} - q}{q^2 - 1} - 1$ 且 $i \not\equiv q - 1 \left(\bmod q^2\right)$，当 $\dfrac{m}{2} + 1 \le \tau \le m - 1$ 时，$\overline{[1 + (q+1)i]q^{2\tau}} > 1 + (q+1)i$。

证明　设 $\gamma = m/2$，$1 + (q+1)i$ 的 q^2-adic 展开为 $\sum_{j=0}^{\gamma} i_j q^{2j}$，其中 $0 \le i_j \le q^2 - 1$。当 $\gamma + 1 \le \tau \le m - 2$，

$$[1 + (q+1)i]q^{2\tau} \equiv \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} + i_{m-1-\tau} q^{2m-2} \ (\bmod (q+1)n) \tag{5}$$

设 $i_{m-1-\tau} \equiv a \ (\bmod q+1)$，其中 $0 \le a \le q$。

(1)如果 $a > 0$。由式(5)得

$$\overline{[1 + (q+1)i]q^{2\tau}} = aq^{2m-2} + \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} - \left(i_{m-1-\tau} - a\right)\sum_{j=0}^{m-2} q^{2j}$$

由此推出，$\overline{[1 + (q+1)i]q^{2\tau}} \ge q^{2m-2} + q^{2\tau} - \left(q^2 - 1 - a\right) \cdot \dfrac{q^{2m-2} - 1}{q^2 - 1} \ge q^{2\tau} + 1 + \dfrac{q^{2m-2} - 1}{q^2 - 1} > q^{m+2} > 1 + (q+1)i$

(2)如果 $a = 0$。由式(5)得

$$[1 + (q+1)i]q^{2\tau} \equiv \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{m-2-\tau} i_j q^{2(\tau+j)} - i_{m-1-\tau}\sum_{j=0}^{m-2} q^{2j} \ (\bmod (q+1)n)$$

接下来，分如下两种情况进行讨论。

(a)如果 $i_0 = i_1 = \cdots = i_{m-1-\tau}$，则

$$\overline{[1 + (q+1)i]q^{2\tau}} = (q+1)n + \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} - i_{m-1-\tau}\sum_{j=0}^{\tau-1} q^{2j} \ \ge (q+1)n - \left(q^{2\tau} - 1\right) > 1 + (q+1)i$$

(b)如果存在 $j \le m - \tau - 2$ 使得 $i_j \ne i_{m-1-\tau}$，并设 v 是这样的整数中的最大值。当 $i_v < i_{m-1-\tau}$，

$$\overline{[1 + (q+1)i]q^{2\tau}} = (q+1)n + \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{v} i_j q^{2(\tau+j)} - i_{m-1-\tau}\sum_{j=0}^{v+\tau} q^{2j} \ge q^{2\tau} + 1 > 1 + (q+1)i$$

当 $i_v > i_{m-1-\tau}$，由于 $i_v \le q^2 - 1$，所以 $i_{m-1-\tau} \le (q+1)(q-2)$。此时，

$$\overline{[1 + (q+1)i]q^{2\tau}} = \sum_{j=0}^{\tau-\gamma} i_{m-\tau+j} q^{2j} + \sum_{j=0}^{v} i_j q^{2(\tau+j)} - i_{m-1-\tau}\sum_{j=0}^{v+\tau} q^{2j} \ \ge \frac{q^{2(v+\tau)} - 1}{q - 1} + 1$$

由此推出 $\overline{[1 + (q+1)i]q^{2\tau}} > 1 + (q+1)i$。

当 $\tau = m - 1$ 时，证明与 $\tau \le m - 2$ 类似，故略去。综上所述，结论成立。　　证毕

引理 8　设 $m \ge 2$ 为偶数。如果 $0 \le i \le \dfrac{q^{m+1} - q}{q^2 - 1} - 1$ 且 $i \not\equiv q - 1 (\bmod q^2)$，有如下结论成立。

(1)如果 q 为奇数，则

$$\left|\mathcal{C}_{1+(q+1)i}\right| = \begin{cases} \dfrac{m}{2}, & i = \dfrac{q^m - 1}{2(q+1)} \\ m, & \text{其它} \end{cases}$$

且 $1 + (q+1)i$ 不是陪集首当且仅当

$$i \in \left\{ \frac{b(q^m - 1)}{q^2 - 1} : \frac{q+1}{2} \le b \le q - 2 \right\}$$

(2)如果 q 为偶数，则 $\left|\mathcal{C}_{1+(q+1)i}\right| = m$ 且 $1 + (q+1)i$ 不是陪集首当且仅当

$$i \in \left\{ \frac{b(q^m - 1)}{q^2 - 1} : \frac{q}{2} \le b \le q - 2 \right\}$$

证明　当 $m = 2$，则 $1 + (q+1)i < q^2$。因此，$\mathcal{C}_{1+(q+1)i} = \{1 + (q+1)i, 1 + (q+1)(q - 1 - i)\}$。直接验证可得结论。设 $m \ge 4$ 为偶数，记 $\gamma = m/2$。当 $1 \le \tau \le \gamma - 1$ 时，$\overline{[1 + (q+1)i]q^{2\tau}} = [1 + (q+1)i]q^{2\tau} > 1 + (q+1)i$。由引理 7，当 $\gamma + 1 \le \tau \le m - 1$ 时，$\overline{[1 + (q+1)i]q^{2\tau}} > 1 + (q+1)i$。当 $\tau = \gamma$ 时，设 $1 +$

$(q+1)i$ 的 q^2 -adic 展开为 $\sum_{j=0}^{\gamma} i_j q^{2j}$，其中 $0 \le i_j \le q^2-1$，则 $[1+(q+1)i]q^{2\tau} \equiv i_\gamma + \sum_{i=0}^{\gamma-1} i_j q^{2(j+\gamma)} \cdot (\mathrm{mod}(q+1)n)$。

当 $i_\gamma = 1$，由 $1+(q+1)i \le \sum_{j=2}^{m} q^j$ 推出存在 $\kappa \ge 1$ 使得 $i_{\kappa+1} = i_{\kappa+2} = \cdots = i_{\gamma-1} = q+1$ 且 $i_\kappa \le q$。因此，$\overline{[1+(q+1)i]q^{2\tau}} = i_\gamma + \sum_{j=0}^{\gamma-1} i_j q^{2(j+\gamma)}$。如果存在 $j \ge 1$ 使得 $i_j > 0$，则 $\overline{[1+(q+1)i]q^{2\tau}} \ge q^{m+2}+1 > 1+(q+1)i$。如果 $i_1 = i_2 = \cdots = i_{\gamma-1} = 0$，即 $1+(q+1)i = i_0 + q^m$，所以 $i_0 \equiv 0 \ (\mathrm{mod}\, q+1)$。此时，$\overline{[1+(q+1)i]q^{2\tau}} = 1+i_0 q^m > q^{m+1}+1 > 1+(q+1)i$。

当 $i_\gamma = 0$，设 $i_{\gamma-1} = (q+1)b + a$，其中 $0 \le a \le q$，

$$[1+(q+1)i]q^{2\tau} \equiv aq^{2m-2} + \sum_{j=0}^{\gamma-2} i_j q^{2(\gamma+j)} - \left(i_{\gamma-1}-a\right)\sum_{j=0}^{m-2} q^{2j} \ (\mathrm{mod}(q+1)n)$$

如果 $a \ge 1$，由于 $i_{\gamma-1} \le q^2-1$，故 $b \le q-2$。因此，

$$\begin{aligned}&\overline{[1+(q+1)i]q^{2\tau}} \\ &= aq^{2m-2} + \sum_{j=0}^{\gamma-2} i_j q^{2(\gamma+j)} - (i_{\gamma-1}-a) \\ &\quad \cdot \sum_{j=0}^{m-2} q^{2j} \ge q^{2m-2} - (i_{\gamma-1}-a)\frac{q^{2(m-1)}-1}{q^2-1} \\ &\ge \frac{q^{2(m-1)}-1}{q-1} + 1 > 1+(q+1)i\end{aligned}$$

如果 $a = 0$，则

$$[1+(q+1)i]q^{2\tau} \equiv \sum_{j=0}^{\gamma-2} i_j q^{2(\gamma+j)} - i_{\gamma-1}\sum_{j=0}^{m-2} q^{2j} \ (\mathrm{mod}(q+1)n)$$

接下来，分如下情况进行讨论。

(1)如果 $i_0 = i_1 = \cdots = i_{\gamma-1}$，则

$$\overline{[1+(q+1)i]q^{2\tau}} = (q+1)n - i_{\gamma-1}\sum_{j=0}^{\gamma-1} q^{2j} > 1+(q+1)i$$

(2)如果存在 $0 \le v \le \gamma-2$ 使得 $i_v \ne i_{\gamma-1}$，并设 v 是这样的整数中的最大值。如果 $i_v < i_{\gamma-1}$，

$$\begin{aligned}\overline{[1+(q+1)i]q^{2\tau}} &= (q+1)n + \sum_{j=0}^{v}\left(i_j - i_{\gamma-1}\right)q^{2(\gamma+j)} \\ &\quad - i_{\gamma-1}\sum_{j=0}^{\gamma-1} q^{2j} \ge (q+1)n + q^m \\ &\quad - i_{\gamma-1}\frac{q^{2(v+\gamma+1)}-1}{q^2-1} \ge (q+1)n \\ &\quad + q^m - q^{2v+m+2} + 1 > 1+(q+1)i\end{aligned}$$

如果 $i_v > i_{\gamma-1}$，由于 $i_v \le q^2-1$，所以，$i_{\gamma-1} \le q^2-q-2$。则

$$\overline{[1+(q+1)i]q^{2\tau}} = \sum_{j=0}^{v}\left(i_j - i_{\gamma-1}\right)q^{2(\gamma+j)} - i_{\gamma-1}\sum_{j=0}^{\gamma-1} q^{2j}$$

当 $v \ge 1$ 时，$\overline{[1+(q+1)i]q^{2\tau}} \ge q^m + \left(i_v - i_{\gamma-1}\right)q^{m+2v} - i_{\gamma-1}\sum_{j=0}^{\gamma+v-1} q^{2j} \ge 2q^m + 1 > 1+(q+1)i$。

当 $v = 0$ 时，由假设可得，$1+(q+1)i = i_0 + i_{\gamma-1}\dfrac{q^m-q^2}{q^2-1}$。

记 $\Delta = \left(q^m-1\right)/\left(q^2-1\right)$，从而推出，$\overline{[1+(q+1)i]q^{2\tau}} - [1+(q+1)i] = \left[\left(q^2-1\right)i_0 - \left(q^2+1\right)i_{\gamma-1}\right]\Delta$。

当 $i_0 \ge i_{\gamma-1}+2$ 时，则 $i_{\gamma-1} < q^2-1$。所以，$\left(q^2-1\right)i_0 - \left(q^2+1\right)i_{\gamma-1} \ge \left(q^2-1\right)\left(i_{\gamma-1}+2\right) - \left(q^2+1\right)i_{\gamma-1} = 2\left(q^2-1\right) - 2i_{\gamma-1} > 0$。

而 $\Delta > 0$，故 $\overline{[1+(q+1)i]q^{2\tau}} > [1+(q+1)i]$。

当 $i_0 = i_{\gamma-1}+1$ 时。设 $i_{\gamma-1} = (q+1)b$，因 $i_0 \le q^2-1$，所以 $0 \le b \le q-2$。此时，$\left(q^2-1\right)i_0 - \left(q^2+1\right) \cdot i_{\gamma-1} = (q+1)[q-1-2b]$。

由此推出，当 $b < (q-1)/2$ 时，$\overline{[1+(q+1)i]q^{2\tau}} > [1+(q+1)i]$。

当 $b > (q-1)/2$ 时，$\overline{[1+(q+1)i]q^{2\tau}} < [1+(q+1)i]$。

综上所述，我们有如下结论。

(1) 当 $b < (q-1)/2$ 时，对任意 $1 \le \tau \le m-1$，$\overline{[1+(q+1)i]q^{2\tau}} > [1+(q+1)i]$。即，$1+(q+1)i$ 是陪集首且 $\left|\mathcal{C}_{1+(q+1)i}\right| = m$。

(2) 当 $(q-1)/2 < b \le q-2$ 时，对任意 $\tau \ne \gamma$，$\overline{[1+(q+1)i]q^{2\tau}} > [1+(q+1)i]$。

当 $\tau = \gamma$，$\overline{[1+(q+1)i]q^{2\tau}} < [1+(q+1)i]$。故 $1+(q+1)i$ 不是陪集首但 $\left|\mathcal{C}_{1+(q+1)i}\right| = m$。

(3)注意到 $(q-1)/2$ 为整数当且仅当 q 为奇数。当 q 为奇数，$b = (q-1)/2$ 时，对任意 $1 \le \tau \le \gamma-1$，$\overline{[1+(q+1)i]q^{2\tau}} > [1+(q+1)i]$。

当 $\tau = \gamma$，$\overline{[1+(q+1)i]q^{2\tau}} = [1+(q+1)i]$。所以，$1+(q+1)i$ 是陪集首且 $\left|\mathcal{C}_{1+(q+1)i}\right| = \gamma$。

综上所述，可以得出结论。 证毕

引理 9 设 $m \ge 2$ 为偶数且 $2 \le \delta \le \dfrac{q^{m+1}-q}{q^2-1}+1$，则 λ-常循环 BCH 码 C_δ 的维数：

$$\dim(C_\delta)=\begin{cases} n-m\delta', & \chi<\left\lfloor\dfrac{q-1}{2}\right\rfloor \\ n-m\delta'+\dfrac{m}{2}(2\chi+2-q), & \left\lfloor\dfrac{q-1}{2}\right\rfloor\le\chi\le q-2 \\ n-m\delta'+\dfrac{m}{2}(q-2), & \chi=q-1 \end{cases}$$

其中，$\delta'=\delta-2-\left\lfloor\dfrac{\delta-q-1}{q^2}\right\rfloor$，$\chi=\left\lfloor\dfrac{(\delta-2)(q^2-1)}{q^m-1}\right\rfloor$。

证明　记 $\Lambda=\left\{i:0\le i\le\delta-2, i\not\equiv q-1\pmod{q^2}\right\}$。设 q 为奇数，当 $\chi<\dfrac{q-1}{2}$，则 $\delta-2<\dfrac{q^m-1}{2(q+1)}$。由引理 8 得，$|Z_\delta|=\sum_{i\in\Lambda}|\mathcal{C}_{1+(q+1)i}|=m\delta'$。由式(2)推出 $\dim(C_\delta)=n-m\delta'$。当 $(q-1)/2\le\chi<q-1$ 时，记 $\Theta=\left\{\dfrac{b(q^m-1)}{q^2-1}:\dfrac{q+1}{2}\le b\le q-2\right\}\cap\Lambda$，注意到 $i_0=\dfrac{q^m-1}{2(q+1)}\in Z_\delta$，由引理 8 可得

$$\begin{aligned}|Z_\delta|&=\sum_{i\in\Lambda}|\mathcal{C}_{1+(q+1)i}|-\sum_{i\in\Theta}|\mathcal{C}_{1+(q+1)i}|\\&=m\delta'-m|\Theta|-m/2\end{aligned}$$

此时，$|\Theta|=\chi-\dfrac{q-1}{2}$，故 $|Z_\delta|=m\delta'-\dfrac{m}{2}(2\chi+2-q)$。由式(2)推出，$\dim(C_\delta)=n-m\delta'+\dfrac{m}{2}(2\chi+2-q)$。

当 q 为偶数，证明与 q 为奇数类似，略去。证毕

由引理 1，引理 3 和引理 9，通过厄米特构造，我们可以得到如下参数的量子码。

定理 2　设 $m\ge2$ 为偶数且 $2\le\delta\le\dfrac{q^{m+1}-q}{q^2-1}+1$。设 $\chi=\left\lfloor\dfrac{(\delta-2)(q^2-1)}{q^m-1}\right\rfloor$ 和 $\delta'=\delta-2-\left\lfloor\dfrac{\delta-q-1}{q^2}\right\rfloor$。则存在参数为 $[[n,k,\ge\delta]]_q$ 的量子码，其中，

$$k=\begin{cases} n-2m\delta', & \chi<\left\lfloor\dfrac{q-1}{2}\right\rfloor \\ n-2m\delta'+m(2\chi+2-q), & \left\lfloor\dfrac{q-1}{2}\right\rfloor\le\chi\le q-2 \\ n-2m\delta'+m(q-2), & \chi=q-1 \end{cases}$$

下面将定理 2 中构造的量子码与文献[3]和文献[4]中的量子 BCH 码进行比较。设 $n=\dfrac{q^{2m}-1}{q^2-1}$，其中 q 为奇素数的方幂，$m\ge2$ 为偶数。设 $2\le\delta\le\dfrac{q^{m+1}-q}{q^2-1}$，$\delta-1=\delta_0q^2+\delta_1$，其中 $0\le\delta_1<q^2$。定义：

$$\varepsilon=\begin{cases}1, & \delta_1\ge q\\ 0, & 0\le\delta_1<q\end{cases}$$

由文献[3]和文献[4]，存在参数为

$$\left[\left[n,n-2m\left[\delta_0\left(q^2-1\right)+\delta_1\right],\ \ge\delta\right]\right]_q \tag{6}$$

的量子 BCH 码。

当 $2\le\delta\le\dfrac{q^m-1}{2(q+1)}+1$ 时，由定理 2，存在参数为

$$\left[\left[n,n-2m\left[\delta_0\left(q^2-1\right)+\delta_1\right]+2m\varepsilon,\ge\delta\right]\right]_q \tag{7}$$

的量子码。

当 $\dfrac{q^m-1}{2(q+1)}+1\le\delta\le\dfrac{q^{m+1}-q}{q^2-1}$ 时，由定理 2，存在参数为

$$\left[\left[n,n-2m\left[\delta_0\left(q^2-1\right)+\delta_1\right]+m(2\varepsilon+2\chi+2-q),\ \ge\delta\right]\right]_q \tag{8}$$

的量子码，其中 $\chi=\left\lfloor\dfrac{(\delta-2)(q^2-1)}{q^m-1}\right\rfloor$。

分别比较式(6)和式(7)，式(6)和式(8)中的量子码，发现在相同设计距离时，定理 2 构造的量子码的维数比文献[3]和文献[4]中的量子 BCH 码的维数大。特别地，定理 2 改进了对偶包含码的最大设计距离。下面，给出一个具体的例子阐述我们的构造。

例 2　设 $q=3$，$m=4$ 且 $\delta=13$。由文献[3]和文献[4]，得到参数为 $[[820,732,\ge13]]_3$ 的量子 BCH 码。由定理 2，利用常循环 BCH 码，得到参数为 $[[820,744,\ge13]]_3$ 的量子码。因此，本文构造的量子码具有较好的参数。

4　结束语

本文研究了 $\mathrm{GF}(q^2)$ 上一类常循环码，给出这类常循环码是厄米特对偶包含码的一个充分必要条件。通过分析分圆陪集的结构，得到这类常循环对偶包含码的维数。利用厄米特构造，得到了一类量子码。与文献[3]和文献[4]中的量子 BCH 码比较，在相同设计距离下，这类常循环码构造的量子码具有更好的参数。

参 考 文 献

[1] ASHIKHMIN A and KNILL E. Nonbinary quantum stabilizer codes[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 3065–3072. doi: 10.1109/18.959298.

[2] CALDERBANK A R, RAINS E M, SHOR P W, *et al*. Quantum error correction via codes over GF(4) [J]. *IEEE*

Transactions on Information Theory, 1998, 44(4): 1369–1387. doi: 10.1109/18.681315.

[3] ALY S A, KLAPPENECKER A, and SARVEPALLI P K. On quantum and classical BCH codes[J]. *IEEE Transactions on Information Theory,* 2007, 53(3): 1183–1188. doi: 10.1109/TIT.2006.890730.

[4] MA Z, LU X, FENG K, *et al.* On non-binary quantum codes[C]. International Conference on Theory and Applications of Models of Computation, Berlin Heidelberg, 2006: 675–683. doi: 10.1007/1175 0321_63.

[5] XU Y, MA Z, and ZHANG C. On classical BCH codes and quantum BCH codes[J]. *Journal of Electronics*, 2009, 26(1): 64–70. doi: 10.1007/s11767-007-0120-2.

[6] GUARDIA G G L. New families of asymmetric quantum BCH codes[J]. *Quantum Information and Computation*, 2011, 11(3): 239–252.

[7] TANG Y, ZHU S, KAI X, *et al.* New quantum codes from dual-containing cyclic codes over finite fings[J]. *Quantum Information Processing*, 2016, 15(11): 4489–4500. doi: 10.1007/s11128-016-1426-5.

[8] GUARDIA G G L. Quantum codes defived from cyclic codes[J]. *International Journal of Theoretical Physics*, 2017, 56(8): 2479–2484. doi: 10.1007/s10773-017 -3399-2.

[9] GUARDIA G G L. On optimal constacyclic codes[J]. *Linear Algebra and Its Applications*, 2016, 496: 594–610. doi: 10.1016/j.laa.2016.02.014.

[10] LIN X. Quantum cyclic and constacyclic codes[J]. *IEEE Transactions on Information Theory*, 2004, 50(3): 547–549. doi: 10.1109/TIT.2004.825502.

[11] KAI X, ZHU S, and TANG Y. Quantum negacyclic codes[J]. *Physical Review A*, 2013, 88: 012326. doi: 10.1103/PhysRevA.88.012326.

[12] XU G, LI R, GUO L, *et al.* New quantum codes constructed from quaternary BCH codes[J]. *Quantum Information Processing*, 2016, 15(10): 4099–4116. doi: 10. 1007/s11128-016-1397-6.

[13] YUAN J, ZHU S, KAI X, *et al.* On the construction of quantum constacyclic codes[J]. *Designs Codes and Cryptography*, 2017, 85(1): 179–190. doi: 10. 1007/s10623-016-0296-2.

[14] LIU Y, LI R, LÜ L, *et al.* A class of constacyclic BCH codes and new quantum codes[J]. *Quantum Information Processing*, 2017, 16(3): 66. doi: 10.1007/s11128-017-1533-y.

[15] XU G, LI R, and GUO L. New optimal asymmetric quantum codes constructed from constacyclic codes[J]. *International Journal of Modern Physics B*, 2017, 31(5): 1750030. doi: 10.1142/S0217979217500308.

[16] KRISHNA A and SARWATE D V. Pseudocyclic maximum-distance-separable codes[J]. *IEEE Transactions on Information Theory*, 1990, 36(4): 880–884. doi: 10.1109/18.53751.

朱士信： 男，1962 年生，教授，博士生导师，研究方向为代数编码理论、信息安全与序列密码等.

黄 山： 女，1993 年生，硕士生，研究方向为代数编码.

李 锦： 女，1987 年生，副教授，研究方向为代数编码.