# 纠错编码技术

《通信译丛》编辑部
一九七四年十二月

# 前　言

由于实践的需要，在五十年代初逐步形成的编码技术，近年来有了很大发展。到目前，它已成为信息论的一个重要分支。现在纠错码广泛应用于高频通信、对流层散射通信、卫星通信和宇宙通信、遥测遥控、电话信道、计算技术、雷达、水声等电子学的各个领域。

随着数字集成电路工艺的发展，几年前在实现上还很复杂的编码技术在实践上得到了重大的突破。例如：利用 Viterbi 算法制成的译码器，功耗只有 6.8瓦，体积只有 9 立方英寸，重量仅为半磅，信息传输速率可达 2 万比特/秒。今后，随着分子电路、微微组件等各种新工艺的发展，编码技术一定会有更大的发展。

遵照伟大领袖毛主席**“洋为中用”**的教导，我们编译了这本《纠错编码技术》，供有关同志参考。本书译自美国“IEEE 通信技术汇刊”1971年第 5 期“纠错码专辑”（13篇），另附“1967～1972年编码理论述评”、Goppa 码和二进制卷积码介绍各一篇，共计 16 篇，约二十余万字。内容主要介绍近年来国外编码理论的三个重大发展：BCH 码的Berlekamp 算法、卷积码的 Viterbi 算法和话频电话信道用的捕获突发技术。这几种译码技术中最有发展前途的要算 Viterbi 算法，近年来受到各方面的极大重视。

本书的翻译工作曾得到四机部情报所的大力帮助，由该所英训班的学员承担了大部分翻译工作，我们谨此表示谢意。由于我们水平有限，本书的错误之处一定不少，敬请读者批评指正。

编　者

一九七四年九月

# 目　录

# 1967—1972年編碼理論述評*


## 提　　要

本文评述了 1967—1972 年间发表的编码理论文献，其中有四方面的贡献被认为是有特殊价值的。本文还简述了几本仅与编码理论有关的书籍，概述了作者所选英文杂志中的主要论文，引证了 100 多篇文献用作这些论文的参考材料。


## 一、引　　言

人们研究代数编码的原动力，乃是探索实现信息论的有效技术，亦即可靠地恢复受噪声干扰的数字数据。这些研究集中在探索具有充分结构的码以供具有中等复杂程度的编码和译码设备使用。总的目标是把山农（Shannon）的概念变成工程系统，而改善这些系统的性能，却要付出一定的代价并增加系统的复杂性。这个目标在某些应用中（例如宇宙通信和计算机高密度存贮）已经达到。由于成本高和带宽的限制，编码在其它一些利用中（例如电话线路上的低速率数据传输）还不能证明是有效的。

就编码理论领域而言，1967—1972年既是稳定发展和成熟的阶段，又是某些方面开始进步的阶段。因为研究开始进步的阶段要比谈论成熟的东西更为有意义，所以本文就从作者认为属于这一范畴的文献中四方面的贡献开始加以述评（关于本文采用的一些编码方面的术语，将在第四节中给出定义）。然后评论这一时期问世的一些书籍，并试图评述一下作者所选杂志中的主要论文。

## 二、四个杰出的贡献

1967年 Viterbi〔1〕发表了一篇关于在传输或存贮过程中出现随机错误时，对卷积码最大似然译码的论文。

这篇文章之所以具有很大意义，乃是因为它导致如下结果：(1) 找到了实现最大似然译码算法的一种有效方法，它是适用于短约束长度的卷积码；(2) 得到了固定计算的一种译码算法，与序列译码一样，可以计算软判决数据；(3) 可以有效地利用卷积编码器作为一种线性有限状态的机器；(4) 找到了有效处理通信和数据存贮中诸如符号间的干扰之类问题的方法〔2〕。后来该算法的最佳性得到了承认〔3〕—〔5〕。

---


* "A Survey of Coding Theory：1967—1972" (Invited Paper), J. K. Wolf, IEEE Trans on Information Theory, Vol.IT-19, № 4, July, 1973, PP.381～389.

第二个贡献乃是用于 BCH 码的 Berlekamp 译码算法。在 Berlekamp 的文章发表之前，这种见解已在 1966—1967 年间广为流传，直到 1968 年 Berlekamp 发表《代数编码理论》〔6〕一书时为止。这种算法可以大大减少译码时的计算次数，而其复杂程度只随着要纠错数的错误数的平方而增加，因此它适用于分组长度为数千位数的译码。例如，使用 50 毫微秒的开关逻辑，就可对分组长度为 1023、数字出现速率为 1 兆赫的任一 BCH 码进行译码〔6〕。这种译码算法的另一种方式乃是 Massey 提出的设计一种最小长度移位寄存器来产生一定的序列〔7〕。对于这种算法的微小改进乃是近年发表的文献〔8〕和〔9〕。

当 Viterbi 和 Berlekamp 的论文在 1967—1972 年间开始发表的时候，Justesen 又作出了这个时期的第三个贡献，他在 1972 年论述了任一编码速率为 R 的一种建设性的编码序列〔10〕，以致当分组长度增加时最小距离与分组长度之比接近于一个非零的极限。在速率为½时，这个极限典型地大约为 Varshamov〔11〕～Gilbert〔12〕可达距离限的 20%。这篇文章在 1972 年国际信息论讨论会全会上宣读时曾引起了极大的兴趣。Justesen 把连续码的概念〔13〕和以前由 Massey〔14〕所描述的一类码，巧妙地结合起来，对于在代数编码理论中被认为是许多尚未解决的若干经典问题提供了一种解决办法。在某种意义上，这种解决办法是令人失望的，因为它似乎不能开辟新的研究途径，也不能对错误控制提供有效的方法。然而，它引起对“建设性”一词的意义的仔细研究。

值得大家特别注意的第四个贡献，乃是 Goppa 在 1970 年和 1971年分别发表的两篇论文〔15〕〔16〕中论述的一类新码。这些码子是线性码，通常是非循环的，而这一类码当中有的循环码是 BCH码，BCH码的主要特点看来是根据它是这类码，而不是循环码这点得出的。最重要的是这一类中有一些码，其最小码距和分组长度之比满足于 Varshamov-Gilbert 限，而且可以用复杂程度适当的算法来译码。

## 三、图书方面

标志着编码领域成熟的图书有如下一些：Berlekamp 的著作〔6〕，Mann 主编的《纠错码》一书〔17〕，Lin 著的《纠错码引论》〔18〕，Van Lint 的《编码理论》〔19〕以及 Peterson 和 Weldon 合写的《纠错码》。这些书籍均是 1967 年以来出版的并且仅与编码理论有关。

Berlekamp〔6〕全面分析了分组码的代数理论，该书在某些方面有独特的见解，其中一章包括 BCH 码的新译码算法（参见该书的书评〔21〕）。

Mann 编了一本 1968 年举行的编码理论会议的会议录〔17〕，该书收录了 Mac Williams 写的一篇关于编码史的评述。

Lin 的书〔18〕是一本很好的编码入门书。为了达到这个目的，他限制该书的篇幅，大部分结果未加证明。该书特别实用于有实践经验而需要了解有关编码理论知识的工程师，同时又是阅读其他更为高深编码论著的入门书（其书评参见〔22〕）。

Van Lint 是一个数学家，因此他的专题论文〔19〕着重论述数学方面的编码理论。该书把编码作为数学科目来处理，而不是文献〔23〕所指出的作为完成可靠的消息传输的机构。

Peterson 和 Weldon 合写的著作〔20〕乃是 Peterson 的经典著作〔24〕的第二版，它包括了第一版的全部内容并且增加了同等数量的新材料和补充材料。例如：第一版第 18 页所

讨论的卷积码，在第二版中就占了60页。它的内容是最新的，对现有最新文献均作了最好的概述（其书评参见文献〔25〕）。该书〔20〕和Berlekamp的著作〔6〕，列出了非常全面的文献目录。

用一章或几章论述代数编码的书籍有：Balakrishnan所编《通信系统的进展》一书中Massey所写的《门限译码的发展》〔26〕、Lucky等人所著《数据通信原理》〔27〕、Jelinek所著《概率信息论》〔28〕、Gallager所著《信息论与可靠通信》〔29〕、Berger所著《速率失真理论》〔30〕和Stiffler所著《同步通信理论》〔31〕。关于苏联在1968年以前的编码理论研究方面的一篇综述是由Kautz和Levitt合写的〔32〕。

## 四、杂 志 方 面

本文的主要目的是为了评述编码理论近期研究的某些情况。因此我对其中某些课题作出简要说明，然后介绍有关各个课题现已发表的若干论文。当然不可能包括与一个课题有关的所有文章，我只选择了那些我认为最适用的文章。这些文章选自部分英文杂志。而且将本文限制在狭义的编码理论方面，忽略了有关编码的如下一些重要课题：无噪声信道、伪噪声序列、速率失真理论、随机编码、反馈通信等等。更多的限制则是讨论文章本身。

**1.分组码：构造和分析**

一个长度为n、大小为M的分组码，乃是不同矢量M的集合，这些矢量叫做码字，每个码矢具有n个分量，均属于某一个有限的字母表 $X=\{0, 1, 2, \cdots, q-1\}$。码的速率R定义为：

$$R=\frac{\log_q M}{n}.$$

因为码字是各不相同的，故 $1\leq M\leq q^n$ 且 $0\leq R\leq 1$。对于二进制编码来说，$q=2$ 而对于非二进制编码来说，$q>2$。通常q选择等于一个素（质）数或者是一个素数的某次幂。

码字的汉明重量等于该码矢中非零分量的数目。码的重量分布（或者是重量枚举）是一个表格，列出了包括每种可能重量（0，1，2，…，n）的码字数目。码的最小重量为正整数，等于码中一个码字的最小非零重量。

以后我们假设：X的元素形成一个有限域GF（q）（因而q等于一个素数或一个素数的某次幂）。如果码字均为一组r个齐次线性方程（即所谓广义奇偶校验方程）之解，则该代码称为线性码。这些方程的系数均为X中的元素。令 $K=n-r$，若方程是线性独立的，则 $M=q^k$，$R=k/n$，并且该代码表示为（n，k）码。一个码若不是线性码，就可以说是非线性码。

两个长为n的码矢之间的汉明距离，等于这些码矢中不同分量的数目。对于一个线性码来说，从任一给定的码字得出的汉明距离为i（$i=0, 1, 2, \cdots\cdots, n$）的码字数目，等于重量为i的码字数目。在一个代码中，一对不同码字之间的最小汉明距离 $d_{min}$（或是一个线性码的最小重量）就是衡量关于该代码纠正随机错误能力的重要因素。而了解有关所有各对码字之间全部距离或者关于一个线性码的重量分布，这对确定代码检测随机错误能力来说是必需的。

大量的研究则致力于求得各具体代码的重量分布和最小重量。Gleason多项式〔33〕—

〔35〕就是对计算重量分布问题的一个重大贡献。重量分布以前只能用大型计算机来计算，现在已经能够手算了。在这方面大量的研究集中了所谓 Reed—Muller 码的一类二进制线性码的重量分布〔31〕—〔40〕。对于 $m>r$ 的每对正整数 m 和 r 来说，一个 Reed—Muller 码具有如下参数〔41〕：

$$n = 2^m$$

$$K = \sum_{i=0}^{r} \binom{m}{i}$$

$$d_{min} = 2^{m-r}$$

关于 Reed—Muller 码的推广，则在文献〔42〕—〔44〕和〔61〕中有所研究。最重要的一类线性码，乃是 BCH 码〔45〕—〔47〕。这些码是线性码，其系数是从任一有限域 GF(q) 中取得的，并且有如下参数：

$$n = \frac{q^m - 1}{c}, \quad m \geq 2$$

$$r \leq mt$$

$$d_{min} \geq 2t + 1$$

式中 t 是任一整数，c 是 $(q^m - 1)$ 的任一除数。Berlekamp〔48〕曾指出，当 $q = 2$ 和 $c = 1$ 时，这些约束对于大的 m 而言是渐近地严密的。这些码是大量研究的课题〔49〕，〔50〕，因为我们尚不了解这些普遍认为较好的代码的特殊构造方法。

BCH 码属于循环码这类普通码。循环码是线性码，其任一码字系数的循环排列也就是一个码字。Kasami 等人〔51〕给出了新的一类循环码，叫做多项式码〔52〕，它把许多其他码作为特例包括进去。同样，这些码在普通线性群中为不变量的更普通一类码〔53〕的特例。在讨论译码时将会更多地提到这些码。

分组码有一个与统计试验设计相类似的数学结构。新的设计是根据这种相似性质求得的〔54〕—〔57〕。

以循环行列式为基础的广义奇偶校验方程系数〔58〕这类码乃是一类特殊的准循环码〔59〕。在这里，只要将一码字的系数循环移动某一常数（$a>1$）的整数倍，就可保证得到一个码字。许多这类码子都非常好〔60〕。

关于多项式积重量保持特性（Weight—retaining properties）的一篇重要文章〔61〕，对于解决分组码和卷积码的许多新的电码结构问题提供了一种途径。

如在第二节中所讨论过的，某些 Goppa 码〔15〕〔16〕满足 Varshamov—Gilbert 限，同样也满足这个限的一类 $R = \frac{1}{2}$ 的电码也已找到〔63〕。有点类似于 Goppa 码的一族电码属于 Srivastava 码，并且已由 Helget〔64〕作了研究。另一族重要线性码（$n = 3\,d_{min}$）也有论述〔65〕。

当 Nordstsom 和 Robinson〔66〕发现了一种分组长度 $n = 15$、$M = 2^8$ 且 $d_{min} = 5$ 的非线性二进制分组码时，大家对非线性码的兴趣也增加了，因为构成这样线性码是不可能的。Preparata〔67〕加以推广，就得出了任一偶数 $m \geq 4$ 时 $d_{min} = 5$、$n = 2^m - 1$ 和 $M = 2^{2^m - 2m}$ 一类非线性二进制码。Kerdoek〔68〕通过任一偶数 $m \geq 4$ 时构造一个 $n = 2^m$、$M = 2^m$ 和 $d_{min} = 2^{m-1} - 2^{(m-2)/2}$ 的二进制非线性码的方法，把 Nordstrom—Robinson 码推广到低速率的应用中。在 $m = 6$ 时，这种码的码字比相应的 BCH 码多三倍。还推导出了 Preparata

码和 Kerdock 码的重量分布。这两种码的分布是作为对偶线性码一样对待的〔69〕。有人对其它非线性码加以综合〔70〕，其中包括一类 $d_{min}=3$ 的二进制码，其码字比最好的同类线性码还多。另一篇文献〔71〕证明存在一些非线性码，它们在一个很大的排列群里面是一个不变量且满足于 Varshamov—Gilbert 限。

Sloane〔72〕集中研究可以导致构造新码的理论问题，从而对代数分组码作出了杰出的评述。该评述引用了 149 篇参考文献，并在文章的结尾列有表格，列出所有分组长度等于 512 最小距离等于 30 的任何目前已知的二进制（线性的或非线性）码的码字的最大值。

当 dmin为奇数时，元素取自 GF（q）的理想码乃是一种分组码，其参数满足如下方程：

$$M=\frac{q^n}{\sum_{i=0}^{(d_{min}-1)/2}\binom{n}{i}(q-1)^i}$$

在编码理论的早期阶段，由 Golay 叙述了两个 $d_{min}>3$ 的非凡理想码，而放松了对其他码的热情探索。当证明了并不存在那些具有诱人的参数值的所谓理想码时，这种探索的效果就受到怀疑。后来这个问题终于放下了。Van Lint〔73〕证明，对于任何 $\alpha$ 和 $P<(d_{min}-1)/2$，在 GF（$q^2$）上没有其他理想码存在，而 Tietäväinen〔74〕则完成了在 $P>(d_{min}-1)2$ 时的情形。

Varshamov〔75〕论述了一类用于非对称错误信道的码，在这种信道里，接受一个符号的错误要多于另一个符号。McEliece〔76〕指出，在用于同样目的情况下，这些码比 BCH 码更为有效。

算术码乃是可以用来检验数字计算机中算术单元运算情况的分组码。第 i 个码字的系数等于整数 $N_i$（$0\leq N_i<q^n$）的展开式诸系数，该整数用常用的位置数即基数 q 表示。一个 AN 算术码乃是表示小于“q”的所有整数 A 倍数的一组码字，而 A 是任意正整数。如果 A 是（$q^n-1$）的一个因子，则码字的每次循环移位仍是一个码字。

同样也可以求出算术权和算术距离。文献〔77〕和〔78〕讨论了用于多重纠错的新型算术码。而 Massey 和 Garcia〔79〕则着重评述 AN 码中循环 AN 码。Slepian〔80〕介绍了为高斯信道设计的一类重要的分组码，这些码与所有前面讨论过的那些码的不同点，在于码字分量是从实数域，而不是从有限域中取得的。码字是一个单位球体上诸点的子集，并且具有群的性质，这意味着任一码字与所有其它码字之间的欧几里德距离，对于每一个码字来说均是相同的。（然而〔81〕指出，不是所有具有这种性质的码均属于这类码。）后来又有大量文献研究了用于高斯信道的编码〔82〕—〔87〕，而有关这方面的一篇杰出文献乃是 Wyner 写的《关于编码与信息论》〔88〕。

**2．分组码：译码**

当码字在通信信道上传送时，如果接收到的字总是同发送的字完全一样，则不需要编码。更确切地说，有干扰的通信信道会使发送的码字产生随机失真。来自 $(X)^n$（来自输入字母表 X 的 n 个符号的序列空间）输入 n 个矢量并且来自 $(Y)^n$（这里 Y 是输出字母表）输出 n 个矢量的信道，对于所有 $x\in(X)^n$ 和 $y\in(Y)^n$ 来说，可以用条件概率分布 $P_{y|x}(y|x)$ 来描述。这里 X 和 Y 分别是同信道的 n 个输入及输出矢量是有关的 n 维随机矢量，而 X 和 Y 则是可以由这些矢量假设的特值。上述说明用在一个记忆存贮系统中同样很好。

编码器乃是用一个译码准则在以接收矢量 y 为基础的传输码字中进行选择的一种设备。

有时可能选择的完全不是码字，这种情况就叫做检错，这种情况经常用于码字的再传输或者从记忆装置中重读。一种总是译成一个码字的特殊译码准则，乃是在给定接收矢量 y 的同时，使所选择的码字在传输时具有最高的条件概率。如果所有的码字均具有相等的先验概率，那么就选择 $P_{y|x}(y|c_i)$ 为最大值的码字 $c_i$，这个准则就叫做最大似然译码准则。这个准则的一种平滑应用(A brute-force application)要求对条件概率分布作 M 次计算。对于一个分组长度为 n = 100、速率 R = $\frac{1}{2}$ 的二进制码来说，这种应用要作出 $2^{50} \approx 10^{15}$ 次计算，即使用大型的计算机也无法完成这一任务。这就是能使我们摆脱困境的代数结构编码。用于代数分组码的大多数译码准则均不能实行最大似然译码准则。更确切地说，只有在信道中的噪声不太大时，才译成最有可能的码字。换句话说，可以选择不译码。这一准则就叫做有界距离译码准则。

以前〔6〕〔7〕所介绍的 BCH 码的 Berlekamp 译码算法就是一种有界距离译码准则，它要求 X = Y 并且仅当接受矢量和传输码字的汉明距离不超过 $(d_{min})/2$ 时，才能正确译码。这些码使用这种译码算法的潜力仍未充分发掘出来。

有一类码不如 BCH 码有力但译码较简单，这就是大数逻辑可译码。这类码已由 Rudolph 在其经典文献〔89〕中加以讨论，该文最初在 1963年提出，但到 1967 年才发表。这些码子的广义奇偶校验方程以有限几何形状的组合形态为基础。在最简单的情况下，这些码的译码是按符号逐个进行的。对于每一个符号来说，若干个广义奇偶校验方程是经过检验的，每个方程预示着该符号是GF (q) 的一个特殊元素。收到大多数表决的该域元素对于那个符号取正确值。前面讨论过的一些码均可用这种方法进行译码〔43〕〔44〕〔51〕。已经有人用这种译码方法设计出具体的码〔90〕、〔91〕。最近有人证明任一码在原则上均可用广义奇偶校验方程的适当加权表决，来实现任一译码准则〔92〕。

刚才讨论过的两种译码算法，均要求输出字母表 Y 等于输入字母表 X。如果在传输中使用模拟波形，则要求接收机量化新接收到的波形，这是破坏译码中有用信息的一个过程。由 Forney〔93〕提出的一种技术，即广义最小距离译码，由Reddy〔94〕应用于二维码 (Two dimensional codes) 的译码，而不受它们的最小距离的限制。这种技术又是 Weldon 的消权 (Weighted-erasure) 译码〔95〕的基础，这种译码用在输入字母表是输出字母表的一个适当子集的情况下。另外两种译码技术则专门用于输出字母表大于输入字母表的一些信道〔96〕、〔97〕。

线性码的子码乃是码字同样为线性码的码字之适当的子集。Reddy〔98〕介绍了一种重要的译码算法，用于子码采用译码算法的线性码。

上述内容仅仅选取了若干题目，纵观分组码及其译码算法。而大量重要的题目则在本篇有限的评述中被忽略过去，诸如编码参数的限、突发纠错分组码、编码同步、使用非汉明量度的码，以及图解原理码(Graph-theoretic codes) 等等。

**3．树形码、栅格码和卷积码：编码结构和分析**

考虑一种如图 1 所示的树形码，图中的小圆圈是节点，从每个节点引出的辐射线是分支。假定每个节点的辐射分支数为 Q，每个分支在字母表 { 0，1，2，…，q—1 } 中具有 $n_0$ 个符号的序列。一个树形码就是每个独特支路通过该树时，由分支上一连串符号组成的序列（可能为无限数）子集。应当注意，虽然在该码中有无穷多个码字，但每个码字的前面 $n_0$ 个符号仅能假设为 Q 个不同的实现。而且还要注意，如果我们允许每个支路仅包含 L 个分支从而构成该树，则我们得到的分组码，其分组长度为 $n = n_0 L$，码字数为 $M = L^Q$。

(这里码字可能不都是相异的)。树形码的速率定义为 $R_0 = (1/n_0)\log_q Q_0$。

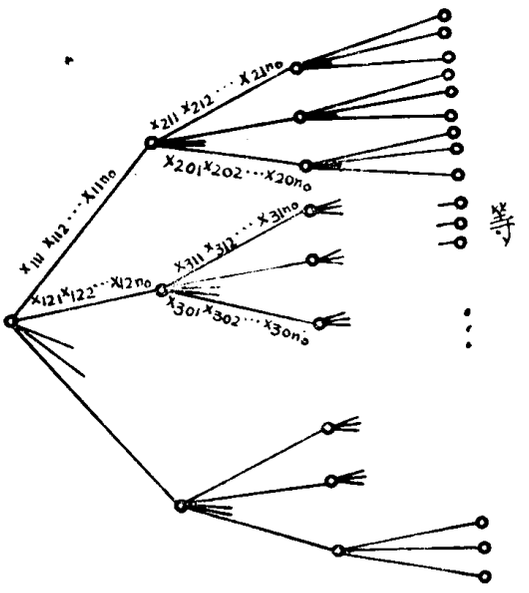


图 1　树形码

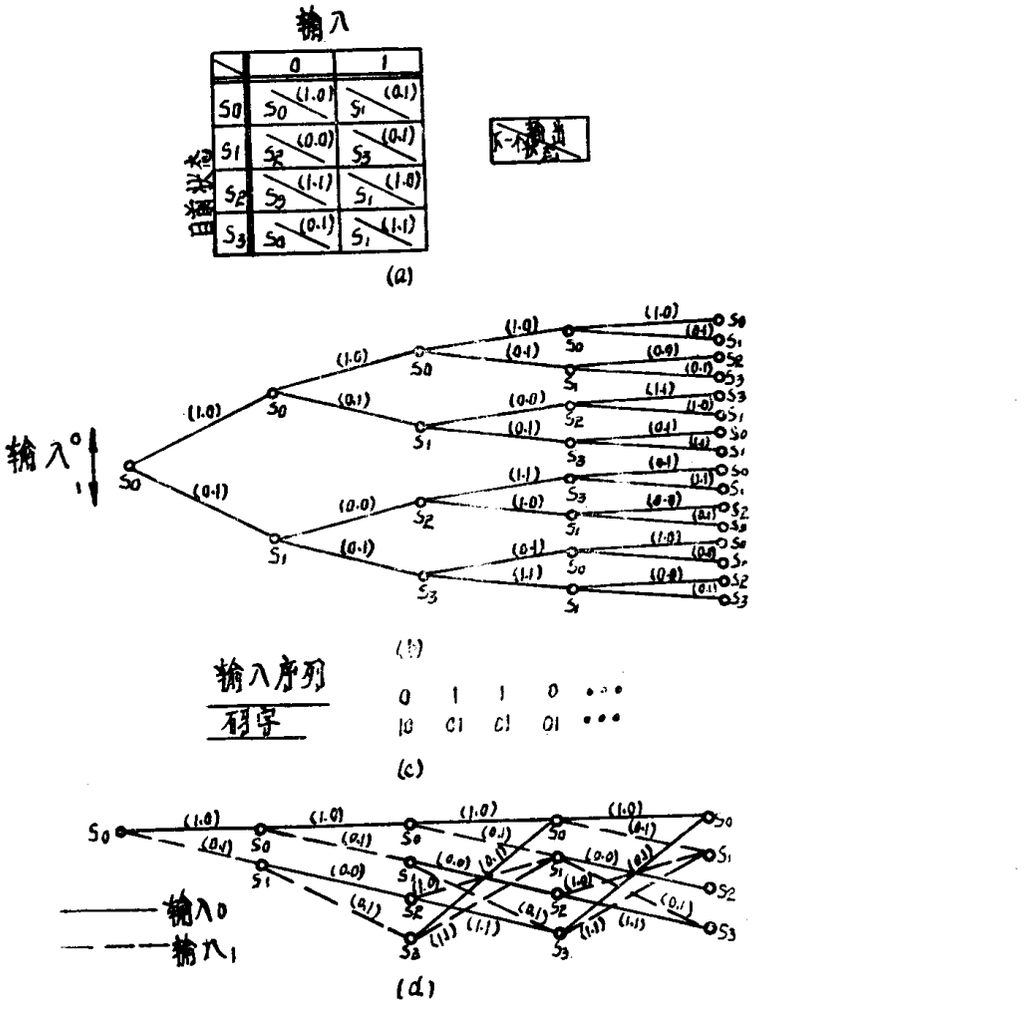


图 2

(a) 状态转移表 (b) 相应的树形码 (c) 输入序列和码字 (d) 栅格结构

现在我们来介绍某种树形结构。假定该树是用一个具有 K 个状态（$s_0, s_1, \cdots, s_{K-1}$）的机器产生的。该机器由集合 { 0, 1, …, Q − 1 } 输入，又由 $(X)^{n_0}$ 中输出，亦即输出是各分量从 X 来的 $n_0$ 矢量。

假定该机器总是由 $S_0$ 状态起动。在输入加来之前，该机器自始至终稳定在一个状态上。由于输入的作用，机器产生一个 $n_0$ 矢量输出并假定下一个状态。这种状态的变化和输出的产生，可用一个状态转换表来描述，表中列有每一个状态和每一个输入，还有下一个状态和相应的输出。

为了从一个 K 状态机器中得到一个树形码，把一个状态同每一个节点结合起来。于是输入就确定从 Q 个分支的那一个从该节点（状态）变到下一个节点（状态）。每一分支上的 $n_0$ 个符号就是该机器的输出。

关于一种四状态机器及其相应的树形码的状态转换表实例之一示于图 2 (a) 和 (b)，这里的 Q = 2，X = { 0, 1 }，$n_0 = 2$。输入序列和相应的码字则在图 2 (c) 中给出。应当注意，因为只有四个状态，所以该树中若干节点可能摺叠成单个的节点。由于这些节点的摺叠，该树形成如图 2 (d) 所示栅格。因此我们说，一个有限状态机器产生一个栅格码。

考虑有一种 X 为有限域 GF(q)、且 $Q = q^{k_0}$，$1 \le K_0 \le n_0$ 的栅格码。于是每一个输入可以看成一个分量从 X = GF(q) 中获得的 $K_0$ 矢量。令输出的 $n_0$ 个分量是这一个输入矢量的 $K_0$ 个分量紧接与前面 υ 个矢量的 $\upsilon K_0$ 个分量的一个固定线性函数。这里“线性”表示如同 GF(q) 中所定义的那样，这些分量相加和相乘以后所得到的加权和。该机器状态的数目绝对不能超过 $q^{\upsilon k_0}$，所产生的栅格码就是一种约束长度为 υ（或 $K_0\upsilon$）的卷积码。该码的速率为 $R_0 = (1/n_0)\log_q Q = k_0/n_0$。

图 3 (a) 和 (b) 示出具有参数为 q = 2，$K_0 = 1$，$n_0 = 2$，υ = 2 的卷积码的状态转换表和栅格。以一个两级移位寄存器实现的这种有限状态机器则示于图 3 (c)。关于卷积码代数结构的综述为 Forney [99] 给出。

如果 $K_0$ 个输出符号等于当时输入 $K_0$ 矢量，那么这种卷积码就叫做系统卷积码。反之则叫做非系统卷积码。Bucher 和 Heller [100] 指出，对于随机错误信道上的最大似然译码来说，非系统卷积码优于系统卷积码。之所以会有这个意外的结果，是因为每种分组码均相当于一种系统分组码，但是并非每种卷积码都等于一种系统卷积码 [99]。

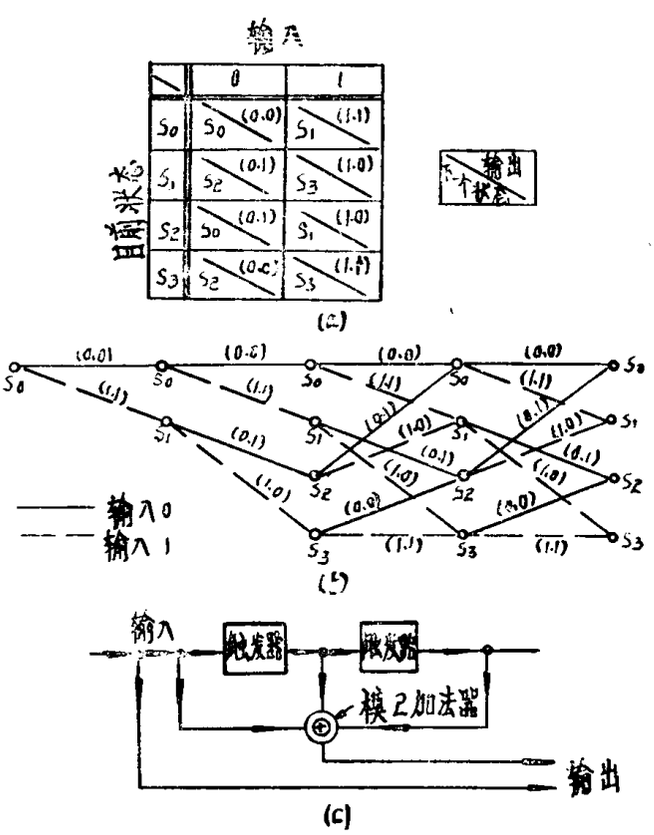


图 3 (a) 卷积码的状态转换表
(b) 卷积码的栅格
(c) 译码器

卷积码的码距有两个计量单位：1．不同码字最初 $(v+1)n_0$ 个符号之间的最小非零汉明距离 $d_{min}$，2．无穷长度的不同码字之间的最小非零汉明距离 $d_{free}$。对于更好的译码算法来说，自由距离 $d_{free}$ 似乎与编码性能的关系更为密切〔101〕。现在已经找到计算卷积码自由距离的一种有效算法〔102〕，同时也发现了探测好码的一种简便方法〔103〕。还有一篇论文〔104〕则研究速率为 $R_0=1/n_0$ 的码字的某些重要特性。

文献〔105〕论述了有记忆信道上成功使用的卷积码。与之密切相联的一种叫做捕获突发技术〔106〕—〔108〕则可用于分组码或者卷积码。至于有关为有记忆信道设计的分组码和卷积码的详细讨论，可参看 Forney 的文章〔124〕。

在设计构造长约束长度的好卷积码方面目前无成效，只是文献〔109〕报导了这方面的某种进展。

**4．树形码、栅格码和卷积码：译码**

接收矢量 y 给定时，要在树形码中求出最可能的码字，而不必探索整个树，序列译码就是最有效的一种方法。在序列译码当中，接收字母表Y要不等于X。因此，接收序列的量化所引起的损耗是能够避免的。在序列译码中，我们从第一个节点开始，并且试验性地选择编码符号与接收序列部分所产生符号的最大似然分支。试验选择的编码符号与相应的接收序列之间差异量度的一种方法已保留下来。我们通过试验选择从每一个连续的节点中选择最大似然分支，直到增长速率表明下一个路径为错误路径时止。然后我们用继续反回到以前的节点并取一个最小似然分支，以便进行反回跟踪。交替使用反回跟踪路径和试验路径，直至找到差异量度的增长速率令人满意的那个路径。当然，使用此法的关键性因素乃是选择适当的差异量度，并找出一种方法，以便确定这种量度的增长速率是否令人满意。早在1963年，Fano〔110〕就发表了有关这种算法的讨论，Zigangirov〔111〕则分析一种只允许有限次数反回搜索的译码器。

对于序列译码来说，每一个节点计算的次数乃是一个随机变量，其分布首先由 Savage〔112〕证明为 Pareto分布。Jacobs 和 Berlekamp〔113〕证明：该分布对于一大类序列译码算法是适用的。

这种算法的一个主要的改进是由 Zigangirov〔114〕和Jelinek〔115〕分别求得的。这种新方法叫做迭加算法（Stack algorithm）。这里，译码器存入若干路径的差异量度并扩大到最大似然为正确的那个路径。当路径由于差异量度的增长速率而被暂时放弃时，则扩展到下一个最大似然路径。所有要研究的路径均存入译码器，直到超出译码器存贮容量为止。然后根据情况丢掉最小的似然路径。这个译码器的性能可以同那种范诺译码器〔116〕相媲美。

包含代数码和卷积码在内的混合方案已经提出〔117〕，〔118〕，就其最简单的形式而言，它们包含若干独立的卷积编码序列，这些卷积编码序列与一个加性序列一起传输，后者的第 i 个符号是若干卷积码字中第 i 个符号的线性组合。在译码过程中，这个线性方程要对每一个符号进行校验，并且这个信息要用于卷积码字的译码。当一个码字被整个译码（或者通过一给定点足够远）时，则在校验线性方程时，被译码的符号要代之以接收符号。这一方案可以有效地运用于编码速率高于普通序列译码的情形。

由于卷积码具有一栅格结构，因而在引言中强调过的 Viterbi 卷积码最大似然译码器〔1〕就有很大的实用价值。事实上，它可以应用于任何栅格码，仅仅是卷积码。该方法的实质是对于栅格中的任何一个节点仅仅保持一个路径。当然，所保持的路径是一个最大似然的

路径。对于任何一个节点来说，所丢弃的路径决不可能导致最大似然的码字。如果栅格是用一个 K 状态的机器产生的，则仅有 K 个路径需要由译码器加以保留。

在这六年间，对序列译码的兴趣明显地移到 Viterbi 译码上来了。这在分析和实现用于无记忆信道（例如宇宙信道）时特别明显。

正如在评述分组码时那样，在评述树形码时也省略了许多问题，其中包括卷积码的代数译码及与其有关联的课题，诸如错误传播和卷积码的参数界限等等。

虽然分组码理论乃是已发表的有关编码的大多数文章的中心问题，但是卷积码在很多应用中已证明是比分组码优越〔119〕〔120〕。有关这方面的另一述评将要进一步讨论这个问题〔125〕。读者也可以参考三本有关编码在通信和计算机中的应用的杂志特辑〔121〕—〔123〕。

## 五、结　论

在 1967—1972 年间，编码理论的发展已产生了大量重要的成果，当然在这方面还有许多未解决的问题。对将来的研究，特别有影响的领域要算编码结构和有关卷积码的分析。将来如能产生一种能给出相当可观的自由距离与约束长度之比并且译码复杂程度适当的编码结构，则有待下一篇述评再作论述。

在编码理论的发展阶段中，我想把这一时期叫做中期阶段。也许我们已经看到这一阶段的大部分贡献，然而更可能的是，在编码理论的成熟阶段将会大大超过其中期阶段所取得的这些成就。

## 参 考 文 献


〔1〕A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," IEEE Trans. Inform. Theory, vol. IT-13, pp. 260-269, Apr. 1967.

〔2〕G. D. Forney, Jr., "The Viterbi algorithm," Proc. IEEE, vol. 61, pp. 268-278, Mar. 1973.

〔3〕——, "Review of random tree codes," in Final Report on a Coding System Design for Advanced Solar Missions, appendix A, Codex Corp., Watertown, Mass., Contract NAS2-3637, Dec. 20, 1967 (no. N 68-16388).

〔4〕J. K. Omura, "On the Viterbi decoding algorithm," IEEE Trans. Inform. Theory (Corresp.), vol. IT-15, pp. 177-179, Jan. 1969.

〔5〕A. J. Viterbi and J. P. Odenwalder, "Further results on optimal decoding of convolutional codes," IEEE Trans. Inform. Theory (Corresp.), vol. IT-15, pp. 732-734, Nov. 1969.

〔6〕E. R .Berlekamp, Algebraic Coding Theory. New York: McGraw-Hill, 1968.

〔7〕J. L. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, Jan. 1969.

〔8〕H. O. Burton, "Inversionless decoding of binary BCH codes," IEEE Trans.

Inform. Theory, vol. IT-17, pp. 464-466, July 1971.

[9] D. D. Sullivan, "A branching control circuit for Berlekamp's BCH decoding algorithm," IEEE Trans. Inform. Theory (Corresp.), vol. IT-18, pp. 690-692, Sept. 1972.

[10] J. Justesen, "A class of constructive, asymptotically good algebraic codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 652-656, Sept. 1972.

[11] R. P. Varshamov, "Estimate of the number of signals in errorcorrecting codes," Dokl. Akad. Nauk. SSSR, vol. 117, pp. 739-741, 1957.

[12] E. N. Gilbert, "A comparison of signalling alphabets," Bell Syst. Tech. J., vol. 31, pp. 504-522, May 1952.

[13] G. D. Forney, Jr., Concatenated Codes. Cambridge, Mass.: M.I.T. Press, 1966.

[14] J. L. Massey, Threshold Decoding. Cambridge, Mass.: M.I.T. Press, 1963.

[15] V. D. Goppa, "A new class of linear correcting codes." Probl. Peredach. Inform., vol. 6, pp. 24-30, 1970.

[16] ——, "Rational representation of codes and (L,g) codes," Probl. Peredach. Inform., vol. 7, pp. 41-49, 1971.

[17] H. B. Mann, Ed., Error Correcting Codes. New York: Wiley, 1968.

[18] S. Lin, Introduction to Error Correcting Codes. Englewood Cliffs, N. J.: Prentice-Hall, 1970.

[19] J. H. Van Lint, Coding Theory. Berlin, Germany: Springer, 1971.

[20] W. W. Peterson and E. J. Weldon, Jr., Error Correcting Codes, 2nd ed. Cambridge, Mass.: M.I.T. Press, 1972.

[21] R. T. Chien, "Review of Algebraic Coding Theory," IEEE Trans. Inform. Theory (Book Rev.), vol. IT-15, pp. 509-510, July 1969.

[22] J. L. Massey, "Review of An Introduction to Error-Correcting Codes," IEEE Trans. Inform. Theory (Book Rev.), vol. IT-17, pp. 768-769, Nov. 1971.

[23] E. R. Berlekamp, "Review of Coding Theory," IEEE Trans. Inform. Theory (Book Rev.), vol. IT-19, p. 138, Jan. 1973.

[24] W. W. Peterson, Error Correcting Codes, 1st ed. Cambridge, Mass.: M.I.T. Press, 1961.

[25] J. L. Massey, "Review of Error Correcting Codes (second edition)," IEEE Trans. Inform. Theory (Book Rev.), vol. IT-19, pp. 373-374, May 1973.

[26] ——,"Advances in threshold decoding," in Advances in Cemmunication Systems, A. V. Balakrishnan, Ed. New York: Academic Press, 1968.

[27] R. W. Lucky, J. Salz, and E. J. Weldon, Jr., Principles of Data Communication. New York: McGraw-Hill, 1968.

[28] F. Jelinek, Probabilistic Information Theory .New York: McGraw-Hill, 1968.

[29] R. G. Gallager, Information Theory and Reliable Communication. New York: Wiley, 1968.

[30] T. Berger, Rate Distortion Theory. Englewood Cliffs, N.J.: Prentice-Hall, 1971.

[31] J. J. Stiffler, Theory of Synchronous Communications. Englewood Cliffs, N.J.: Prentice-Hall, 1971.

[32] W. H. Kautz and K. N. Levitt, "A survey of progress in coding theory in the Soviet Union," IEEE Trans. Inform. Theory, vol. IT-15, part II, Jan. 1969.

[33] A. M. Gleason, "Weight Polynomials of self-dual codes and the MacWilliams identities," in 1970 Acta Congr.Int. Math., vol. 3. Paris: Gauthier-Villars, 1971, pp. 211-215.

[34] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, "Gleason's theorem on self-dual codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 409-414, May 1972.

[35] F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, "Generalizations of Gleason's theorem on weight enumerators of self-dual codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 794-805, Nov. 1972.

[36] N. J. A. Sloane and E. R. Berlekamp, "Weight enumerators for second-order Reed-Muller codes," IEEE Trans. Inform. Theory, vol. IT-16, pp. 745-751, Nov. 1970.

[37] E. R. Berlekamp, "The weight enumerators for certain subcodes of the second-order binary Reed-Muller codes," Inform. Contr., vol. 17, pp. 485-500, Dec. 1970.

[38] T. Kasami and N. Tokura, "On the weight structure of Reed-Muller codes," IEEE Trans. Inform. Theory, vol. IT-16, pp. 752-759, Nov. 1970.

[39] M. Sugino, Y. Ienoga, N. Tokura, and T. Kasami, "Weight distribution of (128, 64) Reed-Muller codes," IEEE Trans. Inform. Theory (Corresp.), vol. IT-17, pp. 627-628, Sept. 1971.

[40] E. R. Berlekamp and L. R. Welch, "Weight distribution of the cosets of the (32, 6) Reed-Muller code," IEEE Trans. Inform. Theory, vol. IT-18, pp. 203-207, Jan. 1972.

[41] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," IRE Trans. Inform. Theory, vol. PGIT-4, pp. 38-49, Sept. 1954.

[42] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, "On generalized Reed-Muller codes and their relatives," Inform. Contr., vol. 16, pp. 403-422, July 1970.

[43] T. Kasami, S. Lin, and W. W. Peterson, "New generalizations of the Reed-Muller codes—part I: Primitive codes," IEEE Trans. Inform. Theory, vol.

IT-14, pp. 189-199, Mar. 1968.

〔44〕 E. J. Weldon, Jr., "New generalizations of the Reed-Muller codes—part II: Nonprimitive codes," IEEE Trans. Inform. Theory, vol. IT-14, pp. 199-206, Mar. 1968.

〔45〕 R. C. Bose and D. K. Ray-Chaudhuri. "On a class of error correcting binary group codes," Inform. Contr., vol. 3, pp. 68-79, Mar. 1960.

〔46〕 ——, "Further results on error correcting binary group codes," Inform. Contr., vol. 3, pp. 279-290, Sept. 1960.

〔47〕 A. Hocquenghem, "Codes correcteurs d'erreurs," Chiffres, vol. 2, pp. 147-156, 1959.

〔48〕 E. R. Berlekamp, "Long primitive binary BCH codes have $d \sim (2n \ln R^{-1})/(\log n)\cdots$," IEEE Trans. Inform. Theory, vol. IT-18, pp. 415-426, May 1972.

〔49〕 T. Kasami and N. Tokura, "Some remarks on BCH bounds and minimum weights of binay primitive BCH codes," IEEE Trans. Inform. Theory, vol. IT-15, pp. 408-413, May 1969.

〔50〕 C. R. P. Hartmann and K. K. Tzeng, "Generalization of the BCH bound," Inform. Contr., vol. 20, pp. 489-498, June 1972.

〔51〕 T. Kasami, S. Lin, and W. W. Peterson, "Polynomial codes," IEEE Trans. Inform. Theory, vol. IT-14, pp. 807-814, Nov. 1968.

〔52〕 S. Lin, "On the number of information symbols in polynomial codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 785-794, Nov. 1972.

〔53〕 P. Delsarte, "On cyclic codes that are invariant under the general linear group," IEEE Trans. Inform. Theory, vol. IT-16, pp. 760-769, Nov. 1970.

〔54〕 E. F. Assmus and H. F. Mattson, "New 5-designs," J. Combinatorial Theory, vol. 9, pp. 122-151, 1969.

〔55〕 V. Pless, "Symmetry codes over GF (3) and new 5-designs," J. Combinatorial Theory, vol. 12, pp. 119-142, 1972.

〔56〕 S. Lin, "Some codes which are invariant under a transitive permutation group and their connection with balanced incomplete block designs," in Proc. Conf. Combinatorial Mathematics and Its Applications. Chapel Hill, N. C.: Univ. North Carolina Press, 1967.

〔57〕 P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," MBLE Res. Lab., Brussels, Belgium, Rep. R. 184, June. 1972.

〔58〕 M. Karlin, "New binary coding results by circulants," IEEE Trans. Inform. Theory, vol. IT-15, pp. 81-92, Jan. 1969.

〔59〕 R. L. Townsend and E. J. Weldon, Jr., "自正交准循环编码" 译文见《通信译丛》1971年第3期第17～33页。

[60] E. J. Weldon, Jr., "Long quasi-cyclic codes are good," presented at the 1969 Int. Symp. Information Theory, Ellenville, N.Y.

[61] J. L. Massey, D. J. Costello, Jr., and J. Justesen, "Polynomial weights and code constructions," IEEE Trans. Inform. Theory, vol. IT-19, pp. 101-110, Jan. 1973.

[62] V. D. Goppa, "A new class of linear error-correcting codes," Probl. Peredach. Inform., vol. 6, pp. 24-30, 1970.

[63] V. Pless and J. N. Pierce, "Self-dual codes over GF(q) satisfy a modified Varshamov-Gilbert bound," Inform. Contr., to be published.

[64] H. J. Helgert, "Srivastava codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 292-297, Mar. 1972.

[65] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," IEEE Trans. Inform. Theory, vol. IT-18, pp. 503-510, July 1972.

[66] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," Inform. Contr., vol. 11, pp. 613-616, Nov. 1967.

[67] F. P. Preparata, "A class of optimum nonlinear double error correcting codes," Inform. Contr., vol. 13, pp. 378-400, Oct. 1968.

[68] A. M. Kerdock, "A class of low-rate nonlinear codes," Inform. Contr., vol. 20, pp. 182-187, Mar. 1972.

[69] F. J. MacWilliams, N. J. A. Sloane, and J. M. Goethals, "The MacWilliams identities for nonlinear codes," Bell Syst. Tech. J., vol. 51, pp. 803-819, Apr. 1972.

[70] N. J. A. Sloane and D. S. Whitehead, "New family of single-error correcting codes," IEEE Trans. Inform. Theory, vol. IT-16, pp. 717-719, Nov. 1970.

[71] R. J. McEliece, "On the symmetry of good nonlinear codes," IEEE Trans. Inform. Theory, vol. IT-16, pp. 609-611, Sept. 1970.

[72] N. J. A. Sloane, "A survey of constructive coding theory, and a table of binary codes of highest known rate," Discrete Math., vol. 3, pp. 265-294, 1972.

[73] J. H. Van Lint, "Nonexistence theorems for perfect error-correcting codes," in Computers in Algebra and Number Theory, SIAM-AMS Proc., vol. 45, G. Birkhoff and M. Hall, Jr., Eds., 1970, pp. 89-96.

[74] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," SIAM J. Appl. Math., vol. 24, pp. 88-96, Jan. 1973.

[75] R. R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers," IEEE Trans. Inform. Theory, vol. IT-19, pp. 92-95, Jan. 1973.

[76] R. J. McEliece, "Comment on 'A class of codes for asymmetric channels