一类量子码的组合构造

郭冠敏，李瑞虎，郭罗斌，王君力
(空军工程大学基础部，西安，710051)

摘要　利用满足一定嵌套关系的 2 个 q^2-元线性码，给出一种构造自正交码的组合方法，并由各成分码的参数确定出所构造的新自正交码的维数和对偶距离下界。进一步用 q^2-分圆陪集理论讨论码长 $n=q^2+1$ 的常循环 BCH 码。刻画满足所需嵌套关系的 2 个 q^2-元常循环 BCH 码的定义集合、设计距离和参数，从而由常循环 BCH 码构造出码长 $2n$ 的 q^2-元自正交码和 q-元量子码。这一方法可得到许多距离 $d>q+1$ 的量子码，而这样参数的量子码是用已知的构造方法不能获得的。方法和结果对于构造更多参数良好的量子码以及给出最优量子码的距离下界都具有借鉴作用。

关键词　Hermitian 自正交码；常循环码；q^2-分圆陪集；量子码
DOI　10.3969/j.issn.1009-3516.2018.02.018
中图分类号　O157.4　　**文献标志码**　A　　**文章编号**　1009-3516(2018)02-0106-05

Combinatorial Construction of a Class of Quantum Codes

GUO Guanmin, LI Ruihu, GUO Luobin, WANG Junli
(Basic Department, Air Force Engineering University, Xi'an 710051, China)

Abstract: By using two q^2-ary linear codes to satisfy a certain nested relation, this paper gives a combinatorial method of constructing Hermitian self-orthogonal codes, and determines the dimensions and the lower bound of dual distances of the new codes through the parameters of each code. By means of the concepts of q^2-cyclotomic coset, the constacyclic BCH codes with length $n=q^2+1$ are discussed further. The defining sets, design distances, parameters of the two q^2-ary constacyclic BCH codes are characterized as a certain nested relation satisfied. Using these constacyclic BCH codes, many q^2-ary Hermitian self-orthogonal codes with length $2n$ and new q-ary quantum codes with $d>q+1$ are constructed without combination of known methods. The methods and results may be employed to construct quantum codes with better parameter and give out the lower bounds of some optimal quantum codes.

Key words: Hermitian self-orthogonal code; constacyclic codes; q^2-cyclotomic coset; quantum codes

量子纠错码是量子计算、量子通信等量子信息处理可靠运行的保障，构造具有良好参数的量子纠错码则是量子纠错码中最重要的研究内容。文献[1～7]先后建立了 q-元(二元和非二元)加性量子纠错码与自正交(或对偶包含)经典线性码的联系，创造出量子码的 3 种构造方法：CSS 构造法，Steane 构造法和 Hermitian 构造法。Hermitian 构造法则是其中最有效、使用最多的构造方法。

收稿日期：2017-10-02
基金项目：国家自然科学基金(11471011)；陕西省自然科学基金(2017JQ1032)
作者简介：郭冠敏(1993—)，男，甘肃平凉人，硕士生，主要从事代数编码研究. E-mail:gmguo_xjtukgd@yeah.net

引用格式：*郭冠敏，李瑞虎，郭罗斌，等. 一类量子码的组合构造[J]. 空军工程大学学报(自然科学版)，2018，19(2)：106-110. GUO Guanmin, LI Ruihu, GUO Luobin, et al. Combinatorial Construction of a Class of Quantum Codes [J]. Journal of Air Force Engineering University (Natural Science Edition), 2018, 19(2): 106-110.*

依据上述 3 种构造方法，利用经典线性码构造量子纠错码首先要解决经典线性码的自正交性（或对偶包含）问题，文献[8～11]先后讨论了二元和非二元循环（及其推广）码类的对偶包含判定条件，再深入研究其中特殊码类 BCH 码和常循环 BCH 码的对偶包含判定条件，以及用对偶包含码确定所构造量子纠错码的参数，并构造出一些具有较好参数的量子纠错码，而直接使用特殊码类来构造较好参数的量子码，对码长需要严格限制，且所构造的量子码的距离相对码长来说比较小。为突破对码长的严格限制，人们探讨用赋值和矩阵乘积码来构造码长较大的量子码，但是所得到的量子码的距离相对码长来说依然比较小。文献[12]利用最优量子码，量子 MDS 码进一步构造码长分别为 $2q^2$ 和 $2(q^2+1)$ 的量子码，所给出的量子码的距离 $d\leqslant q+1$。本文将探讨使用组合方法构造码长为 $2(q^2+1)$ 的距离为 $d>q+1$ 的量子码。

1　预备知识

设 q 为素数的幂，F_{q^2} 为包含 q^2 个元素的有限域，$F_{q^2}^*$ 为 F_{q^2} 的非零元素集合，F_{q^2} 上 n 维行向量空间，$F_{q^2}^n$ 上的 k 维子空间 C 叫做码长为 n 的 k 维 q^2 元码；如果 C 的 Hamming 距离为 d，简记为 $C=[n,k,d]_{q^2}$，如果 $d=n-k+1$，则 C 称为最大距离可分（MDS）码。

设 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}$，$\boldsymbol{Y}=\{y_1,y_2,\cdots,Y_n\}\in F_{q^2}^n$，$C$ 的 Hermitian 对偶码 $C^{\perp h}$ 定义为 $C^{\perp h}=\{\boldsymbol{X}\mid \boldsymbol{X}\in F_{q^2}^n,(\boldsymbol{X},\boldsymbol{Y})=x_1y_1^q+x_2y_2^q+\cdots+x_ny_n^q=0,\forall \boldsymbol{Y}\in C\}$。若 $C^{\perp h}\subseteq C$，则 $C^{\perp h}$ 称 Hermitian 自正交码，相应 C 称 Hermitian 对偶包含的。

利用 F_{q^2} 上满足 Hermitian 对偶包含（或自正交）条件的经典码，可构造出 q 元量子码，文献[5～6]给出如下定理。

定理 1.1[5-6]　若设 C 是 F_{q^2} 上的参数为 $[n,k,d]_{q^2}$ 的线性码并且 $C^{\perp h}\subseteq C$，则存在 q 元 $Q=[[n,2k-n,\geqslant d]]_q$ 量子码。

当 C 满足定理 1.1 条件且为经典 MDS 码时，$Q=[[n,2k-n,d]]_q$ 一定是纯量子码并且为量子 MDS 码。文献[11]中利用码长 $n=q^2+1$ 的常循环 BCH 码构造出量子 MDS 码，下面介绍常循环码以及相关的 Hermitian 对偶包含结果。

设 C 是 F_{q^2} 上参数为 $[n,k]_{q^2}$ 的线性码，$\lambda\in F_{q^2}^*$，如果 $\forall c=\{c_0,c_1,\cdots,c_{n-1}\}\in C$，都有 $\{\lambda c_{n-1},c_0,\cdots,c_{n-2}\}\in C$，则 C 称为 λ-常循环码。其中当 $\lambda=1$ 时，此常循环码为循环码。由文献[13]可知，F_{q^2} 上的 λ-常循环码 C 等同于环 $R_n=\dfrac{F[x]}{(x^n-\lambda)}$ 的理想，能够用 $x^n-\lambda$ 的因式以及多项式代数描述。

下面约定 $n>1$ 为正整数，$\gcd(n,q)=1$，记 $r=ord_{q^2}(\lambda)$ 为 λ 在群 $F_{q^2}^*$ 中的阶。C 是 F_{q^2} 上参数为 $[n,k]_{q^2}$ 的 λ-常循环码 $C=<g(x)>$，其中 $g(x)\mid x^n-\lambda$ 且 $g(x)$ 是 C 中次数最小的首一多项式。设 ξ 为 F_{q^2} 的某个扩域中的 rn 次单位根且有 $\xi^n=\lambda$，由于 $(x^n-\lambda)\mid(x^m-1)$，我们可以验证 $x^n-\lambda$ 的根为 ξ^{ir+1}，$0\leqslant i<n$，见文献[14]。

定义 $\Omega_{r,n}=\{ir+1\mid 0\leqslant i<n\}$，则 λ-常循环码 $C=<g(x)>$ 的定义集为：$T:=\{ir+1\in\Omega_{r,n}\mid \xi^{ir+1}$ 是 $g(x)$ 的根$\}$。显然，C 的维数为 $\dim(C)=n-|T|$，其 Her-mitian 对偶码 $C^{\perp h}$ 的定义集为 $T^{\perp h}=\Omega_{r,n}\setminus(-qT)$。类似于循环码，下面的定理给出了常循环码的 BCH 界。

定理 1.2[13]　（常循环码的 BCH 界）　设 $r=ord_{q^2}(\lambda)$，$C=<g(x)>$ 是 F_{q^2} 上长度为 n 的 λ-常循环码。若 ξ 为 rn 次本原单位根，$g(x)$ 的根为 $\{\xi^{1+ir}\mid b\leqslant i\leqslant b+\delta-1\}$（或等价地 C 的定义集为 $T=\bigcup_{i=b}^{b+\delta-1}C_{ir+1}$），则此时常循环码的最小距离 $d\geqslant\delta$。

引理 1.1[15]　设 C 是 F_{q^2} 上长度为 n 的 λ-常循环码且 $r=\mathrm{ord}_{q^2}(\lambda)$，若 C 是 Hermitian 对偶包含码，则有 $r\mid q+1$。

Hermitian 对偶包含 λ-常循环码的存在性和确定可用分圆陪集理论解决。若 $x\in\Omega_{r,n}$，x 模 rn 的 q^2-分圆陪集 C_x 为：

$C_x=\{x,xq^2,x(q^2)^2,\cdots,x(q^2)^{k-1}\}(\mathrm{mod}\ rn)$。

其中 k 是使得 $x(q^2)^k\equiv x(\mathrm{mod}\ rn)$ 的最小正整数。若 $rn-qx\in C_x$，C_x 为斜对称的；否则称其为斜非对称的。模 rn 的斜非对称 q^2-分圆陪集 C_x 和 $C_{-qx}=C_{rn-qx}$ 成对出现，叫做模 rn 的 q^2-斜非对称偶（简称斜非对称偶），记为 (C_x,C_{-qx})。见文献[16]。

下面的引理给出了 C 是 F_{q^2} 上长度为 n 的 Hermitian 对偶包含 λ-常循环码的充要条件。

引理 1.2[14]　设 $r=ord_{q^2}(\lambda)$，$r\mid q+1$，C 是 F_{q^2} 上长度为 n 的 λ-常循环码，其定义集为 T，则 $C^{\perp h}\subseteq C$ 当且仅当以下条件其中之一成立：① $\forall x,y\in T$ 有 $C_x\neq C_{-qx}$，若 $C_x\neq C_y$ 则它们不构成非对称偶；② $T\cap(-qT)=\varnothing$，其中 $-qT=\{-qt\ \mathrm{mod}\ rn)\mid t\in T\}$。

2　自正交码与量子码的组合构造

假设 q 为奇素数的幂。为利用满足嵌套关系的

线性码构造 Hermitian 自正交码,我们先证明下面的引理。

引理 2.1 设 q 为奇素数的幂,则存在 F_{q^2} 中元素 a 使得 $a^{q+1}+1=0$。

证明 设 $\xi\in F_{q^2}^*$ 为 F_{q^2} 的本原元,则 $\xi^{q^2-1}=1$ 且对于 $1\leqslant a<q^2-1$ 必有 $\xi^a\neq 1$。因 q 为奇素数的幂,则 $\xi^{q^2-1}=(\xi^{\frac{q-1}{2}})^{2(q+1)}=1$ 及 $(\xi^{\frac{q-1}{2}})^{(q+1)}=-1$ 成立。记 $a=\xi^{\frac{q-1}{2}}$,则 $a^{q+1}=-1$,引理得证。

定理 2.1 设 C_1 和 C_2 是参数分别为 $[n,k_1,d_1]_{q^2}$ 和 $[n,k_2,d_2]_{q^2}$ 的线性码,若 $C_1^{\perp_h}\subset C_2^{\perp_h}\subset C_1$,则存在对偶距离 $d\geqslant\min\{2d_1,d_2\}$,参数为 $[2n,2n-(k_1+k_2)]_{q^2}$ 的 Hermitian 自正交码,从而存在参数为 $[[2n,2(k_1+k_2)-2n,\geqslant\min\{2d_1,d_2\}]]_q$ 量子码。

证明 设 C_1 校验阵为 $\boldsymbol{H}_1$,由 $C_1^{\perp_h}\subset C_1$ 可知 $\boldsymbol{H}_1\boldsymbol{H}_1^{\dagger}=0$,并且可选取 C_2 校验阵为 $\boldsymbol{H}_2$,使得 $\boldsymbol{H}_2=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{H}'_2\end{pmatrix}$。再由 $C_2^{\perp_h}\subset C_1$ 可知 $\boldsymbol{H}_1\boldsymbol{H}_2^{\dagger}=0$。

取 $a\in F_{q^2}$ 使得 $a^{q+1}+1=0$,利用 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 构造 $\boldsymbol{H}$ 如下:

$$\boldsymbol{H}=\begin{pmatrix}\boldsymbol{H}_1 & 0\\ a\boldsymbol{H}'_2 & \boldsymbol{H}'_2\\ 0 & \boldsymbol{H}_1\end{pmatrix}=(\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_n,\boldsymbol{\beta}_1,\cdots,\boldsymbol{\beta}_n)$$

式中:$\boldsymbol{\alpha}_i,\boldsymbol{\beta}_j(1\leqslant i,j\leqslant n)$为 $\boldsymbol{H}$ 的列向量。

下面分 3 步证明 $\boldsymbol{H}$ 生成对偶距离 $d\geqslant\min\{2d_1,d_2\}$、参数为 $[2n,2n-(k_1+k_2)]_{q^2}$ 的 Hermitian 自正交码。

步骤 1 由于 $\boldsymbol{H}_1\boldsymbol{H}_1^{\dagger}=0,\boldsymbol{H}_1\boldsymbol{H}_2^{\dagger}=0,a^{q+1}=-1$。则:

$$\boldsymbol{H}\boldsymbol{H}^{\dagger}=\begin{pmatrix}\boldsymbol{H}_1 & 0\\ a\boldsymbol{H}'_2 & \boldsymbol{H}'_2\\ 0 & \boldsymbol{H}_1\end{pmatrix}\begin{pmatrix}\boldsymbol{H}_1^{\dagger} & a^q\boldsymbol{H}'^{\dagger}_2 & 0\\ 0 & \boldsymbol{H}'^{\dagger}_2 & \boldsymbol{H}_1^{\dagger}\end{pmatrix}=$$

$$\begin{pmatrix}0 & 0 & 0\\ 0 & (a^{q+1}+1)\boldsymbol{H}'_2\boldsymbol{H}'^{\dagger}_2 & 0\\ 0 & 0 & 0\end{pmatrix}=0。$$

从而可得 $\boldsymbol{H}$ 生成码长为 $2n$ 的 Hermitian 自正交码。

步骤 2 因为 C_1 和 C_2 分别是参数 $[n,k_1,d_1]_{q^2}$ 和 $[n,k_2,d_2]_{q^2}$ 的线性码,所以 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 的行数分别为 $n-k_1$ 和 $n-k_2$,$\boldsymbol{H}'_2$ 的行数为 k_1-k_2,则 $\boldsymbol{H}$ 的行数为 $2(n-k_1)+k_1-k_2=2n-(k_1+k_2)$。

显然,$\boldsymbol{H}$ 的秩为 $2n-(k_1+k_2)$。

步骤 3 再证 $\boldsymbol{H}$ 生成的 Hermitian 自正交码的对偶距离 $d\geqslant\min\{2d_1,d_2\}$。为了便于说明,不妨设 $m=\min\{2d_1,d_2\}$。由于 C_1 和 C_2 分别以 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 为校验阵,此对偶码以 $\boldsymbol{H}$ 为校验阵,则在矩阵 $\boldsymbol{H}$ 中任取 $m-1$ 列,均有 $m-1\leqslant 2d_1-1,m-1\leqslant d_2-1$。

①若 $m-1$ 列全取自前 n 列,则由 $m-1\leqslant d_2-1$ 可知,这些列是线性无关的;②若 $m-1$ 列全取自后 n 列,则由 $m-1\leqslant d_2-1$ 可知,这些列也是线性无关的;③假定 $m-1$ 列取自 $\alpha_1,\cdots,\alpha_n$ 中 s 列,$\beta_1,\cdots,\beta_n$ 中 $m-1-s$ 列,由于 $m-1\leqslant 2d_1-1$,因此 s 或 $m-1-s$ 中至少有一个小于等于 $\left\lceil\frac{2d_1-1}{2}\right\rceil=d_1-1$,不妨假定 $s\leqslant d_1-1$。

由 $\boldsymbol{H}$ 的构造可知,下面我们设:

$$\boldsymbol{\alpha}_i=\begin{pmatrix}h_{1,i}\\ h'_{2,i}\\ 0\end{pmatrix},\boldsymbol{\beta}_j=\begin{pmatrix}0\\ h'_{2,j}\\ h_{1,j}\end{pmatrix},1\leqslant i,j\leqslant n。$$

令 $\boldsymbol{\alpha}_{i_1},\boldsymbol{\alpha}_{i_2},\cdots,\boldsymbol{\alpha}_{i_s},\boldsymbol{\beta}_{j_1},\boldsymbol{\beta}_{j_2},\cdots,\boldsymbol{\beta}_{j_{m-1-s}}$ 为取出的 $m-1$ 列。若设 $\lambda_1\boldsymbol{\alpha}_{i_1}+\lambda_2\boldsymbol{\alpha}_{i_2}+\cdots+\lambda_s\boldsymbol{\alpha}_{i_s}+\mu_1\boldsymbol{\beta}_{j_1}+\cdots+\mu_{m-1-s}\boldsymbol{\beta}_{j_{m-1-s}}=0$,则有:

$$\begin{cases}\lambda_1h_{1,i_1}+\cdots+\lambda_sh_{1,i_s}=0 & (1)\\ \lambda_1h'_{2,i_1}+\cdots+\lambda_sh'_{2,i_s}+\mu_1h'_{2,j_1}+\cdots & (2)\\ \quad+\mu_{m-1-s}h'_{2,j_{m-1-s}}=0 & \\ \mu_1h_{1,j_1}+\cdots+\mu_{m-1-s}h_{1,j_{m-1-s}}=0 & (3)\end{cases}$$

因为 $s\leqslant d_1-1$,由(1)可知,而 $\boldsymbol{H}_1$ 中的任意 d_1-1 列是线性无关的,则有 $\lambda_1=\lambda_2=\cdots=\lambda_s=0$,则 $\mu_1\beta_{j_1}+\cdots+\mu_{m-1-s}\beta_{j_{m-1-s}}=0$,又因为 $m-1-s\leqslant d_2-1$,而 $\boldsymbol{H}_2$ 中的任意 d_2-1 列是线性无关的,则 $\mu_1=\mu_2=\cdots=\mu_s=0$,故取出的 $m-1$ 列向量 $\boldsymbol{\alpha}_{i_1},\cdots,\boldsymbol{\alpha}_{i_s},\boldsymbol{\beta}_{j_1},\cdots,\boldsymbol{\beta}_{j_{m-1-s}}$ 是线性无关的。同理可证当 $m-1-s\leqslant d_1-1$ 时,以上结论成立。综上可知,$\boldsymbol{H}$ 中任意 $m-1$ 列是线性无关的,由此可知,则 $\boldsymbol{H}$ 生成的 Hermitian 自正交码的对偶距离 $d\geqslant m$,即 $d\geqslant\min\{2d_1,d_2\}$。

综上,则证得 $\boldsymbol{H}$ 生成一个对偶距离 $d\geqslant\min\{2d_1,d_2\}$,参数为 $[2n,2n-(k_1+k_2)]_{q^2}$ 的 Hermitian 自正交码 $C^{\perp_h}$。依据定理 1.1,由 C 可得到量子码 $Q=[[2n,2(k_1+k_2)-2n,\geqslant\min\{2d_1,d_2\}]]_q$。证毕。(注:文献[11]用 q^2-元码和矩阵乘积法构造量子码时,要求 C_1 和 C_2 都是 Hermitian 对偶包含码,定理 3.1 突破 C_2 为 Hermitian 对偶包含码,减弱条件后适用范围更广。)

3 新的量子码的构造

本节通过具体分析码长为 $n=q^2+1$ 的常循环 BCH 码的定义集合,讨论 Hermitian 对偶包含码 C_1 的最大设计距离 $\delta_{\max}$,从而构造出 $2\leqslant\delta\leqslant\delta_{\max}$($\delta$ 为偶数)时的对偶包含常循环 BCH 码 C_1,进而通过

C_1 和 C_2 之间的嵌套关系确定出常循环码 C_2 的设计距离，进而通过 C_1 和 C_2 的组合构造出满足自正交条件的常循环码，利用定理 2.1 提供的量子码的 Hermitian 构造法，从而构造出新的量子码。

设 q 为奇素数的幂，$q\geqslant 5$，C 是 F_{q^2} 上码长为 n 的 λ-常循环码，$r=ord_{q^2}(\lambda)$，设码长 $n=q^2+1$，$r=q+1$，则有 $rn\mid q^4-1$，故有 $|C_{1+ir}|\leqslant 2$，$0\leqslant i<n$，其中 C_{1+ir} 是包含 $1+ir$ 的模 rn 的 q^2-分圆陪集[17]。

类似文献[14]引理 3.12，可给出引理如下。

引理 3.1　设 $n=q^2+1$，$l=\dfrac{q^2+1}{2}$ 且 $r=q+1$，则 $C_l=\{l\}$，$C_{l-i(q+1)}=\{l-i(q+1),l+i(q+1)\}$，$1\leqslant i\leqslant n/2-1$。

为了确定满足所需嵌套关系的 2 个 q^2-元常循环 BCH 码的最大设计距离，有以下定理。

定理 3.1　设 $n=q^2+1$，$\delta_{\max}=q-1$，常循环码 C_1 的定义集为 $T_1=\bigcup_{i=0}^{\delta/2-1}C_{l-i(q+1)}$，常循环码 C_2 的定义集为 $T_2=T_1\cup\left(\bigcup_{j=\delta/2}^{\delta'}C_{l-j(q+1)}\right)$，$\dfrac{\delta}{2}\leqslant\delta'\leqslant q-2$，则 $C_1^{\perp h}\subset C_2^{\perp h}\subset C_1$ 当且仅当 $2\leqslant\delta\leqslant\delta_{\max}$ 且 δ 为偶数。

证明　当常循环码 C_1 的定义集为 $T_1=\bigcup_{i=0}^{\delta/2-1}C_{l-i(q+1)}$，由文献[14]可知，当 $2\leqslant\delta\leqslant\delta_{\max}$ 时，$T_1\bigcap(-qT_1)=\varnothing$，即有 $C_1^{\perp h}\subset C_1$。当常循环码 C_2 的定义集为 $T_2=T_1\cup(\bigcup_{j=\delta/2}^{\delta'}C_{l-j(q+1)})$，$\dfrac{\delta}{2}\leqslant\delta'\leqslant q-2$ 时，易知 $T_1\subset T_2$，则有 $C_2\subset C_1$，即 $C_1^{\perp h}\subset C_2^{\perp h}$。

下面要证当 $2\leqslant\delta\leqslant\delta_{\max}$ 时，$C_2^{\perp h}\subset C_1$，即证 $T_2\bigcap(-qT_1)=\varnothing$。利用反证法，首先假定 $T_2\bigcap(-qT_1)\neq\varnothing$。故存在 $0\leqslant i\leqslant\dfrac{q-1}{2}-1$，$0<j\leqslant q-2$，使得 $-q[l-(q+1)i]=l-(q+1)j\pmod{rn}$，故有 $qi+j-l\equiv 0\pmod{rn}$。又因为 $-\dfrac{q^2+1}{2}<qi+j-l\leqslant q\left(\dfrac{q-1}{2}-1\right)+q-2-\dfrac{q^2+1}{2}$，而 $q\left(\dfrac{q-1}{2}-1\right)+q-2<\dfrac{q^2+1}{2}$，故 $-\dfrac{n}{2}<qi+j-l<0$。这与 $qi+j-l\equiv 0\pmod{rn}$ 矛盾，故假设不成立。由此证得 $T_2\bigcap(-qT_1)=\varnothing$。

下面证明当 $\delta>\delta_{\max}$ 时，$T_2\bigcap(-qT_1)\neq\varnothing$。不妨取 $\delta=\delta_{\max}+2$，即 $\delta=q+1$。故存在 $0\leqslant i\leqslant\dfrac{q-1}{2}$，$0<j\leqslant q-2$，使得 $-q[l-(q+1)i]\equiv l-(q+1)j\pmod{rn}$，即 $qi+j-l\equiv 0\pmod{rn}$ 成立，又因为 $-\dfrac{q^2+1}{2}<qi+j-l\leqslant q\dfrac{q-1}{2}+q-2-\dfrac{q^2+1}{2}$，而当 $q\geqslant 5$ 时，$q\dfrac{q-1}{2}+q-2\geqslant\dfrac{q^2+1}{2}$，故存在 $0\leqslant i\leqslant\dfrac{q-1}{2}$，$0<j\leqslant q-2$，使得 $-q[l-(q+1)i]\equiv l-(q+1)j\pmod{rn}$，故假设成立，则有 $T_2\bigcap(-qT_1)\neq\varnothing$。综上可得，结论成立。证毕。

由文献[14]可知，Hermitian 对偶包含常循环码 C_1 和常循环码 C_2 的参数分别为 $[n,n-\delta_1+1,\delta_1]$ 和 $[n,n-\delta_2+1,\delta_2]$（其中 $2\leqslant\delta_1\leqslant q-1$，$4\leqslant\delta_2\leqslant 2(q-1)$ 且 δ_1 与 δ_2 都为偶数）同时满足 $C_2\subset C_1$，易知 C_1 和 C_2 都是 MDS 码。则通过定理 2.1 中给出的构造方法，可构造出一系列新量子码。如下定理所示。

定理 3.2　1）设 q 为奇素数的幂，$n=q^2+1$，则存在参数为 $[[2(q^2+1),2(q^2+1)+4-6d',2d']]_q$（$2\leqslant d'\leqslant q-1$ 且 d' 为偶数）的量子码。

2）设 q 为奇素数的幂，$n=q^2+1$，则存在参数为 $[[2(q^2+1),2(q^2+1)+2-6d'',2d'']]_q$（$2\leqslant d''\leqslant q-1$ 且 d'' 为奇数）的量子码。

相比较于文献[11]所给出的码长为 $2(q^2+1)$ 距离 $d\leqslant q+1$ 的量子码，本文利用定理 2.1 的组合构造出距离为 $d>q+1$ 部分量子码见表 1。

表 1　利用常循环码构造的新量子码

Tab. 1　New quantum codes derived from constacyclic codes

q	$[n,k_1,d_1]_{q^2}$	$[n,k_2,d_2]_{q^2}$	$[[2n,k,d]]_q$
5	$[26,23,4]_{5^2}$	$[26,19,8]_{5^2}$	$[[52,32,8]]_5$
7	$[50,45,6]_{7^2}$	$[50,41,10]_{7^2}$	$[[100,72,10]]_7$
7	$[50,45,6]_{7^2}$	$[50,39,12]_{7^2}$	$[[100,68,12]]_7$
9	$[82,77,6]_{9^2}$	$[82,71,12]_{9^2}$	$[[164,132,12]]_9$
9	$[82,75,8]_{9^2}$	$[82,69,14]_{9^2}$	$[[164,124,14]]_9$
9	$[82,75,8]_{9^2}$	$[82,67,16]_{9^2}$	$[[164,120,16]]_9$
11	$[122,115,8]_{11^2}$	$[122,109,14]_{11^2}$	$[[244,204,14]]_{11}$
11	$[122,115,8]_{11^2}$	$[122,107,16]_{11^2}$	$[[244,200,16]]_{11}$
11	$[122,113,10]_{11^2}$	$[122,105,18]_{11^2}$	$[[244,192,18]]_{11}$
11	$[122,113,10]_{11^2}$	$[122,103,20]_{11^2}$	$[[244,188,20]]_{11}$
13	$[170,163,8]_{13^2}$	$[170,155,16]_{13^2}$	$[[340,296,16]]_{13}$
13	$[170,161,10]_{13^2}$	$[170,153,18]_{13^2}$	$[[340,288,18]]_{13}$
13	$[170,161,10]_{13^2}$	$[170,151,20]_{13^2}$	$[[340,284,20]]_{13}$
13	$[170,159,12]_{13^2}$	$[170,149,22]_{13^2}$	$[[340,276,22]]_{13}$
13	$[170,159,12]_{13^2}$	$[170,147,24]_{13^2}$	$[[340,272,24]]_{13}$

利用码长为 $2(q^2+1)$ 的 BCH 码，由对偶包含 BCH 码可以构造出距离 $d>q+1$ 量子码，但是所得到的量子 BCH 码的参数不如我们构造的量子码的参数。表 2 列出对比结果，即对于同样的码长和给定距离；从表中可明显看出，本文新构造的量子码比量子 BCH 码具有更高的码率。

表 2 量子码参数比较

Tab. 2 Code comparisons

q	新构造的量子码	由文献[12]得到的量子 BCH 码
5	$[[52,32,8]]_5$	$[[52,24,8]]_5$
7	$[[100,72,10]]_7$	$[[100,64,10]]_7$
7	$[[100,68,12]]_7$	$[[100,56,12]]_7$
9	$[[164,132,12]]_9$	$[[164,120,12]]_9$
9	$[[164,124,14]]_9$	$[[164,112,14]]_9$
9	$[[164,120,16]]_9$	$[[164,104,16]]_9$
11	$[[244,204,14]]_{11}$	$[[244,192,14]]_{11}$
11	$[[244,200,16]]_{11}$	$[[244,184,16]]_{11}$
11	$[[244,192,18]]_{11}$	$[[244,176,18]]_{11}$
11	$[[244,188,20]]_{11}$	$[[244,168,20]]_{11}$
13	$[[340,296,16]]_{13}$	$[[340,280,16]]_{13}$
13	$[[340,288,18]]_{13}$	$[[340,272,18]]_{13}$
13	$[[340,284,20]]_{13}$	$[[340,264,20]]_{13}$
13	$[[340,276,22]]_{13}$	$[[340,256,22]]_{13}$
13	$[[340,272,24]]_{13}$	$[[340,248,24]]_{13}$

4 结语

本文首先给出了满足一定嵌套关系的两个 q^2-元线性码组合构造 Hermitian 自正交码的方法,确定出所构造的新的 Hermitian 自正交码的维数和对偶距离下界;其次讨论了码长为 $n=q^2+1$、满足所需嵌套关系的两个 q^2-元常循环 BCH 码的定义集合、设计距离和参数;进一步由常循环 BCH 码构造出码长 $2n$ 的 q-元量子码。相比较于文献[11],利用这一方法可得到距离 $d>q+1$ 量子码,且构造出的量子码和文献[12]中利用 BCH 码构造的量子码相比参数更优。本文的方法和结果对于构造更多参数良好的量子码以及给出最优量子码的距离下界都具有借鉴意义。

参考文献(References):

[1] CALDERBANK A R, SHOR P W. Good Quantum Error-Correcting Codes Exist [J]. Phys Rev A, 1996, 54: 1098-1105.

[2] STEANE A M. Error Correcting Codes in Quantum Theory [J]. Phys Rev Lett, 1996, 77: 793-797.

[3] CALDERBANK A R, RAINS E M, SHOR P W, et al. Quantum Error Correction Via Codes Over GF(4) [J]. IEEE Trans Inf Theory, 1998, 44: 1369-1387.

[4] STEANE A M. Enlargement of Calderbank-Shor-Steane Quantum Codes [J]. IEEE Trans Inf Theory, 1999, 45: 2492-2495.

[5] ASHIKHMIN A, KNILL E. Nonbinary Quantum Stabilizer Codes [J]. IEEE Trans Inf Theory, 2001, 47: 3065-3072.

[6] KETKAR A, KLAPPENECKER A, KUMAR S, et al. Nonbinary Stablizer Codes over Finite Fields [J]. IEEE Trans Inf Theory, 2006, 52: 4892-4914.

[7] LING S, LUO J, XING C. Generalization of Steane's Enlargement Construction of Quantum Codes and Applications [J]. IEEE Trans Inf Theory, 2010, 56: 4080-4084.

[8] GRASSL M, BETH T, PELLIZZARI T. Codes for the Quantum Erasure Channel [J]. Phys Rev Lett A, 1997, 56: 33-38.

[9] GRASSL M, BETH T. Quantum BCH Codes [J]. Proc X Int Symp Theory Elec, 1999: 207-212.

[10] GRASSL M, BETH T. Cyclic Quantum Error-Correcting Codes and Quantum Shift Registers [J]. Proc Royal Soc London Series A, 2000, 456: 2689-2706.

[11] ALY S A, KLAPPENECKER A, SARVEPALLI P K. On Quantum and Classical BCH codes [J]. IEEE Trans Inf Theory, 2007, 53: 1183-1188.

[12] ZHANG T, GE G. Quantum Codes from Generalized Reed-Solomon Codes and Matrix-Product Codes [J]. Mathematics, 2015.

[13] AYDIN N, SIAP I, RAY-CHAUDHURI D K. The Structure of 1-Generator Codes and New Linear Codes [J]. Designs Codes and Crypt, 2001, 24: 313-326.

[14] KAI X, ZHU S, LI P. Constacyclic Codes and Some New Quantum MDS Codes [J]. IEEE Trans Inf Theory, 2014, 60: 2080-2086.

[15] CHEN B, LING S, ZHANG G. Application of Constacyclic Codes to Quantum MDS Codes [J]. IEEE Trans Inf Theory, 2015, 61(3): 1474-1484.

[16] 李瑞虎, 左飞, 刘杨. 斜对称 q^2-分圆陪集及应用 [J]. 空军工程大学学报(自然科学版), 2011, 12(1): 87-89.
LI R H, ZUO F, LIU Y. A Study of Skew Symmetric q-Cyclotomic Coset and Its Application [J]. Journal of Air Force Engineering University (Natural Science Edition), 2011, 12(1): 87-89. (in Chinese)

[17] HU L, YUE Q, ZHU X. New Quantum MDS Code from Constacyclic Codes [J]. Chinese Annals of Mathematics, 2016, 37: 891-898.

(编辑: 姚树峰)