文章编号: 0583-1431(2008)01-0001-10 **文献标识码: A**

量子纠错码的等价和保距同构

刘太琳

山东财政学院统计与数理系 济南 250014
北京邮电大学理学院 北京 100876
E-mail: tlinliu@sina.com

温巧燕

北京邮电大学理学院 北京 100876

摘 要 研究了量子纠错码的等价性和保距同构, 推广了 Bogart 等人的一些概念, 并给出若干基本定理, 这些定理对进一步研究量子码的等价性和保距同构是非常有用的. 在此基础上构造出一个反例, 证明了在量子情形下, MacWilliams 的一个重要定理不成立.

关键词 辛码; 量子 (稳定子) 码; 等价; 保距同构
MR(2000) **主题分类** 94B99
中图分类 O236.2

Isometries and Equivalences of Quantum Codes

Tai Lin LIU

Department of Statistics and Mathematics, Shandong Finance Institute, Ji'nan 250014*, P. R. China*
School of Science, Beijing University of Post and Telecommunications,
Beijing 100876*, P. R. China*
E-mail: tlinliu@sina.com

Qiao Yan WEN

School of Science, Beijing University of Post and Telecommunications,
Beijing 100876*, P. R. China*

Abstract Some results on the isometries and equivalences of quantum codes are presented, one of which generalizes one of the results of Bogart et al., by these results, we construct an isometry of quantum codes which is not an equivalent mapping but preserves the symplectic inner product, i.e., a theorem of MacWilliams cannot be generalized to the quantum codes.

Keywords symplectic codes; quantum (stabilizer) codes; isometries; equivalences
MR(2000) Subject Classification 94B99
Chinese Library Classification O236.2

本文恒设 $GF(q)$ 是含 $q = p^l$ 个元素的有限域, 这里 p 是任意素数.

1994 年, Shor 给出了关于大数素因子分解的量子算法, 这个算法可以在量子计算机上用多项式时间解决该问题, 震惊了世界. 随后, 人们又发现了各种各样的快速量子算法. 但是, 在量

收稿日期: 2006-11-10; 接受日期: 2007-07-25
基金项目: 国家高技术研究发展 863 计划 (2006AA01Z419); 国家自然科学基金重大研究计划 (90604023); 教育部高校博士点基金 (20040013007); 现代通信国家重点实验室基金 (9140C1101010601); ISN 开放基金

子力学理论中存在退相干问题, 所以如果不加入量子纠错, 任何量子计算的实现都是十分困难的. 因此, 从一开始量子纠错编码技术就在量子信息理论中扮演了一个至关重要的角色. 1995–1996 年期间, Shor [1] 和 Steane [2] 独立地提出了两个著名的量子纠错编码方案, 开启了量子纠错编码的研究. 之后, 量子纠错编码理论迅速地发展起来. 1998 年, Calderbank 等人 [3] 提出了通过构造 $GF(2)$ 和 $GF(4)$ 上具有某中特性的经典纠错码来构造量子 (稳定子) 码的系统数学方法, 由此, 对量子码的研究就转化为对具有某些条件的经典码的研究. 用这些方法, 人们通过经典码如 BCH 码、RM 码和 AG 码等构造出一系列的量子码. 后来文献 [4–6] 又将 Calderbank 等人的方法推广到非二元量子码的情形. 与此同时, 国内众多学者也对量子纠错编码进行了广泛的研究, 并得到了许多好的结果 (见文献 [7–14]). 与经典编码理论一样, 在量子编码理论中对码的等价性研究也是非常重要的, 因此文献 [3] 和文献 [4] 都提出了量子码的等价性概念. 然而, 迄今为止有关这方面的文章却不多见, 本文对此做了一些有益的研究. 下面介绍文献 [4] 中关于量子码等价性概念的相关内容.

记 $GF(p)$ 上的线性空间 $V_n = (GF(p) \times GF(p))^n$, V_n 的一个子空间称为一个辛码. 任取 $v \in V_n$, 并将其写成

$$v = ((v_1^{(1)}, v_1^{(2)}), (v_2^{(1)}, v_2^{(2)}), \ldots, (v_n^{(1)}, v_n^{(2)})),$$

则 v 的重量定义为 $w(v) = |\{i \,|\, v_i^{(1)}, v_i^{(2)}\text{不全为零}, 1 \leq i \leq n\}|$. 对于任意 $v, v' \in V_n$, 它们之间的距离定义为 $d(v, v') = w(v - v')$.

设 C 和 D 是 V_n 的两个辛码, $\varphi : C \to D$ 是一个线性同构, 若 φ 保持重量, 或等价地, φ 保持距离, 则称 φ 为一个保距同构.

V_n 上的辛内积定义为

$$(v, w)_s = \sum_{1 \leq i \leq n} (v_i^{(1)} w_i^{(2)} - v_i^{(2)} w_i^{(1)}).$$

设 C 是 V_n 的一个 $n-k$ 维线性子空间, 本文恒用 $C^{\perp_s}$ 表示 C 在辛内积意义下的对偶码. 如果 C 在辛内积意义下是自正交的, 即 $C \subseteq C^{\perp_s}$, 而且 $C^{\perp_s} \setminus C$ 中所有元素最小重量是 d, 那么由 C 可获得一个参数为 $[[n, k, d]]_p$ 的量子码, 其码长为 n, 维数为 k, 且能纠 $[(d-1)/2]$ 个量子错误. 如果 $C^{\perp_s}$ 中非零元素的最小重量也是 d, 则称 C 为纯的. 习惯上, 用 $[[n, k, d]]$ 来表示二元量子码.

设 S_n 是 n 阶对称群, $SP_2(p)$ 是 $GF(p)$ 上的二阶辛群 (它与 $GF(p)$ 上的特殊线性群 $SL_2(p)$ 同构), G_n 是 S_n 和 $SP_2(p)^n$ 自然构成的半直积. 显然, G_n 在 V_n 上有一个自然的作用 ($SP_2(p)^n$ 作用在码字的相应坐标上, 而 S_n 是对码字的坐标进行相应的置换). G_n 中的一个元素称为一个等价映射. 设 C 和 D 是 V_n 的两个辛码, 如果存在等价映射 $g \in G_n$, 使得 $g(C) = D$, 则称 C 和 D 是等价的. 显然, 一个等价映射 g 保持重量和辛内积, 而且 $g(C^{\perp_s}) = D^{\perp_s}$. 当 C 和 D 都是量子码 (C 和 D 都是辛码, 而且在辛内积意义下是自正交的) 时, 它们之间的等价就称为量子码的等价.

设 C 和 D 是两个 $GF(q)$ 上的 $[n, k]$ 线性码. 双射 $\varphi : C \to D$ 称为单项等价, 如果它可以由一个单项矩阵 M 诱导出来, 即 M 是一个置换矩阵与一个可逆对角矩阵之积, 使得对任意码字 $c = (c_1, c_2, \ldots, c_n) \in C$, 都有 $\varphi(c) = cM$. 显然, 如果两个线性码 C 和 D 是单项等价的, 则它们也是保距同构的. MacWilliams 的一个著名定理是说两个线性码是单项等价的当且仅当它们是保距同构的. 对于这一重要结果, Bogart 等人在文献 [15] 中给出了一个初等证明, Ward 和 Wood 二人在文献 [16] 中利用特征标理论给出了另一个证明. 进一步地发展特征标方法后, Wood 在文

献 [17] 中把这个结果推广到了有限 Frobenius 环上的线性码. 最近樊恽等人在文献 [18] 中又把该结果推广到了广义 Hamming 重量的情形. 本文研究了量子纠错码的等价性和保距同构, 推广了 Bogart 等人的一些概念, 并给出若干基本定理, 这些定理对进一步研究量子码的等价性和保距同构是非常有用的. 在此基础上构造出一个反例, 证明了在量子情形下, MacWilliams 的这个定理是不成立的, 即量子码的保距同构不一定是等价映射.

1 辛码的保距同构

定义 1 设 W_1 和 W_2 是 $GF(p)^k$ 的两个线性子空间, 若从 W_1 和 W_2 中分别任取向量 u_1 和 u_2, 都有 $(u_1,u_2)=0$, 则称 W_1 和 W_2 是相互正交的, 记为 $W_1\perp W_2$, 这里 (u_1,u_2) 是 u_1 和 u_2 的标准内积.

设 $L_1,L_2,\ldots,L_{\mu(k)}$ 和 $P_1,P_2,\ldots,P_{\nu(k)}$ 分别是 $GF(p)^k$ 的所有一维线性子空间和二维线性子空间. 显然

$$\mu(k)=(p^k-1)/(p-1),\quad \nu(k)=(p^k-1)(p^k-p)/(p^2-1)(p^2-p).$$

设 $S=(s_{ij})$ 和 $T=(t_{ij})$ 分别是有理数域上的 $\mu(k)\times\mu(k)$ 阶和 $\mu(k)\times\nu(k)$ 阶矩阵, 其中

$$s_{ij}=\begin{cases}0, & L_i\perp L_j,\\ 1, & \text{其它},\end{cases}\qquad t_{ij}=\begin{cases}0, & L_i\perp P_j,\\ 1, & \text{其它}.\end{cases}$$

由 S,T 可得有理数域上的矩阵 $R=(S\,T)$.

显然, 上面定义的矩阵 R 是文献 [15] 中矩阵 T 的自然推广.

设 C 是 V_n 的一个 k 维辛码, $X=(\alpha_1\beta_1\alpha_2\beta_2\cdots\alpha_n\beta_n)$ 是 C 的一个生成矩阵, 这里 α_i,β_i 是 k 维列向量, $1\le i\le n$, 任取行向量 $u\in GF(p)^k$, 令 $\sigma(u)=uX$, 则可得到一个线性同构映射 $\sigma:GF(p)^k\to C$.

设 $\alpha_1,\alpha_2,\ldots,\alpha_m\in GF^k(p)$, 用 $\langle\alpha_1,\alpha_2,\ldots,\alpha_m\rangle$ 表示由 $\alpha_1,\alpha_2,\ldots,\alpha_m$ 生成的线性子空间.

文献 [15] 中的列向量 r 可自然推广为下面的列向量 r^X.

定义 2 定义列向量 $s^X=(s_1^X,s_2^X,\ldots,s_{\mu(k)}^X)^t$, $t^X=(t_1^X,t_2^X,\ldots,t_{\nu(k)}^X)^t$ 和 $r^X=\binom{s^X}{t^X}$, 其中 $s_i^X=|\{(\alpha_j\beta_j)\,|\,\langle\alpha_j,\beta_j\rangle=L_i,1\le j\le n\}|$, $1\le i\le\mu(k)$, $t_i^X=|\{(\alpha_j\beta_j)\,|\,\langle\alpha_j,\beta_j\rangle=P_i,1\le j\le n\}|$, $1\le i\le\nu(k)$.

文献 [15] 中的引理 2 对于 Bogart 等人的证明是至关重要的, 现将其推广为下面的引理 1.

引理 1 Rr^X 的第 i 个分量 $(Rr^X)_i=w(\sigma(L_i))$, $1\le i\le\mu(k)$, 这里的 $w(\sigma(L_i))=w(\sigma(u_i))$, 其中 $0\ne u_i\in L_i$.

证明

$$\begin{aligned}(Rr^X)_i&=\left((S\ T)\binom{s^X}{t^X}\right)_i=(Ss^X+Tt^X)_i\\&=\sum_{j=1}^{\mu(k)}s_{ij}s_j^X+\sum_{j=1}^{\nu(k)}t_{ij}t_j^X=\sum_{L_j\not\perp L_i}s_j^X+\sum_{P_j\not\perp L_i}t_j^X\\&=\sum_{L_j\not\perp L_i}|\{(\alpha_{j'}\beta_{j'})\,|\,\langle\alpha_{j'},\beta_{j'}\rangle=L_j,1\le j'\le n\}|\\&\quad+\sum_{P_j\not\perp L_i}|\{(\alpha_{j'}\beta_{j'})\,|\,\langle\alpha_{j'},\beta_{j'}\rangle=P_j,1\le j'\le n\}|\\&=w(u_iX)=w(\sigma(u_i))=w(\sigma(L_i)).\end{aligned}$$

设 D 是 V_n 中的另一个辛码, $\varphi : C \to D$ 是一个线性同构, 将 φ 与前面的 σ 合成可得线性同构 $\tau : GF(p)^k \to D$. 令 $Y = \varphi(X)$, 则 Y 是 D 的一个生成矩阵.

定理 1 φ 是保距同构的充分必要条件是 $Rr^X = Rr^Y$, 即 $r^X - r^Y$ 是线性方程组 $Rx = 0$ 的一组解.

证明 φ 是保距同构的当且仅当对于任意的行向量 $u \in GF(p)^k$, 都有 $w(\varphi(uX)) = w(uX)$, 即 $w(\tau(u)) = w(\sigma(u))$, 亦即

$$w(\tau(u_i)) = w(\sigma(u_i)), \quad 1 \le i \le \mu(k),$$

这里的 $u_i \in GF(p)^k$, 且 $\langle u_i \rangle = L_i$, $1 \le i \le \mu(k)$. 所以, 由引理 1, φ 是保距同构的当且仅当对任意的 $1 \le i \le \mu(k)$, 都有 $(Rr^X)_i = (Rr^Y)_i$, 即 $Rr^X = Rr^Y$, 也就是说 $r^X - r^Y$ 是线性方程组 $Rx = 0$ 的一组解.

由定理 1 可知, 矩阵 R 对于研究辛码的保距同构是至关重要的, 因此有必要对其做进一步研究. 下面给出两个相关定理.

定理 2 S 在有理数域上是可逆的. 若记 $S^{-1} = (a_{ij})_{\mu(k)\times\mu(k)}$, 则

$$a_{ij} = \begin{cases} -\dfrac{p-1}{p^{k-1}}, & L_i \perp L_j, \\ \dfrac{1}{p^{k-1}}, & \text{其它.} \end{cases}$$

证明 由于

$$\sum_{l=1}^{\mu(k)} s_{il}s_{lj} = \begin{cases} \dfrac{p^k - p^{k-1}}{p-1} = p^{k-1}, & i = j, \\ \dfrac{p^k - 2p^{k-1} + p^{k-2}}{p-1} = p^{k-2}(p-1), & i \ne j, \end{cases}$$

所以

$$S^2 = \begin{pmatrix} p^{k-1} & p^{k-2}(p-1) & \cdots & p^{k-2}(p-1) \\ p^{k-2}(p-1) & p^{k-1} & \cdots & p^{k-2}(p-1) \\ \vdots & \vdots & \cdots & \vdots \\ p^{k-2}(p-1) & p^{k-2}(p-1) & \cdots & p^{k-1} \end{pmatrix}.$$

易知 S^2 在有理数域上是可逆的, 且

$$(S^2)^{-1} = \frac{1}{p^{2k-2}} \begin{pmatrix} p^k - (p-1) & -(p-1) & \cdots & -(p-1) \\ -(p-1) & p^k - (p-1) & \cdots & -(p-1) \\ \vdots & \vdots & \cdots & \vdots \\ -(p-1) & -(p-1) & \cdots & p^k - (p-1) \end{pmatrix}.$$

注意到 $S^{-1} = (S^2)^{-1}S$, 所以

$$a_{ij} = \begin{cases} -\dfrac{p-1}{p^{2k-2}} \cdot \dfrac{p^k - p^{k-1}}{p-1} = -\dfrac{p-1}{p^{k-1}}, & L_i \perp L_j, \\ \dfrac{p^k - (p-1)}{p^{2k-2}} - \dfrac{p-1}{p^{2k-2}} \cdot \Big(\dfrac{p^k - p^{k-1}}{p-1} - 1\Big) = \dfrac{1}{p^{k-1}}, & \text{其它.} \end{cases}$$

Bogart 等人在文献 [15] 中用与本文不同的方法证明了 S 是可逆的.

定理 3 记 $S^{-1}T = (a_{ij})_{\mu(k)\times\nu(k)}$, 则

$$a_{ij} = \begin{cases} \dfrac{1}{p}, & L_i \subseteq P_j, \\ 0, & \text{其它.} \end{cases}$$

证明 记 $S^{-1}=(b_{ij})_{\mu(k)\times\nu(k)}$.

(1) $L_i\subseteq P_j$,

$$\begin{aligned}a_{ij}&=\sum_{l=1}^{\mu(k)}b_{il}t_{lj}=\sum_{L_l\perp L_i,\,L_l\not\perp P_j}b_{il}t_{lj}+\sum_{L_l\not\perp L_i,\,L_l\not\perp P_j}b_{il}t_{lj}\\&=-\frac{p-1}{p^{k-1}}\cdot\frac{p^{k-1}-p^{k-2}}{p-1}+\frac{1}{p^{k-1}}\cdot\frac{p^k-p^{k-1}}{p-1}=\frac{1}{p}.\end{aligned}$$

(2) $L_i\not\subseteq P_j$,

$$\begin{aligned}a_{ij}&=\sum_{l=1}^{\mu(k)}b_{il}t_{lj}=\sum_{L_l\perp L_i,\,L_l\not\perp P_j}b_{il}t_{lj}+\sum_{L_l\not\perp L_i,\,L_l\not\perp P_j}b_{il}t_{lj}\\&=-\frac{p-1}{p^{k-1}}\cdot\frac{p^{k-1}-p^{k-3}}{p-1}+\frac{1}{p^{k-1}}\cdot\frac{p^k-p^{k-1}-p^{k-2}+p^{k-3}}{p-1}=0.\end{aligned}$$

2 量子码的保距同构

引理 2 设 C 是一个 $[[n,0,d]]_p$ 码, 也就是说 C 在辛内积意义下是自对偶的, 即 $C^{\perp_s}=C$,

$$X=(\alpha_1\beta_1\cdots\alpha_{m_1}\beta_{m_1}\alpha_{m_1+1}\beta_{m_1+1}\cdots\alpha_{m_1+m_2}\beta_{m_1+m_2}\alpha_{m_1+m_2+1}\beta_{m_1+m_2+1}\cdots\alpha_n\beta_n)$$

是 C 的一个生成矩阵, 这里的 $\alpha_i=(a_{1i},\ldots,a_{ni})^t$, $\beta_i=(b_{1i},\ldots,b_{ni})^t$, $1\le i\le n$, 且

$$\dim\langle\alpha_i,\beta_i\rangle=\begin{cases}2, & 1\le i\le m_1,\\ 1, & m_1+1\le i\le m_1+m_2,\\ 0, & m_1+m_2+1\le i\le n\end{cases}$$

(本文恒用 $\dim W$ 表示线性子空间 W 的维数), 则

(1) 矩阵 $(\alpha_1\beta_1\cdots\alpha_{m_1}\beta_{m_1})$ 生成的辛码 C_1 在辛内积意义下也是自对偶的;

(2) $m_1+m_2=n$;

(3) $\langle\alpha_i,\beta_i\rangle\not\subseteq\langle\alpha_1,\beta_1,\ldots,\alpha_{i-1},\beta_{i-1},\alpha_{i+1},\beta_{i+1},\ldots,\alpha_n,\beta_n\rangle$, $m_1+1\le i\le n$.

证明 记 $\gamma_i=((a_{i1},b_{i1}),\ldots,(a_{in},b_{in}))$, $\gamma_i'=((a_{i1},b_{i1}),\ldots,(a_{im_1},b_{im_1}))$, $1\le i\le n$.

由于对于任意的 $1\le i,j\le n$, $(\gamma_i',\gamma_j')_s=\sum_{l=1}^{m_1}(a_{il}b_{jl}-a_{jl}b_{il})=\sum_{l=1}^{n}(a_{il}b_{jl}-a_{jl}b_{il})=(\gamma_i,\gamma_j)_s=0$, 所以 C_1 在辛内积意义下是自正交的. 故 $\dim\langle\alpha_1,\beta_1,\ldots,\alpha_{m_1},\beta_{m_1}\rangle\le m_1$. 设 $\xi_1,\ldots,\xi_m$ 是 $\alpha_1,\beta_1,\ldots,\alpha_{m_1},\beta_{m_1}$ 的一个线性极大无关组, 显然 $m\le m_1$. 对任意的 $m_1+1\le i\le n$, 取 ξ_i, 使得 $\langle\alpha_i,\beta_i\rangle=\langle\xi_i\rangle$, 则 $\langle\xi_1,\ldots,\xi_m,\xi_{m_1+1},\ldots,\xi_n\rangle=\langle\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n\rangle$, 所以

$$\dim\langle\xi_1,\ldots,\xi_m,\xi_{m_1+1},\ldots,\xi_n\rangle=\dim\langle\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n\rangle=n.$$

因此, $m=m_1$, 同时 $\xi_1,\ldots,\xi_n$ 是线性无关的. 所以

(1) 矩阵 $(\alpha_1\beta_1\cdots\alpha_{m_1}\beta_{m_1})$ 生成的码 C_1 在辛内积意义下也是自对偶的;

(2) $m_1+m_2=n$;

(3) $\langle\alpha_i,\beta_i\rangle\not\subseteq\langle\alpha_1,\beta_1,\ldots,\alpha_{i-1},\beta_{i-1},\alpha_{i+1},\beta_{i+1},\ldots,\alpha_n,\beta_n\rangle$, $m_1+1\le i\le n$.

定理 4 设 C 是一个 $[[n,k,d]]_p$ 码

$$X=(\alpha_1\beta_1\cdots\alpha_m\beta_m\alpha_{m+1}\beta_{m+1}\cdots\alpha_n\beta_n)$$

是 $C^{\perp_s}$ 的一个生成矩阵, 这里 $\alpha_i,\beta_i\in GF(p)^{n+k}$, $1\le i\le n$, 且满足条件

$$\dim\langle\alpha_i,\beta_i\rangle=\begin{cases}2, & 1\le i\le m,\\ \le 1, & m+1\le i\le n.\end{cases}$$

则 $\langle\alpha_i,\beta_i\rangle \not\subseteq \langle\alpha_1,\beta_1,\ldots,\alpha_{i-1},\beta_{i-1},\alpha_{i+1},\beta_{i+1},\ldots,\alpha_n,\beta_n\rangle$, $m+1\le i\le n$.

证明 否则, 存在 $m+1\le i_0\le n$, 使得

$$\langle\alpha_{i_0},\beta_{i_0}\rangle \subseteq \langle\alpha_1,\beta_1,\ldots,\alpha_{i_0-1},\beta_{i_0-1},\alpha_{i_0+1},\beta_{i_0+1},\ldots,\alpha_n,\beta_n\rangle.$$

所以, 存在 $GF(p)$ 上的 $(2n-2)\times 2$ 矩阵 B, 使得

$$(\alpha_{i_0}\beta_{i_0}) = (\alpha_1\beta_1\cdots\alpha_{i_0-1}\beta_{i_0-1}\alpha_{i_0+1}\beta_{i_0+1}\cdots\alpha_n\beta_n)B.$$

由于 $C\subseteq C^{\perp_s}$, 所以存在辛内积意义下的自对偶码 D, 使得 $C\subseteq D=D^{\perp_s}\subseteq C^{\perp_s}$. 设 $X'=(\alpha_1'\beta_1'\cdots\alpha_n'\beta_n')$ 是 $D^{\perp_s}$ 的一个生成矩阵, 则存在 $GF(p)$ 上的 $n\times(n+k)$ 矩阵 A, 使得 $X'=AX$. 因此对任意的 $1\le i\le n$, 都有 $(\alpha_i'\beta_i')=A(\alpha_i\beta_i)$. 由于当 $m+1\le i\le n$ 时, $\dim\langle\alpha_i,\beta_i\rangle\le 1$, 故当 $m+1\le i\le n$ 时, $\dim\langle\alpha_i',\beta_i'\rangle\le 1$. 所以

$$\begin{aligned}(\alpha_{i_0}'\beta_{i_0}') &= A(\alpha_{i_0}\beta_{i_0}) = A(\alpha_1\beta_1\cdots\alpha_{i_0-1}\beta_{i_0-1}\alpha_{i_0+1}\beta_{i_0+1}\cdots\alpha_n\beta_n)B\\ &= (A(\alpha_1\beta_1)\cdots A(\alpha_{i_0-1}\beta_{i_0-1})A(\alpha_{i_0+1}\beta_{i_0+1})\cdots A(\alpha_n\beta_n))B\\ &= (\alpha_1'\beta_1'\cdots\alpha_{i_0-1}'\beta_{i_0-1}'\alpha_{i_0+1}'\beta_{i_0+1}'\cdots\alpha_n'\beta_n')B.\end{aligned}$$

这与引理 2 矛盾.

引理 3 取 $p=2$. 设 C 和 D 分别是 $[[n,k,d]]$ 码和 $[[n,k,d']]$ 码, 而

$$X=(\alpha_1^X\beta_1^X\alpha_2^X\beta_2^X\cdots\alpha_n^X\beta_n^X) \text{ 和 } Y=(\alpha_1^Y\beta_1^Y\alpha_2^Y\beta_2^Y\cdots\alpha_n^Y\beta_n^Y)$$

分别是 $C^{\perp_s}$ 和 $D^{\perp_s}$ 的生成矩阵, $\varphi: C^{\perp_s}\to D^{\perp_s}$ 是一个保距同构. 记 $S^{-1}T=(a_{ij})_{\mu(n+k)\times\nu(n+k)}$, 若存在 $1\le i_0\le\mu(n+k)$, 使得

$$\sum_{j=1}^{\nu(n+k)} a_{i_0j}(t_j^X-t_j^Y)\neq 0,$$

则对任意的 $1\le l, m\le\nu(n+k)$, 都有 $a_{i_0l}(t_l^X-t_l^Y)a_{i_0m}(t_m^X-t_m^Y)\ge 0$.

证明 否则, 存在 $1\le l_0, m_0\le\nu(n+k)$, 使得

$$a_{i_0l_0}(t_{l_0}^X-t_{l_0}^Y)a_{i_0m_0}(t_{m_0}^X-t_{m_0}^Y)<0.$$

因此, $a_{i_0l_0}(t_{l_0}^X-t_{l_0}^Y)$, $a_{i_0m_0}(t_{m_0}^X-t_{m_0}^Y)$ 中有一个与 $s_{i_0}^X-s_{i_0}^Y=-\sum_{j=1}^{\nu(n+k)}a_{i_0j}(t_j^X-t_j^Y)$ (定理 1)$\neq 0$ 同号. 不妨设 $a_{i_0l_0}(t_{l_0}^X-t_{l_0}^Y)$ 与 $s_{i_0}^X-s_{i_0}^Y$ 同号, 那么 L_{i_0}, P_{l_0} 在集合 $\{\langle\alpha_i^X,\beta_i^X\rangle\,|\,1\le i\le n\}$ 或在集合 $\{\langle\alpha_i^Y,\beta_i^Y\rangle\,|\,1\le i\le n\}$ 中同时出现. 由于 $a_{i_0l_0}\neq 0$, 所以由定理 3 可得 $L_{i_0}\subseteq P_{l_0}$. 这与定理 4 矛盾.

定理 5 取 $p=2$. 设 C 和 D 分别是 $[[n,k,d]]$ 码和 $[[n,k,d']]$ 码

$$X=(\alpha_1^X\beta_1^X\alpha_2^X\beta_2^X\cdots\alpha_n^X\beta_n^X) \quad \text{和} \quad Y=(\alpha_1^Y\beta_1^Y\alpha_2^Y\beta_2^Y\cdots\alpha_n^Y\beta_n^Y)$$

分别是 $C^{\perp_s}$ 和 $D^{\perp_s}$ 的生成矩阵, $\varphi: C^{\perp_s}\to D^{\perp_s}$ 是一个保距同构, 则 $s^X=s^Y$.

证明 记 $S^{-1}T=(a_{ij})_{\mu(n+k)\times\nu(n+k)}$.

如若不然, 则存在 $1\le i_0\le\mu(n+k)$, 使得 $s_{i_0}^X\neq s_{i_0}^Y$. 因而由定理 1 可得

$$\sum_{j=1}^{\nu(n+k)} a_{i_0j}(t_j^X-t_j^Y)=-(s_{i_0}^X-s_{i_0}^Y)\neq 0.$$

由引理 3, 要么对任意的 $1\le j\le\nu(n+k)$, $a_{i_0j}(t_j^X-t_j^Y)\ge 0$; 要么对任意的 $1\le j\le\nu(n+k)$, $a_{i_0j}(t_j^X-t_j^Y)\le 0$.

不妨设对任意的 $1\le j\le\nu(n+k)$, $a_{i_0j}(t_j^X-t_j^Y)\ge 0$.

由于 $\sum_{j=1}^{\nu(n+k)} a_{i_0 j}(t_j^X - t_j^Y) \neq 0$, 所以至少存在一个 $1 \leq j_0 \leq \nu(n+k)$, 使得 $a_{i_0 j_0}(t_{j_0}^X - t_{j_0}^Y) > 0$. 由于 $a_{i_0 j_0} \neq 0$, 所以由定理 3 可得 $L_{i_0} \subseteq P_{j_0}$. 注意到 P_{j_0} 共包含 3 个一维子空间, 所以存在不同的 $1 \leq i_0', i_0'' \leq \mu(n+k)$, 使得 $P_{j_0} = L_{i_0} \cup L_{i_0'} \cup L_{i_0''}$. 设 $L_{i_0} = \langle\alpha\rangle$, $L_{i_0'} = \langle\beta\rangle$, $L_{i_0''} = \langle\gamma\rangle$.

下面分四种情形讨论:

(1) $\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y) \neq 0$, $\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) \neq 0$.

由于

$$a_{ij} = \begin{cases} \dfrac{1}{p}, & L_i \subseteq P_j, \\ 0, & \text{其它}, \end{cases} \quad (\text{定理 3}),$$

所以由定理 1 可知 $s_{i_0}^X - s_{i_0}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0 j}(t_j^X - t_j^Y)$, $s_{i_0'}^X - s_{i_0'}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y)$, $s_{i_0''}^X - s_{i_0''}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) < 0$. 因此, $L_{i_0}, L_{i_0'}, L_{i_0''}$ 同时在集合 $\{\langle\alpha_i^Y, \beta_i^Y\rangle \,|\, 1 \leq i \leq n\}$ 中出现. 设 $L_{i_0} = \langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle$, $L_{i_0'} = \langle\alpha_{i_1'}^Y, \beta_{i_1'}^Y\rangle$, $L_{i_0''} = \langle\alpha_{i_1''}^Y, \beta_{i_1''}^Y\rangle$, 则 $\langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle \subseteq \langle\alpha_{i_1'}^Y, \beta_{i_1'}^Y, \alpha_{i_1''}^Y, \beta_{i_1''}^Y\rangle$. 这与定理 4 矛盾.

(2) $\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y) \neq 0$, $\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) = 0$.

由于 $\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) = 0$, 且 $a_{i_0'' j_0}(t_{j_0}^X - t_{j_0}^Y) > 0$ ($L_{i_0''} \subseteq P_{j_0}$ 及 $t_{i_0}^X - t_{j_o}^Y > 0$), 所以存在 $1 \leq j_0' \leq \nu(n+k)$, 使得 $a_{i_0'' j_0'}(t_{j_0'}^X - t_{j_0'}^Y) < 0$, 故 $t_{j_0'}^X - t_{j_0'}^Y < 0$ 且 $a_{i_0'' j_0'} \neq 0$. 再由定理 1, 可得

$$s_{i_0}^X - s_{i_0}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0 j}(t_j^X - t_j^Y), s_{i_0'}^X - s_{i_0'}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y) < 0,$$

所以 $L_{i_0}, L_{i_0'}, P_{j_0'}$ 同时在集合 $\{\langle\alpha_i^Y, \beta_i^Y\rangle \,|\, 1 \leq i \leq n\}$ 中出现. 设 $L_{i_0} = \langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle$, $L_{i_0'} = \langle\alpha_{i_1'}^Y, \beta_{i_1'}^Y\rangle$, $P_{j_0'} = \langle\alpha_{j_1'}^Y, \beta_{j_1'}^Y\rangle$. 由于 $a_{i_0'' j_0'} \neq 0$, 所以由定理 3 可知 $L_{i_0''} \subseteq P_{j_0'}$. 因此 $\gamma \in P_{j_0'}$, 但是 $\alpha = \beta + \gamma$, 所以 $\langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle \subseteq \langle\alpha_{i_1'}^Y, \beta_{i_1'}^Y, \alpha_{j_1'}^Y, \beta_{j_1'}^Y\rangle$. 这与定理 4 矛盾.

(3) $\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y) = 0$, $\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) \neq 0$.

证明与 (2) 类似.

(4) $\sum_{j=1}^{\nu(n+k)} a_{i_0' j}(t_j^X - t_j^Y) = 0$, $\sum_{j=1}^{\nu(n+k)} a_{i_0'' j}(t_j^X - t_j^Y) = 0$.

由于 $a_{i_0 j_0}(t_{j_0}^X - t_{j_0}^Y) > 0$, 所以 $a_{i_0' j_0}(t_{j_0}^X - t_{j_0}^Y) > 0$, $a_{i_0'' j_0}(t_{j_0}^X - t_{j_0}^Y) > 0$, 因此存在 $1 \leq j_0', j_0'' \leq \nu(n+k)$, 使得 $a_{i_0' j_0'}(t_{j_0'}^X - t_{j_0'}^Y)$, $a_{i_0'' j_0''}(t_{j_0''}^X - t_{j_0''}^Y) < 0$. 但是 $s_{i_0}^X - s_{i_0}^Y = -\sum_{j=1}^{\nu(n+k)} a_{i_0 j}(t_j^X - t_j^Y) < 0$, 所以 $L_{i_0}, P_{j_0'}, P_{j_0''}$ 同时在集合 $\{\langle\alpha_i^Y, \beta_i^Y\rangle \,|\, 1 \leq i \leq n\}$ 中出现. 设 $L_{i_0} = \langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle$, $P_{j_0'} = \langle\alpha_{j_1'}^Y, \beta_{j_1'}^Y\rangle$, $P_{j_0''} = \langle\alpha_{j_1''}^Y, \beta_{j_1''}^Y\rangle$. 由于 $a_{i_0' j_0'} \neq 0$, $a_{i_0'' j_0''} \neq 0$, 所以由定理 3 可得

$$L_{i_0'} \subseteq P_{j_0'}, \quad L_{i_0''} \subseteq P_{j_0''},$$

故 $\beta \in P_{j_0'}$, $\gamma \in P_{j_0''}$. 注意到 $\alpha = \beta + \gamma$, 所以 $\langle\alpha_{i_1}^Y, \beta_{i_1}^Y\rangle \subseteq \langle\alpha_{j_1'}^Y, \beta_{j_1'}^Y, \alpha_{j_1''}^Y, \beta_{j_1''}^Y\rangle$. 这与定理 4 矛盾.

3 应用

3.1 一个反例

先给出两个关于等价映射的定理.

定理 6 设 C 和 D 是 V_n 的两个 k 维辛码, $X = (\alpha_1^X \beta_1^X \alpha_2^X \beta_2^X \cdots \alpha_n^X \beta_n^X)$ 和 $Y = (\alpha_1^Y \beta_1^Y \alpha_2^Y \beta_2^Y \cdots \alpha_n^Y \beta_n^Y)$ 分别是 C 和 D 的生成矩阵, $g \in G_n$ 是一个等价映射, 且 $Y = gX$, 则

$$\sum_{i=1}^{\mu(k)} s_i^X = \sum_{i=1}^{\mu(k)} s_i^Y, \quad t_i^X = t_i^Y, \quad 1 \leq i \leq \nu(k).$$

证明 任取 $A \in SP_2(p)$, 列向量 $\alpha,\beta \in GF(p)^k$, 记 $(\alpha'\beta') = (\alpha\beta)A$, 则 $\dim\langle\alpha',\beta'\rangle = \dim\langle\alpha,\beta\rangle$, 且当 $\dim\langle\alpha,\beta\rangle = 2$ 时, $\langle\alpha',\beta'\rangle = \langle\alpha,\beta\rangle$. 由于 $g \in G_n$, 所以存在 $A_i \in SP_2(p)$, $1 \le i \le n$, 使得 $gX = ((\alpha_{i_1}^X\beta_{i_1}^X)A_1(\alpha_{i_2}^X\beta_{i_2}^X)A_2\cdots(\alpha_{i_n}^X\beta_{i_n}^X)A_n)$. 再由 $Y = gX$ 可知定理成立.

定理 7 设 $p = 2$, C 和 D 是 V_n 中的两个 k 维辛码, $X = (\alpha_1^X\beta_1^X\alpha_2^X\beta_2^X\cdots\alpha_n^X\beta_n^X)$ 和 $Y = (\alpha_1^Y\beta_1^Y\alpha_2^Y\beta_2^Y\cdots\alpha_n^Y\beta_n^Y)$ 分别是 C 和 D 的生成矩阵. 则 C 和 D 是等价的, 即存在 $g \in G_n$, 使得 $Y = gX$ 的充分必要条件是

$$\sum_{i=1}^{\mu(k)} s_i^X = \sum_{i=1}^{\mu(k)} s_i^Y \ \text{ 和 } \ t_i^X = t_i^Y, \ \ 1 \le i \le \nu(k).$$

证明 由于 $SP_2(2)$ 与 $GF(2)$ 上的一般线性群 $GL_2(2)$ 同构, 所以对于任意的列向量 $\alpha,\beta,\xi,\eta \in GF(2)^k$, 如果 $\langle\alpha,\beta\rangle = \langle\xi,\eta\rangle$, 那么存在 $A \in SP_2(2)$, 使得 $(\xi\eta) = (\alpha\beta)A$. 因此如果 $\sum_{i=1}^{\mu(k)} s_i^X = \sum_{i=1}^{\mu(k)} s_i^Y$ 和 $t_i^X = t_i^Y$, $1 \le i \le \nu(k)$, 则存在 $g \in G_n$, 使得 $Y = gX$. 再由定理 6 可知定理成立.

设 $p = 2$, $k = 4$, 则 $\mu(k) = 15$, $\nu(k) = 35$. 记

$\gamma_1 = (1,0,0,0)^t$, $\gamma_2 = (0,1,0,0)^t$, $\gamma_3 = (1,1,0,0)^t$, $\gamma_4 = (0,0,1,0)^t$, $\gamma_5 = (1,0,1,0)^t$,

$\gamma_6 = (0,1,1,0)^t$, $\gamma_7 = (1,1,1,0)^t$, $\gamma_8 = (0,0,0,1)^t$, $\gamma_9 = (1,0,0,1)^t$, $\gamma_{10} = (0,1,0,1)^t$,

$\gamma_{11} = (1,1,0,1)^t$, $\gamma_{12} = (0,0,1,1)^t$, $\gamma_{13} = (1,0,1,1)^t$, $\gamma_{14} = (0,1,1,1)^t$, $\gamma_{15} = (1,1,1,1)^t$;

$L_1 = \langle\gamma_1\rangle$, $L_2 = \langle\gamma_2\rangle$, $L_3 = \langle\gamma_3\rangle$, $L_4 = \langle\gamma_4\rangle$, $L_5 = \langle\gamma_5\rangle$, $L_6 = \langle\gamma_6\rangle$, $L_7 = \langle\gamma_7\rangle$, $L_8 = \langle\gamma_8\rangle$,

$L_9 = \langle\gamma_9\rangle$, $L_{10} = \langle\gamma_{10}\rangle$, $L_{11} = \langle\gamma_{11}\rangle$, $L_{12} = \langle\gamma_{12}\rangle$, $L_{13} = \langle\gamma_{13}\rangle$, $L_{14} = \langle\gamma_{14}\rangle$, $L_{15} = \langle\gamma_{15}\rangle$;

$P_1 = \langle\gamma_1,\gamma_2\rangle$, $P_2 = \langle\gamma_1,\gamma_4\rangle$, $P_3 = \langle\gamma_1,\gamma_6\rangle$, $P_4 = \langle\gamma_1,\gamma_8\rangle$, $P_5 = \langle\gamma_1,\gamma_{10}\rangle$,

$P_6 = \langle\gamma_1,\gamma_{12}\rangle$, $P_7 = \langle\gamma_1,\gamma_{14}\rangle$, $P_8 = \langle\gamma_2,\gamma_4\rangle$, $P_9 = \langle\gamma_2,\gamma_5\rangle$, $P_{10} = \langle\gamma_2,\gamma_8\rangle$,

$P_{11} = \langle\gamma_2,\gamma_9\rangle$, $P_{12} = \langle\gamma_2,\gamma_{12}\rangle$, $P_{13} = \langle\gamma_2,\gamma_{13}\rangle$, $P_{14} = \langle\gamma_3,\gamma_4\rangle$, $P_{15} = \langle\gamma_3,\gamma_5\rangle$,

$P_{16} = \langle\gamma_3,\gamma_8\rangle$, $P_{17} = \langle\gamma_3,\gamma_9\rangle$, $P_{18} = \langle\gamma_3,\gamma_{12}\rangle$, $P_{19} = \langle\gamma_3,\gamma_{13}\rangle$, $P_{20} = \langle\gamma_4,\gamma_8\rangle$,

$P_{21} = \langle\gamma_4,\gamma_9\rangle$, $P_{22} = \langle\gamma_4,\gamma_{10}\rangle$, $P_{23} = \langle\gamma_4,\gamma_{11}\rangle$, $P_{24} = \langle\gamma_5,\gamma_8\rangle$, $P_{25} = \langle\gamma_5,\gamma_9\rangle$,

$P_{26} = \langle\gamma_5,\gamma_{10}\rangle$, $P_{27} = \langle\gamma_5,\gamma_{11}\rangle$, $P_{28} = \langle\gamma_6,\gamma_8\rangle$, $P_{29} = \langle\gamma_6,\gamma_9\rangle$, $P_{30} = \langle\gamma_6,\gamma_{10}\rangle$,

$P_{31} = \langle\gamma_6,\gamma_{11}\rangle$, $P_{32} = \langle\gamma_7,\gamma_8\rangle$, $P_{33} = \langle\gamma_7,\gamma_9\rangle$, $P_{34} = \langle\gamma_7,\gamma_{10}\rangle$, $P_{35} = \langle\gamma_7,\gamma_{11}\rangle$.

根据定理 5 和定理 7, 为了得到一个不是等价映射的二元量子码的保距同构, 需要找线性方程组 $S^{-1}Tx = 0$ 的一组非零整数解. 由定理 3 可得

$$S^{-1}T = \frac{1}{2}\begin{pmatrix}
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&1&0&0&1&0&0&1&0&0&0&1&0&0&0&0
\end{pmatrix}.$$

由此确定线性方程组 $S^{-1}Tx=0$ 的一组非零整数解 $x_0=(0,1,1,-1,-1,0,0,-1,-1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)^t$.

由此可构造 $GF(2)$ 上两个矩阵

$$X=\begin{pmatrix} 10 & 10 & 00 & 01\\ 00 & 01 & 10 & 10\\ 01 & 01 & 00 & 00\\ 00 & 00 & 01 & 01 \end{pmatrix} \text{ 和 } Y=\begin{pmatrix} 10 & 10 & 00 & 01\\ 00 & 01 & 10 & 10\\ 00 & 00 & 01 & 01\\ 01 & 01 & 00 & 00 \end{pmatrix}.$$

显然, X 和 Y 生成同一个 $[[4,0,2]]$ 码 C, 对应的 $t^X=(0,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)^t$, $t^Y=(0,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)^t$, 且 $x_0=t^X-t^Y$. 令 $\varphi: C\to C$, 使得 $Y=\varphi(X)$. 由定理 1, φ 是一个保距同构, 但由定理 6, $\varphi\notin G_4$, 即 φ 不是一个等价映射. 因此, 在量子情形下, MacWilliams 定理不成立.

由于量子码的一个等价映射是保持辛内积的, 所以一个自然的问题是: 量子码的保持辛内积的保距同构是不是等价映射呢? 对于这个问题, 下面的定理 8 给出了一个否定的回答.

定理 8 设 $p=2$, C 和 D 是 V_n 中的两个辛码, $\varphi: C\to D$ 是一个线性同构, 若 φ 是保距同构, 则 φ 保持辛内积.

证明 任取 $\alpha,\beta\in C$, $\alpha\neq\beta$, 设 $\alpha=((a_1,b_1),\ldots,(a_n,b_n))$, $\beta=((c_1,d_1),\ldots,(c_n,d_n))$. 记 $\varphi(\alpha)=((a_1',b_1'),\ldots,(a_n',b_n'))$, $\varphi(\beta)=((c_1',d_1'),\ldots,(c_n',d_n'))$. 令 n_1 为集合

$$\left\{\begin{pmatrix} a_i & b_i\\ c_i & d_i\end{pmatrix}\,\middle|\, 1\le i\le n\right\}$$

中可逆矩阵的个数, n_2,n_3 和 n_4 分别为集合

$$\left\{\begin{pmatrix} a_i & b_i\\ c_i & d_i\end{pmatrix}\,\middle|\, 1\le i\le n\right\} \text{ 中形如 } \begin{pmatrix} x & y\\ x & y\end{pmatrix},\ \begin{pmatrix} x & y\\ 0 & 0\end{pmatrix} \text{ 和 } \begin{pmatrix} 0 & 0\\ x & y\end{pmatrix}$$

的矩阵的个数, 这里的 $(x,y)\neq 0$. 类似地, 令 n_1' 为集合 $\{\left(\begin{smallmatrix} a_i' & b_i'\\ c_i' & d_i'\end{smallmatrix}\right)\,|\,1\le i\le n\}$ 中可逆矩阵的个数, n_2',n_3' 和 n_4' 分别为集合

$$\left\{\begin{pmatrix} a_i' & b_i'\\ c_i' & d_i'\end{pmatrix}\,\middle|\, 1\le i\le n\right\} \text{ 中形如 } \begin{pmatrix} x & y\\ x & y\end{pmatrix},\ \begin{pmatrix} x & y\\ 0 & 0\end{pmatrix} \text{ 和 } \begin{pmatrix} 0 & 0\\ x & y\end{pmatrix}$$

的矩阵的个数, 这里的 $(x,y)\neq 0$. 由于 $w(\varphi(\alpha))=w(\alpha)$, $w(\varphi(\beta))=w(\beta)$, $w(\varphi(\alpha)+\varphi(\beta))=w(\varphi(\alpha+\beta))=w(\alpha+\beta)$, 所以

$$\begin{cases} n_1+n_2+n_3=n_1'+n_2'+n_3',\\ n_1+n_2+n_4=n_1'+n_2'+n_4',\\ n_1+n_3+n_4=n_1'+n_3'+n_4', \end{cases} \text{ 即 } \begin{cases} (n_1-n_1')+(n_2-n_2')+(n_3-n_3')=0,\\ (n_1-n_1')+(n_2-n_2')+(n_4-n_4')=0,\\ (n_1-n_1')+(n_3-n_3')+(n_4-n_4')=0. \end{cases}$$

因此 $(n_1-n_1',n_2-n_2',n_3-n_3',n_4-n_4')^t$ 是线性方程组

$$\begin{cases} x_1+x_2+x_3=0,\\ x_1+x_2+x_4=0,\\ x_1+x_3+x_4=0 \end{cases}$$

的一个解. 注意到这个线性方程组的通解为 $a(-2,1,1,1)^t$, 故 n_1-n_1' 是个偶数. 由于 $(\varphi(\alpha),\varphi(\beta))_s=n_1'=n_1=\sum_{i=1}^n(a_id_i-b_ic_i)=(\alpha,\beta)_s$, 所以 φ 保持辛内积.

3.2 V_n 上的保距同构

定理 9 设 φ 是 V_n 上的一个保距同构, 那么 φ 也是一个等价映射.

证明 设 $X=(\alpha_1^X\beta_1^X\alpha_2^X\beta_2^X\cdots\alpha_n^X\beta_n^X)$ 和 $Y=(\alpha_1^Y\beta_1^Y\alpha_2^Y\beta_2^Y\cdots\alpha_n^Y\beta_n^Y)$ 是 V_n 的两个生成矩阵, 且 $Y=\varphi X$. 由于 X 和 Y 的秩都是 $2n$, 所以

$$s_i^X=s_i^Y=0,\quad 1\le i\le\mu(2n).$$

因此只需要证明 $t_j^X=t_j^Y$, $1\le j\le\nu(2n)$ 即可.

否则, 存在 $1\le j_0\le\nu(2n)$, 使得 $t_{j_0}^X\ne t_{j_0}^Y$, 不妨设 $t_{j_0}^X-t_{j_0}^Y>0$.

设 P_{j_0} 的三个不同一维子空间为 $L_{i_1}=\langle\alpha\rangle$, $L_{i_2}=\langle\beta\rangle$, $L_{i_3}=\langle\gamma\rangle$. 显然 α,β,γ 中至少有一个向量可由另外两个向量线性表出, 不妨设 α 可由 β,γ 线性表出.

由于 φ 是一个保距同构, 所以由定理 1 和定理 2 可知 t^X-t^Y 是线性方程组 $S^{-1}Tx=0$ 的一个非零解. 由 $S^{-1}T(t^X-t^Y)=0$ 的第 i_1,i_2,i_3 个等式可知, 存在不同的 j_1,j_2,j_3, 使得

$$L_{i_1}\subseteq P_{j_1},\quad L_{i_2}\subseteq P_{j_2},\quad L_{i_3}\subseteq P_{j_3}\ \text{且}\ t_{j_1}^X-t_{j_1}^Y,\quad t_{j_2}^X-t_{j_2}^Y,\quad t_{j_3}^X-t_{j_3}^Y<0,$$

即 P_{j_1},P_{j_2},P_{j_3} 在集合 $\{\langle\alpha_j^Y,\beta_j^Y\rangle\,|\,1\le j\le n\}$ 中同时出现, 不妨设 $P_{j_1}=\langle\alpha_{j_1'}^Y,\beta_{j_1'}^Y\rangle$, $P_{j_2}=\langle\alpha_{j_2'}^Y,\beta_{j_2'}^Y\rangle$, $P_{j_3}=\langle\alpha_{j_3'}^Y,\beta_{j_3'}^Y\rangle$. 由于 $\alpha\in P_{j_1}$, $\beta\in P_{j_2}$, $\gamma\in P_{j_3}$, 所以

$$\langle\alpha_{j_1'}^Y,\beta_{j_1'}^Y\rangle\cap\langle\alpha_{j_2'}^Y,\beta_{j_2'}^Y,\alpha_{j_3'}^Y,\beta_{j_3'}^Y\rangle\ne\{0\},$$

这与 Y 的秩是 $2n$ 相矛盾.

参 考 文 献

[1] Shor P. W., Scheme for reducing decoherence in quantum memory, *Phys. Rev. A*, 1995, **52**: 2493.

[2] Steane A. M., Multiple particle interference and quantum error correction, *Proc. Roy. Soc. London A*, 1996, **452**: 2551–2557.

[3] Calderbank A. R., Rains E. M., Shor P. W. et al., Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory*, 1998, **44**(7): 1369–1387.

[4] Rains E. M., Nonbinary quantum codes, *IEEE Trans. Inform. Theory*, 1999, **45**(9): 1827–1832.

[5] Ashikhmim A., Knill E., Nonbinary quantum stabilizer codes, *IEEE Trans. Inform. Theory*, 2001, **47**(11): 3065–3072.

[6] Matsumoto R., Uyematsu T., Constructing quantum Error-correcting codes for p^m-state sysetems from classical Error-correcting codes, 1999, quant-ph/9911011.

[7] Feng K. Q., Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ ($p\ge3$) exist, *IEEE Trans. Inform. Theory*, 2002, **48**(8): 2384–2391.

[8] Feng K. Q., Ma Z., A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, *IEEE Trans. Inform. Theory*, 2004, **50**(12): 3323–3325.

[9] Chen H., Some good quantum Error-correcting codes from Algebric-geometric codes, *IEEE Trans. Inform. Theory*, 2001, **47**(5): 2059–2061.

[10] Chen H., Ling S., Xing C. P., Quantum codes from concatenated Algebric-geometric codes, *IEEE Trans. Inform. Theory*, 2005, **51**(8): 2915–2920.

[11] Lin X. Y., Quantum cyclic and constacyclic codes, *IEEE Trans. Inform. Theory*, 2004, **50**(3): 547–549.

[12] Li R. H., Li X. L., Binary construction of quantum codes of minimum distance three and four, *IEEE Trans. Inform. Theory*, 2004, **50**(6): 1331–1336.

[13] Liu T. L., Wen Q. Y., Liu Z. H., Construction of nonbinary quantum cyclic codes by using graph method, *Science in China, Ser. F*, 2005, **48**(6): 693–702.

[14] Liu T. L., Wen F. T., Wen Q. Y., On the automorphism groups of a family of binary quantum Error-Correcting codes, *International Journal of Quantum Information*, 2006, **4**(6): 1013–1022.

[15] Bogart K., Goldberg D., Gordon J., An elementary proof of the macWilliams theorem on equivalence of codes, *Inform and Control*, 1978, **37**: 19–22.

[16] Ward H. N., Wood J. A., Characters and the equivalence of codes, *J. Combin Theory, Ser A*, 1996, **73**: 348–352.

[17] Wood J. A., Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.*, 1999, **121**: 555–575.

[18] Fan Y., Liu H. W., Lluis P., Generalized hanmming weights and equivalence of codes, *Science in China, Ser. A*, 2003, **46**(5): 690–695.