文章编号: 1673-1549(2011)01-0032-03

非平凡向量空间稳定子的刻划

程　茜[1], 于　慧[2]

(1.青海师范大学数学系, 西宁　810008; 2.大连交通大学数理系, 辽宁　大连　116028)

摘　要: 利用 Pauli群的子群可成为非平凡向量空间的稳定子的充要条件, 刻划了 Pauli群 G_1 的子群能成为非平凡向量空间 V_S 稳定子的所有稳定子, 并由此得到对于 Pauli群 G_n 而言, 构成非平凡向量空间 V_S 稳定子的生成元中算子的性质。

关键词: Pauli群; 稳定子; 生成元

中图分类号: O151.24　　文献标识码: A

量子计算技术的计算能力强大, 但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[1-7]。它的基本思想是将 k位量子比特嵌入到 n(n> k)位量子比特中, 以达到对量子信息的保护。迄今为止, 多种量子纠错码以及相关理论已经被发现和提出, 其中以 CSS码[2-3]和稳定子码[4]最为重要和成熟, 不少学者利用量子稳定子码构造了一系列量子码[5-6], 可见稳定子体系极其适合描述量子码。稳定子体系的中心思路可通过一个例子容易地来说明。考虑双量子比特的

$$|\psi\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

容易验证, 这个状态满足恒等式 $X_1X_2|\psi\rangle=|\psi\rangle$和 $Z_1Z_2|\psi\rangle=|\psi\rangle$, 于是称这个状态被算子 X_1X_2 和 Z_1Z_2 稳定。有点不太显然的是, 状态 $|\psi\rangle$是用这些算子 X_1X_2 和 Z_1Z_2 稳定的唯一量子状态(除了一个全局相位)。稳定子体系的基本思想是, 比之用显式的研究状态自身, 许多量子状态可通过它们的算子更容易描述, 这就导出, 比之用状态向量描述, 许多量子码(包括 CSS码和 Shor码)可用稳定子得到更为简洁的描述, 更为重要的是, 量子比特上的差错, 各种运算如 Hadamard门、相位门和受控非门, 以及计算机中的测量, 所有这一切都可以用稳定子形式来容易地描述。使稳定子体系强有力的关键在于群论的灵活运用, 最主要的群是 n个量子比特上的 Pauli群 G_n。对于单量子比特, Pauli群定义为由所有 Pauli矩阵与 ±1, $\pm i$相乘组成: $G_1\equiv\{\pm I,\ \pm iI,\ \pm X,\ \pm iX,\ \pm Y,\ \pm iY,\ \pm Z,\ \pm iZ\}$, 这个矩阵集合构成矩阵乘法运算下的一个群。Pauli群 G_n 定义为由 Pauli矩阵的所有 n重张量积所组成, 且允许有乘子 ±1, $\pm i$。稳定子定义为: 设 S为 G_n 的一个子群, V_S 为由 S的每个元所固定的 n量子比特状态的集合, V_S 为由 S所稳定的向量空间, S被称为空间 V_S 的稳定子。本文讨论对于 Pauli群 G_1的子群能成为非平凡向量空间 V_S的稳定子的所有稳定子。

1　稳定子的生成元

设 S为 G_n的一个子群, V_S 为由 S所稳定的向量空间, S是空间 V_S 的稳定子。在检验 V_S 由 S稳定时, 只需检验 V_S 可由 S的生成元稳定, 事实上, 设 S的生成元是 $g_1, g_2\cdots g_l$, 即 $S=\langle g_1, g_2\cdots g_l\rangle$, 所以任意 S中的元 g都可被写为序列 $g_1, g_2\cdots g_l$ 的乘积; 若任意 V_S 中的元 $|\psi\rangle$能由 $g_1, g_2, \cdots, g_l$稳定, 即 $g_i|\psi\rangle=|\psi\rangle$, $i=1,2,\cdots,l$, 当然 g可稳定 $|\psi\rangle$。因而可通过生成元来描述群

收稿日期: 2010-10-18

基金项目: 青海师范大学科研基金资助项目(20094)

作者简介: 程　茜(1975-), 女, 重庆长寿人, 副教授, 硕士, 主要从事半群代数、量子编码方面的研究。

S, 这样为描述群 S 提供了一个简洁的手段。

文献 [1]关于稳定子生成元的几个重要命题。

定理 1 令 $S = \langle g_1, g_2 \cdots g_l \rangle$, 则当且仅当对所有 j 有 $g_j^2 = I$和对所有 j有 $g_j \neq -I$, $-I$不是 S的一个元。

并非 Pauli群的任一子群 S 都可被用作非平凡向量空间的稳定子, 文献 [1]给出:

定理 2 S稳定一个非平凡向量空间 V_S 的充分必要条件是 S由独立的可对易生成元生成且 $-I \notin S$。

2 能稳定非平凡向量空间 V_S 的 Pauli群 G_1 的子群

对于 Pauli群 $G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$, 为考察稳定非平凡向量空间 V_S 的 G_1 的子群, 给出 G_1 的乘法表 (表 1)。

表 1 Pauli群 G_1 的乘法运算表

	I	$-I$	iI	$-iI$	X	$-X$	iX	$-iX$	Y	$-Y$	iY	$-iY$	Z	$-Z$	iZ	$-iZ$
I	I	$-I$	iI	$-iI$	X	$-X$	iX	$-iX$	Y	$-Y$	iY	$-iY$	Z	$-Z$	iZ	$-iZ$
$-I$	$-I$	I	$-iI$	iI	$-X$	X	$-iX$	iX	$-Y$	Y	$-iY$	iY	$-Z$	Z	$-iZ$	iZ
iI	iI	$-iI$	$-I$	I	iX	$-iX$	$-X$	X	iY	$-iY$	$-Y$	Y	iZ	$-iZ$	$-Z$	Z
$-iI$	$-iI$	iI	I	$-I$	$-iX$	iX	X	$-X$	$-iY$	iY	Y	$-Y$	$-iZ$	iZ	Z	$-Z$
X	X	$-X$	iX	$-iX$	I	$-I$	iI	$-iI$	iZ	$-iZ$	$-Z$	Z	$-iY$	iY	Y	$-Y$
$-X$	$-X$	X	$-iX$	iX	$-I$	I	$-iI$	iI	$-iZ$	iZ	Z	$-Z$	iY	$-iY$	$-Y$	Y
iX	iX	$-iX$	$-X$	X	iI	$-iI$	$-I$	I	$-Z$	Z	$-iZ$	iZ	Y	$-Y$	iY	$-iY$
$-iX$	$-iX$	iX	X	$-X$	$-iI$	Ii	I	$-I$	Z	$-Z$	iZ	$-iZ$	$-Y$	Y	$-iY$	iY
Y	Y	$-Y$	iY	$-iY$	$-iZ$	iZ	Z	$-Z$	I	$-I$	iI	$-iI$	iX	$-iX$	$-X$	X
$-Y$	$-Y$	Y	$-iY$	iY	iZ	$-iZ$	$-Z$	Z	$-I$	I	$-iI$	iI	$-iX$	iX	X	$-X$
iY	iY	$-iY$	$-Y$	Y	Z	$-Z$	iZ	$-iZ$	iI	$-iI$	$-I$	I	$-X$	X	$-iX$	iX
$-iY$	$-iY$	iY	Y	$-Y$	$-Z$	Z	$-iZ$	iZ	$-iI$	iI	I	$-I$	X	$-X$	iX	$-iX$
Z	Z	$-Z$	iZ	$-iZ$	iY	$-iY$	$-Y$	Y	$-iX$	iX	X	$-X$	I	$-I$	$-iI$	iI
$-Z$	$-Z$	Z	$-iZ$	iZ	$-iY$	iY	Y	$-Y$	iX	$-iX$	$-X$	X	$-I$	I	iI	$-iI$
iZ	iZ	$-iZ$	$-Z$	Z	$-Y$	Y	$-iY$	iY	X	$-X$	iX	$-iX$	iI	$-iI$	$-I$	I
$-iZ$	$-iZ$	iZ	Z	$-Z$	Y	$-Y$	iY	$-iY$	$-X$	X	$-iX$	iX	$-iI$	iI	I	$-I$

定理 3 Pauli群 G_1 的子群能成为非平凡向量空间 V_S 的稳定子的所有稳定子为 $S_1 = \langle X \rangle$, $S_2 = \langle -X \rangle$, $S_3 = \langle Y \rangle$, $S_4 = \langle -Y \rangle$, $S_5 = \langle Z \rangle$, $S_6 = \langle -Z \rangle$。

证明 首先考虑 G_1 的子群, 由 Lagrange定理[1] (如果 S是有限群 G 的子群, 则 S 的阶 $|S|$整除 G 的阶 $|G|$)知, 因为 $|G| = 16$, 所以 $|S|$ 只可能等于 1, 2, 4, 8, 16, 分以下五种情形讨论:

(1)若 $|S| = 1$, 且 S要成为 G_1 的子群, 则 $S = \{I\}$ 即 $S = \langle I \rangle$, 但此时生成元 I不独立, 这与定理 2中要求生成元独立不符合, 因此 $S \neq \{I\}$。

(2)若 $|S| = 16$, 则 $S = G_1$, 当然 $-I \in S$, 这与定理 2中 $-I \notin S$相矛盾, 因此 $S \neq G_1$。

(3)若 $|S| = 2$, 且 S要成为 G_1 的子群, 则单位元 I 必属于 S; 又因为定理 2中 $-I \notin S$和子群中的元对乘法有封闭性, S中的另一个元一定不是 $\pm iW$, $W = I, X, Y, Z$。再由表 1知, $S = \{I, X\}$, $\{I, -X\}$, $\{I, Y\}$, $\{I, -Y\}$, $\{I, Z\}$, $\{I, -Z\}$, 或 $S = \langle X \rangle$, $\langle -X \rangle$, $\langle Y \rangle$, $\langle -Y \rangle$, $\langle Z \rangle$, $\langle -Z \rangle$。

(4)若 $|S| = 4$, 同情形 (3)讨论一样, S 要成为 G_1 的子群, 且满足 $-I \notin S$, 则 S中除元 I外, 其它三个元只能在元 $\pm X$, $\pm Y$, $\pm Z$ 中选取, 如此一来, 由表 1中的运算知 S的元又不满足封闭性, 因而满足定理 2的稳定非平凡向量空间 V_S 的稳定子不存在。

(5)若 $|S| = 8$, 同情形 (4), 此时满足定理 2的稳定非平凡向量空间 V_S 的稳定子不存在。

综上所述, Pauli群 G_1 的子群稳定非平凡向量空间 V_S的稳定子为 $S_1 = \langle X \rangle$, $S_2 = \langle -X \rangle$, $S_3 = \langle Y \rangle$, $S_4 = \langle -Y \rangle$, $S_5 = \langle Z \rangle$, $S_6 = \langle -Z \rangle$。

对于 Pauli群 G_n, $n \geqslant 2$, 因为其中的元是 G_1中元的 n重张量积组成, 又结合定理 1所以有:

推论 1 对于 Pauli群 G_n 的子群稳定非平凡向量空间 V_S 的稳定子的每一生成元只能是算子 I和 W 的张量积, $W = X, -X, Y, -Y, Z, -Z$。

参 考 文 献:

[1] 尼尔森 M A, 庄 IL. 量子计算和量子信息 [M]. 北京: 清华大学出版社, 2005.

[2] Calderbank A R, Shor P W. Good Quantum Error-correcting Codes Exist[J]. Phys Rev A, 1996, 54(2): 1098-1105.

[3] Calderbank A R, Rains E M, Shor P W, et al Quantum Error Correction and Orthogonal Geomet try[J]. Phys Rev Lett, 1997, 78(3): 405-408.

[4] Calderbank A R, Rains E M, Shor P W, et al Quantum Error Correction via code over GF(4) [J]. IEEE Trans Inform Theory, 1998, 44(7): 1369-1387.

(下转第 37页)

[4] 郑兆顺. 不定方程组 $11x^2 - 9y^2 = 2$, $40y^2 - 11z^2 = 29$的正整数解的上界[J]. 数学的实践与认识, 2008, 38(11): 210-214.
[5] 柯召, 孙琦. 谈谈不定方程[M]. 上海: 上海教育出版社, 1980.
[6] 郑德勋. 关于不定方程 $a_2x^2 - a_1y^2 = a_2 - a_1$, $a_3y^2 - a_2z^2 = a_3 - a_2$[J]. 四川大学学报: 自然科学版, 1992, 29(3): 348-351.
[7] Baker A, Davnpirt H. The Equations $3x^2 - 2 = y^2$, $8x^2 - 7 = z^2$[J]. Quart J Math Oxford, 1969, 20(2): 129-137.

On the Upper Bound for the Positive Integer Solutions of the System of Diophantine Equations

HE La-rong
(School of Mathematics, Northwest University, Xi'an 710127, China)

Abstract By *Baker*′*s* method, this paper solutes the upper bound for the positive integer solution of the system of Diophantine equations $\begin{cases} 13x^2 - 11y^2 = 2 \\ 48y^2 - 13z^2 = 35 \end{cases}$, was soluted and let $S = \{(x, y, z) \mid x, y, z \in Z, \text{ and, } 13x^2 - 11y^2 = 2, 48x^2 - 13z^2 = 35\}$, $T = \{y \mid (x, y, z) \in S\}$, If we can get the upper bounds of T and as long as we let y of solution put the system of Diophantine equations, we may get all integer solutions of the system of Diophantine equations and we can get the upper bounds are $(x, y, z) = (0.92 \times 24^{18^{393}}, 24^{18^{398}}, 1.92 \times 24^{18^{393}})$

Key words Diophantine equations system; the upper bound of solution; Baker's method

---

(上接第 33页)

[5] 刘太琳, 温巧燕, 刘子辉. 非二元量子循环码的一种图论方法构造[J]. 中国科学, 2005, 30(6): 588-596.
[6] 李卓, 邢莉娟, 王新梅. 一类量子循环码的构造方法[J]. 西安电子科技大学学报: 自然科学版, 2007, 34(2): 187-189.
[7] 蔡乐才. 量子纠错码的研究[J]. 四川理工学院学报: 自然科学版, 2004, 17(4): 163-168.

Description of Stabilizer to Non-trivial Vector Space

CHENG Qian[1], *YU Hui*[2]
(1. School of Mathematics, Qinghai Normal University, Xining 810008, China;
2. School of Mathematics, Dalian Jiaotong University, Dalian 116028, China)

Abstract All stabilizers of non-trivial vector space V_S is described as the subgroups of Pauli group G_1 by the necessary and sufficient condition that the subgroups of Pauli group become stabilizers, and the operator property of the generating elements of stabilizers is discussed.

Key words Pauli group; stabilizer; generating element