信息系统编码理论中的重量谱研究[1]

陈文德　中国科学院数学与系统科学研究院

一、汉明重量

在数字通信系统与数据存储系统中广泛应用着的纠错码，顾名思义，它是一种能自动纠正错误的码。我们先来简单说明一下纠错原理。数字信息都可用 0，1 序列来表示，这里 1 加 1 定义为等于 0（即 mod 2 运算），也就是说 0 与 1 构成了一个二元有限域，它是由二个元素构成的代数结构：域，元素间加减乘除后的结果仍在域内。一般来说，对于 q 元有限域，q 必须是素数幂，如 q 可等于 2，3，4，5，7，8，9 …… 可定义有限域上的矩阵，设它是 k 行 n 列的。如矩阵的行向量线性无关，则可以用它的 k 个行向量生成一个 k 维线性空间，这个线性空间称为（线性）码，线性空间里每个向量（或称为每个点）称为码字，向量的每个分量称为码元或分量，n 称为码长，k 称为码的维数，这个矩阵称为码的生成矩阵，一般记作 G。

编码理论的创始人之一，汉明（Hamming）提出了汉明重量与汉明距离的概念。一个码字的非零分量个数称为该码字的汉明重量，码的所有非全零码字的汉明重量的最小值，称为该码的最小汉明重量。两个码字的不同分量个数，称为这两个码长的汉明距离，码的所有码字两两之间的汉明距离的最小值，称为这码的最小汉明距离，简称最小距离，可记为 d_1。对于线性码，它含全零分量码字，两个码字之差仍是码字（这个码字的汉明重量等于那两个码字的汉明距离），因此，线性码的最小汉明重量就是最小距离。最小距离是极为重要与基本的参数。下面举个例子

例 1　由下面三个行向量生成一个码：

[111000]，[100110]，[010101]

这是一个码长为 6 的 3 维 2 元线性码，共有 8

[1] 本文根据作者在河北工业大学（天津）人工智能与数据科学学院的线上演讲（2021 年 11 月 18 日）录音补充、修改、整理而成。

个码字，其它 5 个码字为：

[110011]，[101101]，[001011]，[011110]，[000000]

容易看出：这个码的最小汉明重量与最小距离是 3。

由于信道干扰等原因，发方发出码字后，收方可能会收到含错误的字。如果含有 1 个错误，即码字的一个分量错了，而码的最小距离是 3。这时，收方可以这样做：把以这个码字为球心、半径为 1 的球中所有错字都译成球心；而全体码字为球心的所有球之间，没有公共点，这就纠正了一个错，这就是自动纠错的基本原理。例 1 中的码就能纠一个错。若最小距离小于 3，比如是 2，则球之间有公共点，若错字是公共点，收方就不知道该译成哪个球心，纠不了错。一般来说，想纠正 t 个错。最小距离应不小于 $2t+1$。也就是说：最小距离约是纠错能力的两倍，线性码的最小汉明重量给出了码的纠错能力 。

科学家们发明与构造出了各种线性纠错码。如汉明码、循环码、BCH 码、RS 码等。

二、重量谱的价值与两个公开问题

1991 年，曾在香港大学任教的华裔通信工程教授魏（Wei），以 II 型窃密信道问题为应用背景，提出了广义汉明重量的概念与理论。码的任意线性子空间称为子码，一个子码中，所有码字非零分量的数目，称为子码的支撑重量。一个 q 元有限域上 k 维线性码 C 的广义汉明重量，也简称为重量谱，它定义为一个正整数序列 $(d_1, d_2, \cdots, d_k)$，它含有 k 个正整数，其中 d_r 为 C 的所有 r 维子码的支撑重量的最小值，也被称为第 r 个广义汉明重量。d_1 就是上节中定义的最小距离。

例 2 考察上节例 1 中的码。它的一维子码，由一个码字与全零码字组成，7 个一维子码的支撑重量为 3 或 4，所以 d_1=3。再看 7 个二维子码，每个由三个码字与全零码字组成，它们的支撑重量为 5 或 6，比如 [111000] 与 [011110] 生成的子码，含 [100110]，支撑重量为 5，[110011] 与 [101101] 生成的子码，含 [011110]，支撑重量为 6，所以 d_2=5。三维码就是由全部八个码字组成，所以 d_3=6。我们得到重量谱为（3，5，6）。

重量谱不仅包含了重要参数：最小距离，它本身有独立的重要应用价值：对于 II 型窃密信道的一种编码方案，魏教授证明了：若窃听的敌方可获得码长为 n 中的 s 个分量，则窃听者想从中获得 r 个信息分量的充要条件是：s 不小于 d_r。此外，重量谱在译码分析、检错分析、码的格子复杂度分析等方面都有重要应用。因此，重量谱概念一提出就成为国际前沿研究热点，很快有一百多篇重要论文发表。

从数学理论角度，重量谱也可用纯数学语言表示为“q 元有限域上 k 维线性空间的各维线性子空间支撑集的最小尺寸 ”，这是有限域上线性空间理论中的一个重要概念。在当今计算机网络与数字技术时代，有限域的这些相关理论凸显出了其重要性。

1992 年，数学家出身的挪威信息学教授克楼夫（Klove）（他是 IEEE Fellow，曾任 IEEE Trans. Information Theory 副主编，挪威卑尔根大学理学院副院长）提出了一个基本理论问题：“一个正整数序列成为重量谱的充要条件是什么？ ”或者说“当且仅当一个序列满足什么条件时，存在一个线性码 C，使得该序列成为码 C 的重量谱？ ”满足该条件的序列集，正是 k 维 q 元一般线性码的所有重量谱，所以我们可以重述第一个公开问题：

问题 1 如何确定 k 维 q 元一般线性码的所有重量谱?

k 不大于 4 时，克楼夫用组合方法确定了 k 维 2 元一般线性码的所有重量谱。

1995 年夏，我第三次应克楼夫邀请，出访卑尔根大学前，做预备研究时发现：可以用有限射影几何方法来研究问题 1。我用彩笔画出了 2 维 3 元有限射影空间中的各条奇怪的线，进而确定了 3 维 3 元一般线性码的所有重量谱。在卑尔根大学蓝白色新楼——高科技中心的办公室里，我与克楼夫兴奋地展望着几何方法的前景：比原组合方法更有效，可打开一小片新天地。方法框架有了，还需智慧、技巧、各种具体方法与大量时间去做具体研究。从 1995 年到 2004 年，在挪威国家研究理事会的资金支持下，我六次出访卑尔根大学，每次约三个月，加上通信合作，十年间与克楼夫合作发表重量谱的论文 14 篇，其中在 IEEE Trans. Information Theory 上发表 4 篇 [1-4]。我与克楼夫最近一次见面，是在 2016 年武汉华中师范大学数学系的学术报告会上，我俩分别作了报告，我报告了本文主要内容。

多年的研究经验表明，只能对很小的 k，q 值，解决公开问题 1，当 k，q 稍大时，未知序列的数目急剧增加，呈组合爆炸之势，解决问题 1 是不可能的。为了拓展研究范围与成果，2003 年我提出了严密的“几乎所有重量谱”新概念，详细数学定义见本文第四节。于是，自然形成了以下第二个公开问题：

问题 2 如何确定 k 维 q 元一般线性码的几乎所有重量谱?

我与我的博士生及青年教师，围绕这两个问题与派生重量谱，扩大成果，发表了一系列的论文。以上全部成果（1996—2011 年），又系统总结在 2012 年 1 月发表的学术专著 [5] 中，该专著包含了我们 30 多篇论文的核心内容。

国际上大量文献研究了如何确定各类具体线性纠错码的重量谱。由于最小距离 d_1 的确定，尚是编码理论中未完全解决的难题，因而重量谱的确定更为困难，只有少数类的纠错码确定了重量谱，大多数纠错码仅给出了界，或确定了重量谱中极少数参数。关于一般线性码（这里，码 C 是指由任意一个生成矩阵 G 生成的线性码），国际文献有了一定研究：给出了重量谱的基本性质，如单调性，对偶性等；提出了链条件，即在取到 d_r 值的子码 D_r 中，存在一条长为 k 的 D_r 包含在 $D_{(r+1)}$ 中的链，$r=1, 2, \cdots, k-1$，这类码我们称为链码，它们具有重要的良好性质：积码的重量谱可用因子码的重量谱简单表示。克楼夫等证明了重量谱的广义格里斯末（Greismer）界。困难的上述公开问题 2 若能解决，则与已有的广义格里斯末解相比，是一个质的飞跃与重要突破。

三、有限射影几何方法

称任意正整数序列 $(d_1, d_2, \cdots, d_k)$ 为 d 序列，定义 i 序列

$$i_r=d_{(k-r)}-d_{(k-r-1)}, \qquad r=1, 2, \cdots, k-1,$$

这里令 $d_0=0$。当 d 序列为重量谱时，称对应的 i 序列为差序列。显然，确定重量谱可归结为确定差序列，为方便用几何方法，下面我们经常用差序列。

生成矩阵 G 可导出赋值函数的概念。把 G 中列 x 出现的次数赋为 x 的值 $m(x)$，适当取 q 元有限域中非零元 a，使得 $ax=p$，这些 p 在 q 元有限域上 k-1 维射影空间 $PG(k-1, q)$ 中，该过程不会改变支撑重量与重量谱，但维数降了一维。对于上述射影空间中的子集，定义子集的赋值为子集内所有点的赋值之和。

可以证明，一个 i 序列成为某个码 C 的差序列的充要条件是：存在赋值函数 $m(p)$，使得 $PG(k-1, q)$ 中所有 r 维线性子空间的赋值函数的极大值等于

$$i_0+i_1+i_2+\cdots+i_r, \qquad r=0, 1, 2, \cdots, k-1,$$

这个充要条件称为差序列条件。

例 3 q=11 时，检验 d 序列（21，24，26）是否为重量谱。由定义，相应的 i 序列易知为（2，3，21）。在 PG(2, 11) 中尝试构造赋值函数，参见图 1。

在该射影空间中，过每个点有 12 条线，这里 1 维线性子空间称为线。过 B、C 两点各画两条线，这两条线与过 A 点的 12 条线的交点上适当赋值 1，再在 BC 线的适当 4 个点（m_1 到 m_4）赋值 1，使得过 A 点 12 条线上赋值为 2，A 点赋值为 2，其它点都赋值为零。这样，所有 0 维线性子空间（即点）上，赋值函数极大值为 2。由于赋值为 1 的点都在图 1 中过 B 或 C 的 5 条线上（这每条线赋值都不大于 5），而任意不过 A 的线与 5 条线之一仅有一个交点，所以该线的赋值不大于 5；另外，过 A 的线的赋值恰为 4，因此，所有 1 维线性子空间的赋值函数极大值为 5，它等于 2 + 3。最后，2 维空间的赋值函数为图 1 中所有点的赋值之和，即 26，它等于 2 + 3 + 21。于是，满足差序列条件，所以，这个 d 序列是重量谱。只要把图 1 中赋值为 1 的 24 个点（每个点为 一个 3 维列向量），与两个 A 点的列向量拼合，就得到了 3 行 26 列的生成矩阵 G，它的重量谱为（21，24，26）。注意，图 1 中 4 条线的交点 E, F, G, H 都赋值为零，否则会有麻烦。 上例仅讨论一个固定序列，进一步需要讨论序列集，不用数字而用参数表示。

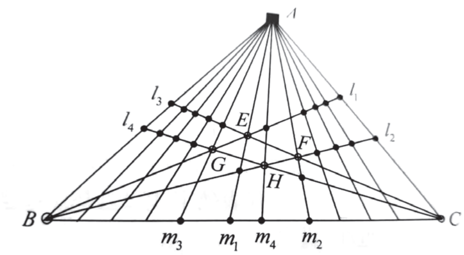
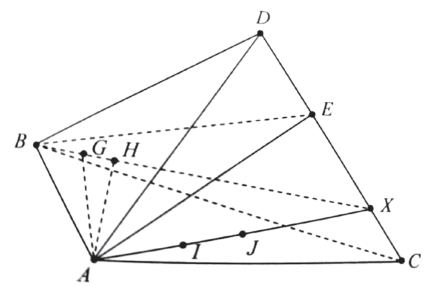


图1 差序列（2，3，21）对应的赋值函数

例 4 用以下图 2 构造赋值函数 m(p)，可证这时满足差序列条件下对应的差序列为 4 维 H 类差序列中的上界序列。

图中 $ABD \backslash AB$ 表示：面 ABD 中去掉线 AB 后的点集。构造上述赋值函数需要技巧。从这些上界序列集出发，再适当减或增 i 序列的分量，并对赋值函数作适当调整变型，可以在紧必要条件范围内，构造出绝大部分差序列。这里我们研究出了具体的有效构造方法，如子空间集方法，落差法等。



$m(p)$	p
i_0-2	$p \in \widehat{ABD} \backslash \overline{AB}$, $p \in \overline{AG} \backslash \{A\}$, $p \in \{I, J\}$ $p \in \widehat{ABE} \backslash \overline{AB}$, $p \in \overline{AH} \backslash \{A\}$
i_0	$p = X$
i_0-1	其他

图2 4 维 H 类上界差序列集对应的赋值函数

四、成果简介

先来严密定义几乎所有重量谱的概念。由于对稍大的 k，q，正整数序列成为重量谱的充要条件不可能得到，于是退一步如下：令 $i_0<i$, M(i) 为满足重量谱必要条件的某类线性码 i 序列的数目，N(i) 为满足重量谱充分条件的该类线性码 i 序列的数目；若 i 趋于无穷时，M(i)/N(i) 的极限为 1，则称为该必要条件是几乎充分的，也称该充分条件

是几乎必要的；应用这个充分条件，确定的这类线性码的重量谱集，称为几乎所有重量谱。这里 i 趋于无穷就意味着码长趋于无穷。打个比方，必要条件确定的序列集像一个带皮的苹果，而充分条件确定的序列集像去了皮的这个苹果，两者差别极小，当苹果无穷大时，皮只是常数厚，相对于苹果为无穷小。苹果皮上的重量谱序列好比是非常复杂的斑点，难以确定，放弃了。

克楼夫等给出了一个序列成为重量谱的必要条件，它很重要，称它为条件 A。k 维时条件式子较多，这里不便给出，详可参文献［5］第 11 章。在 4 维时，由下例给出条件 A 的一部分（用差序列语言）。

例 5　4 维 II 型 H 类 q 元码的差序列的必要条件 A 如下：

$$i_0/q<i_1 \leqslant qi_0,$$
$$qi_1<i_2 \leqslant (i_0+i_1)q/(q+1),$$
$$i_0 \leqslant i_3 \leqslant q(q+1)\,i_1-i_2$$

以上条件确定的序列集可比喻成带皮的苹果。下面来削苹果皮：在上述 3 行不等式的左端加 q 的多项式，右端减 q 的多项式，这些多项式可比喻成苹果皮，已被我们计算确定，多项式次数不超过 6 次。对满足这新的 3 行不等式的所有序列（比喻成在削去了皮的苹果中的所有序列），我们用几何方法构造出了赋值函数，满足差序列条件。因此，所有 i 序列都是差序列，新条件是差序列的充分条件。因为 q 是取定常数（苹果皮是常数厚），而码长可趋无穷大，通过计算易知该充分条件是几乎必要的，用它确定了几乎所有这类重量谱，而必要条件 A 是几乎充分的。

条件 A 对 3 维 2 元码也是充分的，因而也是充要条件；但当 q 大于 2 时，就不是充分的了。对 3 维 q 元码、4 维 q 元码，我们用几何方法证明了条件 A 是几乎充分的。4 维 q 元 码分为两大类，称为 I 型、II 型，其中 II 型又包含 H、F 两小类。i_0 取定且比 q 大很多时，图 3 示意性地表示了：坐标平面 i_1Oi_2 中，条件 A 确定的这两大类差序列集，

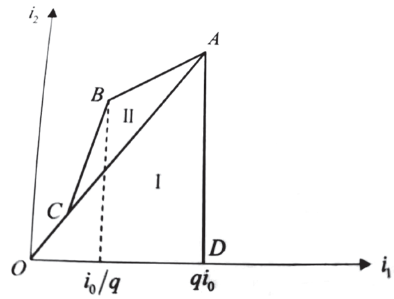


图3 坐标平面 i_1O i_2 中的 I、II两类差序列集

II 型中虚线右侧部分为例 5 的 H 类。

专著［5］包含的主要成果分 3 部分。

1. 关于低维码的重量谱

a）完全确定了以下码的所有重量谱：3 维 q 元码，q 不大于 5；对不是链码的类别，q 不大于 11；4 维 2 元码细分为 9 类的每一类；4 维 3 元码细分为 9 类中的 6 类；

b）确定了以下码的几乎所有重量谱：3 维、4 维 q 元码，5 维 q 元码中的两类。

2. 关于一般 k 维码的重量谱

由于不能使用具体的几何图形，比低维码困难得多。我与克搂夫的论文[6]，用结构复杂的赋值函数，确定了 k 维链码的几乎所有重量谱。我的博士后，骆源教授改进了上文，用极为漂亮简洁的结构，确定了更多的重量谱。我的两位博士生：刘子辉与王勇慧进一步分别确定了：类似链码的近链码与断链码的几乎所有重量谱[7,8]。

3. 关于派生重量谱

国际学术界集中研究重量谱时，导出了一系

列新的、可统称为派生重量谱的概念。如环上重量谱、贪婪重量谱、相对重量谱、维数 / 维度轮廓等；它们更复杂、困难，但又各有用处。骆源等在 IEEE Trans. Information Theory 上发表的文献 [9] 中原创性地提出了相对重量谱的概念与理论，当通信网中某些明文有泄漏被窃听到时，就导出了相对重量谱的概念。刘子辉用有限射影几何方法，针对上述各种派生重量谱，发表了一系列成果。

从专著发表的 2012 年后至今，我们又进一步研究，发表了十余篇论文。我在武汉的学生，青年教师王丽君、胡国香等取得了若干成果：王丽君等把 5 维重量谱分成 6 类，总共确定了 4 类 5 维 q 元码的几乎所有重量谱，发表 4 文，文献 [10] 为其中一篇；胡国香等把剩下的较困难的第 6 类再分成 6 小类，确定了 3 小类 5 维 q 元码的几乎所有重量谱，发表 3 文，文献 [11] 为其中一篇。至此，仅有一类半 5 维码的重量谱没被确定了。

我在文献［12］中，用递推算法解决了 k 维 q 元码的分类问题。

刘子辉等发表了一系列论文，对低维码的相对重量谱等，用有限射影几何方法做了进一步研究。最近，他们有两篇论文发表在 IEEE Trans. Information Theory 上[13,14]，他们得到了国家自然科学基金委的书面表扬，并两次获基金委资助面上项目 。

五、重量谱集猜想

公开问题 2 至今仍是未解决的难题。王丽君等在文献［10］等中证明了：重量谱的必要条件 A，对某些类 5 维 q 元码不是几乎充分的，并找出了新的几乎充分的必要条件。前面把条件 A 打比方为带皮的苹果，现在发现它被咬了一口（像苹果公司的商标），对一般 k 维 q 元码，苹果到底被精确咬掉了多少？我们提出以下猜想。

重量谱集猜想：对一般 k 维 q 元码，在条件 A 的基础上，用递推算法与有限射影几何方法结合，可以得到重量谱新的必要条件，它是几乎充分的。用它可确定几乎所有重量谱，解决问题 2。

在当今的人工智能、计算机算法时代，递推算法解也是一个好的解答，它可从 4 维解推出 5 维解…… 从 k 维解推出 k+1 维解。可以估计：几乎所有重量谱集本身就是一大堆“积木”似的序列集堆在一起，本身不大可能有非递推的解。4 维时，它是图 3 示意的坐标平面 i_1Oi_2 中的两块“积木”。

为了证明这个猜想，建议按以下三步走：

1. 先解决 5 维 q 元码，确定剩下的一类半的几乎所有重量谱。这里有困难，但估计花时间后能克服。

2. 从 4 维递推到 5 维。这步很难，本质上是要从 4 维码的赋值函数，递推构造出 5 维码需要的全部赋值函数。

3. 得到从 k 维递推到 k+1 维的算法，也很难。

欢迎对问题 2 有兴趣的年青学者，来投身这一猜想。

作者与克楼夫教授合影

参考文献

[1] W D Chen，T Klove. The weight hierarchies of q−ary codes of dimension 4, IEEE Trans. Information Theory，1996，42(6)：2265−2272.

[2] W D Chen，T Klove. Bounds on the weight hierarchies of q−ary codes of dimension 4,IEEE Trans. Information Theory，1997，43(6)：2047−2054.

[3] W D Chen，T Klove. Weight hierarchies of extremal non−chain binary codes of dimension 4, IEEE Trans. Information Theory，1999，45(1)：276−281.

[4] W D Chen，T Klove. On the second greedy weight for linear codes of dimension at least 4, IEEE Trans. Information Theory，2004，50(2)：354−356.

[5] 陈文德，刘子辉. 码的重量谱——有限射影几何方法，中国科学技术大学出版社，2012，

[6] W D Chen，T Klove. Weight hierarchies of linear codes of satisfying the chain condition， Des. Codes Criptogr，1998，15(1)：47−66.

[7] Y Luo, M Chaichana, A J H Vinck, et al. Some new characters on the wire−tap channel of type II,IEEE Trans. Information Theory，2005，51(3)：1222−1229.

[8] Z H Liu, W D Chen. Weight hierarchies of linear codes of satisfying the near−chain condition，Progress in Natural Science，2005, 15(9)：784−792.

[9] 王勇慧，陈文德. 一类满足断链条件线性码的重量谱， 北京邮电大学学报， 2004， 27(5)：21−25.

[10] L J Wang, W D Chen. The determination on weight hierarchies of q−ary linear codes of dimension 5 in class IV,Journal of Systems Science and Complexity, 2016, 29(1): 243−258.

[11] 胡国香，张焕国. VI−2 类 5 维 q元线性码的汉明重量谱的确定，通信学报，2016，37(2)：98 ~ 105.

[12] 陈文德. k维q元线性码重量谱的分类，应用数学学报，2012，35(5)：918−927.

[13] L Bai, Z H Liu. On the second relative geeedy weight of 4−dimension codes, IEEE Trans. InformationTheory，2019, 65(9)：5503−5518.

[14] Z H Liu. Y Wei. Further results on the relative generalized Haming weight, IEEE Trans. Information Theory，2021, 67(10)：6344−6355.

【作者简介】陈文德，中国科学院数学与系统科学研究院研究员，博士生导师。毕业于中国科学技术大学，曾是华罗庚的研究生。研究兴趣为：编码理论，控制理论与工程，堆垒数论。共发表论文 100 余篇，编著图书 4 本。20 余次出访欧美 20 余国，在欧洲大学做合作研究共计近 3 年。获得哈佛大学何毓琦院士颁发的“何潘清漪论文奖”。曾任中国电子学会信息论分会委员及国内外某些学术刊物的编委。主持国家自然科学基金面上项目 4 项。小传收入美国出版的《世界名人录》。