第 57 卷 第 1 期 2008 年 1 月
1000-3290/2008/57(01)/0028-03

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.1, January, 2008

量子 Generalized Reed-Solomon 码

李 卓 邢莉娟

(西安电子科技大学综合业务网国家重点实验室,西安 710071)

(2007 年 4 月 2 日收到;2007 年 4 月 17 日收到修改稿)

构造出了一族量子纠错码,这族码具有参数$[[n, n-2k, k+1]]_q$,是 q 维量子系统上的码,q 是任意素数的幂.这族码的最小距离达到了理论上限,因此,以码距来说,它是最优的.证明了当 $2 \leqslant n \leqslant q$ 或者 $q^2 - q + 2 \leqslant n \leqslant q^2$ 时,码都是存在的.

关键词:量子 Generalized Reed-Solomon 码,量子 MDS 码,量子纠错码,量子信息

PACC:0367,0365,0210

1. 引 言

量子计算[1,2]技术因其强大的计算能力,近十几年来,引起了人们极大的兴趣.但是,在实际构建量子计算机或者量子通信设备的过程中,不可避免的就会遇到差错问题.存储在设备中的或在信道中传输的量子比特会因为噪声或环境的作用而发生差错,严重时就会导致计算和通信的失败.近年来发展起来的量子纠错编码技术能够比较有效地解决这一难题.它的基本思想是将 k 位量子比特嵌入到 $n(>k)$ 位量子比特中,以达到对量子信息的保护.迄今为止,许多种量子纠错码以及相关理论已经被发现和提出[3—9].

本文利用经典 Generalized Reed-Solomon 码,构造出了一族量子码,这是一族量子 MDS 码,因此是最优的量子码.第二节给出了本文所需的预备知识;第三节是本文的主要工作,首先证明了一个引理,然后借助它构造出量子码;最后对所构造的量子码进行了分析和评价.

2. 基础知识

为了文章的完整性,本节介绍一些相关的基础知识.

在本文中,用$[[n, k, d]]_q$ 来表示一个量子纠错码,它将 k 位 q 维量子系统编码为 n 位 q 维量子系统,码距为 d,其中 q 是素数的幂.

给定 GF(q^2)上的两个向量 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ 和 $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$,它们的厄米内积定义为

$$\boldsymbol{x} * \boldsymbol{y} = \sum_{i=1}^{n} x_i y_i^q .$$

对于量子码与经典码之间的关系有如下定理:

定理 1[10] 令 C 是 GF(q^2)上的一个$[n, k]$经典线性码,$C^{\perp_h}$ 是 C 关于厄米内积的对偶码,若 $C \subseteq C^{\perp_h}$,且 $C^{\perp_h} \setminus C$ 的最小重量为 d,则存在一个$[[n, n-2k, d]]_q$ 量子码.

定理 2[11] (量子 Singleton 限)对于量子码$[[n, k, d]]_q$,其码参数满足如下关系:

$$k + 2d \leqslant n + 2. \tag{1}$$

定义 1 (量子 MDS 码)使(1)式等号成立的量子码称为量子 MDS 码.

定义 2[12] (经典 Generalized Reed-Solomon 码)令 $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_N)$,其中 α_i 是 GF(q)中互不相同的元素,再令 $\boldsymbol{v} = (v_1, \cdots, v_N)$,其中 v_i 是 GF(q)中的非零元素.那么 GF(q)上的经典 Generalized Reed-Solomon 码,表示为 $\mathrm{GRS}_K(\boldsymbol{\alpha}, \boldsymbol{v})$,包含所有向量

$$(v_1 F(\alpha_1), \cdots, v_N F(\alpha_N)),$$

其中,$F(z)$ 取遍所有 GF(q)上次数小于 K 的多项式.

众所周知,如上定义的 Generalized Reed-Solomon 码 $\mathrm{GRS}_K(\boldsymbol{\alpha}, \boldsymbol{v})$是一个$[N, K, N-K+1]$经典 MDS 码.

3. 量子码

引理 1 假设 $\alpha_1, \cdots, \alpha_N$ 是任意域上 N 个互不

相同的元素，则有下式成立：

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_N \\ & & & \\ \alpha_1^{N-2} & \alpha_2^{N-2} & \cdots & \alpha_N^{N-2} \end{bmatrix} \begin{bmatrix} 1\Big/\prod\limits_{\substack{j=1\\ j\neq 1}}^{N}(\alpha_1-\alpha_j) \\ 1\Big/\prod\limits_{\substack{j=1\\ j\neq 2}}^{N}(\alpha_2-\alpha_j) \\ \\ 1\Big/\prod\limits_{\substack{j=1\\ j\neq N}}^{N}(\alpha_N-\alpha_j) \end{bmatrix} = 0.$$

证明　对于域中任意元素 $x_1, x_2, \cdots, x_N$，有如下等式成立：

$$\sum_{i=1}^{N} \frac{x_i}{\prod\limits_{\substack{j=1\\ j\neq i}}^{N}(\alpha_i-\alpha_j)} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_N \\ & & & \\ \alpha_1^{N-2} & \alpha_2^{N-2} & \cdots & \alpha_N^{N-2} \\ x_1 & x_2 & \cdots & x_N \end{vmatrix} \Bigg/ \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_N \\ & & & \\ \alpha_1^{N-2} & \alpha_2^{N-2} & \cdots & \alpha_N^{N-2} \\ \alpha_1^{N-1} & \alpha_2^{N-1} & \cdots & \alpha_N^{N-1} \end{vmatrix}.$$

在上式中，分别令 $x_i = \alpha_i^j, j = 0, 1, \cdots, N-2$ 即得证.

本文的主要结果由下面的定理给出：

定理 3　（量子 Generalized Reed-Solomon 码）存在量子码 $[[n, n-2k, k+1]]_q$，其中，码参数满足 $\begin{cases} 2 \leqslant n \leqslant q \\ 1 \leqslant k \leqslant [n/2] \end{cases}$ 或者 $\begin{cases} n = q^2 - l \\ 1 \leqslant k \leqslant q-l-1 \end{cases}, 0 \leqslant l \leqslant q-2$，$q$ 是素数的幂.

证明　（构造性证明）令 $\mathrm{GF}(q^2) = \{\alpha_1 = 0, \alpha_2, \cdots, \alpha_{q^2}\}$，考察 $\mathrm{GF}(q^2)$ 上的经典 Generalized Reed-Solomon 码：

当 $n = q^2$ 时，令 $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_{q^2})$，$\boldsymbol{\mu} = \boldsymbol{\nu} = (1, \cdots, 1)$，则对于 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$，由引理 1 可得

$$\begin{aligned} &\sum_{i=1}^{n}(\mu_i\alpha_i^{qs})^q(\nu_i\alpha_i^t) \\ &= \sum_{i=1}^{n}(\alpha_i^{q^2})^s\alpha_i^t = \sum_{i=1}^{n}\alpha_i^{s+t} = \Big(\prod_{j=2}^{q^2}\alpha_j\Big)\sum_{i=1}^{n}\frac{\alpha_i^{s+t}}{\prod\limits_{j=2}^{q^2}\alpha_j} \\ &= \Big(\prod_{j=2}^{q^2}\alpha_j\Big)\sum_{i=1}^{n}\frac{\alpha_i^{s+t}}{\prod\limits_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i-\alpha_j)} = 0, \end{aligned}$$

$0 \leqslant s \leqslant k-1, 0 \leqslant t \leqslant n-k-1$，即 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$ 关于厄米内积互为对偶码. 这时若令 $1 \leqslant k \leqslant q-1$，显然又有 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu}) \subseteq \mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$，则由定理 1 可知，存在量子码 $[[q^2, q^2-2k, k+1]]_q$.

当 $n = q^2 - 1$ 时，令 $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_{q^2-1})$，$\boldsymbol{\mu} = (\alpha_1^q - \alpha_{q^2}^{q^2}, \cdots, \alpha_{q^2-1}^q - \alpha_{q^2}^{q^2})$，$\boldsymbol{\nu} = (1, \cdots, 1)$，则对于 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$，由引理 1 可得

$$\begin{aligned} &\sum_{i=1}^{n}(\mu_i\alpha_i^{qs})^q(\nu_i\alpha_i^t) \\ &= \sum_{i=1}^{n}(\alpha_i^q - \alpha_{q^2}^{q^2})^q(\alpha_i^{q^2})^s\alpha_i^t = \sum_{i=1}^{n}(\alpha_i - \alpha_{q^2})\alpha_i^{s+t} \\ &= \Big(\prod_{j=2}^{q^2}\alpha_j\Big)\sum_{i=1}^{n}\frac{(\alpha_i - \alpha_{q^2})\alpha_i^{s+t}}{\prod\limits_{j=2}^{q^2}\alpha_j} \\ &= \Big(\prod_{j=2}^{q^2}\alpha_j\Big)\sum_{i=1}^{n}\frac{(\alpha_i - \alpha_{q^2})\alpha_i^{s+t}}{\prod\limits_{\substack{j=1\\ j\neq i}}^{q^2}(\alpha_i-\alpha_j)} \\ &= \Big(\prod_{j=2}^{q^2}\alpha_j\Big)\sum_{i=1}^{n}\frac{\alpha_i^{s+t}}{\prod\limits_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i-\alpha_j)} = 0, \end{aligned}$$

$0 \leqslant s \leqslant k-1, 0 \leqslant t \leqslant n-k-1$，即 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$ 关于厄米内积互为对偶码. 这时若令 $1 \leqslant k \leqslant q-2$，显然又有 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu}) \subseteq \mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$，则由定理 1 可知，存在量子码 $[[q^2-1, q^2-2k-1, k+1]]_q$.

同理继续这样做下去，直到当 $n = q^2 - q + 2$ 时，令 $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_{q^2-q+2})$，$\boldsymbol{\mu} = \Big(\prod\limits_{r=q^2-q+3}^{q^2}(\alpha_1^q - \alpha_r^q), \cdots, \prod\limits_{r=q^2-q+3}^{q^2}(\alpha_{q^2-q+2}^q - \alpha_r^q)\Big)$，$\boldsymbol{\nu} = (1, \cdots, 1)$，则 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$ 关于厄米内积互为对偶码. 这时只有当 $k = 1$ 时，才能令 $\mathrm{GRS}_k(\boldsymbol{\alpha}^q, \boldsymbol{\mu}) \subseteq \mathrm{GRS}_{n-k}(\boldsymbol{\alpha}, \boldsymbol{\nu})$，从而得到量子码 $[[q^2-q+2, q^2-q, 2]]_q$.

综上所述，存在量子码 $[[n, n-2k, k+1]]_q$，$\begin{cases} n = q^2 - l \\ 1 \leqslant k \leqslant q-l-1 \end{cases}, \quad 0 \leqslant l \leqslant q-2.$

当 $2 \leqslant n \leqslant q$ 时，令 $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_n)$，其中 $\beta_i \in \mathrm{GF}(q) \subseteq \mathrm{GF}(q^2)$ 互不相同，则有 $1\Big/\prod\limits_{\substack{j=1\\ j\neq i}}^{n}(\beta_i - \beta_j) \in \mathrm{GF}(q) \subseteq \mathrm{GF}(q^2)$，因此，存在元素 $\omega_i \in \mathrm{GF}(q^2)$，使

得 $\omega_i^{q+1} = 1\Big/\prod_{\substack{j=1\\ j\neq i}}^{n}(\beta_i - \beta_j)$. 令 $\boldsymbol{\omega} = (\omega_1, \cdots, \omega_n)$，则对于 $\mathrm{GRS}_k(\boldsymbol{\beta}, \boldsymbol{\omega})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\beta}, \boldsymbol{\omega})$，由引理 1 可得

$$\sum_{i=1}^{n}(\omega_i\beta_i^s)^q(\omega_i\beta_i^t)$$

$$= \sum_{i=1}^{n}\omega_i^{q+1}\beta_i^{s+t} = \sum_{i=1}^{n}\frac{\beta_i^{s+t}}{\prod_{\substack{j=1\\ j\neq i}}^{n}(\beta_i - \beta_j)} = 0,$$

$$0 \leqslant s \leqslant k-1, 0 \leqslant t \leqslant n-k-1,$$

即 $\mathrm{GRS}_k(\boldsymbol{\beta}, \boldsymbol{\omega})$ 和 $\mathrm{GRS}_{n-k}(\boldsymbol{\beta}, \boldsymbol{\omega})$ 关于厄米内积互为对偶码；这时只要令 $1 \leqslant k \leqslant [n/2]$，就有 $\mathrm{GRS}_k(\boldsymbol{\beta}, \boldsymbol{\omega}) \subseteq \mathrm{GRS}_{n-k}(\boldsymbol{\beta}, \boldsymbol{\omega})$，从而由定理 1 可知，存在量子码 $[[n, n-2k, k+1]]_q$.

4. 结 论

我们称定理 3 中构造的码为量子 Generalized Reed-Solomon 码，这是一族量子 MDS 码，因此是最优的量子码. 由于它是通过经典 Generalized Reed-Solomon 码得到的，而对于经典 Generalized Reed-Solomon 码的研究已经相当成熟，因此，我们相信，与其他结构的量子码相比，对量子 Generalized Reed-Solomon 码性质和应用的研究将会是非常有前景的，比如说它的编译码算法和它在级联码中的应用等方面. 遗憾的是，当 $q < n < q^2 - q + 2$ 时，利用定理 3 的构造方法并不能得到相应的量子码，我们还没有找到有效的方法来构造这个范围的量子 Generalized Reed-Solomon 码，也没能证明在这个范围内不存在量子 Generalized Reed-Solomon 码，这些都可以作为未来的研究课题.

[1] Song K H 2005 *Acta Phys. Sin.* **54** 4730 (in Chinese) [宋克慧 2005 物理学报 **54** 4730]

[2] Grover L 1996 *Proc. 28th ACM Symp. Theo. Comp.* 212

[3] Li Z, Xing L J 2007 *Acta Phys. Sin.* **56** 5602 (in Chinese) [李卓、邢莉娟 2007 物理学报 **56** 5602]

[4] Steane A M 1996 *Phys. Rev. Lett.* **77** 793

[5] Laflamme R, Miquel C, Paz J P, Zurek W 1996 *Phys. Rev. Lett.* **77** 198

[6] Calderbank A R, Shor P W 1996 *Phys. Rev.* A **54** 1098

[7] Steane A M 1996 *Proc. Roy. Soc. London Ser.* A **452** 2551

[8] Gottesman D 1996 *Phys. Rev.* A **54** 1862

[9] Calderbank A R, Rains E M, Shor P W, Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405

[10] Ashikhmin A, Knill E 2001 *IEEE Trans. Inform. Theory* **47** 3065

[11] Rains E M 1999 *IEEE Trans. Inform. Theory* **45** 1827

[12] MacWilliams F J, Sloane N J A 1977 *The Theory of Error-Correcting Codes* (New York: North-Holland) p303

Quantum Generalized Reed-Solomon codes

Li Zhuo Xing Li-Juan

(*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*)

(Received 2 April 2007; revised manuscript received 17 April 2007)

Abstract

We construct a family of quantum error-correcting codes with parameters $[[n, n-2k, k+1]]_q$ which are defined in q-dimensional quantum systems, where q is an arbitrary prime power. These codes are optimal in the sense that the minimum distance is maximal. It is shown that codes exist for all n satisfying $2 \leqslant n \leqslant q$ or $q^2 - q + 2 \leqslant n \leqslant q^2$.

Keywords: quantum Generalized Reed-Solomon codes, quantum MDS codes, quantum error-correcting codes, quantum information

PACC: 0367, 0365, 0210