利用扭曲的Reed-Solomon码构造两类极大距离可分纠缠辅助量子纠错码

潘 鑫 高 健*

(山东理工大学数学与统计学院 淄博 255000)

摘 要：随着量子通信和量子计算技术的飞速发展，高效量子纠错编码技术已成为保障量子系统可靠性的核心需求。传统量子纠错码在参数灵活性和最小距离约束方面存在显著局限性，难以适应复杂量子通信场景中的动态需求。该文基于扭曲的Reed-Solomon(TGRS)码，根据码长中i的奇偶性的不同具体讨论矩阵$\boldsymbol{GG}^{\mathrm{H}}$的秩，进一步通过分析该矩阵的秩确定厄米特正交包的维数，从而得到两类极大距离可分纠缠辅助量子纠错码(MDS EAQECCs)。研究发现，通过特定的扭曲操作，所构造的两类MDS EAQECCs不仅能够灵活调整码长，还能显著提升最小距离，突破了传统理论界限。此外，该文利用扭曲操作将两类MDS EAQECCs提升为最大纠缠态极大距离可分纠缠辅助量子纠错码 (ME-MDS EAQECCs)。该文研究成果不仅为量子纠错码设计提供了更广泛的参数选择，还为动态量子通信场景中的高效纠错提供了理论支撑。

关键词：纠缠辅助量子码；扭曲的Reed-Solomon码；厄米特正交包

中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2025)10-3804-10

DOI: 10.11999/JEIT250258 **CSTR**: 32379.14.JEIT250258

1 引言

作为21世纪信息技术的革命性领域，量子通信利用量子密钥分发(Quantum Key Distribution, QKD)实现了理论上无条件安全的信息传输[1]。然而，量子系统的脆弱性导致其在环境噪声和退相干效应下极易产生信息误差，成为制约实用化的核心瓶颈。基于此，量子纠错码作为保护量子信息的关键技术[2,3]成为近年的研究焦点。

量子纠错码基于稳定子理论框架，通过构造具有特定代数结构的码空间实现错误检测与修正[4,5]。纠缠辅助量子纠错码(Entanglement-Assisted Quantum Error-Correcting Code, EAQECC)理论的发展是量子纠错领域的一项重大突破。Brun等人[6] 提出了一个通用的框架体系，即纠缠辅助稳定子体系。该体系表明，如果发送方和接收方之间存在共享纠缠，那么任意不满足对偶包含约束的经典线性纠错码都能转化为EAQECCs。近年来，利用不满足对偶包含条件的任意经典线性码来构造EAQECCs已成为一个重要的研究领域，越来越多的编码学者致力于构造具有优良参数的EAQECCs。极大距离可分纠缠辅助量子纠错码 (Maximum Distance Separable EAQECCs, MDS EAQECCs)因其在给定码长和维度下达到Singleton界的最优最小距离，展现出卓越的纠错能力[7–9]。Chen等人[10]基于循环码构造了多类MDS EAQECCs，其最小距离较此前已知的EAQECCs具有显著优势；Guenda等人[11]系统分析了MDS EAQECCs存在的条件，为参数优化提供了理论依据。Gao等人[12]基于有限非链环上的常循环码构造出新参数的MDS EAQECCs，推广和改进了前人的工作[13–16]。

文献[17]基于厄米特内积，通过Reed-Solomon (RS)码构造了EAQECCs。不过在厄米特内积下，该方法并未涵盖所有Reed-Solomon码。Galindo等人[18]基于Reed-Solomon码构造了厄米特自正交码，为设计纠缠辅助量子码奠定了理论基础。扭曲的广义Reed-Solomon(Twisted Generalized Reed-Solomon codes, TGRS)码作为Reed-Solomon码的重要扩展，通过引入扭曲操作突破了传统Reed-Solomon码的参数限制[19]。Huang等人[20]研究了TGRS码的代数构造，证明其可灵活调整码长与最小距离，并保持极大距离可分性。这一特性使其成为构造MDS EAQECCs的理想候选线性码类[21–26]。尽管现有研究取得显著进展，MDS EAQECCs的构造仍面临挑战：其一，很多MDS EAQECCs受限于固定码长，难以适应动态量子通信场景的需求；其二，多数MDS EAQECCs的最小距离受限于有限域大小(如$d \le q+1$)，限制了高噪声环境下的纠错能力。

本文基于TRS码，通过分析矩阵的秩确定了厄米特正交包的维数，从而得到两类MDS EAQECCs。

收稿日期：2025-04-11；改回日期：2025-07-27；网络出版：2025-08-06
*通信作者： 高健 dezhougaojian@163.com
基金项目：山东省自然科学基金(ZR2024YQ057, ZR2022MA024)，国家自然科学基金(12071264)

Foundation Items: The Natural Science Foundation of Shandong Province (ZR2024YQ057, ZR2022MA024), The National Natural Science Foundation of China (12071264)

此外，本文通过对MDS EAQECCs进行参数可调性的扭曲操作，得到了ME-MDS EAQECCs。本文构造的MDS EAQECCs在保持最小距离优势的同时，实现了码长的灵活可调，并且所构造的码的参数是新的，没有被之前的研究所覆盖。

2　预备知识

设$\mathbb{F}_{q^2}$是q^2-元有限域，对于任意正整数n，$\mathbb{F}_{q^2}^n$表示$\mathbb{F}_{q^2}$上的n维向量空间。$\mathbb{F}_{q^2}^n$的任意非空线性子空间C，称作q^2-元线性码，其中n是码长。C中的向量称为码字。码字$\boldsymbol{c}$的Hamming重量定义为向量$\boldsymbol{c}$中非零分量的个数，码字$\boldsymbol{\mu}$和$\boldsymbol{\nu}$的Hamming距离定义为二者相异位的数量，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线性码中非零码字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C记为$[n,k,d]_{q^2}$，C的生成矩阵为秩为k的$k\times n$矩阵

$$\boldsymbol{G}=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

定义$\boldsymbol{G}^{\mathrm{H}}$是$\boldsymbol{G}$的共轭转置，即

$$\boldsymbol{G}^{\mathrm{H}}=\begin{pmatrix} g_{11}^q & g_{21}^q & \cdots & g_{k1}^q \\ g_{12}^q & g_{22}^q & \cdots & g_{k2}^q \\ \vdots & \vdots & \ddots & \vdots \\ g_{1n}^q & g_{2n}^q & \cdots & g_{kn}^q \end{pmatrix}$$

对于$[n,k,d]_{q^2}$线性码C而言，若$d=n-k+1$，则称C为极大距离可分(MDS)线性码。给定两个向量$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$，$\boldsymbol{b}=(b_1,b_2,\cdots,b_n)\in\mathbb{F}_{q^2}^n$，向量$\boldsymbol{a}$和$\boldsymbol{b}$的厄米特内积为$\langle\boldsymbol{a},\boldsymbol{b}\rangle=\sum_{i=1}^{n}a_ib_i^q$。线性码$C$的厄米特对偶码定义为$C^{\perp_{\mathrm{H}}}=\{\boldsymbol{a}\in\mathbb{F}_{q^2}^n\mid\langle\boldsymbol{a},\boldsymbol{b}\rangle=0,\forall\boldsymbol{b}\in C\}$。令$\mathrm{Hull}_{\mathrm{H}}(C)=C\cap C^{\perp_{\mathrm{H}}}$，$\mathrm{Hull}_{\mathrm{H}}(C)$称为$C$的厄米特正交包。若$C=\mathrm{Hull}_{\mathrm{H}}(C)$，则称码$C$是厄米特自对偶的。

Brun等人[6]引入EAQECCs的定义和纠错机制。在复向量空间$(\mathbb{C}^q)^{\otimes n}$中，EAQECCs利用发送方和接收方预先共享的$c$对最大纠缠态，将$\kappa$维信息编码到$n$个信道量子位中，形成一个特定的子空间。这个子空间能够在受到一定错误影响时，通过特定的纠错操作(复向量空间上的线性变换)恢复出原始的信息量子态。通过这种方式，EAQECC在复向量空间的框架下实现了对量子信息的有效保护和处理。EAQECC的参数表示为$[[n,\kappa,\delta;c]]_q$，其中n是编码后的量子比特数，κ是信息量子比特数，δ是码的最小距离，c是共享纠缠对数。该码能纠正多达$\lfloor(\delta-1)/2\rfloor$个量子错误。当$c=0$时，EAQECC退化为量子稳定子码 (QECC)。

定理1 [27](Singleton界)设C是一个$[[n,k,d;c]]_q$ EAQECC，其中$d\le\dfrac{(n+2)}{2}$。

(1) 若$2(d-1)=n-k+c$，则C称为MDS EAQECC；

(2) 若$c=n-k$，则C称为ME EAQECC。

若$[[n,k,d;c]]_q$同时满足条件(1)和(2)，即$c=d-1$，则C称为ME-MDS EAQECC。

引理1 [28] 设C为$[n,k,d]_{q^2}$线性码，δ为$C^{\perp_{\mathrm{H}}}$的最小距离。则存在参数为$[[n,n-2k+c,\delta;c]]_q$的EAQECC，其中$c=k-\dim(\mathrm{Hull}(C))$。

文献[28]针对参数为$[[n,\kappa,\delta;c]]_q$的EAQECCs给出了Singleton界的以下几种变形形式

$$\kappa\le c+\max\{0,n-2\delta+2\} \tag{1}$$

$$\kappa\le n-\delta+1 \tag{2}$$

$$\kappa\le\frac{(n-\delta+1)(c+2\delta-2-n)}{3\delta-3-n},\ \delta-1\ge n/2 \tag{3}$$

若EAQECCs在$\delta\le n/2$时满足式(1)，且在$\delta>n/2$时满足式(3)，则称该EAQECCs为MDS的。当$k\le\lfloor n/2\rfloor$时，基于具有ℓ维厄米特正交包的$[n,k,n-k+1]_{q^2}$ MDS线性码，引理1可产生参数为$[[n,n-k-\ell,k+1;k-\ell]]_q$的MDS EAQECCs。

下面回顾TRS码的定义及相关性质。

定义2 [29] 设n,k,l是正整数且满足$k<n$。通常，l称为扭曲次数。定义扭曲向量$\boldsymbol{t}=(t_1,t_2,\cdots,t_l)\in\{1,2,\cdots,n-k\}^l$，挂钩向量$\boldsymbol{h}=(h_1,h_2,\cdots,h_l)\in\{0,1,\cdots,k-1\}^l$，系数向量$\boldsymbol{\eta}=(\eta_1,\eta_2,\cdots,\eta_l)\in\mathbb{F}_{q^2}^l$，且要求向量组$\{\boldsymbol{h}_i,\boldsymbol{t}_i\}(i=1,2,\cdots,l)$各不相同。扭曲操作通过引入向量$\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}$，对多项式集合进行特定的变形得到扭曲多项式。定义$(k,\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$-扭曲多项式集合为$\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}=\{f(x)=\sum_{i=0}^{k-1}f_ix^i+\sum_{j=1}^{l}\eta_jf_{h_j}x^{k-1+t_j}:f_i\in\mathbb{F}_{q^2}\}$。显然，$\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}$是$\mathbb{F}_{q^2}$上的$k$维线性空间。

定义3 [29] 设$\alpha_1,\alpha_2,\cdots,\alpha_n$为$\mathbb{F}_{q^2}$中的互异元素，记$\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$。设非零元$v_1,v_2,\cdots,v_n\in\mathbb{F}_{q^2}$，记$\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$。取定义2中的$\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{h},\eta}$，则码长为$n$、维数为$k$的TRS码定义为$C_k(\boldsymbol{\alpha},1,\eta)=ev_{\boldsymbol{\alpha}}(\mathcal{V}_{k,1,k-1,\eta})\subseteq\mathbb{F}_{q^2}^n$；码长为$n$、维数为$k$的TGRS码定义为$C_k(\boldsymbol{\alpha},\boldsymbol{v},\eta)=ev_{\boldsymbol{\alpha},\boldsymbol{v}}(\mathcal{V}_{k,1,k-1,\eta})\subseteq\mathbb{F}_{q^2}^n$。

其中，$ev_{\alpha}(\cdot)$是从$\mathbb{F}_{q^2}$上多项式集合$\mathbb{F}_{q^2}[X]$到$\mathbb{F}_{q^2}^n$的映射

$$ev_\alpha(\cdot):\mathbb{F}_{q^2}[X]\to\mathbb{F}_{q^2}^n,\quad f\mapsto[f(\alpha_1),f(\alpha_2),\cdots,f(\alpha_n)]$$

设$\boldsymbol{G}_k$为$C_k(\boldsymbol{\alpha},\boldsymbol{v},\eta)$的生成矩阵，即

$$\boldsymbol{G}_k=\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\left(\alpha_1^{k-1}+\eta\alpha_1^k\right) & v_2\left(\alpha_2^{k-1}+\eta\alpha_2^k\right) & \cdots & v_n\left(\alpha_n^{k-1}+\eta\alpha_n^k\right) \end{pmatrix} \tag{4}$$

特别地，当$\boldsymbol{v}=(1,1,\cdots,1)=1$时，有$C_k(\boldsymbol{\alpha},\boldsymbol{v},\eta)=C_k(\boldsymbol{\alpha},1,\eta)$。本文主要讨论$\boldsymbol{v}=(1,1,\cdots,1)=1$的情形，此时生成矩阵(4)简化为

$$\boldsymbol{G}_k=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1}+\alpha_1^k & \alpha_2^{k-1}+\alpha_2^k & \cdots & \alpha_n^{k-1}+\alpha_n^k \end{pmatrix} \tag{5}$$

3 MDS EAQECCs的构造

本节将利用$\mathbb{F}_{q^2}$上的TRS码构造MDS EAQECCs，并通过特定的扭曲操作构造ME-MDS EAQECCs。与已知MDS EAQECCs相比，本文构造的码具有新的参数，并且在码长、极小距离以及最大纠缠态上有着更大的优势。

3.1 MDS EAQECCs的第1种构造

设γ是$\mathbb{F}_{q^2}$的一个本原元，$H=\langle\gamma^{q+1}\rangle$是$\mathbb{F}_{q^2}$的阶为$q-1$的乘法子群。令$H=\{a_1,a_2,\cdots,a_{q-1}\}$，其中$a_s=\gamma^{s(q+1)}$，$1\le s\le q-1$。设

$$\boldsymbol{a}=\left(a_1,a_2,\cdots,a_{q-1},a_1\gamma,a_2\gamma,\cdots,a_{q-1}\gamma,\cdots,a_1\gamma^{i-1},a_2\gamma^{i-1},\cdots,a_{q-1}\gamma^{i-1}\right) \tag{6}$$

其中，$2\le i\le q-1$，$\mathcal{RS}_{q+j}(\boldsymbol{a})$是一个长度为$i(q-1)$、维数为$q+j$的RS码。

下面的定理给出了$\mathcal{RS}_{q+j}(\boldsymbol{a})$的厄米特正交包的维数。

定理1 设$q=p^m$，其中p为奇素数，m为正整数。令C是由式(6)定义的$\mathcal{RS}_{q+j}(\boldsymbol{a})$，其中$j=\dfrac{q-3}{2}$，$t=\gcd(i,q+1)$，$v=\left\lfloor\dfrac{(1+j)t}{q+1}\right\rfloor$且$i$满足$i^2\equiv1(\bmod p)$或$i\equiv0(\bmod p)$。按照式(5)的扭曲操作对生成矩阵$\boldsymbol{G}$进行扭曲后，有

(1) 当i为奇数时，$\dim(\mathrm{Hull_H}(C))=j+(t-2v-2)$；

(2) 当i为偶数时，$\dim(\mathrm{Hull_H}(C))=j+(t-2v-3)$。

证明 设$\boldsymbol{A}_\beta$为$\mathbb{F}_{q^2}$上的$(q+j)\times(q-1)$矩阵，其中$\beta\in\left(\mathbb{F}_{q^2}\setminus\mathbb{F}_q\right)\cup\{1\}$，$\boldsymbol{A}_\beta$的具体形式为

$$\boldsymbol{A}_\beta=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1\beta & a_2\beta & \cdots & a_{q-1}\beta \\ \vdots & \vdots & \ddots & \vdots \\ (a_1\beta)^{q-2} & (a_2\beta)^{q-2} & \cdots & (a_{q-1}\beta)^{q-2} \\ \beta^{q-1} & \beta^{q-1} & \cdots & \beta^{q-1} \\ a_1\beta^q & a_2\beta^q & \cdots & a_{q-1}\beta^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^j\beta^{q+j-1}+a_1^{j+1}\beta^{q+j} & a_2^j\beta^{q+j-1}+a_2^{j+1}\beta^{q+j} & \cdots & a_{q-1}^j\beta^{q+j-1}+a_{q-1}^{j+1}\beta^{q+j} \end{pmatrix} \tag{7}$$

那么，C的生成矩阵为$\boldsymbol{G}=\left[\boldsymbol{A}_1:\boldsymbol{A}_\gamma:\cdots:\boldsymbol{A}_{\gamma^{i-1}}\right]$。因此，$\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}=[\boldsymbol{A}_1:\boldsymbol{A}_\gamma:\cdots:\boldsymbol{A}_{\gamma^{j-1}}]\begin{bmatrix}\boldsymbol{A}_1^{\mathrm{H}}\\ \boldsymbol{A}_\gamma^{\mathrm{H}}\\ \vdots\\ \boldsymbol{A}_{\gamma^{j-1}}^{\mathrm{H}}\end{bmatrix}=\boldsymbol{A}_1\boldsymbol{A}_1^{\mathrm{H}}+\boldsymbol{A}_\gamma\boldsymbol{A}_\gamma^{\mathrm{H}}+\cdots+\boldsymbol{A}_{\gamma^{j-1}}\boldsymbol{A}_{\gamma^{j-1}}^{\mathrm{H}}=\sum_{j=0}^{i-1}\boldsymbol{A}_{\gamma^j}\boldsymbol{A}_{\gamma^j}^{\mathrm{H}}$。设$0\le w\le i-1$，则

$$\boldsymbol{A}_{\gamma^w}\boldsymbol{A}_{\gamma^w}^{\mathrm{H}}=\begin{pmatrix} q-1 & 0 & \cdots & 0 & \cdots & \cdots & 0 & b_q & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & b_{q-1} & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & b_{q-j-1} & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & c_{j+1}\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & c_j\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & b_2 & \cdots & 0 & \cdots & \cdots & 0 & 0 & c_1 & \cdots & 0\\ b_1 & 0 & \cdots & 0 & \cdots & \cdots & 0 & q-1 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & d_1 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & d_{j+1} & d_j & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{8}$$

其中，$b_r=(q-1)\gamma^{wr(q-1)}\ (1\le r\le q)$，$c_o=(q-1)\gamma^{wo(q-1)}$，$d_o=(q-1)\gamma^{wo(1-q)}\ (1\le o\le j)$，$d_{j+1}=\sum_{m=1}^{q-1}\gamma^{mj-j+w-1+(m+w)j-w+1}\left(1+\gamma^{m(q+1)+w}\right)$，$c_{j+1}=\sum_{m=1}^{q-1}\gamma^{(q-1)jw}\left(1+\gamma^{m(q+1)+w}\right)^q$。由式(8)，可得

$$\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}=\begin{pmatrix} i(q-1) & 0 & \cdots & 0 & \cdots & \cdots & 0 & e_q & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & e_{q-1} & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & e_{q-j-1} & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & f_{j+1}\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & f_j\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & e_2 & \cdots & 0 & \cdots & \cdots & 0 & 0 & f_1 & \cdots & 0\\ e_1 & 0 & \cdots & 0 & \cdots & \cdots & 0 & i(q-1) & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 & \cdots & \cdots & g_1 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & g_{j+1} & g_j & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{9}$$

对于$1\le r\le q$，定义$e_r=(q-1)\sum_{u=0}^{i-1}\gamma^{ru(q-1)}$；对于$1\le z\le j$，定义$f_z=(q-1)\sum_{u=0}^{i-1}\gamma^{zu(q-1)}$与$g_z=(q-1)\sum_{u=0}^{i-1}\gamma^{zu(i-q)}$。此外，定义$f_{j+1}=\sum_{n=0}^{i-1}\sum_{m=1}^{q-1}\gamma^{(q-1)jn}\left(1+\gamma^{m(q+1)+n}\right)^q$，$g_{j+1}=\sum_{n=0}^{i-1}\sum_{m=1}^{q-1}\gamma^{zj-j+n-1+(m+j)n-j+1}\left(1+\gamma^{m(q+1)+n}\right)$。由于$\gamma$是$\mathbb{F}_{q^2}$的本原元，所以$\gamma^{l(q-1)}-1\ne 0$，其中$1\le l\le q$。因此，当且仅当$\left(1+\gamma^{r(q-1)}+\cdots+\gamma^{(i-1)r(q-1)}\right)\left(\gamma^{r(q-1)}-1\right)=\gamma^{ri(q-1)}-1=0$时，$\sum_{u=0}^{i-1}\gamma^{ru(q-1)}=0$，即$ri\equiv 0(\mathrm{mod}q+1)$。

当$t=1$时，对于$1\le r\le q$，可得$\gamma^{ri(q-1)}-1\ne 0$。此时$e_r\ne 0$，$f_z\ne 0$且$g_z\ne 0$。设$\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}=(k_{i,j})$，则$k_{1+z,q-z}\ne 0$，$k_{q+z,q-z}\ne 0$且$k_{q-m+1,m}\ne 0$，其中$1\le z\le j$，$1\le m\le i$。通过构造可逆矩阵$\boldsymbol{P}$和$\boldsymbol{Q}$，矩阵$\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}$可化为

$$\boldsymbol{P}\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{Q}=\begin{pmatrix} i\,(q-1) & 0 & \cdots & 0 & e_q & 0 & \cdots & 0\\ 0 & 0 & \cdots & e_{q-1} & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & e_2 & \cdots & 0 & 0 & 0 & \cdots & 0\\ e_1 & 0 & \cdots & 0 & i\,(q-1) & 0 & \cdots & 0\\ 0 & 0 & \cdots & g_{j+1} & g_j & \cdots & 0 & 0 \end{pmatrix} \tag{10}$$

当$p\mid i$时，$y_{1,1}=y_{q,q}=0$，故$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q+1$；当$p\nmid i$时，通过列变换消元得

$$y_{q,q}=i-i^{-1}\sum_{u=0}^{i-1}\gamma^{uq(q-1)}-\sum_{u=0}^{i-1}\gamma^{u(q-1)} \tag{11}$$

将式(11)两边乘以$i\left(\gamma^{q-1}-1\right)\left(\gamma^{iq(q-1)}-1\right)$后化简得

$$\begin{aligned}T=&i^2\left(2-\gamma^{q-1}-\gamma^{iq(q-1)}\right)\\&-\left(2-\gamma^{i(q-1)}-\gamma^{iq(q-1)}\right)\end{aligned} \tag{12}$$

若$T=0$，令$u=\gamma^{q-1}$，则方程(12)化为 $u^i+u^{-i}-u-u^{-1}=0$，矛盾。故$T\neq 0$，$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q+1$。

当$t=\gcd(i,q+1)\geq 2$时，与$t=1$时情况类似，有

$$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=\begin{cases}q-(t-2v-2)，i为偶数\\ q-(t-2v-3)，i为奇数\end{cases}$$

证毕

注 下面对式(7)进行新的扭曲操作

$$\begin{pmatrix}1+(a_1\beta)^{q+j} & 1+(a_2\beta)^{q+j} & \cdots & 1+(a_{q-1}\beta)^{q+j}\\ a_1\beta & a_2\beta & \cdots & a_{q-1}\beta\\ \vdots & \vdots & \ddots & \vdots\\ (a_1\beta)^x+(a_1\beta)^{q+j+x} & (a_2\beta)^x+(a_2\beta)^{q+j+x} & \cdots & (a_{q-1}\beta)^x+(a_{q-1}\beta)^{q+j+x}\\ (a_1\beta)^{x+1} & (a_2\beta)^{x+1} & \cdots & (a_{q-1}\beta)^{x+1}\\ (a_1\beta)^{x+2}+(a_1\beta)^{q+j+x+2} & (a_2\beta)^{x+2}+(a_2\beta)^{q+j+x+2} & \cdots & (a_{q-1}\beta)^{x+2}+(a_{q-1}\beta)^{q+j+x+2}\\ \vdots & \vdots & \ddots & \vdots\\ a_1^j\beta^{q+j-1}+y_1 & a_2^j\beta^{q+j-1}+y_2 & \cdots & a_{q-1}^j\beta^{q+j-1}+y_{q-1}\end{pmatrix}$$

即当$m\equiv 1\,(\mathrm{mod}2)$时，式(7)中$(a_n\beta)^m$所在位置的元素变为$(a_n\beta)^m+(a_n\beta)^{q+j+m}$；当$m\equiv 0\,(\mathrm{mod}2)$时，式(7)中$(a_n\beta)^m$所在位置的元素不变，其中$0\leq m\leq q+j-1$，$1\leq n\leq q-1$。进一步，若$q+j-1\equiv 1\,(\mathrm{mod}2)$，则$y_n=a_n^j\beta^{q+j-1}+a_n^{q+2j}\beta^{2q+2j-1}$；若$q+j-1\equiv 0\,(\mathrm{mod}2)$，则$y_n=0$。

该扭曲操作使得$\mathrm{rank}(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}})=q+j$。由定义1，该扭曲操作将MDS EAQECCs 提升为ME-MDS EAQECCs，码的参数为$[[i(q-1),i(q-1)-q-j,q+j+1;q+j]]_q$。

下面的定理将具体分析$i=2,3,4$时的情形。

定理2 设$q=p^m$，其中p为奇素数，m为正整数。设i为正整数且$t=\gcd(i,q+1)$。令C为由式(6)定义的RS码$\mathcal{RS}_{q+j}(\boldsymbol{a})$，其中$j=\dfrac{q-3}{2}$，$v=\left\lfloor\dfrac{(1+j)\,t}{q+1}\right\rfloor$，则

(1) 当$i=2$时，$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j-1$；

(2) 当$i=3$且$m\geq 2$时，$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j+(t-2v-2)$；

(3) 当$i=4$且满足$p\equiv 1\,(\mathrm{mod}4)\,(m\geq 2)$或$p\equiv 3\,(\mathrm{mod}4)\,(m\neq 2)$时，$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j+(t-2v-3)$。

证明 (1)设$\boldsymbol{G}$为码C的生成矩阵。当$i=2$时，式(12)可表示为$T=6-4\gamma^{q-1}-4\gamma^{q(q-1)}+\gamma^{2(q-1)}+\gamma^{2q(q-1)}$。由于$j=\dfrac{q-3}{2}$，故当$T\neq 0$时，$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q$。若$T=0$，令$u=\gamma^{q-1}$，则上式变形为$u^4-4u^3+6u^2-4u+1=(u-1)^4=0$，这与$u\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$矛盾。故$T\neq 0$，$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q$，从而$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j-1$。

(2) 令$u=\gamma^{q-1}$。当$i=3$时，$T=16-9u-9u^{-1}+u^3+u^{-3}$。若$T=0$，则$u^6-9u^4+16u^3-9u^2+1=(u-1)^4\left(u^2+4u+1\right)=0$。由$u$的阶为$q+1$可知$u^2+4u+1=0$不成立，故$T\neq 0$，$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q-t+2v+2$，从而$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j+(t-2v-2)$。

(3) 当$i=4$时，$T=30-16u-16u^{-1}+u^4+u^{-4}$。同理，设$T=0$，则$(u+1)^4+4u^2=0$。令$s^2=-1$，$s\in\mathbb{F}_{q^2}$，有

(a) 当$p\equiv 1\,(\mathrm{mod}4)$时，$s\in\mathbb{F}_p$。则上式分解为$(u+1)^2=\pm 2su$，由类似(2)的方法得出矛盾；

(b) 当$p\equiv 3\,(\mathrm{mod}4)$时，$s\in\mathbb{F}_{p^2}$。由$u+u^{-1}\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p$得出类似矛盾。

故$T\neq 0$，$\mathrm{rank}\left(\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\right)=q-t+2v+3$，从而$\dim\left(\mathrm{Hull}_{\mathrm{H}}(C)\right)=j+(t-2v-3)$。 证毕

定理3 设$q=p^m$，其中p为奇素数，$m\geq 2$。令$i^2\equiv 1\,(\mathrm{mod}p)$或$i\equiv 0\,(\mathrm{mod}p)$，$2\leq i\leq q-1$。设$j=\dfrac{q-3}{2}$，$t=\gcd(i,q+1)$，$v=\left\lfloor\dfrac{(j+1)\,t}{q+1}\right\rfloor$，则

(1) 当i为奇数时，存在参数为$[[i(q-1),i(q-1)-2j-q-t+2v+2,q+j+1;q-t+2v+2]]_q$的MDS EAQECCs；

(2) 当i为偶数时，存在参数为$[[i(q-1),i(q-1)-2j-q-t+2v+3,q+j+1;q-t+2v+3]]_q$的MDS EAQECCs。

定理4 设$q=p^m$，其中p为奇素数，$m\geq 2$。取$i=2$，令$j=\dfrac{q-3}{2}$，$t=\gcd(2,q+1)$，$v=\left\lfloor\dfrac{(j+1)\,t}{q+1}\right\rfloor$，则存在参数为$[[2(q-1),2(q-1)-2j-q+1,q+j+1;q+1]]_q$的MDS EAQECCs。

定理5　设$q=p^m$，其中p为奇素数，$m\geq 2$。令$t=\gcd(3,q+1)$，$j=\dfrac{q-3}{2}$，$v=\left\lfloor\dfrac{(j+1)t}{q+1}\right\rfloor$，则存在参数为$[[3(q-1),3(q-1)-2j-q+2v-1,q+j+1;q+2v-1]]_q$的MDSEAQECCs；

定理6　设$q=p^m$，其中p为奇素数，$m\geq 2$。令$t=\gcd(4,q+1)$，$j=\dfrac{q-3}{2}$，$v=\left\lfloor\dfrac{(j+1)t}{q+1}\right\rfloor$，则存在参数为$[[4(q-1),4(q-1)-2j-q-t+2v+3,q+j+1;q-t+2v+3]]_q$的MDS EAQECCs。

3.2 MDS EAQECCs的第2种构造

本节通过$\mathcal{RS}_{q+1}(\boldsymbol{b})$构造第二类MDS EAQECCs。设$U_{q+1}$为$\mathbb{F}_{q^2}^*$中所有$q+1$次单位根构成的子群，其中$\gamma$为$\mathbb{F}_{q^2}^*$的生成元，则$U_{q+1}=\langle\gamma^{q-1}\rangle$。记$U_{q+1}=\{b_1,b_2,\cdots,b_{q+1}\}$，构造向量

$$\begin{aligned}\boldsymbol{b}=(&b_1,b_2,\cdots,b_{q+1},b_1\gamma,b_2\gamma,\cdots,b_{q+1}\gamma,\cdots,\\&b_1\gamma^{i-1},b_2\gamma^{i-1},\cdots,b_{q+1}\gamma^{i-1})\end{aligned}\tag{13}$$

其中$2\leq i\leq q-2$。由此得到码长为$i(q+1)$，维数为$q+1$的$\mathcal{RS}_{q+1}(\boldsymbol{b})$。$\mathcal{RS}_{q+1}(\boldsymbol{b})$的厄米特正交包维数由下面定理给出。

定理7　设$q=p^m$，其中p为奇素数，m是正整数。取奇数i满足$i^2\equiv 1(\mathrm{mod}p)$或$i\equiv 0(\mathrm{mod}p)$，令$s=\gcd(i,q-1)$。设$C$为由式(13)定义的$\mathcal{RS}_{q+1}(\boldsymbol{b})$，$\boldsymbol{W}$为$C$在$\mathbb{F}_{q^2}$上的生成矩阵。根据式(5)对$\boldsymbol{W}$进行扭曲操作后，可得$\dim(\mathrm{Hull}_{\mathrm{H}}(C))=s$。

注　定义$(q+1)\times(q+1)$阶矩阵$\boldsymbol{B}_\delta$

$$\boldsymbol{B}_\delta=\begin{pmatrix}1&1&\cdots&1\\b_1\delta&b_2\delta&\cdots&b_{q+1}\delta\\\vdots&\vdots&\ddots&\vdots\\b_1^q\delta^q&b_2^q\delta^q&\cdots&b_{q+1}^q\delta^q\end{pmatrix}$$

其中，$\delta\in\mathbb{F}_{q^2}^*$，从而$C$的生成矩阵可表示为$\boldsymbol{W}=\left[\boldsymbol{B}_1:\boldsymbol{B}_\gamma:\cdots:\boldsymbol{B}_{\gamma^{i-1}}\right]$。

对$\boldsymbol{B}_\delta$进行新的扭曲改造

$$\begin{pmatrix}1+(b_1\delta)^{q+1}&1+(b_2\delta)^{q+1}&\cdots&1+(b_{q+1}\delta)^{q+1}\\b_1\delta&b_2\delta&\cdots&b_{q+1}\delta\\\vdots&\vdots&\ddots&\vdots\\(b_1\delta)^x+(b_1\delta)^{q+1+x}&(b_2\delta)^x+(b_2\delta)^{q+1+x}&\cdots&(b_{q+1}\delta)^x+(b_{q+1}\delta)^{q+1+x}\\(b_1\delta)^{x+1}&(b_2\delta)^{x+1}&\cdots&(b_{q+1}\delta)^{x+1}\\(b_1\delta)^{x+2}+(b_1\delta)^{q+x+3}&(b_2\delta)^{x+2}+(b_2\delta)^{q+x+3}&\cdots&(b_{q+1}\delta)^{x+2}+(b_{q+1}\delta)^{q+x+3}\\\vdots&\vdots&\ddots&\vdots\\(b_1\delta)^q+y_1&(b_2\delta)^q+y_2&\cdots&(b_{q+1}\delta)^q+y_{q+1}\end{pmatrix},$$

即当$m\equiv 1(\mathrm{mod}2)$时，$\boldsymbol{B}_\delta$中$(b_n\delta)^m$所在位置的元素变为$(b_n\delta)^m+(b_n\delta)^{q+1+m}$；当$m\equiv 0(\mathrm{mod}2)$时，$\boldsymbol{B}_\delta$中$(b_n\delta)^m$所在位置的元素不变，其中$0\leq m\leq q+1$，$1\leq n\leq q+1$。进一步，若$q\equiv 1(\mathrm{mod}2)$，则$y_n=(b_n\delta)^q+(b_n\delta)^{2q+1}$；若$q\equiv 0(\mathrm{mod}2)$，则$y_n=0$。

该扭曲操作使得$\mathrm{rank}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=q+1$。由定义1可知，该扭曲操作将MDS EAQECCs提升为ME-MDS EAQECCs，码的参数为$[[i(q+1),(i-1)(q+1),q+2;q+1]]_q$。

根据定理7，本文得到如下新参数的MDS EAQECCs。

定理8　设$q=p^m$，其中p为奇素数，m是正整数。取奇数i满足$i^2\equiv 1(\mathrm{mod}p)$或$i\equiv 0(\mathrm{mod}p)$，$2\leq i\leq q-2$。令$s=\gcd(i,q-1)$，则存在参数为$[[i(q+1),(i-1)(q+1)-s,q+2;q-s+1]]_q$的MDS EAQECCs。

定理9　设$q=p^m$，其中p为奇素数，m是正整数。取$i=3$，$s=\gcd(i,q-1)$，则存在参数为$[[3(q+1),2q+1,q+2;q]]_q$的MDS EAQECCs。

本文构造的MDS EAQECCs见表1。

表 1　本文构造的MDS EAQECCs

构造类	构造参数	参数来源
1	$[[120,58,37;10]]_{25}$	定理3
	$[[156,106,40;28]]_{27}$	定理3
	$[[288,194,73;50]]_{49}$	定理3
	$[[160,2,121;82]]_{81}$	定理4
	$[[78,11,40;11]]_{27}$	定理5
	$[[72,22,40;28]]_{25}$	定理5
	$[[496,250,187;126]]_{125}$	定理6
	$[[32,18,13;10]]_9$	定理6
	$[[32,20,13;12]]_9$	定理3的ME提升
	$[[78,39,40;39]]_{25}$	定理3的ME提升
2	$[[130,103,27;25]]_{25}$	定理8
	$[[30,23,7;5]]_5$	定理8
	$[[630,503,127;125]]_{125}$	定理8
	$[[84,55,29;27]]_{27}$	定理9
	$[[12,7,5;3]]_3$	定理9
	$[[30,19,11;9]]_9$	定理9
	$[[12,8,5;4]]_3$	定理8的ME提升
	$[[30,24,7;6]]_5$	定理8的ME提升

基于定理1与定理7，本文得到几类新参数的MDS EAQECCs，具体见定理3～6, 8, 9。

注： 表2总结了码长小于q^2且最小距离超过$q+1$的已知MDS EAQECCs。在文献[30]中，虽然码的码长较为灵活，但是最小距离需要保持一定限制，即只有在$\lambda \geq \frac{q+3}{8}$时，最小距离才能优于$q+1$。文献[31,32]也存在同样的缺陷。而文献[33–36]中的MDS EAQECCs虽然在最小距离上优于$q+1$，但是码长$\frac{q^2-1}{4}, \frac{(q-1)(q+1)}{8}, \frac{q^2-1}{i}\ (i \in \{3,5,7\})$与$\frac{q^2+1}{2}$都固定不变，不够灵活。与表2 中已知的 MDS EAQECCs 对比可知，本文构造的码在保持最小距离优势的同时，实现了码长的灵活可调，并且所构造码的参数是新的，没有被之前的研究所覆盖。

4 结束语

本文利用TRS码构造了两类MDS EAQECCs，对比分析表明，本文构造的EAQECCs具有以下优势：

(1)相较于表2中已知的MDS EAQECCs，本文的 MDS EAQECCs参数是新的，没有被之前的研究所覆盖；

(2)本文构造的EAQECCs不仅实现了码长灵活可调，所构造码的最小距离也显著突破了$q+1$的理论界限；

表 2 与已知q-元MDS EAQECCs的参数对比

构造类	n	d	c	限制条件	文献
1	$2\lambda(q-1)$	d	$2i$	$i \in \{1,2\}$, λ为奇数, $\lambda \mid (q-1)$, $8 \mid (q+1)$ $\frac{q-1}{2}(i-1)+4\lambda+1 \leq d \leq \frac{q-1}{2}+2(i+1)\lambda$	[30]
2	$\frac{q^2-1}{\lambda}$	$y+1$	y	$1 \leq y \leq \left\lfloor \frac{q^2-1}{2\lambda} \right\rfloor$	[31]
3	q^2+i	d	1	$2 \leq d \leq 2q+i-1), i \in \{-1,1\}$,	[32]
	$\frac{q^2-1}{i}$	d	2	$\frac{q+1}{2}+2 \leq d \leq \frac{3}{2}q-\frac{1}{2}$	
4	q^2+1	$2q+2$	5	$q \equiv 3 \pmod 4$	[33]
	q^2+1	$2\lambda+2$	9	$q \equiv 3 \pmod 4$, $q+1 \leq \lambda \leq 2q-2$	
	$\frac{q^2-1}{4}$	d	4	$q \equiv 3 \pmod 4$, $\frac{3q+7}{4} \leq d \leq \frac{5q+1}{4}$	
5	$\frac{(q-1)(q+1)}{8}$	d	8	$q+1 \leq d \leq \frac{9q-1}{8}$	[34]
6	$\frac{q^2-1}{i}$	d	i	$i \in \{3,5,7\}, q+1 \leq d \leq \frac{(i+1)(q+1)}{j}-1$	[35]
	$\frac{q^2-1}{j}$	d	7	$d=\frac{8(q+1)}{j}-1$	
7	$\frac{q^2+1}{2}$	$3q-1$	13	$q \geq 5$	[36]
		$4q-2$	25	$q \geq 7$	
		$6q-4$	61	$q \geq 11$	
8	$i(q-1)$	$q+j+1$	$q-t+2v+2$	$i^2 \equiv 1 \pmod p$或$i \equiv 0 \pmod p$, i为奇数, $j=\frac{q-3}{2}$, $v=\left\lfloor \frac{(j+1)t}{q+1} \right\rfloor$, $t=\gcd(i,q+1)$	定理3
	$i(q-1)$	$q+j+1$	$q-t+2v+3$	$i^2 \equiv 1 \pmod p$或$i \equiv 0 \pmod p$, i为偶数, $j=\frac{q-3}{2}$, $v=\left\lfloor \frac{(j+1)t}{q+1} \right\rfloor$, $t=\gcd(i,q+1)$	
	$i(q-1)$	$q+j+1$	$q+j$	$c=d-1$	ME提升
	$2(q-1)$	$q+j+1$	$q-t+2v+3$	$c=d-1$，$i=2$	
	$3(q-1)$	$q+j+1$	$q-t+2v+2$	$c=d-1$，$i=3$	
9	$i(q+1)$	$q+2$	$q-s+1$	i为奇数, $i^2 \equiv 1 \pmod p$或$i \equiv 0 \pmod p$，$2 \leq i \leq q-2$, $s=\gcd(i,q-1)$	定理8
	$i(q+1)$	$q+2$	$c=d-1$		ME提升
	$3(q+1)$	$q+2$	q	$c=d-1$，$i=3$	

(3)通过给出特定的扭曲操作，本文的MDS EAQECCs达到了ME-MDS EAQECCs。

本文的研究成果表明，TRS码是构造性能良好EAQECCs的重要线性码类。

参 考 文 献

[1] GISIN N, RIBORDY G, TITTEL W, *et al*. Quantum cryptography[J]. *Reviews of Modern Physics*, 2002, 74(1): 145–195. doi: 10.1103/RevModPhys.74.145.

[2] NI Zhongchu, LI Sai, DENG Xiaowei, *et al*. Beating the break-even point with a discrete-variable-encoded logical qubit[J]. *Nature*, 2023, 616(7955): 56–60. doi: 10.1038/s41586-023-05784-4.

[3] 吕欣, 马智, 冯登国. 基于量子Calderbank-Shor-Steane纠错码的量子安全直接通信[J]. 软件学报, 2006, 17(3): 509–515. doi: 10.1360/jos170509.

LÜ Xin, MA Zhi, and FENG Dengguo. Quantum secure direct communication using quantum Calderbank-Shor-Steane error correcting codes[J]. *Journal of Software*, 2006, 17(3): 509–515. doi: 10.1360/jos170509.

[4] 王玉, 开晓山, 朱士信. 一种2^m元域上量子纠错码的构造方法[J]. 电子与信息学报, 2023, 45(5): 1731–1736. doi: 10.11999/JEIT221145.

WANG Yu, KAI Xiaoshan, and ZHU Shixin. A construction method of quantum error-correcting codes over F_{2^m} [J]. *Journal of Electronics & Information Technology*, 2023, 45(5): 1731–1736. doi: 10.11999/JEIT221145.

[5] CHEN Bocong, LING San, and ZHANG Guanghui. Application of constacyclic codes to quantum MDS codes[J]. *IEEE Transactions on Information Theory*, 2015, 61(3): 1474–1484. doi: 10.1109/TIT.2015.2388576.

[6] BRUN T, DEVETAK I, and HSIEH M H. Correcting quantum errors with entanglement[J]. *Science*, 2006, 314(5798): 436–439. doi: 10.1126/science.1131563.

[7] LI Yang, WAN Ruhao, and ZHU Shixin. MDS codes with Euclidean and Hermitian hulls of flexible dimensions and their applications to EAQECCs[J]. *Quantum Information Processing*, 2023, 22(153): 1–33. doi: 10.1007/s11128-023-03900-x.

[8] JIANG Wan, ZHU Shixin, and CHEN Xiaojing. Optimal entanglement-assisted quantum codes with larger minimum distance[J]. *IEEE Communications Letters*, 2021, 25(1): 45–48. doi: 10.1109/LCOMM.2020.3025012.

[9] BISWAS S and BHAINTWAL M. A new construction of quantum codes from quasi-cyclic codes over finite fields[J]. *Indian Journal of Pure and Applied Mathematics*, 2023, 54(2): 375–388. doi: 10.1007/s13226-022-00259-0.

[10] CHEN Xiaojing, ZHU Shixin, and JIANG Wan. Cyclic codes and some new entanglement-assisted quantum MDS codes[J]. *Designs, Codes and Cryptography*, 2021, 89(11): 2533–2551. doi: 10.1007/s10623-021-00935-y.

[11] GUENDA K, JITMAN S, and GULLIVER T A. Constructions of good entanglement-assisted quantum error correcting codes[J]. *Designs, Codes and Cryptography*, 2018, 86(1): 121–136. doi: 10.1007/s10623-017-0330-z.

[12] GAO Jian, ZHANG Yaozong, LIU Ying, *et al*. New MDS EAQECCs derived from constacyclic codes over $\mathbb{F}_{q^2}+v\mathbb{F}_{q^2}$ [J]. *Discrete Mathematics*, 2023, 346(9): 113513. doi: 10.1016/j.disc.2023.113513.

[13] FANG Weijun, FU Fangwei, LI Lanqiang, *et al*. Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs[J]. *IEEE Transactions on Information Theory*, 2020, 66(6): 3527–3537. doi: 10.1109/TIT.2019.2950245.

[14] CAO Meng. Several new families of MDS EAQECCs with much larger dimensions and related application to EACQCs[J]. *Quantum Information Processing*, 2023, 22(12): 447. doi: 10.1007/s11128-023-04197-6.

[15] LUO Gaojun, CAO Xiwang, and CHEN Xiaojing. MDS codes with hulls of arbitrary dimensions and their quantum error correction[J]. *IEEE Transactions on Information Theory*, 2019, 65(5): 2944–2952. doi: 10.1109/TIT.2018.2874953.

[16] CAO Meng. MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction[J]. *IEEE Transactions on Information Theory*, 2021, 67(12): 7964–7984. doi: 10.1109/TIT.2021.3117562.

[17] PEREIRA F R F and MANCINI S. Entanglement-assisted quantum codes from cyclic codes[J]. *Entropy*, 2023, 25(1): 37. doi: 10.3390/e25010037.

[18] GALINDO C, HERNANDO F, and RUANO D. Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2[J]. *Quantum Information Processing*, 2021, 20(5): 158. doi: 10.1007/s11128-021-03101-4.

[19] ZHU Shixin and WAN Ruhao. On the existence of Galois self-dual GRS and TGRS codes[J]. *Finite Fields and Their Applications*, 2025, 105: 102608. doi: 10.1016/j.ffa.2025.102608.

[20] HUANG Daitao, YUE Qin, NIU Yongfeng, *et al*. MDS or NMDS self-dual codes from Twisted generalized Reed–Solomon codes[J]. *Designs, Codes and Cryptography*, 2021, 89(9): 2195–2209. doi: 10.1007/s10623-021-00910-7.

[21] BEELEN P, BOSSERT M, PUCHINGER S, *et al*. Structural properties of twisted Reed-Solomon codes with applications to cryptography[C]. IEEE International Symposium on Information Theory, Vail, USA, 2018: 946–950. doi: 10.1109/ISIT.2018.8437923.

[22] LIU Hongwei and LIU Shengwei. Construction of MDS twisted Reed-Solomon codes and LCD MDS codes[J]. *Designs, Codes and Cryptography*, 2021, 89(9): 2051–2065. doi: 10.1007/s10623-021-00899-z.

[23] LAVAUZELLE J and RENNER J. Cryptanalysis of a system based on twisted Reed-Solomon codes[J]. *Designs, Codes and Cryptography*, 2020, 88(7): 1285–1300. doi: 10.1007/s10623-020-00747-6.

[24] ZHU Canze and LIAO Qunying. The non-GRS properties for the twisted generalized Reed-Solomon code and its extended code[Z]. arXiv: 2204.11955, 2022. doi: 10.48550/arXiv.2204.11955.

[25] ZHU Canze and LIAO Qunying. The (+)-extended twisted generalized Reed-Solomon code[J]. *Discrete Mathematics*, 2024, 347(2): 113749. doi: 10.1016/j.disc.2023.113749.

[26] LIU Hualu and LIU Xiusheng. New EAQEC codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$[J]. *Quantum Information Processing*, 2020, 19(3): 85. doi: 10.1007/s11128-020-2580-3.

[27] GRASSL M, HUBER F, and WINTER A. Entropic proofs of singleton bounds for quantum error-correcting codes[J]. *IEEE Transactions on Information Theory*, 2022, 68(6): 3942–3950. doi: 10.1109/TIT.2022.3149291.

[28] GALINDO C, HERNANDO F, MATSUMOTO R, *et al*. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields[J]. *Quantum Information Processing*, 2019, 18(4): 116. doi: 10.1007/s11128-019-2234-5.

[29] BEELEN P, PUCHINGER S, and ROSENKILDE J. Twisted reed-Solomon codes[C]. IEEE International Symposium on Information Theory, Aachen, Germany, 2017: 336–340. doi: 10.1109/ISIT.2017.8006545.

[30] LU Liangdong, MA Wenping, and GUO Luobin. Two families of entanglement-assisted quantum MDS codes from constacyclic codes[J]. *International Journal of Theoretical Physics*, 2020, 59(6): 1657–1667. doi: 10.1007/s10773-020-04433-0.

[31] SARI M and KÖROĞLU M E. New entanglement-assisted quantum MDS codes with maximal entanglement[J]. *International Journal of Theoretical Physics*, 2021, 60(1): 243–253. doi: 10.1007/s10773-020-04682-z.

[32] FAN Jihao, CHEN Hanwu, and XU Juan. Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q+1$[J]. *Quantum Information & Computation*, 2016, 16(5/6): 423–434.

[33] SARI M and KOLOTOĞLU E. An application of constacyclic codes to entanglement-assisted quantum MDS codes[J]. *Computational and Applied Mathematics*, 2019, 38(2): 75. doi: 10.1007/s40314-019-0837-1.

[34] LI Ruihu, GUO Guanmin, SONG Hao, *et al*. New constructions of entanglement-assisted quantum MDS codes from negacyclic codes[J]. *International Journal of Quantum Information*, 2019, 17(3): 1950022. doi: 10.1142/S0219749919500229.

[35] LIU Yang, LI Ruihu, LV Liangdong, *et al*. Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes[J]. *Quantum Information Processing*, 2018, 17(8): 210. doi: 10.1007/s11128-018-1978-7.

[36] PANG Binbin, ZHU Shixin, LI Fulin, *et al*. New entanglement-assisted quantum MDS codes with larger minimum distance[J]. *Quantum Information Processing*, 2020, 19(7): 207. doi: 10.1007/s11128-020-02698-2.

潘 鑫：女，硕士生，研究方向为编码理论及其应用.

高 健：男，副教授，博士，博士生导师，研究方向为编码理论及其应用.

责任编辑：马秀强

Constructing Two Classes of Maximum Distance Separable Entanglement-Assisted Quantum Error-Correcting Codes by Using Twisted Generalized Reed-Solomon Codes

PAN Xin GAO Jian

(*School of Mathematics and Statistics, Shandong University of Technology, Zibo* 255000, *China*)

Abstract:

Objective With the rapid development of quantum communication and computation, efficient error-correction technologies are critical for ensuring the reliability of quantum systems. Maximal Distance Separable (MDS) Entanglement-Assisted Quantum Error-Correcting Codes (EAQECCs) with flexible code lengths and larger minimum distances offer significant advantages in enhancing quantum system robustness. However, classical quantum codes face limitations in parameter flexibility and minimum distance constraints. This study addresses these challenges by leveraging Twisted Generalized Reed-Solomon (TGRS) codes to construct novel MDS EAQECCs, aiming to improve performance in complex quantum communication scenarios. In this paper, TGRS codes are innovatively applied to construct MDS EAQECCs. Different from polynomial construction methods,

we determine the dimension of the Hermitian Hull through special matrix rank analysis, and successfully construct q-ary MDS EAQECCs with a minimum distance exceeding$q+1$. Two construction schemes with flexible code lengths are proposed. Notably, the minimum distances of the constructed q-ary codes all exceed $q+1$. Table 2 systematically summarizes the known MDS EAQECCs with a length less than q^2 and a minimum distance exceeding $q+1$. The novelty of the construction schemes in this paper is highlighted through parameter comparison. Reasoning shows that our schemes achieve flexible adjustment of the code length while maintaining the advantage of the minimum distance.

Methods　The proposed approach integrates TGRS codes with algebraic techniques to design MDS EAQECCs. Two families of MDS EAQECCs are constructed by using TGRS codes over finite fields. The key steps are as follows: (1) TGRS Code Construction: Utilizing twisted polynomials and hook parameters to generate TGRS codes with adjustable dimensions and minimum distances. (2) Hermitian Hull Analysis: Applying matrix rank analysis to determine the dimensions of the Hermitian Hull of the constructed codes, which is crucial for satisfying the Singleton bound in quantum codes. (3) Twisted Operation Optimization: Employing twisted operations to transform the constructed MDS EAQECCs into ME-MDS EAQECCs.

Results and Discussions　This paper constructs two families of MDS EAQECCs using TGRS codes and gives certain twisted conditions under which the codes are ME-MDS EAQECCs. Compared with other known codes, these new codes have more flexible parameters and significant advantages in terms of code length, minimum distance, and maximum entanglement state. This paper constructs q-ary EAQECCs with $[[i(q-1), i(q-1)-2j-q-t+2v+2, q+j+1; q-t+2v+2]]_q$ when i is odd and $[[i(q-1), i(q-1)-2j-q-t+2v+3, q+j+1; q-t+2v+3]]_q$ when i is even. Based on Theorem 1 and Theorem 2, several types of MDS EAQECCs are obtained, and their parameters are listed in Table 1.Theorems 3～6 give the existence conditions of specific q-ary EAQECCs under different parameter settings. Furthermore, this paper upgrades the MDS EAQECCs to ME-MDS EAQECCs with $[[i(q-1), i(q-1)-q-j, q+j+1; q+j]]_q$ by a twisted operation. Meanwhile, this paper constructs q-ary EAQECCs with $[[i(q+1), (i-1)(q+1)-s, q+2; q-s+1]]_q$. Moreover, this paper upgrades the MDS EAQECCs to ME-MDS EAQECCs with $[[i(q+1), (i-1)(q+1), q+2; q+1]]_q$ by a twisted operation. Theorem 7 gives the dimension of the Hermitian Hull of this RS code after the twisted operation on its generating matrix. Similar to the first construction, a new twisted operation is applied, which upgrades the MDS EAQECCs to ME-MDS EAQECCs with specific parameters. Theorems 8, 9 give the existence conditions of specific q-ary EAQECCs under different parameter settings based on this construction method.

Conclusions　Two families of MDS EAQECCs are constructed using TGRS codes, and the parameters of known MDS EAQECCs are systematically summarized. Comparative analysis reveals that the EAQECCs proposed in this paper offer the following advantages: Compared with the known q-ary MDS EAQECCs (Table 2), the parameters of the MDS EAQECCs constructed here are new and have not been covered by previous studies; The codes not only enable flexible code-length adjustments but also achieve a minimum distance that significantly exceeds traditional theoretical bounds; Under specific twisted conditions, the constructed MDS EAQECCs are upgraded to ME-MDS EAQECCs. By introducing the twisted operation on RS codes, more flexible parameter combinations are obtained. This provides greater flexibility in the design of quantum error-correcting codes, enabling better adaptation to different quantum communication requirements. This improvement further optimizes the performance of quantum error-correcting codes, enhancing the entanglement-assisted error-correcting ability and improving the overall efficiency of quantum systems. These research results indicate that TGRS codes are important theoretical tools for constructing high-performance EAQECCs with excellent parameters. They play a pivotal part in advancing the development of quantum communication technology. Moreover, they offer a firm theoretical underpinning for the practical implementation of quantum error-correcting codes. Future research can focus on further exploring the potential of TGRS codes in constructing more advanced quantum error-correcting codes and expanding their applications in different quantum communication scenarios.

Key words: Entanglement-assisted quantum codes; Twisted generalized reed-solomon codes; Hermitian hull