量子力学新进展

第四辑

Recent Progress in Quantum Mechanics

Fourth Volume

龙桂鲁 裴寿镛 曾谨言 主编

Long Guilu Pei Shouyong Zeng Jinyan

清华大学出版社

量子力学新进展

第四辑

Recent Progress in Quantum Mechanics

Fourth Volume

龙桂鲁 裴寿镛 曾谨言 主编

Long Guilu Pei Shouyong Zeng Jinyan

清华大学出版社

北京

内 容 简 介

本书由10个专题组成，从多个角度对量子力学近年来的发展进行了评述，内容涉及量子纠缠、量子纠错、量子计算、量子通信、光信息存储以及量子力学转动对称性和强关联电子模型等方面。作者是国内活跃于量子力学各研究领域的专家和学者。

对于从事量子力学和量子信息学研究的科技人员、大学物理教师、研究生和高年级本科生，本书是一本有益的参考读物。

图书在版编目（CIP）数据

量子力学新进展. 第四辑/龙桂鲁，裴寿镛，曾谨言主编. —北京：清华大学出版社，2007.3
ISBN 978-7-302-13594-0

Ⅰ.量…　Ⅱ.①龙…②裴…③曾…　Ⅲ.量子力学—进展　Ⅳ.O413.1

中国版本图书馆CIP数据核字(2006)第090979号

责任编辑：朱红莲　赵从棉
责任校对：赵丽敏
责任印制：孟凡玉

出版发行：清华大学出版社
http://www.tup.com.cn
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175
投稿咨询：010-62772015
地　　址：北京清华大学学研大厦A座
邮　　编：100084
邮购热线：010-62786544
客户服务：010-62776969
印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：新华书店总店北京发行所
开　　本：185×230　　**印　张**：21.5
字　数：429千字
版　　次：2007年3月第1版
印　次：2007年3月第1次印刷
印　　数：1～3000
定　　价：39.80元

PREFACE 序言

1900年12月14日，普朗克教授在柏林亥姆霍兹研究所召开的德国物理学会年会上宣读了划时代论文《论正常光谱能量分布定律》，提出了能量量子化的概念，并由此从理论上导出了他在此前不久所发现的与实验非常符合的黑体辐射定律，从而创立了量子论。后经过爱因斯坦、海森堡、薛定谔、玻恩、约当和狄拉克等一批杰出物理学家的努力，建立了现称之为量子力学的理论体系。20世纪，量子力学相继应用于基本粒子、原子核、原子和分子、固体和液体等各种物理系统，都取得了巨大的成功。可以毫不夸张地说，20世纪的科学是量子力学的科学。

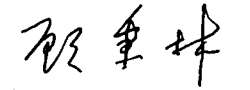
历史上，以爱因斯坦和玻尔为代表的两方，在量子力学的基本问题上展开了激烈的论争，这种论争对量子力学的发展起到了巨大的推动作用。但由于争论的关键问题在当时无法用实验检验，长期以来争论一直停留在思辨性的层面上。近年来，一方面由于实验技术的进展，关于量子力学基本概念的一些论争已经可以用实验来直接检验，另一方面由于量子信息科学的发展，重新激发了人们对这些问题研究的热情。现今这些基本问题不再是局限于少数几个科学天才的论争，而是具有巨大的应用潜力。由于量子计算机的潜在的巨大能力，西方发达国家投入了大量的人力和物力开展研究，从而使这一领域得到了迅速发展。1935年爱因斯坦等为反驳量子力学的哥本哈根诠释而提出的EPR佯谬中所指出的量子力学的奇特性质即纠缠态所展现的非局域关联，现在已经被实验证实，并且在量子信息、量子计算、密集编码、量子离物传态等方面得到了广泛的应用。

回顾过去一个世纪，在量子力学的创始阶段，我国正处于帝国主义列强侵略和军阀混战的贫穷落后时期，民不聊生，根本谈不上科学研究。解放后，在

文化大革命的十年动乱期间,我们又失去了许多发展良机。改革开放后我国的经济取得了持续高速的发展,特别是最近党和国家实施科教兴国的战略方针,我们具有了前所未有的发展条件。相信我国的科学家一定会在量子力学这一新的发展阶段中作出重要的贡献。

这套量子力学新进展系列专辑从多个角度对量子力学的最新发展进行了专门的评述和介绍。这套专辑对于量子力学的研究和教学有重要的参考价值。相信它们对从事量子力学和量子信息研究的广大科技人员、研究生和高年级本科生会起到帮助作用。

适逢《量子力学新进展》出版之际,特写以上数语,与大家共勉。



清华大学校长
中国科学院院士
2003 年 1 月 11 日

CONTENTS

目录

1 量子纠错码

冯克勤

清华大学数学科学系，北京 100084

1.1 引　　言

数字通信中为了纠正信道中产生的错误，自 20 世纪 50 年代以来发展出了系统的纠错码数学理论。目前这种正在有效使用的纠错码，已经被研究量子纠错码的学者们称为“经典”(classical)纠错码。

在量子通信和量子计算中，纠错问题同样是一个重要问题。长期以来，人们一直认为量子纠错比数字通信纠错更为困难，这是由量子通信和量子计算的机制(量子信息与环境的相互影响、不可复制性、信息状态的连续性、纠缠态等)所造成的。但是在 1995—1996 年，量子纠错的研究取得了重要的突破。Peter Shor[1] 和 Steane[2] 在物理机制上，把复杂的纠缠态量子错误归结和简化为只需考虑每个量子位上独立发生的错误，并且错误类型只有三种：Pauli 算子 σ_x，σ_y 和 σ_z。基于这种物理模型的简化，构造出世界上第一个量子纠错码[[9,1,3]](参数的意义见 1.3 节)。随后不久，人们把它又改进为[[7,1,3]]和[[5,1,3]]，后者是最佳量子码(见 1.4 节)。

1997 年以来,Calderbank,Rains,Shor,Sloane 等人建立了量子纠错码理论的数学形式,并且给出一种构造量子码的系统而有效的数学方法。这种方法给出了经典纠错码和量子纠错码之间的密切联系,从而用经典纠错码的结果构造出一批好的量子码。他们的讨论班文章在同行中流传一年之后,于 1998 年正式发表[3]。这项工作极大地推动了量子纠错码数学理论的研究。1999 年以来,人们不仅利用各种经典纠错码得到一批纠错性能不断改善的量子码,而且开展了关于量子码性能的其他课题的研究(量子码的界估计、权多项式和 MacWilliam 恒等式、多态量子码、构造量子码的其他方法等)。而在实验方面,量子码[[5,1,3]]已于 2001 年在实验室中成功地实现了量子通信的纠错功能[4]。这一切表明,尽管量子纠错码的历史只有短暂的 8 年,但发展很快。

本文对量子纠错码的发展做一综述,介绍量子纠错码的严格数学概念以及用经典纠错码构造量子码的 CRSS 方法。由于这是介绍性文章,对于数学结果着重解释其意义并列举一些例子,证明从略或只阐述其证明思想。

在讨论量子码之前,首先介绍经典纠错码的一些基本知识。这不仅由于经典码是构造量子码的重要工具,而且对于理解量子码也是有益的。经典纠错码和量子纠错码的物理机制很不相同,但是很多概念和结果至少在数学表现形式上有相似之处。

1.2 经典纠错码

在数字通信中,信息用有限个离散状态(数字位)表示。每个位(bit)是有限集合 S 中的元素。若 S 有 m 个元素($m\geqslant 2$),可以取 S 为整数模 m 的同余类 $\bar{0},\bar{1},\cdots,\overline{m-1}$(注意 $\bar{m}=\bar{0}$)形成的环,表示成 Z_m。这时 Z_m 中有加、减、乘运算,从而可使用数论工具。当 $m=p^l$ 是某个素数 p 的方幂时($l\geqslant 1$),通常取 S 为 $q=p^l$ 元有限域,表示成 F_q。这时可以进行四则运算,使用有限域和有限域理论一系列美妙的代数性质。(伽罗华,Galois,1811—1832 年,在建立有限域理论时,不会想到在 150 多年后会用于通信上!)这里只介绍 q 元有限域 F_q 上的经典纠错码,$q=p^l$。事实上,最常使用的是 $q=2$ 的情形,即最简单的二元域 $F_2=\{0,1\}$。其中 $1+1=0$(从而 $1=-1$,于是加法和减法一样),其余运算都是自然的。

对每个正整数 k,以 F_q^k 表示有限域 F_q 上的 k 维向量空间,其中元素是长为 n 的向量:$v=(v_1,v_2,\cdots,v_n)$,$v_i\in F_q$。这样的向量共有 q^k 个,用来表示信息。例如,8 个信息 $\{0,1,\cdots,7\}$ 可以用 F_2 上长为 3 的 8 个向量来表示:

$$0=(000),\quad 1=(100),\quad 2=(010),\quad 3=(110)$$
$$4=(001),\quad 5=(101),\quad 6=(011),\quad 7=(111)$$

一般地,q^k 个信息可以用 F_q 上长为 k 的向量来表示。但是用这种方式通信是不能纠错的,这是因为 F_q^k 中每个向量都代表某种信息,都是有意义的。设想发送方把信息

1=(100)通过信道传给接收方。如果信道传输时第二位 0 错成 1,即收到(110),而(110)代表信息 3(数学上表示成:发送方发出信息 $x=(100)$,信道出错,错误向量为 $\varepsilon=(010)$,接收方收到 $y=x+\varepsilon=(100)+(010)=(110)$),接收方无法判别是否出错。

为使通信系统有纠错能力,想法是:将 q^k 个信息用比 k 长的向量来表示,取 $n>k$,q^k 个信息用 F_q^n 中 q^n 个向量当中的一部分向量(q^k 个)来表示,它们形成 F_q^n 的一个 q^k 元子集合 S。S 中向量代表信息,而其余 q^n-q^k 个向量是没有意义的。S 选取得要好,使得发送方发出信息 $x\in S$,在信道产生少数几位错误 ε 时(即向量 ε 只有少数几位为 1,其余位均为 0),收到的 $y=x+\varepsilon$ 不属于 S,这样接收方可以检查到出错(因为 y 不代表信息),并且还能够纠正错误。

例 1.2.1 (重复码)将上述{0,1,…,7}代表的向量均重复 3 次:

$$0=(000000000),\quad 1=(100100100),\quad 2=(010010010),\cdots$$
$$6=(011011011),\quad 7=(111111111)$$

用 F_2^9 中上述 8 个向量表示 8 个信息,这 8 个向量形成集合 S,其余 2^9-8 个向量不代表信息。每个 $x\in S$ 在其中 1 位或 2 位出错时,如 $x=(100100100)$ 变成 $y=(101110100)$,它都不属于 S,因为 S 中任 2 个不同向量至少有 3 位是不同的。进而,若 $x=(100100100)$只有 1 位出错,成为 $y=(100110100)$,易知发出的为 $x=(100100100)$,因为 S 中只有 x 与 y 只相差 1 位,而 S 中其余向量($\neq x$)与 y 均至少有两位不同。综合上述内容可知,S 可以检查 2 位错误,可以纠正 1 位错误。

有了以上直观解释,现在给出数学上的形式化定义。

定义 1.2.1 F_q^n 中每个子集合 S 都称为一个**纠错码**。S 中的向量称为**码字**,n 称为 S 的**码长**,$K=|S|$ 表示**码字个数**,$k=\log_q K$ 表示**信息位数**(如果不考虑纠错性能,K 个信息用长为 k 的向量表示即可)。

除了 n 和 K(或 k)之外,S 还有另一个参数 d,用来反映纠错能力。

定义 1.2.2 对于 $u=(u_1,\cdots,u_n)$,$v=(v_1,\cdots,v_n)\in F_q^n$,定义向量 u 的**汉明权**(Hamming weight)为非零分量 u_i 的个数,即

$$w_{\mathrm{H}}(u)=\#\{i\mid 1\leqslant i\leqslant n,u_i\neq 0\}$$

而向量 u 和向量 v 的 Hamming 距离 $d_{\mathrm{H}}(u,v)$为它们相异位的个数,即

$$d_{\mathrm{H}}(u,v)=\#\{i\mid 1\leqslant i\leqslant n,u_i\neq v_i\}=w_{\mathrm{H}}(u-v)$$

容易验证,Hamming 距离满足数学上一个距离所具有的以下 3 条性质:

对于 $u,v,w\in F_q^n$,有

(1) 非负性,$d_{\mathrm{H}}(u,v)\geqslant 0$,并且当且仅当 $u=v$ 时,$d_{\mathrm{H}}(u,v)=0$;

(2) 对称性,$d_{\mathrm{H}}(u,v)=d_{\mathrm{H}}(v,u)$;

(3) 三角形不等式,$d_{\mathrm{H}}(u,w)\leqslant d_{\mathrm{H}}(u,v)+d_{\mathrm{H}}(v,w)$。

定义 1.2.3 对于码长为 n 的 q 元码 S(即 S 为 F_q^n 的非空子集合),S 的最小距离 $d=d(S)$定义为 S 中任意 2 个不同码字之间 Hamming 距离的最小值,即

$$d = d(S) = \min\{d_H(u,v) \mid u,v \in S, u \neq v\}$$

下面的结果是经典纠错码的基础,它表明一个码 S 的最小距离恰好反映了其纠错能力。

定理 1.2.1 若 d 为码 S 的最小距离,则码 S 可用来检查小于等于 $d-1$ 位错误,也可纠正小于等于$\left[\frac{d-1}{2}\right]$位错误(这里$[\alpha]$表示实数 α 的整数部分,即不超过 α 的最大整数)。于是

$$\left[\frac{d-1}{2}\right] = \begin{cases} l, & d = 2l+1 \text{ 为奇数} \\ l-1, & d = 2l \text{ 为偶数} \end{cases}$$

证 发送方把码字 $x \in S$ 发给接收方。如果信道发生错误 $0 \neq \varepsilon \in F_q^n$,并且错位数不超过 $d-1$,即 $1 \leqslant w_H(\varepsilon) \leqslant d-1$,则接收方得到的 $y=x+\varepsilon$ 不是码字(由 $\varepsilon \neq 0$ 可知,$y=x+\varepsilon \neq x$。又由于 S 中其他码字 $x'(x' \neq x)$与 x 的 Hamming 距离都大于等于 d,而 $d_H(y,x)=w_H(y-x)=w_H(\varepsilon) \leqslant d-1$,所以 y 也不是 x')。因此,接收方发现出错,即可检查出小于等于 $d-1$ 位的错误。

现在设码字 x 在信道中发生小于等于$\left[\frac{d-1}{2}\right]$位错误,即 $w_H(\varepsilon) \leqslant \left[\frac{d-1}{2}\right]$,接收方得到 $y=x+\varepsilon$,它与 x 的距离为 $d_H(y,x)=w_H(\varepsilon) \leqslant \left[\frac{d-1}{2}\right]$。而对于 S 中其他码字 $x'(x' \neq x)$,由三角形不等式:

$$d \leqslant d_H(x,x') \leqslant d_H(y,x) + d_H(y,x')$$

于是,有

$$d_H(y,x') \geqslant d - d_H(y,x) \geqslant d - \left[\frac{d-1}{2}\right] > \left[\frac{d-1}{2}\right]$$

其几何表示如图 1.1 所示。

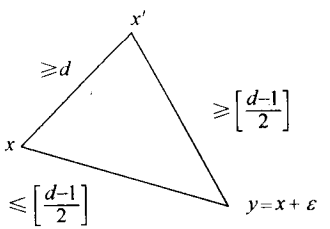


图 1.1 码字距离的几何表示

这表明:在 S 的所有码字当中,只有 x 与所收到的向量 y 最接近。将 y 译成 x,就完成了纠错功能。

对于一个 q 元(即 F_q 上)纠错码 S,码长 n、码字数 K(或信息位数 $k=\log_q K$)和最小距离 d 是 3 个最基本的参数。该码可表示成(n,K,d)或者$[n,k,d]$。

由于 $K=|S| \leqslant |F_q^n| = q^n$,可知 $k=\log_q K \leqslant n$。如果不考虑纠错,一个信息用 k 位向量传送即可。现在为了有纠错能力,改用 n 位向量来传送,$\frac{k}{n}$表示纠错码的效

率。所以，我们是在损失效率(增加传送时间)之下得到了纠错功能。一个好的纠错码即指有大的$\frac{k}{n}$(效率高)和大的d(纠错性能强)。

例 1.2.2 考虑由以下 16 个码字组成的二元码 C(码长 $n=7$，码字数 $K=16$，信息位数 $k=\log_2 K=4$)：

0010111　1101000
1001011　0110100
1100101　0011010
1110010　0001101
0111001　1000110
1011100　0100011
0101110　1010001
0000000　1111111

可以验证，该码 C 的最小距离为 3，即 C 为二元码$[n,k,d]=[7,4,3]$。效率为$\frac{4}{7}$，可纠正 1 位错。

例 1.2.1 中的重复码是二元码$[9,3,3]$。码 C 和该重复码有同样的纠错性能，但是 C 的 k 值大(可传送 16 个信息，而重复码只可传送 8 个信息)，并且 C 的效率高$\left(\text{对于 } C,\frac{k}{n}=\frac{4}{7},\text{而重复码的效率为}\frac{3}{9}=\frac{1}{3}\right)$。这表明：构造好的纠错码是很有讲究的。

构造好的纠错码是经典纠错码理论的一个重要数学课题。从工程角度考虑，另一个重要课题是对于纠错码 S 要有好的纠错译码算法。由定理 1.2.1 的证明过程可知：每收到 y 之后，要将 y 与 S 中所有码字相比较，找到与 y 距离最近的那个码字 x。该算法太花时间。所以，尽管有好的纠错码，如果没有好的译码算法，工程上也不实用。

为了寻求性能好的纠错码和好的译码算法，要研究 F_q^n 的一些特殊的子集合 S，即将 S 加上某些代数结构，从而可使用更多的代数工具。一个自然的想法是考虑 F_q^n 的 F_q－向量子空间，从而可采用线性代数工具。

定义 1.2.4 F_q^n 的一个 F_q－向量子空间 C 称作码长为 n 的 q 元**线性码**。

设 k 是向量子空间 C 的维数$(1\leqslant k\leqslant n)$，则 C 存在一组基 $u_1,\cdots,u_k$，其中，

$$u_i=(a_{i1},\cdots,a_{in}),\quad a_{ij}\in F_q, 1\leqslant i\leqslant k$$

而 C 中每个码字均惟一地表示成它们的 F_q－线性组合：

$$c=b_1u_1+\cdots+b_ku_k,\quad b_i\in F_q$$

所以，C 中每个码字个数为 $K=q^k$，而 $k=\log_q K$。这表明向量子空间 C 的维数 k 就是信息位数。

以 $u_1,\cdots,u_k$ 为行的矩阵

$$G=\begin{bmatrix}u_1\\u_2\\\vdots\\u_k\end{bmatrix}=\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{k1}&a_{k2}&\cdots&a_{kn}\end{bmatrix}$$

称作线性码 C 的一个**生成阵**。这是 F_q 上(即元素属于 F_q)的一个 k 行 n 列矩阵,并且矩阵 G 的秩为 k。

对于每个 $c\in F_q^n$,

$$c\text{ 是码字}(c\in C)\Leftrightarrow c=b_1u_1+\cdots+b_ku_k\qquad(\text{对于某些 }b_i\in F_q)$$

$$\Leftrightarrow c=(b_1,\cdots,b_k)\begin{bmatrix}u_1\\u_2\\\vdots\\u_k\end{bmatrix}=(b_1,\cdots,b_k)G$$

$K=q^k$ 个信息本来可以用 F_q^k 中长为 k 的向量$(b_1,\cdots,b_k)$来表示,现在为了有纠错能力,将每个$(b_1,\cdots,b_k)$改用 F_q^n 中长为 n 的向量$c=(b_1,\cdots,b_k)G$。这称作**纠错编码**。所以对于线性码,纠错编码相当于乘以生成矩阵 G。

另一方面,从线性代数可知,F_q^n 的一个 k 维线性子空间还可看成是变量 $x_1,\cdots,x_n$ 在 F_q 上(即系数属于 F_q)$n-k$ 个齐次线性方程组

$$\begin{cases}b_{11}x_1+b_{12}x_2+\cdots+b_{1n}x_n=0\\b_{21}x_1+b_{22}x_2+\cdots+b_{2n}x_n=0\\\qquad\cdots\\b_{n-k,1}x_1+b_{n-k,2}x_2+\cdots+b_{n-k,n}x_n=0\end{cases}\tag{1.1}$$

的解空间。其中系数矩阵

$$H=(b_{ij})_{1\leqslant i\leqslant n-k,1\leqslant j\leqslant n}\tag{1.2}$$

是 F_q 上 $n-k$ 行 n 列的矩阵,并且 H 的秩为 $n-k$,即式(1.1)中 $n-k$ 个线性方程是独立的。H 称作线性码 C 的一个**校验阵**。由于方程组(1.1)可写成

$$H\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}=Hx^{\mathrm{T}}=0\in F_q^{n-k}$$

其中 $x=(x_1,\cdots,x_n)$,x^{T} 表示向量 x 的转置(列向量)。所以对于每个 $v\in F_q^n$,有

$$v\in C\Leftrightarrow Hv^{\mathrm{T}}=0$$

也就是说,用校验阵乘以 v^{T} 可判断 v 是否为码字。即线性码的检错问题只需简单地乘以校验阵即可:若收到 y,而 $Hy^{\mathrm{T}}\neq0$,则 y 不属于 C,从而信道产生错误。

校验阵 H 的功能不仅于此，它还可以用来决定线性码的最小距离。

定理 1.2.2 设 C 是参数$[n,k,d]$的 q 元线性码，则

(1) C 的最小距离 d 等于 C 中非零码字 Hamming 权的最小值，即

$$d = \min\{w_{\mathrm{H}}(c) \mid 0 \neq c \in C\}$$

(2) 将 C 的校验阵 H 写成 n 个列向量：

$$H = [v_1 \quad v_2 \quad \cdots \quad v_n], \quad v_j = \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{n-k,j} \end{bmatrix} \in F_q^{n-k}$$

则线性码 C 的最小距离 d 即是满足以下两个条件的正整数 d：

① H 中任意 $d-1$ 个不同的列向量都是 F_q 线性无关的；

② H 中存在 d 个不同的列向量，它们是 F_q 线性相关的。

证 (1) 根据定义，d 是 C 中不同码字 c 和 c' $\left(\text{共有}\frac{1}{2}K(K-1)\text{对}\right)$的 Hamming 距离 $d_{\mathrm{H}}(c,c')=w_{\mathrm{H}}(c-c')$的最小值。但是对于线性码 C，$c-c'$是 C 中的非零码字，所以 d 为 C 中所有非零码字(共 $K-1$ 个)Hamming 权的最小值。

(2) H 中有 l 个不同的列向量线性相关，当且仅当 C 中有 Hamming 权为 l 的码字。比如 $H=[v_1 \quad v_2 \quad \cdots \quad v_n]$的前 l 个向量 $v_1,\cdots,v_l$ 线性相关，即

$$b_1 v_1 + \cdots + b_l v_l = 0 \qquad b_1,\cdots,b_l \text{ 为 } F_q \text{ 中的非零元素}$$

即

$$H\begin{bmatrix} b_1 \\ \vdots \\ b_l \\ 0 \\ \vdots \\ 0 \end{bmatrix} = [v_1 \quad v_2 \quad \cdots \quad v_n]\begin{bmatrix} b_1 \\ \vdots \\ b_l \\ 0 \\ \vdots \\ 0 \end{bmatrix} = b_1 v_1 + \cdots + b_l v_l = 0$$

即 $c=(b_1,\cdots,b_l,0,\cdots,0)\in C$，而 $w_{\mathrm{H}}(c)=l$。由定理 1.2.2(1)可知，C 中有权为 d 的码字，但是没有权为 $1,2,\cdots,d-1$ 的码字，这就相当于条件①和条件②。

例 1.2.3 设 C 是以

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

为校验阵的二元线性码。H 是 $3(n-k=3)$行 $7(n=7)$列，元素属于二元域，$F_2=\{0,1\}$，

并且 H 的秩为 3(由于后三列线性无关)。于是 C 的码长为 $n=7$,信息位数为 $k=7-3=4$。所以 C 共有 16 个码字。H 的 7 个列向量是不同的非零向量,所以任意两列均线性无关。但是由于

$$\begin{bmatrix}1\\1\\0\end{bmatrix}+\begin{bmatrix}0\\1\\1\end{bmatrix}=\begin{bmatrix}1\\0\\1\end{bmatrix}$$

即 H 的第 1,2,4 列线性相关。由定理 1.2.2(2)可知线性码 C 的最小距离 d 为 3,即 C 为二元线性码 $[n,k,d]=[7,4,3]$。

将 H 记为

$$H=[P\quad I_3],\quad P=\begin{bmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{bmatrix}$$

$$I_3=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\quad 3\text{ 阶单位方阵}$$

则

$$G=[I_4\quad P^{\mathrm{T}}]=\begin{bmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&1\end{bmatrix}$$

是 C 的一个生成阵,这是由于 $HG^{\mathrm{T}}=0$($n-k$ 行 k 列的零矩阵)。计算出 G 的 4 个行向量(这是 C 的一组基)的所有 16 个线性组合,便给出 C 中的全部码字。可以验证,这 16 个码字就是例 1.2.2 中的那些码字,也就是说,例 1.2.2 中的纠错码 C 是如此构造出来的二元线性码。

例 1.2.3 中的线性码是“最优”码。如何判别一个纠错码是好码?在 3 个基本参数 n,k,d 之间有相互制约的关系。这些关系用不等式来描述,称作纠错码的**界**(bound)。使不等式达到等式的码就是某种意义上的最优码。下面是经典纠错码的 3 个最著名的界。

定理 1.2.3 (1) 若存在参数为 $[n,k,d]$ 的 q 元纠错码,则

① (Hamming 界) $q^{n-k}\geqslant\sum_{i=0}^{\left[\frac{d-1}{2}\right]}(q-1)^i\binom{n}{i}$,其中 $\binom{n}{i}$ 为 n 个物体中取 i 个的组合数,即 $\binom{n}{i}=\frac{n(n-1)\cdots(n-i+1)}{i!}$;

② (Singleton 界) $n\geqslant k+d-1$。

(2) (Gilbert-Varshamov 界)设 $1\leqslant d\leqslant n, 2\leqslant K\leqslant q^n$, q 为素数幂。如果

$$(K-1)\left(\sum_{i=1}^{d-1}(q-1)^i\binom{n}{i}\right)<q^n$$

则必存在参数为(n,K,d)的 q 元纠错码。

证 (1) 对于 F_q^n中每个向量 v 和整数 l,用 $B(v;l)$表示以 v 为中心、以 l 为半径的球:

$$B(v;l)=\{x\in F_q^n \mid d_H(v,x)\leqslant l\}$$

则该球的体积为

$$b(l)=\mid B(v;l)\mid=\sum_{i=0}^{l}(q-1)^i\binom{n}{i}$$

若 C 是 q 元纠错码$[n,k,d]$,则以 q^k 个码字为中心,半径为$\left[\frac{d-1}{2}\right]$的 q^k 个球两两不相交。它们的体积之和应不超过整个空间 F_q^n 的体积 q^n,即 $q^n\geqslant q^k b\left(\left[\frac{d-1}{2}\right]\right)$,这就是 Hamming 界。

考虑由 C 给出的新码。对每个 $a\in F_q$,记

$$C_a=\{(c_1,\cdots,c_{n-1})\in F_q^{n-1}\mid (c_1,\cdots,c_{n-1},a)\in C\}$$

该码的码长为 $n-1$,最小距离大于等于 d。由于 $\mid C\mid=\sum_{a\in F_q}\mid C_a\mid$,所以存在 $a\in F_q$,使得 $\mid C_a\mid\geqslant\mid C\mid/q=q^{k-1}$。这表明 C_a 参数为$[n-1,\geqslant k-1,\geqslant d]$。递推下去,可知存在纠错码$[d,k-n+d,d]$。于是必然 $k-n+d\leqslant 1$,即 $n\geqslant k+d-1$,这就是 Singleton 界。

(2) 如果存在 q 元码$[n,N,d]$,其中 $1\leqslant N<K$,以 N 个码字为中心,$d-1$ 为半径的 N 个球总体积不超过 $N\cdot b(d-1)$。由假设 $N\cdot b(d-1)\leqslant(K-1)b(d-1)<q^n$,所以在这 N 个球之外还有向量 $v\in F_q^n$。v 与所有码字的距离均大于等于 d。将 v 加入之后,新的码为$[n,N+1,d]$。由此可知必存在 q 元码$[n,K,d]$。

Hamming 界和 Singleton 界都是码的必要条件。达到定理 1.2.3 中①、②等式条件的码都是最优码。满足 $q^{n-k}=b\left(\left[\frac{d-1}{2}\right]\right)$ 的码称作**完全码**(perfect),满足 $n=k+d-1$ 的码称作**极大距离可分码**(maximal distance separable 简称 **MDS 码**)。这是两类好的纠错码。对于例 1.2.3 中的二元码$[7,4,3]$,$\left[\frac{d-1}{2}\right]=1$,而

$$q^{n-k}=2^{7-4}=8,\quad b(1)=\sum_{i=0}^{1}(2-1)^i\binom{7}{i}=1+7=8$$

所以这是完全码。

G-V 界是纠错码存在的充分条件。当 $q^{n-k}\geqslant b(d-1)$时,一定存在 q 元码$[n,k,d]$。

但是证明本身并没有给出这种码的具体构造方式。G-V 界建立于 1952 年。直到 30 年后,在发明代数几何码以后,人们才于 1982 年具体给出达到和超过 G-V 界的一批纠错码。

利用抽象代数工具,人们研究了线性码的一个子类:循环码。特别是其中一类循环码(称为 BCH 码)可以设计出最小距离 d 很大的码,并且有很实用的纠错译码算法,目前在数字通信中得以普遍采用。1980 年以后用代数几何构造出的代数几何码,其性能比 BCH 码要好,但目前译码算法还不能达到实用程度。

以上是经典纠错码的简要介绍,关于经典纠错码的详细内容可参考文献[5]或[6]。

1.3 什么是量子纠错码

本节介绍量子纠错码的基本数学概念。请与经典情况相参照。

一个量子位(quantum bit,qubit)是 2 维复向量空间 $\mathbf{C}^2$ 中的非零向量,量子物理中把 $\mathbf{C}^2$ 的一组基表示成$|0\rangle$和$|1\rangle$,所以一个量子位为

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (\alpha,\beta \in \mathbf{C},(\alpha,\beta) \neq (0,0))$$

一个量子状态是 n 个 $\mathbf{C}^2$ 的张量积$(\mathbf{C}^2)^{\otimes n}$中的非零向量。这是 2^n 维复向量空间,它有一组基

$$|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_n\rangle, \quad (a_i \in \{0,1\} = F_2,(1 \leqslant i \leqslant n))$$

该向量也简记为$|a_1a_2\cdots a_n\rangle = |a\rangle$,其中 $a=(a_1,a_2,\cdots,a_n)\in F_2^n$。所以每个量子状态$|v\rangle$是它们的复线性组合:

$$|v\rangle = \sum_{(a_1,a_2,\cdots,a_n)\in F_2^n} c(a_1,a_2,\cdots,a_n)|a_1a_2\cdots a_n\rangle = \sum_{a\in F_2^n} c(a)|a\rangle$$

其中,$c(a_1,a_2,\cdots,a_n)=c(a)\in\mathbf{C}$(不全为零)。

在 2^n 维复向量空间中有厄米特内积$\langle v|u\rangle$,对于

$$|v\rangle = \sum_a c(a)|a\rangle, \quad |u\rangle = \sum_a d(a)|a\rangle$$

它们的厄米特内积定义为

$$\langle v|u\rangle = \sum_{a\in F_2^n} \overline{c(a)}d(a) \in \mathbf{C}$$

其中,$\overline{c(a)}$表示复数 $c(a)$的共轭复数。

在量子物理中,

(1) 彼此相差一个非零复数因子的两个非零向量看成是同一个量子态。即若$|v\rangle = \alpha|u\rangle$(相当于对每个 $a\in F_2^n$,有 $c(a)=\alpha d(a)$),其中 α 是非零复数,则$|v\rangle$和$|u\rangle$为同一个量子态。

(2) $|v\rangle$和$|u\rangle$是完全可区分的,这是指$\langle v|u\rangle=0$(正交)。

定义 1.3.1 $V=(\mathbf{C}^2)^{\otimes n}=\mathbf{C}^{2^n}$中每个复向量子空间$Q$都称作一个**量子码**。$n$称作$Q$的**码长**,$Q$的**维数**记为$K=\dim Q$,而令$k=\log_2 K$。由$1\leqslant K\leqslant 2^n$可知$0\leqslant k\leqslant n$。

除了n和K(或k)之外,量子码还应有一个参数反映其纠错能力。这就需要解释什么是量子错误。

在经典的数字通信中,信息$x=(x_1,x_2,\cdots,x_n)$和错误$\varepsilon=(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)$都是$F_q^n$中的向量,错误$\varepsilon$对信息$x$的作用是相加:$y=x+\varepsilon$。在量子通信中,信息是$V$中的非零向量$|v\rangle$,而错误是复空间$V$上的酉(unitary)线性算子$e$,$e$在$V$上的作用是酉线性变换$e|v\rangle$。

每个量子位为$|v\rangle=\alpha|0\rangle+\beta|1\rangle$,根据 P. Shor 的简化,只需考虑 3 种错误作用,它们的矩阵表示为 3 个 Pauli 阵:

$$\sigma_x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\quad \sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$\sigma_y=\mathrm{i}\sigma_x\sigma_z=\begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix},\quad \mathrm{i}=\sqrt{-1}$$

所以在$|v\rangle$上的作用为

$$\sigma_x|v\rangle=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\beta\\ \alpha\end{bmatrix}=\beta|0\rangle+\alpha|1\rangle$$

$$\sigma_z|v\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\alpha\\ -\beta\end{bmatrix}=\alpha|0\rangle-\beta|1\rangle$$

$$\sigma_y|v\rangle=\begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}-\mathrm{i}\beta\\ \mathrm{i}\alpha\end{bmatrix}=\mathrm{i}(-\beta|0\rangle+\alpha|1\rangle)$$

这 3 个作用都是酉作用,并且满足

$$\sigma_x^2=\sigma_y^2=\sigma_z^2=I_2(\text{单位阵}),\quad \sigma_x\sigma_z=-\sigma_z\sigma_x$$

由于

$$\sigma_x|0\rangle=|1\rangle,\quad \sigma_x|1\rangle=|0\rangle,\quad \sigma_z|0\rangle=|0\rangle,\quad \sigma_z|1\rangle=-|1\rangle$$

这可以写成

$$\sigma_x|a\rangle=|a+1\rangle,\quad \sigma_z|a\rangle=(-1)^a|a\rangle,\quad a\in F_2=\{0,1\}$$

注意:$\sigma_y=\mathrm{i}\sigma_x\sigma_z$和$\sigma_x\sigma_z$是同样的量子作用,因为$\mathrm{i}\sigma_x\sigma_z|v\rangle=\mathrm{i}(\sigma_x\sigma_z|v\rangle)$,而$\mathrm{i}\sigma_x\sigma_z|v\rangle$和$\sigma_x\sigma_z|v\rangle$是同一个量子态。将$\mathrm{i}\sigma_x\sigma_z$乘以 i 是由于

$$\mathrm{i}\sigma_x\sigma_z=\begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}$$

不但为酉阵,而且是厄米特阵,其本征值均为实数。

在复空间$V=\mathbf{C}^2\otimes\cdots\otimes\mathbf{C}^2=(\mathbf{C}^2)^{\otimes n}$上的错误作用有以下形式: