Pure Mathematics 理论数学, 2020, 10(9), 876-888
Published Online September 2020 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2020.109102

Hans汉斯

由GRS码构造新的量子MDS码

陈　硕，唐西林

华南理工大学数学学院，广东 广州
Email: chenshuocyg@163.com, xltang@scut.edu.cn

收稿日期：2020年8月29日；录用日期：2020年9月18日；发布日期：2020年9月25日

摘　要

量子MDS码的构造如今变得越来越重要。本文我们对 q^2-1 作素数分解并讨论了 q 的奇偶性，在有限域 F_{q^2} 上构造了4类新的量子MDS码。这些量子MDS码参数更灵活，最小距离大。此外，我们通过 L_1-forms和 L_2-forms可以找到那些极小距离大于 $\frac{q}{2}+1$ 的那些量子MDS码。

关键词

量子码，厄米特自正交，GRS码

New Quantum MDS Codes from GRS Codes

Shuo Chen, Xilin Tang

School of Mathematics, South China University of Technology, Guangzhou Guangdong
Email: chenshuocyg@163.com, xltang@scut.edu.cn

Received: Aug. 29th, 2020; accepted: Sep. 18th, 2020; published: Sep. 25th, 2020

Abstract

It becomes more important to construct quantum maximum-distance-separable (MDS) codes by means of the self-dual Generalized Reed-Solomon (GRS) codes. In this paper, we construct four classes of quantum MDS codes over a finite field F_{q^2} through the prime decomposition of q^2-1 and the discussion of the parity of q. These quantum MDS codes have more flexible parameters with large minimum distance. Further, those quantum codes of the minimum distances larger than $\frac{q}{2}+1$ can be found by L_1-forms and L_2-forms.

文章引用: 陈硕, 唐西林. 由 GRS 码构造新的量子 MDS 码[J]. 理论数学, 2020, 10(9): 876-888.
DOI: 10.12677/pm.2020.109102

Keywords

Quantum MDS Code, Hermitian Self-Orthogonal, GRS Codes

1. 引言

近年来，量子纠错码的研究进展迅速。量子误差校正是实现量子计算和量子通信的重要保证。设 q 为一个素数的 m 次幂，F_q 为含有 q 个元素的有限域。一个长度为 n，维数为 K 的量子码是 q^n 维希尔伯特空间的一个 K 维子空间。同时我们把一个长度为 n，维数为 K，极小距离为 d 的 q 元量子码记为 $q-((n,K,d))$。一个长度为 n，维数为 q^k，极小距离为 d 的量子码的 q 元量子码则记为 $[[n,k,d]]_q$。

近年来，针对量子 MDS 码的构造进行了大量的研究工作，并构建了很多类新的量子 MDS 码(参考[1]-[7])。在本文中，假设 $q^2-1=2^{t_0}p_1^{t_1}\cdots p_s^{t_s}$ 是对 q^2-1 的一个素数分解，我们通过 GRS 码构造了 4 类新的量子 MDS 码。与[7] [8]相比，上述量子 MDS 编码的长度更灵活，同时通过 L_1-forms 和 L_2-forms 我们也可以找到一个较大的极小距离。

在第二节中，我们简要回顾了厄米特自正交性和 GRS 码的定义及基本结论。在第三节中，我们从 GRS 码出发，利用有限域等工具，构造了一些新的量子 MDS 码。在最后一部分，我们对本文的结论进行了总结。

2. 预备知识

在本节中，我们将介绍一些关于线性码和 GRS (Generalized Reed-Solomon)码的一些符号和结论。

2.1. 基本符号

假设 $q=p^m$，其中 p 是一个素数，m 是一个正整数，F_q 为含有 q 个元素的有限域，$F_q^*=F_q\setminus\{0\}$。

对于任意两个向量 $u=(u_1,u_2,\cdots,u_n)$，$v=(v_1,v_2,\cdots,v_n)\in F_q^n$，它们的欧几里得内积和厄米特内积被分别定义为：

$$\langle u,v\rangle_E=\sum_{i=1}^n u_iv_i,\quad \langle u,v\rangle_H=\sum_{i=1}^n u_iv_i^q$$

假设 C 是 F_q^n 中一个长度为 n 的线性码，则 C 的厄米特对偶码定义为：

$$C^{\perp H}=\{u\in F_q^n:\langle u,v\rangle_H=0\text{对任意的}v\in C\}$$

如果 C 满足 $C\subseteq C^{\perp H}$，则 C 被称为厄米特自正交码。若 C 的参数为 $[n,k,d]$，则当 $d=n-k+1$ 时，我们称 C 为 MDS 码(maximum distance separable code)。

假设 $a_1,a_2,\cdots,a_n$ 是 F_q 中 n 个不同的元素，$v_1,v_2,\cdots,v_n$ 是 F_q 中 n 个非零元素，则关于向量 $a=(a_1,a_2,\cdots,a_n)$ 和 $v=(v_1,v_2,\cdots,v_n)$ 的 GRS 码定义为

$$GRS_k(a,v)=\{(v_1f(a_1),v_2f(a_2),\cdots,v_nf(a_n)):f(x)\in F_q[x],\deg(f(x))\le k-1\}。$$

我们知道 $GRS_k(a,v)$ 是一个参数为 $[n,k,n-k+1]$ 的 MDS 码。

2.2. 基本引理和推论

引理 2.2.1 [9]. 假设 $a=(a_0,a_1,\cdots,a_{n-1})\in F_{q^2}^n$，$v=(v_0,v_1,\cdots,v_{n-1})\in\left(F_{q^2}^*\right)^n$，这里 $a_0,a_1,\cdots,a_{n-1}$ 是 F_q 中 n 个不同的元素，则 $GRS_k(a,v)\subseteq GRS_k(a,v)^{\perp H}$ 当且仅当 $\left\langle a^{qj+l},v^{q+1}\right\rangle=0$ 对于任意的 $0\le j,l\le k-1$。

我们定义 $\mathbf{0}$ 为元素全为 0 的一维行向量，对于元素在 F_{q^2} 中的矩阵 $A=(a_{ij})$，定义 $A^{(q)}$ 为矩阵 $\left(a_{ij}^q\right)$，0^0 我们记为 1。

引理 2.2.2 [3] [10].假设 $r>0$，A 为元素在 F_{q^2} 中的 $r\times(r+1)$ 阶矩阵并且满足以下两个条件：

(1) A 的任意 r 列线性无关。

(2) $A^{(q)}$ 与 A 行等价。

则方程组 $Au^{\mathrm{T}}=\mathbf{0}^{\mathrm{T}}$ 存在一个解 $u=(u_0,u_1,\cdots,u_r)\in\left(F_q^*\right)^{r+1}$。

推论 2.2.3. 假设 $r>0$，$1\le a\in\mathbb{Z}^*$ 和 $r+a<q+1$。A 为元素在 F_{q^2} 中的 $r\times(r+1)$ 阶矩阵并且满足以下两个条件：

(1) A 的任意 r 列线性无关。

(2) $A^{(q)}$ 与 A 行等价。

则方程组 $Au^{\mathrm{T}}=\mathbf{0}^{\mathrm{T}}$ 存在一个解 $u=(u_0,u_1,\cdots,u_{r+a-1})\in\left(F_q^*\right)^{r+a}$

证明：我们对 a 应用数学归纳法。

(1) 当 $a=1$ 时，由引理 2.2.2，结论成立。

(2) 假设结论在 $a\le x-1$ 时成立，其中 $x\ge 2$ 是一个正整数。

(3) 当 $a=x$ 时，假设 A_1 (A_{r+x})为由矩阵 A 删除第一列(最后一列)获得的 $r\times(r+x-1)$ 阶矩阵。根据(2)的假设，A_1 和 A_{r+x} 对于结论成立，因此方程组

$$A_1u^{\mathrm{T}}=\mathbf{0}^{\mathrm{T}},\quad A_{r+x-1}v^{\mathrm{T}}=\mathbf{0}^{\mathrm{T}}$$

分别存在一个非零解 $u=(u_2,u_3,\cdots,u_{r+x})$ 和 $v=(v_1,v_2,\cdots,v_{r+x-1})$。由于 $r+x<q+1$，我们可以选出一个元素

$$\theta\in F_q^*\setminus\left\{\frac{u_2}{v_2},\frac{u_3}{v_3},\cdots,\frac{u_{r+x-1}}{v_{r+x-1}}\right\}$$

取 $x=(0,u)-\theta(v,0)$，则 $x\in\left(F_q^*\right)^{r+x}$，我们有

$$Ax=\begin{pmatrix}0\\A_1u^{\mathrm{T}}\end{pmatrix}+\theta\begin{pmatrix}A_{r+x-1}v^{\mathrm{T}}\\0\end{pmatrix}=\mathbf{0}$$

故结论成立。

引理 2.2.4 [1]. 如果存在一个元素在 F_{q^2} 上的 $[n,k,d]$ 线性码 C 且 $C^{\perp H}\subseteq C$，则存在一个参数为 $[\![n,k,\ge d]\!]_q$ 的量子码。

引理 2.2.5 [8]. 如果存在一个厄米特自正交的 $[n,k,n-k+1]_{q^2}$ MDS 码，则存在一个参数为 $[\![n,n-2k,k+1]\!]_q$ 的量子码。

假设 $\alpha=(a_0,a_1,\cdots,a_{n-1})\in F_{q^2}^n$，$\beta=(b_0,b_1,\cdots,b_{m-1})\in F_{q^2}^m$，定义他们的张量积：

$$\alpha\otimes\beta=(a_0\beta,a_1\beta,\cdots,a_{n-1}\beta)\in F_{q^2}^{mn}。$$

可以看出

$$\langle \alpha\otimes\beta,\alpha_1\otimes\beta_1\rangle=\langle \alpha,\alpha_1\rangle\langle \beta,\beta_1\rangle。$$

假设 $F_{q^2}^*=\langle\omega\rangle$，其中 ω 为 F_{q^2} 的一个本原元。设 $q^2-1=2^{t_0}p_1^{t_1}\cdots p_s^{t_s}$ 是对 q^2-1 的一个素数分解，再者，我们可以假设 $q-1=2^{t_0'}p_1^{t_1}\cdots p_w^{t_w}$，$q+1=2^{t_0''}p_{w+1}^{t_{w+1}}\cdots p_s^{t_s}$，$M_1=\dfrac{q-1}{2^{k_0'}p_1^{k_1}\cdots p_w^{k_w}}$，$M_2=\dfrac{q+1}{2^{k_0''}p_{w+1}^{k_{w+1}}\cdots p_s^{k_s}}$ 和 $p_0=2$，$t_0=t_0'+t_0''$，$k_0=k_0'+k_0''$，$M=M_1M_2$，$0\le k_i\le t_i$ 对于 $0\le i\le s$。很容易可以看出

$$q\left(\mathrm{mod}\,p_i\right)=\begin{cases}1; & 1\le i\le w\\ -1; & w+1\le i\le s\end{cases}，\quad q\left(\mathrm{mod}\,4\right)=\begin{cases}1; & 1=t_0''<t_0'\\ -1; & 1=t_0'<t_0''\end{cases}$$

假设 $\alpha_i=\omega^{\frac{q^2-1}{p_i^{t_i}}}$ 对于 $i=0,1,\cdots,s$，则 $ord\left(\alpha_i\right)=p_i^{t_i}$，我们可以得出

$\gcd\left(ord\left(\alpha_i\right),ord\left(\alpha_j\right)\right)=1$ 对任意的 $i\ne j$

因此 $F_{q^2}^*=\langle\alpha_0\rangle\times\langle\alpha_1\rangle\times\cdots\times\langle\alpha_s\rangle$ 是 $s+1$ 个子群的直积。

设 $\gamma_i=\alpha_i^{p_i^{k_i}}$，则 $ord\left(\gamma_i\right)=p_i^{t_i-k_i}$，设 $\Gamma_i=\langle\gamma_i\rangle$ 以及

$$\left(\Gamma_i\right)=\left(1,\gamma_i,\cdots,\gamma_i^{p_i^{t_i-k_i}-1}\right)。$$

则有 $\langle\alpha_i\rangle=\bigcup_{t=0}^{p_i^{k_i}-1}\alpha_i^t\langle\gamma_i\rangle$ 对任意的 $i=0,1,\cdots,s$。

3. 主要结果

记 $n=\dfrac{\left(r_0+1\right)\left(r_1+1\right)\cdots\left(r_s+1\right)\left(q^2-1\right)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}}$，在这一节，我们利用厄米特自正交的 GRS 码来构造新的长度为 $1+n$ 的量子 MDS 码。在此之前，我们先给出以下几个引理。

引理 3.1 [3]. 设 $q>2$ 和 $r\ge1$，则存在 $u_0,u_1,\cdots,u_r$ 使得

$$\sum_{i=0}^{r}u_i=0$$

根据引理 3.1，我们有如下推论。

推论 3.2. 设 $q>2$ 和 $r\ge1$，$v\in F_q^*$，则存在 $u_0,u_1,\cdots,u_r$ 使得

$$\sum_{i=0}^{r}u_i=v$$

证明：我们分两种情况来证明此推论。

(1) $r=1$。任取 $u_0\in F_q^*$ 及

$$u_1=v-u_0\in F_q^*$$

则有 $\sum_{i=0}^{r}u_i=v$。

(2) $r>1$。由引理 3.1，则存在 $u_0,u_1,\cdots,u_r$ 使得 $\sum_{i=0}^{r-1}u_i=0$，取 $u_r=v\in F_q^*$，我们有

$$\sum_{i=0}^{r}u_i=0+v=v$$

故结论成立。

3.1. 当 $q=2^m$ 时

对于一个向量 $c=(c_1,\cdots,c_n)\in F_{q^2}^n$ 和 $u\in F_{q^2}$，我们定义

$$c\oplus u=(c_1,\cdots,c_n,u)\in F_{q^2}^{n+1}。$$

当 $q=2^m$ 的时候，$t_0=0$，$q^2-1=p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s}$，对于 $i=1,2,\cdots,s$ 令

$$a_i=(\Gamma_i)\otimes\left(\alpha_i^0,\alpha_i^1,\cdots,\alpha_i^{r_i}\right)$$

$$a=a_1\otimes a_2\otimes\cdots\otimes a_s\oplus 0.$$

引理 3.1.1. 假设 $r_1=\max\{r_1,\cdots,r_w\}$。则存在 $v\in\left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$ 对所有 $0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。

证明：我们分两步来证明这个引理。

第一步：我们先证明 $\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E$ 对所有 $0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。

对于 $i=1,2,\cdots,s$，通过对 α_i 和 γ_i 的选择，向量 a 里面的元素各不相同，同时令

$$v_i=\mathbf{1}_{p_i^{t_i-k_i}}\otimes\left(v_{i0},v_{i1},\cdots,v_{ir_i}\right)\in\left(F_{q^2}^*\right)^{(r_i+1)p_i^{t_i-k_i}},$$

以及

$$v^*=v_1\otimes v_2\otimes\cdots\otimes v_s\in\left(F_{q^2}^*\right)^n,$$

这里 $\mathbf{1}_{p_i^{t_i-k_i}}=(1,1,\cdots,1)\in\left(F_{q^2}^*\right)^{p_i^{t_i-k_i}}$。

由于 $0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$，我们有

$$\begin{aligned}\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E&=\left\langle a_1^{qj+l},v_1^{q+1}\right\rangle_E\left\langle a_2^{qj+l},v_2^{q+1}\right\rangle_E\cdots\left\langle a_s^{qj+l},v_s^{q+1}\right\rangle_E\\&=\prod_{i=1}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\\&=\prod_{i=1}^{w}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\prod_{i=w+1}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\end{aligned}$$

我们考虑一下两种情况：

(1) 存在 $x:1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid qj+l$，或者存在 $x:1\le x\le w$ 使得 $p_x^{t_x-k_x}\nmid j+l$，或者存在 $x:w+1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid j-l$。我们有 $\left\langle a_x^{qj+l},v_x^{q+1}\right\rangle_E=0$。因此 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$。

(2) 当对于任意的 $x:1\le x\le s$，$p_x^{t_x-k_x}\mid qj+l$，对于任意的 $x:1\le x\le w$，$p_x^{t_x-k_x}\mid j+l$，对于任意的 $x:w+1\le x\le s$，$p_x^{t_x-k_x}\mid j-l$ 时，由于 $\gcd(p_i,p_j)=1$ 对于 $1\le i\ne j\le s$ 和 $ord(\alpha_i)=p_i^{t_i}$，我们可以得到 $M\mid qj+l$，$M_1\mid j+l$，$M_2\mid j-l$。考虑 $i=1$ 时的情况，有

$$\alpha_1^{qj+l}=\alpha_1^{(q-1)j+j+l}=\alpha_1^{j+l}$$

所以存在整数 c_1 和 c_2 使得 $j+l=c_1M+c_2p_1^{r_1}$。考虑一下两种情况。

(2.1) r_1 为奇数时。

由于 r_1 为奇数，故 $0\le j+l\le(r_1-1)M_1$，则存在 $l_1\in\mathbb{Z}^*$ 使得 $j+l=l_1M_1$，故有

$$\alpha_1^{j+l}=\left(\alpha_1^{M_1}\right)^{l_1}\text{ 和 }\sum_{y_1=0}^{\eta_1}\alpha_1^{y_1(qj+l)}v_{1y_1}^{q+1}=\sum_{y_1=0}^{\eta_1}\left(\alpha_1^{M_1}\right)^{y_1l_1}v_{1y_1}^{q+1}\text{。}$$

同时，我们可以得到 $l_1\in\{0,1,2,\cdots,r_1-1\}$。即要去找出 $\left(z_0,z_1,\cdots,z_{\eta_1}\right)\in\left(F_q^*\right)^{\eta_1+1}$ 使得

$$\sum_{i=0}^{\eta_1}\alpha_1^{i(j+l)}z_i=0$$

记 $\Delta_1=\alpha_1^{M_1}$，则 $ord\left(\Delta_1\right)=p_1^{k_1}$，由于 $q\equiv1\bmod\left(p_1\right)$，我们有 $\Delta_1^q=\Delta_1$。

令

$$A=\begin{pmatrix}1&1&1&\cdots&1\\1&\Delta_1&\Delta_1^2&\cdots&\Delta_1^{\eta_1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&\Delta_1^{\eta_1-2}&\Delta_1^{2(\eta_1-2)}&\cdots&\Delta_1^{\eta_1(\eta_1-2)}\\1&\Delta_1^{\eta_1-1}&\Delta_1^{2(\eta_1-1)}&\cdots&\Delta_1^{\eta_1(\eta_1-1)}\end{pmatrix},\quad z=\begin{pmatrix}z_0\\z_1\\\vdots\\z_{\eta_1}\end{pmatrix}.$$

考虑 r_1+1 次线性方程组

$$AZ=\mathbf{0}^{\mathrm{T}}\tag{1}$$

由于 $\Delta_1^{ijq}=\Delta_1^{ij}$，则意味着 $A^q=A$。由引理 2.2 知，方程组 $AZ=\mathbf{0}^{\mathrm{T}}$ 存在一个解 u^{T} 和 $u=\left(u_0,u_1,\cdots,u_{\eta_1}\right)\in\left(F_q^*\right)^{\eta_1+1}$，取 v_{1i} 使得 $v_{1i}^{q+1}=u_i$ 对于 $i=0,1,\cdots,r_1$，令

$$v_1=1_{p_1^{\eta_1-k_1}}\otimes\left(v_{10},v_{11},\cdots,v_{1\eta_1}\right)\in\left(F_{q^2}^*\right)^{(\eta_1+1)p_1^{\eta_1-k_1}},$$

则有 $\left\langle a_1^{qj+l},v_1^{q+1}\right\rangle_E=0$，即 $\left\langle a^{qj+l},(v^*)^{q+1}\right\rangle_E$。

(2.1) r_1 为偶数时。

由于 r_1 为偶数，故 $0\le j+l\le(r_1-2)M_1$，我们可以得到 $l_1\in\{0,1,2,\cdots,r_1-2\}$。记 $\Delta_1=\alpha_1^{M_1}$，则 $ord\left(\Delta_1\right)=p_1^{k_1}$，由于 $q\equiv1\bmod\left(p_1\right)$，我们有 $\Delta_1^q=\Delta_1$。

令

$$A_1=\begin{pmatrix}1&1&1&\cdots&1\\1&\Delta_1&\Delta_1^2&\cdots&\Delta_1^{\eta_1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&\Delta_1^{\eta_1-3}&\Delta_1^{2(\eta_1-3)}&\cdots&\Delta_1^{\eta_1(\eta_1-3)}\\1&\Delta_1^{\eta_1-2}&\Delta_1^{2(\eta_1-2)}&\cdots&\Delta_1^{\eta_1(\eta_1-2)}\end{pmatrix}\text{。}$$

由推论 2.3，我们同样可以得出方程组

$$A_1Z=\mathbf{0}^{\mathrm{T}}\tag{2}$$

存在一个解 u^{T} 和 $u=\left(u_0,u_1,\cdots,u_{\eta_1}\right)\in\left(F_q^*\right)^{\eta_1+1}$，与(2.1)类似，我们也可以得到向量 v_1 使得 $\left\langle a_1^{qj+l},v_1^{q+1}\right\rangle_E=0$，即 $\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E$。

故由上述讨论可得$\left\langle a^{qj+l},\left(v^{*}\right)^{q+1}\right\rangle_{E}$对所有$0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。

第二步：令$v=v^{*}\oplus 0$。

对所有$0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$，当$j+l=0$时，有

$$\left\langle a^{0},v^{q+1}\right\rangle=v_0^{q+1}+p_1^{t_1-k_1}\sum_{i=1}^{r_1}v_{1i}^{q+1}+\cdots+p_s^{t_s-k_s}\sum_{i=1}^{r_s}v_{si}^{q+1}\in F_q。$$

当$j+l>0$时，有

$$\left\langle a^{qj+l},v^{q+1}\right\rangle_{E}=\prod_{i=1}^{s}\left(p_i^{t_i-k_i}\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)。$$

对于$j+l>0$的情况，由第一步知，存在

$$v_1=1_{p_1^{t_1-k_1}}\otimes\left(v_{10},v_{11},\cdots,v_{1r_1}\right)\in\left(F_{q^2}^{*}\right)^{(r_1+1)p_1^{t_1-k_1}}，$$

使得$\left\langle a_1^{qj+l},v_1^{q+1}\right\rangle_{E}=0$，则有$\left\langle a^{qj+l},v^{q+1}\right\rangle_{E}=0$。

由推论 3.2，存在

$\delta_0,\delta_{ci}\in F_q^{*}$

使得

$$\delta_0+\sum_{c\ne 1}\left(p_c^{t_c-k_c}\sum_{i=0}^{r_i}\delta_{ci}\right)=-p_1^{t_1-k_1}\left(v_{11}^{q+1}+\cdots+v_{1r_1}^{q+1}\right)\in F_q^{*}。$$

则存在e_0，$e_{ci}\in F_{q^2}^{*}$使得$e_0^{q+1}=\delta_0$，$e_{ci}^{q+1}=\delta_{ci}$。令$v_0=e_0$，对于$i=2,\cdots,s$，取

$$v_i=\mathbf{1}_{p_i^{t_i-k_i}}\otimes\left(e_{i0},e_{i1},\cdots,e_{ir_i}\right)$$

则有$\left\langle a^{0},v^{q+1}\right\rangle=0$。最后，令

$$v=v_1\otimes v_2\otimes\cdots\otimes v_s\oplus e_0\in\left(F_{q^2}^{*}\right)^{n+1}。$$

有$\left\langle a^{qj+l},v^{q+1}\right\rangle_{E}=0$对所有$0\le j,l\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。

基于引理 2.4，我们可以得出如下定理。

定理 3.1.2.设$q=2^m$，则存在参数为

$$\left[\left[1+\frac{(r_1+1)\cdots(r_s+1)\left(q^2-1\right)}{p_1^{k_1}\cdots p_s^{k_s}},\frac{(r_1+1)\cdots(r_s+1)\left(q^2-1\right)}{p_1^{k_1}\cdots p_s^{k_s}}-2k+1,k+1\right]\right]$$

的量子 MDS 码，其中$r_1=\max\left\{r_1,\cdots,r_w\right\}$，$M_1=\frac{q-1}{p_1^{k_1}\cdots p_w^{k_w}}$，$0\le k\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。

由于$\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1<\frac{q}{2}+1$，但通过下列例子可以得出极小可以再次扩大，以至于大于$\frac{q}{2}+1$。

例 3.1.3.当$q=2^5$时，$q^2-1=31\times 3\times 11$，令$p_1=31,p_2=3,p_3=11$，则

$$n=\frac{(r_1+1)(r_2+1)(r_3+1)(q^2-1)}{31^{k_1}3^{k_2}11^{k_3}}$$

其中 $0\le r_1\le 31^{k_1}-1, 0\le r_2\le 3^{k_2}-1, 0\le r_3\le 11^{k_3}-1$， $0\le k_1,k_2,k_3\le 1$ 和 $0\le k\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。取 $M_1=1,r_1=30,M_2=11$，则 $\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1=14<\frac{q}{2}=16$。考虑方程 $\sum_{i=0}^{31}\alpha_1^{i(j+l)}z_i=0$，注意到此时 $l_1\in\{0,1,2,\cdots,28\}$，而当 $l_1>30$ 时，由于， $ord(\alpha_1)=31$，方程与 l_1-31 时同解，然而只有当 $j+l=l_1$ 且 $11\mid j-l$ 时， l_1 才会出现在方程中，通过计算，方程中 l_1 第一次出现数依次为：0，32，2，34，4，36，6，38，8，40，10，42，12，13，…，29，30。这里面最大为 42，故当 $j,l\le 20$ 时， $j+l<42$。因此极小距离 d 可以达到 42，大于 17。

通过上述例子，我们可以找出有定理 3.1.2 给出的量子 MDS 码使其极小距离 $d>\frac{q}{2}+1$。由于 $\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1<\frac{q}{2}$， 当 $r_1=p_1^{k_1}-1$ 及 $M_1=\frac{q-1}{p_1^{k_1}}$ 时， $\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1=\frac{q-1-3M_1}{2}$。所以只需要去检查方程 $\sum_{i=0}^{\eta}\alpha_1^{i(j+l)}z_i=0$ 对于 $j>\frac{q-1-3M_1}{2}$ 或者 $l>\frac{q-1-3M_1}{2}$， $l_1'\equiv l_1 \bmod(r_1)$， $j+l\equiv 0(\bmod M_1)$， $l-j\equiv 0\bmod(M_2)$，然后利用中国剩余定理去计算 l_1' 第一次出现在方程中的数。我们称数 l_1' 为 L_1-forms。

引理 3.1.4. 假设 $1+r_s=\max\left\{p_{w+1}^{k_{w+1}},\cdots,p_s^{k_s}\right\}$。则存在 $v\in\left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$ 对所有

$$0\le j,l\le\frac{r_s-2}{2}M_2。$$

证明：我们仍然分两步来证明这个引理。

第一步：我们先证明 $\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E$ 对所有 $0\le j,l\le\frac{r_s-2}{2}M_2$。

对于 $i=1,2,\cdots,s$，通过对 α_i 和 γ_i 的选择，向量 a 里面的元素各不相同，同时令

$$v_i=\mathbf{1}_{p_i^{t_i-k_i}}\otimes\left(v_{i0},v_{i1},\cdots,v_{ir_i}\right)\in\left(F_{q^2}^*\right)^{(r_i+1)p_i^{t_i-k_i}},$$

以及

$$v^*=v_1\otimes v_2\otimes\cdots\otimes v_s\in\left(F_{q^2}^*\right)^n,$$

这里 $\mathbf{1}_{p_i^{t_i-k_i}}=(1,1,\cdots,1)\in\left(F_{q^2}^*\right)^{p_i^{t_i-k_i}}$。

由于 $0\le j,l\le\frac{r_s-2}{2}M_2$，我们有

$$\begin{aligned}\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E&=\left\langle a_1^{qj+l},v_1^{q+1}\right\rangle_E\left\langle a_2^{qj+l},v_2^{q+1}\right\rangle_E\cdots\left\langle a_s^{qj+l},v_s^{q+1}\right\rangle_E\\&=\prod_{i=1}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\\&=\prod_{i=1}^{w}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\prod_{i=w+1}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\end{aligned}$$

我们考虑一下两种情况：

(1) 存在 $x:1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid qj+l$，或者存在 $x:1\le x\le w$ 使得 $p_x^{t_x-k_x}\nmid j+l$，或者存在 $x:w+1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid j-l$。我们有 $\left\langle a_x^{qj+l},v_x^{q+1}\right\rangle_E=0$。因此 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$。

(2) 当对于任意的 $x:1\le x\le s$，$p_x^{t_x-k_x}\mid qj+l$，对于任意的 $x:1\le x\le w$，$p_x^{t_x-k_x}\mid j+l$，对于任意的 $x:w+1\le x\le s$，$p_x^{t_x-k_x}\mid j-l$ 时，由于 $\gcd\left(p_i,p_j\right)=1$ 对于 $1\le i\ne j\le s$ 和 $ord\left(\alpha_i\right)=p_i^{t_i}$，我们可以得到 $M\mid qj+l$，$M_1\mid j+l$，$M_2\mid j-l$。考虑 $i=s$ 时的情况，有

$$\alpha_s^{qj+l}=\alpha_s^{(q+1)j-j+l}=\alpha_s^{l-j}$$

所以存在整数 c_1 和 c_2' 使得 $l-j=c_1M+c_2'p_s^{t_s}=l_2M_2$。

由于 r_1 为偶数，故 $-\frac{r_s-2}{2}M_2\le l-j\le\frac{r_s-2}{2}M_2$，我们可以得到

$l_1\in\left\{-\frac{r_s-2}{2},1-\frac{r_s-2}{2},\cdots,\frac{r_s-2}{2}-1,\frac{r_s-2}{2}\right\}$。故

$$\sum_{y_s=0}^{r_s}\alpha_s^{y_s(qj+l)}v_{sy_s}^{q+1}=\sum_{y_s=0}^{r_s}\left(\alpha_s^{M_s}\right)^{y_sl_2}v_{sy_s}^{q+1}。$$

记 $\Delta_s=\alpha_s^{M_2}$，则 $ord\left(\Delta_s\right)=p_s^{k_s}$，由于 $q\equiv-1\bmod\left(p_s\right)$，我们有 $\Delta_s^q=\Delta_s^{-1}$。令 $R=\frac{r_s-2}{2}$，故 $p_s^{k_s}=2R+3$。即要去找出 $\left(z_0,z_1,\cdots,z_{r_s}\right)\in\left(F_q^*\right)^{r_s+1}$ 使得 $\sum_{i=0}^{r_s}\alpha_s^{i(j+l)}z_i=0$ 对每个 $-R\le l_2\le R$。令

$$B=\begin{pmatrix}1&\Delta_s^{-R}&\cdots&\Delta_s^{-R(2R+2)}\\1&\Delta_s^{1-R}&\cdots&\Delta_s^{(1-R)(2R+2)}\\\vdots&\vdots&\ddots&\vdots\\1&\Delta_s^{2R}&\cdots&\Delta_s^{R(2R+2)}\end{pmatrix},\quad z^{(1)}=\begin{pmatrix}z_0\\z_1\\\vdots\\z_{2R+2}\end{pmatrix}$$

考虑方程组

$$Bz^{(1)}=\mathbf{0}^{\mathrm{T}}\tag{3}$$

对矩阵 B 中的任意一个元素 $\Delta_s^{(i-R)l_2}$，对于 $0\le i\le 2R$，我们有

$$\Delta_s^{(i-R)l_2q}=\Delta_s^{-(i-R)l_2}=\Delta_s^{(2R-i-R)l_2}$$

已知 $\Delta_s^{(2R-i-R)l_2}$ 也是矩阵 B 中的一个元素，故 $B^{(q)}$ 与 B 行等价。由推论 2.3，方程组(3)存在一个解 u^{T} 和 $u=\left(u_0,u_1,\cdots,u_{r_s}\right)\in\left(F_q^*\right)^{r_s+1}$，与引理 3.1.1 中的(2.1)类似，我们也可以得到向量 v_s 使得 $\left\langle a_s^{qj+l},v_s^{q+1}\right\rangle_E=0$，即

$$\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E=0。$$

故由上述讨论可得 $\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E$ 对所有 $0\le j,l\le\frac{r_s-2}{2}M_2$。

第二步：与引理 3.1.1 中第二步类似，令 $v=v^*\oplus 0$，我们可以找到 $v_1,v_2,\cdots,v_{s-1}$，e_0 和

$$v=v_1\otimes v_2\otimes\cdots\otimes v_s\oplus e_0\in\left(F_{q^2}^*\right)^{n+1}。$$

使得 $\left\langle a^{qj+l}, v^{q+1}\right\rangle_E = 0$ 对所有 $0 \le j,l \le \dfrac{r_s-2}{2}M_2$。

定理 3.1.5. 设 $q = 2^m$，则存在参数为

$$\left[\left[1+\frac{(r_1+1)\cdots(r_{s-1}+1)(q^2-1)}{p_1^{k_1}\cdots p_{s-1}^{k_{s-1}}}, \frac{(r_1+1)\cdots(r_{s-1}+1)(q^2-1)}{p_1^{k_1}\cdots p_{s-1}^{k_{s-1}}} - 2k+1, k+1\right]\right]$$

的量子 MDS 码，其中 $1+r_s = \max\left\{p_{w+1}^{k_{w+1}}, \cdots, p_s^{k_s}\right\}$，$M_2 = \dfrac{q+1}{p_{w+1}^{k_{w+1}}\cdots p_s^{k_s}}$，$0 \le k \le \dfrac{r_s-2}{2}M_2$。

同样的，我们可以找出有定理 3.1.5 给出的量子 MDS 码使其极小距离 $d > \dfrac{q}{2}+1$。由于 $\dfrac{r_s-2}{2}M_2 < \dfrac{q}{2}$，$r_s = p_s^{k_s}-1$，当 $M_2 = \dfrac{q+1}{p_s^{k_s}}$ 时，$\dfrac{r_s-2}{2}M_2 = \dfrac{q+1-2M_2}{2}$。所以只需要去检查方程 $\sum_{i=0}^{n_1}\alpha_1^{i(j+l)}z_i = 0$ 对于 $j > \dfrac{q+1-2M_2}{2}$ 或者 $l > \dfrac{q+1-2M_2}{2}$，$l_2' \equiv l_2 \bmod (r_s)$，$l+j \equiv 0 (\bmod M_1)$，$l-j \equiv 0 \bmod (M_2)$，然后利用中国剩余定理去计算 l_2' 第一次出现在方程中的数。我们称数 l_2' 为 L_2-forms。

例 3.1.6. 当 $q = 2^4$ 时，$q^2-1 = 3\times 5\times 17$，令 $p_1 = 3, p_2 = 5, p_3 = 17$，则 $n = \dfrac{(r_1+1)(r_2+1)(q^2-1)}{3^{k_1}5^{k_2}}$ 其中 $0 \le r_1 \le 3^{k_1}-1, 0 \le r_2 \le 5^{k_2}-1$，$0 \le k_1, k_2 \le 1$ 和 $0 \le k \le 7M_2$。取 $M_1 = 5, M_2 = 1$，则 $7M_2 = 7 < \dfrac{q}{2} = 8$。注意到此时的 L_2-forms 为 $l_2 \in \{9,10,\cdots,16,0,1,2,\cdots,8\}$，当 $|l_2| = 7$ 时，$j = 11$ 或者 $l = 11$，则 d 可以达到 11，大于 8。

3.2. $q = p^m$ 为一个奇数时

引理 3.2.1. 设 $q = p^m$ 为一个奇数，我们有

(1) 若 $r_1 = \max\{r_1, \cdots, r_w\}$。则存在 $v \in \left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l}, v^{q+1}\right\rangle_E = 0$ 对任意的

$$0 \le j,l \le \left\lfloor \frac{r_1-1}{2} \right\rfloor M_1。$$

(2) 若 $t_0'' = 1$，$r_0 > \max\{r_1, \cdots, r_w\}$，则存在 $v \in \left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l}, v^{q+1}\right\rangle_E = 0$ 对任意的

$$0 \le j,l \le \left\lfloor \frac{r_0-1}{4} \right\rfloor M_1。$$

证明：(1)第一种情况的证明与引理 3.1.1 的证明类似。

(3) 对于 $0 \le j,l \le \left\lfloor \dfrac{r_0-1}{4} \right\rfloor M_1$，我们有

$$\begin{aligned}\left\langle a^{qj+l}, \left(v^*\right)^{q+1}\right\rangle_E &= \left\langle a_0^{qj+l}, v_0^{q+1}\right\rangle_E \left\langle a_1^{qj+l}, v_1^{q+1}\right\rangle_E \cdots \left\langle a_s^{qj+l}, v_s^{q+1}\right\rangle_E \\ &= \prod_{i=0}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right) \\ &= \prod_{i=0}^{w}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\prod_{i=w+1}^{s}\left(\sum_{m_i=0}^{p_i^{t_i-k_i}-1}\gamma_i^{m_i(qj+l)}\sum_{y_i=0}^{r_i}\alpha_i^{y_i(qj+l)}v_{iy_i}^{q+1}\right)\end{aligned}$$

同样的，我们考虑如下两种情况。

(2.1)存在 $x:1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid qj+l$，或者存在 $x:1\le x\le w$ 使得 $p_x^{t_x-k_x}\nmid j+l$，或者存在 $x:w+1\le x\le s$ 使得 $p_x^{t_x-k_x}\nmid j-l$。我们有 $\left\langle a_x^{qj+l},v_x^{q+1}\right\rangle_E=0$。因此 $\left\langle a^{qj+l},\left(v^*\right)^{q+1}\right\rangle_E=0$。

(2.2)当对于任意的 $x:0\le x\le s$， $p_x^{t_x-k_x}\mid qj+l$，对于任意的 $x:1\le x\le w$， $p_x^{t_x-k_x}\mid j+l$，对于任意的 $x:w+1\le x\le s$， $p_x^{t_x-k_x}\mid j-l$ 时，由于 $2^{t_0-k_0}\mid qj+l$，则 $2^{t_0'-k_0'}\mid qj+l$，$2^{t_0''-k_0''}\mid qj+l$，我们可以得到 $M\mid qj+l$，$M_1\mid j+l$，$M_2\mid j-l$。由于 $t_0''=1$，$t_0=1+t_0'$，假设 $j+l=l_1M_1, l-j=l_2M_2$，则 $0\le l_1\le 2\left\lfloor\frac{r_0-1}{4}\right\rfloor$，由于 $\alpha_0^{2^{t_0'}}=1$，则 $\alpha_0^{2^{t_0'}}=-1$， $\alpha_0^{q-1}=-1$，有

$$\sum_{y_0=0}^{r_0}\alpha_0^{y_0(qj+l)}v_{0y_0}^{q+1}=\sum_{y_0=0}^{r_0}\alpha_0^{y_0((q-1)j+j+l)}v_{0y_0}^{q+1}=\sum_{y_0=0}^{r_0}(-1)^{jy_0}\alpha_0^{y_0(j+l)}v_{0y_0}^{q+1}=\sum_{y_0=0}^{r_0}(-1)^{jy_0}\left(\alpha_0^{M_1}\right)^{y_0l_1}v_{0y_0}^{q+1}。$$

即要去找出 $\left(z_0,z_1,\cdots,z_{r_0}\right)\in\left(F_q^*\right)^{r_0+1}$ 使得 $\sum_{i=0}^{r_0}(-1)^{ji}\left(\alpha_0^{M_1}\right)^{il_1}z_i=0$ 对每个 $0\le l_1\le 2\left\lfloor\frac{r_0-1}{4}\right\rfloor$，这个方程组共包含 $2\left(2\left\lfloor\frac{r_0-1}{4}\right\rfloor\right)+1$ 个等式。余下的证明跟引理 3.1.1 类似。

定理 3.2.2. 设 $q=p^m$ 为一个奇数，若有

(1) 若 $r_1=\max\{r_1,\cdots,r_w\}$， $0\le k\le\left\lfloor\frac{r_1-1}{2}\right\rfloor M_1$。或者

(2) 若 $t_0''=1$， $r_0>\max\{r_1,\cdots,r_w\}$， $0\le k\le\left\lfloor\frac{r_0-1}{4}\right\rfloor M_1$。

则存在参数为

$$\left[\left[1+\frac{(r_0+1)(r_1+1)\cdots(r_s+1)\left(q^2-1\right)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}},\frac{(r_0+1)(r_1+1)\cdots(r_s+1)\left(q^2-1\right)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}}-2k+1,k\right]\right]_q$$

的量子 MDS 码。

由例子 3.1.3 下面的讨论，我们同样可以根据 l_1-forms 去找出那些极小距离大于 $\frac{q}{2}+1$ 的量子 MDS 码。

与引理 3.2.1 类似，我们可以得到如下引理。

引理 3.2.3. 设 $q=p^m$ 为一个奇数，我们有

(1) 若 $1+r_s=\max\left\{p_0^{k_0''},p_{w+1}^{k_{w+1}},\cdots,p_s^{k_s}\right\}$。则存在 $v\in\left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$ 对任意的

$$0\le j,l\le\frac{r_s-2}{2}M_2。$$

(2) 若 $t_0'=1$， $r_0>\max\left\{p_{w+1}^{k_{w+1}},\cdots,p_s^{k_s}\right\}$，则存在 $v\in\left(F_{q^2}^*\right)^{n+1}$ 使得 $\left\langle a^{qj+l},v^{q+1}\right\rangle_E=0$ 对任意的

$$0\le j,l\le\frac{p_0^{k_0''}-2}{2}M_2$$

定理 3.2.4.设 $q=p^m$ 为一个奇数，若有

(1) 若 $r_1=\max\{r_1,\cdots,r_w\}$， $0\le k\le\frac{r_s-2}{2}M_2$。或者

(2) 若 $t_0''=1$， $r_0>\max\{r_1,\cdots,r_w\}$， $0\le k\le \dfrac{p_0^{k_0''}-2}{2}M_2$。

则存在参数为

$$\left[\left[1+\frac{(r_0+1)(r_1+1)\cdots(r_s+1)(q^2-1)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}},\frac{(r_0+1)(r_1+1)\cdots(r_s+1)(q^2-1)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}}-2k+1,k\right]\right]_q$$

的量子 MDS 码。

同样的，我们可以根据 l_2-forms 去找出那些极小距离大于 $\dfrac{q}{2}+1$ 的量子 MDS 码。

Table 1. New quantum MDS codes
表 1. 新的量子 MDS 码

类别	q	$q \bmod (p_i)$	长度	码距
1	2^m	1	$1+n_1$	$[1,d_1]$
2	2^m	-1	$1+n_2$	$[1,d_2]$
3	p^m	1	$1+n_1$	$[1,d_3]$ 或者 $[1,d_3']$
4	p^m	-1	$1+n_1$	$[1,d_4]$ 或者 $[1,d_4']$

4. 总结

在文章中，我们利用厄米特自正交的 GRS 码，并通过有限域等工具构造了四类新的量子 MDS 码，它们的码长都可以表示为 $1+n$ 的形式，在表 1 中，我们对第三部分构造的量子码作了一个总结。表中 $n_1=\dfrac{(r_0+1)(r_1+1)\cdots(r_s+1)(q^2-1)}{2^{k_0}p_1^{k_1}\cdots p_s^{k_s}}$， $n_2=\dfrac{(r_1+1)\cdots(r_{s-1}+1)(q^2-1)}{p_1^{k_1}\cdots p_{s-1}^{k_{s-1}}}$， $d_1=\dfrac{r_1-1}{2}M_1$， $d_2=\dfrac{r_s-2}{2}M_2$，

$d_3=\dfrac{r_1-1}{2}M_1$， $d_3'=\dfrac{r_0-1}{4}M_1$， $d_4=\dfrac{r_s-2}{2}M_2$， $d_4'=\dfrac{2^{k_0''}-2}{2}M_2$。

参考文献

[1] Ashikhmin, A. and Knill, E. (2001) Nonbinary Quantum Stabilizer Codes. *IEEE Transactions on Information Theory*, **47**, 3065-3072. https://doi.org/10.1109/18.959288

[2] Fang, W. and Fu, F. (2019) New Constructions of MDS Euclidean Self-Dual Codes from GRS Codes and Extended GRS Codes. *IEEE Transactions on Information Theory*, **65**, 5574-5579. https://doi.org/10.1109/TIT.2019.2916367

[3] Fang, W. and Fu, F. (2019) Some New Constructions of Quantum MDS Codes. *IEEE Transactions on Information Theory*, **65**, 7840-7847. https://doi.org/10.1109/TIT.2019.2939114

[4] Fang, W. and Fu, F. (2018) Two New Classes of Quantum MDS Codes. *Finite Fields and Their Applications*, **53**, 85-98. https://doi.org/10.1016/j.ffa.2018.06.003

[5] Harada, M. and Kharaghani, H. (2006) Orthogonal Designs and MDS Self-Dual Codes. *The Australasian Journal of Combinatorics*, **35**, 57-67.

[6] Niu, Y., Yue, Q., Wu, Y. and Hu, L. (2019) Hermitian Self-Dual, MDS, and Generalized Reed-Solomon Codes. *IEEE Communications Letters*, **23**, 781-784. https://doi.org/10.1109/LCOMM.2019.2908640

[7] Shi, X., Yue, Q. and Zhu, X.M. (2017) Construction of Some New Quantum MDS Codes. *Finite Fields and Applications*, **46**, 347-362. https://doi.org/10.1016/j.ffa.2017.04.002

[8] Shi, X., Yue, Q. and Wu, Y. (2019) New Quantum MDS Codes with Large Minimum Distance and Short Length from Generalized Reed-Solomon Codes. *Discrete Mathematics*, **342**, 1989-2001. https://doi.org/10.1016/j.disc.2019.03.019

[9] Zhang, T. and Ge, G. (2016) Quantum MDS Codes with Large Minimun Distance. *Designs*, *Codes and Cryptography*, **83**, 503-517. https://doi.org/10.1007/s10623-016-0245-0

[10] Chen, B., Ling, S. and Zhang, G. (2015) Application of Constacyclic Codes to Quantum MDS Codes. *IEEE Transactions on Information Theory*, **61**, 1474-1484. https://doi.org/10.1109/TIT.2015.2388576