Pure Mathematics 理论数学, **2020, 10(11), 1015-1024**
Published Online November 2020 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/pm.2020.1011120

Hans汉斯

具有ℓ维Hermitian正交包的MDS码的构造

韩雨慧，邱宇廷*，卢啸华

上海大学理学院，上海
Email: *qqyytt@shu.edu.cn

收稿日期：2020年10月14日；录用日期：2020年11月4日；发布日期：2020年11月11日

摘　要

达到 Singleton 界的码称为极大距离可分码(简称为 MDS 码)，其纠错能力最强，在纠错码中有着非常广泛的应用。本文研究了 MDS 码的 Hermitian 正交包，利用广义 Reed-Solomon 码构造了具有 $\ell(\ell \geq 1)$ 维 Hermitian 正交包的 MDS 码。

关键词

MDS码，广义Reed-Solomon码，Hermitian正交包

Construction of MDS Code with ℓ-Dimensional Hermitian Hull

Yuhui Han, Yuting Qiu*, Xiaohua Lu

College of Sciences, Shanghai University, Shanghai
Email: *qqyytt@shu.edu.cn

Received: Oct. 14^{th}, 2020; accepted: Nov. 4^{th}, 2020; published: Nov. 11^{th}, 2020

Abstract

The codes achieving the Singleton bound are called maximum distance separable (for

* 通讯作者。

文章引用: 韩雨慧, 邱宇廷, 卢啸华. 具有ℓ维Hermitian正交包的MDS码的构造[J]. 理论数学, 2020, 10(11): 1015-1024.
DOI: 10.12677/pm.2020.1011120

short MDS) codes, which have the strongest error correction ability and are widely applied in error-correcting code. In this paper, we study the Hermitian hulls of MDS codes. We use the generalized Reed-Solomon code to construct MDS codes with ℓ-dimensional ($\ell \geq 1$) Hermitian hull.

Keywords

MDS Codes, Generalized Reed-Solomon Codes, Hermitian Hull

1. 引言

线性码 $\mathcal{C}$ 的正交包是指 $\mathcal{C}$ 与其对偶码 $\mathcal{C}$ 的交空间. 正交包的维数影响着计算 $\mathcal{C}$ 的自同构群的复杂度 [1] [2]和由 $\mathcal{C}$ 构造的纠缠量子纠错码的相关参数 [3], 文献 [4] [5] [6] [7] 讨论了 Euclidean 正交包和 Hermitian 正交包的维数和平均维数. 正交包维数最小的码是线性互补对偶码 (简称为 LCD 码) , 即正交包维数为 0 , 在密码学中设计抵抗侧信道分析和错误注入攻击以及构造最优或极大纠缠的纠缠辅助量子纠错码中有相关应用. 极大距离可分码(简称为 MDS 码)是达到 Singleton 界的码. MDS 码因其纠错能力较强, 在工程上有广泛的应用, 因而研究 MDS 码的正交包也引起了研究人员的关注 [8–13].

金在文献 [8]中给出所有偶特征有限域上的 Euclidean LCD MDS 码和部分奇特征有限域上的 Euclidean LCD MDS 码. 之后她和 Beelen 在文献中利用代数函数域又构造了奇特征有限域上一些新的 Euclidean LCD MDS 码. 罗等在文献 [10]中研究了广义 Reed-Solomon 码和扩展的广义 Reed-Solomon 码的正交包, 并将结果应用于构造纠缠辅助量子纠错码. 陈等人在文献 [11]中利用广义 Reed-Solomon 码也构造了几类奇特征有限域上的 Euclidean LCD MDS 码. 与Euclidean 内积定义对偶码类似, 同样可以利用Hermitian内积、Galois内积等来定义对偶码, 得到相应的正交包. 文献 [14]中构造了几类 Hermitian LCD 循环码, 并给出这些码的基本参数; 文献 [12]确定了所有可能的 Euclidean LCD MDS 码和 Hermitian LCD MDS 码的参数范围, 但是这些码的明确构造并没有完全给出. 对于正交包维数大于 0 的情形, 文献 [13]利用广义 Reed-Solomn 码构造了一些 MDS 码, 这些 MDS 的 Euclidean 正交包和 Hermitian 正交包的维数几乎可以取所有可能的值. 本文同样研究的是正交包维数大于 0 的 MDS 码的构造. 对于广义 Reed-Solomon 码, 通过建立其正交包维数和多项式次数之间的关联, 构造了具有ℓ ($\ell \geq 1$)维 Hermitian 正交包的 MDS 码. 我们构造出的MDS码的参数和 [13]中不同.

文章内容编排如下, 第二节我们介绍了一些关于正交包和广义Reed-Solomon码的相关知识. 第三节构造了具有 1 维 Hermitian 正交包的 MDS 码, 并给出例子, 最后在第四节中构造了具有ℓ- 维 Hermitian 正交包的 MDS 码.

2. 预备知识

在本文中, 我们设 q 为素数幂, r 为正整数, s 是满足 $0 \leq s \leq r-1$ 的整数. 令 $Q=q^r$, $\mathbb{F}_Q$ 表示含有 Q 个元素的有限域, $\mathbb{F}_Q^*$ 表示 $\mathbb{F}_Q$ 的所有非零元素形成的乘法群, 易知映射

$$\begin{aligned} F_s : \mathbb{F}_Q &\to \mathbb{F}_Q , \\ x &\mapsto x^{[s]}=x^{q^s} \end{aligned}$$

是 $\mathbb{F}_Q$ 上保 $\mathbb{F}_q$ 的自同构. $\mathbb{F}_Q^n$ 表示 $\mathbb{F}_Q$ 上的 n 维向量空间. 向量空间 $\mathbb{F}_Q^n$ 的每个 $\mathbb{F}_Q$ 上的线性子空间 $\mathcal{C}$ 都叫做一个Q- 元$[n,k]$线性码. 若码 $\mathcal{C}$ 的最小距离满足 $d=n-k+1$, 则称 $\mathcal{C}$ 为极大距离可分码.

2.1. s-Galois 正交包

设 $\mathcal{C}$ 是参数为 $[n,k]$ 的 Q 元线性码. 定义线性码 $\mathcal{C}$ 的 Euclidean 对偶码$\mathcal{C}^{\perp}$为

$$\mathcal{C}^{\perp}=\left\{\mathbf{b}\in\mathbb{F}_Q^n : \langle \mathbf{b},\mathbf{c}\rangle=\sum_{i=1}^{n} b_i c_i=0, \forall \mathbf{c}\in\mathcal{C}\right\}.$$

其中, $\langle \mathbf{b},\mathbf{c}\rangle$ 为向量 $\mathbf{b}$ 和 $\mathbf{c}$ 的 Euclidean 内积.

定义 2.1. 线性码 $\mathcal{C}\subseteq\mathbb{F}_Q^n$ 的 Euclidean 正交包 $Hull(\mathcal{C})$ 定义为

$$Hull(\mathcal{C})=\mathcal{C}\cap\mathcal{C}^{\perp}.$$

注 1. 当 $Hull(\mathcal{C})=0$ 时, 称 $\mathcal{C}$ 为线性互补对偶码, 简称为 LCD 码. 当 $Hull(\mathcal{C})=\mathcal{C}$ 时, 称 $\mathcal{C}$ 为自正交码.

定义 2.2 (s-共轭). (1) 设 $\alpha\in\mathbb{F}_Q$, α 的 s-共轭 $\alpha^{[s]}$ 定义为 $\alpha^{[s]}=\alpha^{q^s}$.

(2) 设 $\mathbf{a}=(a_1,a_2,\cdots,a_n)\in\mathbb{F}_Q^n$, 向量 $\mathbf{a}$ 的 s-共轭 $\mathbf{a}^{[s]}$ 定义为

$$\mathbf{a}^{[s]}=(a_1^{[s]},a_2^{[s]},\cdots,a_n^{[s]}),$$

由此我们也可定义码 $\mathcal{C}\subseteq\mathbb{F}_Q^n$ 的 s-共轭

$$\mathcal{C}^{[s]}=\{\mathbf{c}^{[s]}\in\mathbb{F}_Q^n : \mathbf{c}\in\mathcal{C}\}.$$

定义 2.3. $\mathbb{F}_Q^n$ 中两个向量 $\mathbf{b}=(b_1,b_2,\cdots,b_n)$ 和 $\mathbf{c}=(c_1,c_2,\cdots,c_n)$ 的 s-Galois 内积定义为

$$\langle \mathbf{b},\mathbf{c}\rangle_s=\langle \mathbf{b},\mathbf{c}^{[s]}\rangle.$$

注 2. 当 $s=0$ 时, s-Galois内积就是 Euclidean 内积. 当 r 为偶数, $s=\frac{r}{2}$ 时, s-Galois内积就是 Hermitian 内积.

在 s-Galois 内积下我们可定义线性码的 s-Galois 对偶码.

定义 2.4. 线性码 $\mathcal{C}\subseteq\mathbb{F}_Q^n$ 的 s-Galois 对偶码定义为

$$\mathcal{C}^{\perp_s}=\left\{\mathbf{b}\in\mathbb{F}_Q^n : \langle \mathbf{b},\mathbf{c}\rangle_s=0, \forall \mathbf{c}\in\mathcal{C}\right\}.$$

注 3. 由文献 *[15]*可知, 线性码 $\mathcal{C}$ 的 s-Galois 对偶码就是 $\mathcal{C}^{[s]}$ 的Euclidean对偶码, 即

$$\mathcal{C}^{\perp_s} = (\mathcal{C}^{[s]})^{\perp}.$$

类似的, 我们可定义相应的 s-Galois 正交包.

定义 2.5. 线性码 $\mathcal{C} \subseteq \mathbb{F}_Q^n$ 的 s-Galois 正交包 $Hull_s(\mathcal{C})$ 定义为

$$Hull_s(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp_s}.$$

显然, Q 元线性码 $\mathcal{C}$ 的 s-Galois 正交包 $Hull_s(\mathcal{C})$ 也是 Q 元线性码.设 $\mathcal{C} \subseteq \mathbb{F}_Q^n$ 是线性码. 若

$$\dim_{\mathbb{F}_Q} Hull_s(\mathcal{C}) = \ell,$$

则称 $\mathcal{C}$ 是具有 ℓ 维 s-Galois 正交包的线性码.

定义 2.6. 设系数在 $\mathbb{F}_Q$ 上的 t 次多项式

$$f(x) = f_t x^t + f_{t-1}x^{t-1} + \cdots + f_1 x + f_0 \ ,$$

其中 $f_0 f_t \neq 0$. 多项式 $f(x)$ 的 s-共轭多项式 $f^{[s]}(x)$ 定义为

$$f^{[s]}(x) = f_t^{[s]} x^t + f_{t-1}^{[s]} x^{t-1} + \cdots + f_1^{[s]} x + f_0^{[s]}.$$

2.2. 广义 Reed-Solomon 码

设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是有限域 $\mathbb{F}_Q$ 中 n 个不同的元素 (从而 $n \leq Q$), k 是满足 $1 \leq k \leq n$的整数. 记

$$\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$$

和

$$\mathbf{v} = (v_1, v_2, \cdots, v_n) \in (\mathbb{F}_Q^*)^n.$$

我们称如下定义的线性码

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \cdots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_Q[x]; \deg f(x) < k\} \tag{2.1}$$

为广义 Reed-Solomon 码(简称为 GRS 码). 显然, $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ 是参数为 $[n, k, n-k+1]_Q$ 的线性码 [16], 即 $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ 是 MDS 码. 易知, GRS码的对偶码仍为GRS码, 并且有:

引理 2.7. [16] $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ 的 Euclidean 对偶码是

$$\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{w}),$$

其中 $\mathbf{w} = (w_1, w_2, \cdots, w_n)$, $w_i = \frac{1}{v_i} \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ $(i = 1, 2, \cdots, n)$.

类似地, 我们可给出广义 Reed-Solomon 码的 s-Galois 对偶码的刻画.

引理 2.8. 设整数 k 满足 $1 \leq k \leq n$. $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ 的 s-Galois 对偶码是

$$\mathrm{GRS}_{n-k}(\mathbf{a}', \mathbf{w}),$$

其中 $\mathbf{a}'=(\alpha_1^{[s]},\alpha_2^{[s]},\cdots,\alpha_n^{[s]})$, $\mathbf{w}=(w_1,w_2,\cdots,w_n)$, 这里

$$w_i=\frac{1}{v_i^{[s]}}\prod_{1\le j\le n,j\neq i}(\alpha_i^{[s]}-\alpha_j^{[s]})^{-1}(i=1,2,\cdots,n).$$

证明 因为线性码 $\mathcal{C}$ 的 s-Galois 对偶码是 $\mathcal{C}^{[s]}$ 的 Euclidean 对偶码, 以及映射 F_s 是 $\mathbb{F}_Q$ 上保 $\mathbb{F}_q$ 的自同构, 所以

$$\begin{aligned}[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{\perp_s}&=\left\{[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{[s]}\right\}^{\perp}\\&=\left\{(v_1^{[s]}f^{[s]}(\alpha_1^{[s]}),\cdots,v_n^{[s]}f^{[s]}(\alpha_n^{[s]})):f(x)\in\mathbb{F}_Q[x];\deg f(x)<k\right\}^{\perp}\\&=\left\{(v_1^{[s]}f(\alpha_1^{[s]}),\cdots,v_n^{[s]}f(\alpha_n^{[s]})):f(x)\in\mathbb{F}_Q[x];\deg f(x)<k\right\}^{\perp}\\&=[\mathrm{GRS}_k(\mathbf{a}',\mathbf{v}')]^{\perp},\end{aligned}$$

其中 $\mathbf{a}'=(\alpha_1^{[s]},\alpha_2^{[s]},\cdots,\alpha_n^{[s]})$, $\mathbf{v}'=(v_1^{[s]},v_2^{[s]},\cdots,v_n^{[s]})$. 由引理 2.7 即可证明该结论.

3. 具有 1 维 Hermitian 正交包的 MDS 码的构造

为了方便, 下面的部分我们总是假设 q 为素数幂, $Q=q^2$, $\mathbb{F}_Q$ 表示含有 Q 个元素的有限域, $\mathbb{F}_Q^*$ 表示 $\mathbb{F}_Q$ 的所有非零元素形成的乘法群, 此时线性码 $\mathcal{C}\subseteq\mathbb{F}_Q^n$ 的 Hermitian 对偶码也可记为

$$\mathcal{C}^{\perp_H}=\left\{(b_1,b_2,\cdots,b_n)\in\mathbb{F}_Q^n:\sum_{i=1}^{n}b_ic_i^q=0,\forall(c_1,c_2,\cdots,c_n)\in\mathcal{C}\right\}.$$

设 t 是满足 $1\le t\le Q-q$ 的整数, $n=q+t$ (从而 $q+1\le n\le Q$), 整数 k 满足 $1\le k\le n$, $\mathbb{F}_q=\{\alpha_1,\alpha_2,\cdots,\alpha_q\}$ 和 $\mathbb{F}_Q=\{\alpha_1,\alpha_2,\cdots,\alpha_q,\beta_1,\beta_2,\cdots,\beta_{Q-q}\}$, 其中 $\beta_i\in\mathbb{F}_Q\backslash\mathbb{F}_q$ ($i=1,2,\cdots,Q-q$). 令

$$\mathbf{a}=(\alpha_1,\alpha_2,\cdots,\alpha_q,\beta_1,\beta_2,\cdots,\beta_t)$$

和

$$\mathbf{v}=(v_1,v_2,\cdots,v_n)\in(\mathbb{F}_Q^*)^n.$$

由引理 2.8 即可得到 $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 对偶码.

推论 3.1. $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 对偶码是

$$\mathrm{GRS}_{n-k}(\mathbf{a}',\mathbf{w}),$$

其中 $\mathbf{a}'=(\alpha_1,\alpha_2,\cdots,\alpha_q,\beta_1^q,\beta_2^q,\cdots,\beta_t^q)$, $\mathbf{w}=(w_1,w_2,\cdots,w_n)$, 这里

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le q,j\neq i}(\alpha_i-\alpha_j)^{-1}\prod_{1\le m\le t}(\alpha_i-\beta_m^q)^{-1},\quad i=1,2,\cdots,q,$$

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le q}(\beta_{i-q}^q-\alpha_j)^{-1}\prod_{1\le m\le t,m\neq i-q}(\beta_{i-q}^q-\beta_m^q)^{-1},\quad i=q+1,q+2,\cdots,n.$$

定理 3.2. 设 $k \le q$ 和 $(n-k-1)q < n$. 若对于任意满足 $1 \le i \le q$ 的整数 i 都有

$$\prod_{1\le j\le q, j\ne i}(\alpha_i-\alpha_j)^{-1}\prod_{1\le m\le t}(\alpha_i-\beta_m^q)^{-1}=v_i^{q+1}, \tag{3.1}$$

对于任意满足 $q+1 \le i \le n$ 的整数 i 都有

$$\prod_{1\le j\le q}(\beta_{i-q}^q-\alpha_j)^{-1}\prod_{1\le m\le t, m\ne i-q}(\beta_{i-q}^q-\beta_m^q)^{-1}=v_i^{q+1}, \tag{3.2}$$

则 $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 是具有 1 维 Hermitian 正交包的 MDS 码, 且其参数为 $[n,k,n-k+1]_Q$.

证明 由推论 3.1 可知:

$$[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{\perp_H}=\mathrm{GRS}_{n-k}(\mathbf{a}',\mathbf{w}),$$

其中 $\mathbf{a}'=(\alpha_1,\alpha_2,\cdots,\alpha_q,\beta_1^q,\beta_2^q,\cdots,\beta_t^q)$, $\mathbf{w}=(w_1,w_2,\cdots,w_n)$, 这里

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le q, j\ne i}(\alpha_i-\alpha_j)^{-1}\prod_{1\le m\le t}(\alpha_i-\beta_m^q)^{-1},\quad i=1,2,\cdots,q;$$

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le q}(\beta_{i-q}^q-\alpha_j)^{-1}\prod_{1\le m\le t, m\ne i-q}(\beta_{i-q}^q-\beta_m^q)^{-1},\quad i=q+1,q+2,\cdots,n.$$

下面决定 $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 正交包, 不妨设

$$(v_1f(\alpha_1),\cdots,v_qf(\alpha_q),v_{q+1}f(\beta_1),\cdots,v_nf(\beta_t))\in\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\cap[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{\perp_H},$$

其中 $\deg f(x)\le k-1$. 因此, 存在一个次数不超过 $n-k-1$ 的多项式 $g(x)$, 使得

$$(v_1f(\alpha_1),\cdots,v_qf(\alpha_q),v_{q+1}f(\beta_1),\cdots,v_nf(\beta_t))=(w_1g(\alpha_1),\cdots,w_qg(\alpha_q),w_{q+1}g(\beta_1^q),\cdots,w_ng(\beta_t^q)),$$

故

$$\begin{cases} v_if(\alpha_i)=w_ig(\alpha_i), & i=1,2,\cdots,q;\\ v_if(\beta_{i-q})=w_ig(\beta_{i-q}^q), & i=q+1,q+2,\cdots,n.\end{cases}$$

由等式 (3.1) 和 (3.2) 可得 $w_i=v_i\ne 0$, 对 $1\le i\le n$, 因此有如下等式:

$$\begin{cases} f(\alpha_i)=g(\alpha_i), & i=1,2,\cdots,q;\\ f(\beta_{i-q})=g(\beta_{i-q}^q), & i=q+1,q+2,\cdots,n.\end{cases}$$

上式表明: $g(x^q)-f(x)=0$ 至少有 n 个不同的根, $g(x)-f(x)=0$ 至少有 q 个不同的根. 因为 $(n-k-1)q<n$, 所以 $\deg[g(x^q)-f(x)]<n$, 因此 $g(x^q)=f(x)$. 此时 $\deg f(x)=q\cdot\deg g(x)$, 也就是说 $\deg f(x)\ge\deg g(x)$. 又因为 $k\le q$, 所以 $\deg[g(x)-f(x)]\le\deg f(x)\le k-1\le q-1$. 由于 $g(x)-f(x)=0$ 至少有 q 个不同的根, 因此 $g(x)=f(x)$, 进而有 $\deg f(x)=\deg g(x)=0$. 因此, $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 正交包是由向量 v 生成的 1 维线性空间. 定理得证.

下面我们给出几个具体的例子.

例 3.1. 设 $q=4$, $Q=q^2=16$, γ 是有限域 $\mathbb{F}_Q$ 的本原元, 则

$$\mathbb{F}_{16}=\{0,1,\gamma,\gamma^2,\cdots,\gamma^{14}\}$$

和

$$\mathbb{F}_4 = \{0, 1, \gamma^5, \gamma^{10}\}.$$

令 $n = 6$ 和 $k = 4$, 此时 $n \geq q + 1$, $k \leq q$ 且 $(n - k - 1)q < n$. 选取

$$\mathbf{a} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2)$$

和

$$\mathbf{v} = (v_1, v_2, v_3, v_4, v_5, v_6) \in (\mathbb{F}_{16}^*)^6,$$

其中 $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = \gamma^5$, $\alpha_4 = \gamma^{10}$, $\beta_1 = \gamma$, $\beta_2 = \gamma^4$; $v_1 = \gamma^{14}$, $v_2 = 1$, $v_3 = \gamma^{14}$, $v_4 = 1$, $v_5 = \gamma^{13}$, $v_6 = \gamma^{13}$.

可以验证, 对于任意满足 $1 \leq i \leq 4$ 的整数 i, *(3.1)* 式成立. 对于任意满足 $5 \leq i \leq 6$ 的整数 i, *(3.2)* 式成立. 由定理 *3.2* 可知: $\mathrm{GRS}_4(\mathbf{a}, \mathbf{v})$ 是具有 1 维 Hermitian 正交包的 MDS 码, 且其参数为 $[6, 4, 3]_{16}$.

例 3.2. 设 $q = 3$, $Q = q^2 = 9$, γ 是有限域 $\mathbb{F}_Q$ 的本原元, 则

$$\mathbb{F}_9 = \{0, 1, \gamma^1, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6, \gamma^7\}$$

和

$$\mathbb{F}_3 = \{0, 1, \gamma^4\}.$$

其中, $\gamma^4 = 2$.

令 $n = 5$ 和 $k = 3$, 此时 $n \geq q + 1$, $k \leq q$ 和 $(n - k - 1)q < n$. 选取

$$\mathbf{a} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$$

和

$$\mathbf{v} = (v_1, v_2, v_3, v_4, v_5) \in (\mathbb{F}_9^*)^5,$$

其中 $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 2$, $\alpha_4 = \gamma^2$, $\alpha_5 = \gamma^6$; $v_1 = \gamma$, $v_2 = 1$, $v_3 = 1$, $v_4 = 1$, $v_5 = 1$.

可以验证, 对于任意满足 $1 \leq i \leq 3$ 的整数 i, *(3.1)* 式成立. 对于任意满足 $4 \leq i \leq 5$ 的整数 i, *(3.2)* 式成立. 由定理 *3.2* 可知: $\mathrm{GRS}_3(\mathbf{a}, \mathbf{v})$ 是具有 1 维 Hermitian 正交包的 MDS 码, 且其参数为 $[5, 3, 3]_9$.

4. 具有 $\ell(\ell \geq 1)$ 维 Hermitian 正交包的 MDS 码的构造

本节中, 设 $\mathbb{F}_Q = \{\alpha_1, \alpha_2, \cdots, \alpha_Q\}$, n 是满足 $1 \leq n \leq Q$ 的整数, 整数 k 满足 $1 \leq k \leq n$. 令

$$\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$$

和

$$\mathbf{v} = (v_1, v_2, \cdots, v_n) \in (\mathbb{F}_Q^*)^n.$$

由引理 2.8 即可得到 $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ 的 Hermitian 对偶码.

推论 4.1. $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 对偶码是

$$\mathrm{GRS}_{n-k}(\mathbf{a}',\mathbf{w}),$$

其中 $\mathbf{a}'=(\alpha_1^q,\alpha_2^q,\cdots,\alpha_n^q)$, $\mathbf{w}=(w_1,w_2,\cdots,w_n)$, 这里

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le n,j\ne i}(\alpha_i^q-\alpha_j^q)^{-1},\quad i=1,2,\cdots,n.$$

定理 4.2. 设 $(n-k-1)q<n$. 若对于任意满足 $1\le i\le n$ 的整数 i 都有

$$\prod_{1\le j\le n,j\ne i}(\alpha_i^q-\alpha_j^q)^{-1}=v_i^{q+1}, \tag{4.1}$$

则 $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 是具有 $\lceil\frac{k}{q}\rceil$ 维 Hermitian 正交包的 MDS 码, 且其参数为 $[n,k,n-k+1]_Q$.

证明 由推论 4.1 可知:

$$[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{\perp_H}=\mathrm{GRS}_{n-k}(\mathbf{a}',\mathbf{w})$$

其中 $\mathbf{a}'=(\alpha_1^q,\alpha_2^q,\cdots,\alpha_n^q)$, $\mathbf{w}=(w_1,w_2,\cdots,w_n)$, 这里

$$w_i=\frac{1}{v_i^q}\prod_{1\le j\le n,j\ne i}(\alpha_i^q-\alpha_j^q)^{-1},\quad i=1,2,\cdots,n.$$

下面决定 $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ 的 Hermitian 正交包, 不妨设

$$(v_1f(\alpha_1),v_2f(\alpha_2),\cdots,v_nf(\alpha_n))\in\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\cap[\mathrm{GRS}_k(\mathbf{a},\mathbf{v})]^{\perp_H},$$

其中 $\deg f(x)\le k-1$. 因此, 存在一个次数不超过 $n-k-1$ 的多项式 $g(x)$, 使得

$$(v_1f(\alpha_1),v_2f(\alpha_2),\cdots,v_nf(\alpha_n))=(w_1g(\alpha_1^q),w_2g(\alpha_2^q),\cdots,w_ng(\alpha_n^q)),$$

故

$$v_if(\alpha_i)=w_ig(\alpha_i^q),\quad i=1,2,\cdots,n.$$

由等式 (4.1) 可得 $w_i=v_i\ne0$, 对 $1\le i\le n$, 因此有如下等式:

$$f(\alpha_i)=g(\alpha_i^q),\quad i=1,2,\cdots,n.$$

上式表明 $g(x^q)-f(x)=0$ 至少有 n 个不同的根. 因为 $(n-k-1)q<n$, 所以 $\deg[g(x^q)-f(x)]<n$, 因此 $g(x^q)=f(x)$. 此时 $\deg f(x)=q\cdot\deg g(x)$, 又 $\deg f(x)\le k-1$, 所以 $\deg g(x)\le\frac{k-1}{q}$. 即 $\deg g(x)\le\lfloor\frac{k-1}{q}\rfloor$. 所以 Hermitian 正交包的维数为 $\lfloor\frac{k-1}{q}\rfloor+1=\lceil\frac{k}{q}\rceil$. 定理得证.

下面给出几个具体例子

例 4.1. 设 $q=4$, $Q=q^2=16$, γ 是有限域 $\mathbb{F}_Q$ 的本原元, 则

$$\mathbb{F}_{16}=\{0,1,\gamma,\gamma^2,\cdots,\gamma^{14}\}.$$

令 $n=8$ 和 $k=6$, 此时 $(n-k-1)q<n$, $\lceil\frac{k}{q}\rceil=2$. 选取

$$\mathbf{a}=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8)$$

和

$$\mathbf{v}=(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8)\in(\mathbb{F}_{16}^*)^8,$$

其中 $\alpha_1=0,\alpha_2=1,\alpha_3=\gamma^5,\alpha_4=\gamma^{10},\alpha_5=\gamma,\alpha_6=\gamma^4,\ \alpha_7=\gamma^3,\alpha_8=\gamma^{12}$; $v_1=\gamma^{14},v_2=\gamma^{14},v_3=\gamma^{14},v_4=\gamma^{14},\ v_5=\gamma^{14},v_6=\gamma^8,v_7=\gamma^{14},v_8=\gamma^5$.

可以验证, 对于任意满足 $1\le i\le 8$ 的整数 i, *(4.1)* 式成立. 由定理 *4.2* 可知: $\mathrm{GRS}_6(\mathbf{a},\mathbf{v})$ 是具有 2 维 Hermitian 正交包的 MDS 码, 且其参数为 $[8,6,3]_{16}$.

例 4.2. 设 $q=4$, $Q=q^2=16$, γ 是有限域 $\mathbb{F}_Q$ 的本原元, 则

$$\mathbb{F}_{16}=\{0,1,\gamma,\gamma^2,\cdots,\gamma^{14}\}.$$

令 $n=12$ 和 $k=9$, 此时 $(n-k-1)q<n$, $\lceil\frac{k}{q}\rceil=3$. 选取

$$\mathbf{a}=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8,\alpha_9,\alpha_{10},\alpha_{11},\alpha_{12})$$

和

$$\mathbf{v}=(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8,v_9,v_{10},v_{11},v_{12})\in(\mathbb{F}_{16}^*)^{12},$$

其中 $\alpha_1=0,\alpha_2=1,\alpha_3=\gamma^5,\alpha_4=\gamma^{10},\alpha_5=\gamma,\alpha_6=\gamma^4,\ \alpha_7=\gamma^2,\alpha_8=\gamma^8,\alpha_9=\gamma^3,\alpha_{10}=\gamma^{12},\alpha_{11}=\gamma^{11},\ \alpha_{12}=\gamma^{14}$; $v_1=v_2=v_3=v_4=\gamma,\ \ v_5=v_6=v_7=v_8=\gamma^2,\ v_9=v_{10}=v_{11}=v_{12}=1$.

可以验证, 对于任意满足 $1\le i\le 12$ 的整数 i, *(4.1)* 式成立. 由定理 *4.2* 可知: $\mathrm{GRS}_9(\mathbf{a},\mathbf{v})$ 是具有 3 维 Hermitian 正交包的 MDS 码, 且其参数为 $[12,9,4]_{16}$.

例 4.3. 设 $q=5$, $Q=q^2=25$, γ 是有限域 $\mathbb{F}_Q$ 的本原元, 则

$$\mathbb{F}_{25}=\{0,1,\gamma,\gamma^2,\cdots,\gamma^{23}\}.$$

其中, $\gamma^6=2,\ \gamma^{12}=4,\ \gamma^{18}=3$.

令 $n=9$ 和 $k=7$, 此时 $(n-k-1)q<n$, $\lceil\frac{k}{q}\rceil=2$. 选取

$$\mathbf{a}=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8,\alpha_9)$$

和

$$\mathbf{v}=(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8,v_9)\in(\mathbb{F}_{25}^*)^9,$$

其中 $\alpha_1=0,\alpha_2=1,\alpha_3=2,\alpha_4=3,\alpha_5=4,\alpha_6=\gamma^2,\ \alpha_7=\gamma^{10},\alpha_8=\gamma^7,\alpha_9=\gamma^{11}$; $v_1=\gamma^5,v_2=\gamma^6,v_3=\gamma^5,v_4=\gamma^5,\ v_5=\gamma^5,v_6=\gamma^5,v_7=\gamma^5,v_8=\gamma^5,v_8=\gamma^5$.

可以验证, 对于任意满足 $1\le i\le 9$ 的整数 i, *(4.1)* 式成立. 由定理 *4.2* 可知: $\mathrm{GRS}_7(\mathbf{a},\mathbf{v})$ 是具有 2 维 Hermitian 正交包的 MDS 码, 且其参数为 $[9,7,3]_{25}$.

参考文献

[1] Leon, J. (1982) Computing Automorphism Groups of Error-Correcting Codes. *IEEE Transactions on Information Theory*, **28**, 496-511. https://doi.org/10.1109/TIT.1982.1056498

[2] Sendrier, N. and Skersys, G. (2001) On the Computation of the Automorphism Group of a Linear Code. *Proceedings of the 2001 IEEE International Symposium on Information Theory*, Washington DC, 29 June 2001, 13. https://doi.org/10.1109/ISIT.2001.935876

[3] Brun, T., Devetak, I. and Hsieh, M.H. (2006) Correcting Quantum Errors with Entanglement. *Science*, **314**, 436-439. https://doi.org/10.1126/science.1131563

[4] Sendrier, N. (1997) On the Dimension of the Hull. *SIAM Journal on Discrete Mathematics*, **10**, 282-293. https://doi.org/10.1137/S0895480195294027

[5] Sangwisut, E., Jitman, S., Ling, S. and Udomkavanich, P. (2015) Hulls of Cyclic and Negacyclic Codes over Finite Fields. *Finite Fields and Their Applications*, **33**, 232-257. https://doi.org/10.1016/j.ffa.2014.12.008

[6] Skersys, G. (2003) The Average Dimension of the Hull of Cyclic Codes. *Discrete Applied Mathematics*, **128**, 275-292. https://doi.org/10.1016/S0166-218X(02)00451-1

[7] Jitman, S. and Sangwisut, E. (2018) The Average Dimension of the Hermitian Hull of Constacyclic Codes over Finite Fields of Square Order. *Advances in Mathematics of Communications*, **12**, 451-463. https://doi.org/10.3934/amc.2018027

[8] Jin, L. (2016) Construction of MDS Codes with Complementary Duals. *IEEE Transactions on Information Theory*, **63**, 2843-2847. https://doi.org/10.1109/TIT.2016.2644660

[9] Beelen, P. and Jin, L. (2018) Explicit MDS Codes with Complementary Duals. *IEEE Transactions on Information Theory*, **64**, 7188-7193. https://doi.org/10.1109/TIT.2018.2816934

[10] Luo, G. and Cao, X. (2018) MDS Codes with Arbitrary Dimensional Hull and Their Applications. arXiv:1807.03166

[11] Chen, B. and Liu, H. (2017) New Constructions of MDS Codes with Complementary Duals. *IEEE Transactions on Information Theory*, **64**, 5776-5782. https://doi.org/10.1109/TIT.2017.2748955

[12] Carlet, C., Mesnager, S., Tang, C. and Qi, Y. (2018) Euclidean and Hermitian LCD MDS Codes. *Designs, Codes and Cryptography*, **86**, 2605-2618. https://doi.org/10.1007/s10623-018-0463-8

[13] Fang, W., Fu, F.W., Li, L. and Zhu, S. (2020) Euclidean and Hermitian Hulls of MDS Codes and Their Applications to EAQECCs. *IEEE Transactions on Information Theory*, **66**, 3527-3537. https://doi.org/10.1109/TIT.2019.2950245

[14] Li, C. (2018) Hermitian LCD Codes from Cyclic Codes. *Designs, Codes and Cryptography*, **86**, 2261-2278. https://doi.org/10.1007/s10623-017-0447-0

[15] Ding, Y. and Lu, X.H. (2020) Galois Hulls of Cyclic Codes over Finite Fields. *IEICE Transactions on Communication*, **103**, 370-375. https://doi.org/10.1587/transfun.2019EAL2087

[16] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes. Elsevier, Amsterdam.