第 19 卷 第 2 期
1997 年 3 月

电子科学学刊
JOURNAL OF ELECTRONICS

Vol.19 No.2
March 1997

分组码的格图结构和译码 [1]

马建峰　　王育民 *

(西安电子科技大学计算机学院 西安 710071)
*(西安电子科技大学通信工程学院 西安 710071)

摘 要 本文讨论了分组码的格图结构，给出了某些 BCH 码 L 段格图结构，并据此提出了 BCH 码的快速最大似然译码算法，同时讨论了 q^m 元分组码的 q 元映象的译码问题，给出了 q 元映象的直和划分结构和相应的译码算法。

关键词 格图，译码，BCH 码，RS 码，q 元象，直和划分

中图号 TN911.22

1 引 言

分组码是实现可靠数字通信的重要手段之一，但由于没有有效的最大似然软判决译码算法而限制了分组码的应用。所谓最大似然译码是指当所有码字的发送概率一样时，译码的错误概率达到最小的译码，软判决译码是指接收序列为实数序列 (如与信号相匹配的滤波器的模拟输出) 时的译码，亦即译码利用了信道的度量信息。Wolf[1] 提出分组码的格图理论，从而给出了分组码有效的 Viterbi 译码算法，而且证明了对于 (n,k) 线性分组码，其格图最多有 $q^{\min(n-k,k)}$ 个状态。Forney[2] 研究了分组码的格图结构，并导出了状态数最小的格图结构，证明了 RM 码有相当简单的 4 段格图结构，(24, 12, 8)Golay 码也有很简单的 3 段格图结构，从而提出这些码有效的最大似然译码算法。本文在此基础上，进一步讨论了分组码的格图结构，提出了相应的译码算法，分析了译码的时间复杂性。

2 分组码格图的构造

本节我们讨论线性分组码的 L 段格图结构，某些讨论也适合于非线性分组码。设 T 是 GF(q) 上的 (N,K) 线性分组码 C 的 N 段格图。对于 $0 \le h \le N$，设 S_h 表示 T 的第 h 段后的状态集合，$s = \log_q \max\{|S_h| : 0 \le h \le N\}$，称 s 为格图 T 的尺寸，则 $s \le \min(K, N-K)$[1] 。设 $L(s,s')$ 为从状态 s 到 s' 的所有路径的标号序列的集合，于是 $L(s_0,s_f) = C$，其中 s_0，s_f 分别为初始状态和终止状态。对于满足 $0 \le h_1 < h_2 \le N$ 的整数 h_1，h_2，设 C_{h_1,h_2} 是除第 h_1+1 个分量到第 h_2 个分量外其余分量均为 0 的码 C 的码字构成的集合，显然 C_{h_1,h_2} 是 C 的一个子码。设 C_{h_1,h_2} 的维数为 K_{h_1,h_2}，即 $K_{h_1,h_2} = \log_q |C_{h_1,h_2}|$，其中 $|C_{h_1,h_2}|$ 表示 C_{h_1,h_2} 中的码字的数目，对于满足 $0 = h_1 < h_2 < \cdots < h_m = N$ 的 m 个整数，存在码 C 的 $m-1$ 个线

[1] 1995-02-06 收到，1996-06-20 定稿
国家自然科学基金资助课题

性子码 $C_{h_1,h_2},\cdots,C_{h_{m-1},h_m}$，于是码 C 包含子码 $\oplus\sum_{i=1}^{m-1}C_{h_i,h_{i+1}}$，码 C 的格图尺寸 $s(C)\le K-\sum_{i=1}^{m-1}K_{h_i,h_{i+1}}+\max_{i=1}^{m-1}(s(C_{h_i,h_{i+1}}))$。

假设码长 N 是 L 的整数倍，则由码 C 的 N 段格图可得 L 段格图 $T(L)$: 删去 S_h 中的状态和与这些状态相连的分支，状态 $s\in S_{jN/L}$ 与 $s'\in S_{(j+1)N/L}$ 用一个标号为 α 的分支相连，当且仅当在码 C 的 N 段格图 T 中存在从 s 到 s' 的标号为 α 的路径，其中 $h\in\{0,1,\cdots,N\}-\{0,N/L,2N/L,\cdots,N\}$, $0\le j<L$。显然 $T(N)=T$。$T(L)$ 中相邻两个状态可能有标号不同的并行分支，每个分支代表 N/L 个码元。事实上，在某些 BCH 码或扩展的 BCH 码中存在这种结构良好的 L 段格图。

3 BCH 码的结构和译码

定义 1 GF(q) 上的码长为 n，设计距离为 δ 的 BCH 码是由根集包含 $\delta-1$ 个不同元素 $\alpha^b,\alpha^{b+1},\cdots,\alpha^{b+\delta-1}$ 的多项式 $g(x)\in$GF(q)[X] 生成的循环码，其中 α 是 n 次本原单位根，b 是某个整数。如果码长 $n=q^m-1,m$ 为某一正整数，则称该码为本原 BCH 码；如果 $b=1$，则称该码为狭义 BCH 码。

引理 1[3] 长为 2^m 的扩展本原 BCH 码，如果其设计距离为 2^{m-r}，则该 BCH 码包含 RM(r,m)；如果其设计距离为 5，则该 BCH 码的对偶码包含 RM($1,m$)。

由于每个线性分组码的最小距离不大于其子码的最小距离，所以扩展 BCH($2^m,k,2^{m-r}$) $\supset$ RM(r,m)。RM(r,m) 码具有规则的直和划分结构[2]，所以包含 RM(r,m) 的扩展 BCH 码也具有直和子码划分的结构，如 BCH(32, 16, 8) $\supset C_1$(16, 5)$\oplus C_1$(16, 5); BCH(64, 18, 16)$\supset C_1$(32, 6) $\oplus C_1$(32, 6); BCH(64, 40, 8)$\supset C_1$(32, 16)$\oplus C_1$(32, 16)。

由于某些长为 2^m 的扩展本原 BCH 码含设计距离为 2^{m-r} 的扩展本原 BCH 码，如 BCH(64, 10, 28)$\supset$BCH(64, 7, 32); BCH(64, 16, 24)$\supset$BCH(64, 7, 32); BCH(64, 18, 22)$\supset$BCH(64, 7, 32); BCH(64, 30, 14)$\supset$BCH(64, 24, 16); BCH(16, 7, 6)$\supset$BCH(16, 5, 8); BCH(32, 11, 12)$\supset$BCH(32, 6, 16); 所以这些 BCH 码也具有相应的直和划分结构，如 BCH(64, 30, 14)$\supset C_1$ (32, 6)$\oplus C_1$(32, 6); BCH(64, 10, 28)$\supset C_1$(32, 1)$\oplus C_1$ (32, 1); BCH(64, 16, 24)$\supset C_1$(32, 1)$\oplus C_1$(32, 1)。

由于 QR(32, 16, 8) 码是设计距离为 5 的 BCH 码，且为自对偶码，所以 QR(32, 16, 8) $\supset$RM(1, 5)，因此，QR(32, 16, 8)$\supset C_1$(16, 1)$\oplus C_1$ (16, 1)。

由上面的划分可得 BCH 码的两段格图，并且每段构成的子格图与有关 RM 码的格图同构。

Vardy 和 Be'ery[4] 采用穷举搜索的方法给出了某些码长为合数的设计距离与实际距离相等的 BCH 码的直和划分结构，例如，BCH(93, 53, 8)$\supset C_1$(31, 11) $\oplus C_1$(31, 11), 而已知有些 BCH 码之间存在子码关系，所以这一部分码长为合数。设计距离与实际距离不等的 BCH 码也具有直和划分的结构，例如，对于 BCH(35, 23, 3)$\supset$BCH(35, 22, 4)；BCH(45, 33, 3)$\supset$BCH(45, 29, 5)；BCH(45, 27, 3)$\supset$BCH(45, 23, 7)；BCH(49, 28, 3)$\supset$BCH(49, 27, 4)；BCH(69, 36, $\le$8)$\supset$BCH(69, 35, 8)；BCH(69, 46, $\le$8)$\supset$BCH(69, 35, 8)`；BCH(75, 35, $\le$7)$\supset$BCH(75, 31, 7) 存在相应的直和划分结构，如 BCH(45, 27, 3)$\supset\oplus\sum_{i=1}^{3}C_1(15,5)$。

由于构成上述 BCH 码的直和子码的短码均具有规则的格图结构，所以容易导出相应的 BCH 码的格图尺寸的上界，部分结果如表 1 所示，其它结果参见文献 [5]。

表 1

码	格图尺寸 s 的上界	
	Wolf 界	直和结构的界
BCH(45, 27, 3)	18	16
BCH(49, 28, 3)	19	10
BCH(69, 36, ≤8)	33	9
BCH(69, 46, ≤8)	23	19
BCH(75, 35, ≤7)	35	14

对于具有直和结构的 BCH 码，可用陪集译码的方法进行译码，也可用 Viterbi 译码算法进行译码，并且整个 BCH 码的译码器可由若干小的译码器构成，对于一般二元 (n,k) 线性分组码，容易证明其 Viterbi 译码算法的最坏时间复杂性为

$$N=\begin{cases}2^{n-k}(6k-3n+5)-5), & n\le 2k;\\ 2^{k}(3n-6k+5)-5), & n>2k;\end{cases}$$

而对于尺寸为 s 的最小格图，对应分组码的 Viterbi 译码算法的时间复杂性为

$$2^{s}(3n-6s+5)-5.$$

所以高码率码的 Viterbi 译码算法的计算增益为

$$\frac{2^{n-k}(6k-3n+5)-5}{2^{s}(3n-6s+5)-5},$$

而低码率码的 Viterbi 译码算法的计算增益为

$$\frac{2^{k}(3n-6k+5)-5}{2^{s}(3n-6s+5)-5}.$$

如 BCH(64, 45, 8) 码的基于上述划分的 Viterbi 译码算法的计算增益 2.41 ； BCH(45, 27, 3) 码的计算增益为 6.40 ； BCH(16, 7, 6) 码的计算增益为 3.04 。

4　线性分组码的映象码的译码

本节讨论 q^m 元线性分组码的 q 元映象的译码问题

设 $\mathrm{GF}(q^m)$ 关于 $\mathrm{GF}(q)$ 的基为 $\boldsymbol{B}=(b_0,b_1\cdots,b_{m-1})$， dB 是从 $\mathrm{GF}(q^m)^n$ 到 $\mathrm{GF}(q)^{mn}$ 的映射：$dB(\boldsymbol{x})=(\cdots,x_{i0},x_{i1},\cdots,x_{im-1},\cdots)$，其中 $\boldsymbol{x}=(x_1,\cdots,x_n)$，$x_i=\sum_{j=0}^{m-1}x_{ij}b_j, i=1,\cdots,n$，显然， dB 是 $\mathrm{GF}(q^m)^n$ 到 $\mathrm{GF}(q)^{mn}$ 上的一一映射。

定义 2　如果 C 是 $\mathrm{GF}(q^m)$ 上的 (N,K) 线性码，则 $dB(C)$ 称为码 C 关于基 $\boldsymbol{B}$ 的 q 元映象，或简单地称为 C 的 $dB-q$ 元象。

性质 1　设 $\mathrm{GF}(q^m)$ 上的线性码 $C(N,K)$ 的生成矩阵为 G， $\mathrm{GF}(q^m)$ 关于 $\mathrm{GF}(q)$ 的基为 $\boldsymbol{B}=\{b_0,b_1,\cdots,b_{m-1}\}$，则 $dB(C)$ 的生成矩阵为 $dB(G)=(dB(b_0G),\cdots,dB(b_{m-1}G))^t$ 。

性质 2　设 $\mathrm{GF}(q^m)$ 上的线性码为 $C(N,K,D)$，则 q 元映象为 $dB(C)=(mN,mK,d\ge D)$ 。

性质 3　设 $(u_1,\cdots,u_s)$, $(v_1,\cdots,v_t)$ 分别为 $\mathrm{GF}(q^{st})$ 关于 $\mathrm{GF}(q^t)$， $\mathrm{GF}(q^t)$ 关于 $GF(q)$ 的基，则 $(\cdots,u_iv_1,\cdots,u_iv_t,\cdots)$ 是 $\mathrm{GF}(q^{st})$ 关于 $GF(q)$ 的基。

设 C_0 是 GF(q^m) 上的线性码 $C(N,K,D)$ 的 q 元子码，即 C_0 是 C 的子域子码。设 C_0 的生成矩阵为 $G_0=(\boldsymbol{u}_1,\cdots,\boldsymbol{u}_k)^t$，则 G_0 可以扩张为 C 的生成矩阵 $G=(\boldsymbol{u}_1,\cdots,\boldsymbol{u}_k,\boldsymbol{u}_{k+1},\cdots,\boldsymbol{u}_K)^t$。显然 $dB(C)\supset dB(C_0)$，并且 dim $dB(C_0)$=dim C_0，即 $dB(C_0)$ 可收缩为 C_0，而 $dB(C)$ 的生成矩阵 $dB(G)=(dB(b_0(\boldsymbol{u}_1,\cdots,\boldsymbol{u}_k,\boldsymbol{u}_{k+1},\cdots,\boldsymbol{u}_k)),\cdots,dB(b_{m-1}(\boldsymbol{u}_1,\cdots,\boldsymbol{u}_{k+1},\cdots,\boldsymbol{u}_K)))^t$，由 $dB(G)$ 的形式可以看出，经过行和列的交换可得 $dB(C)$ 的直和子码 $\oplus\sum_{i=1}^{m}C_0$.

性质 4 如果 GF(q^m) 上的分组码 C 存在 GF(q) 上的生成矩阵，则 $dB(C)$ 是一个可分码。

容易证明下列结论。

引理 2 设 C 是 GF(q^m) 上以 $\alpha_1,\cdots,\alpha_s$ 为根的循环码。C_0 是 GF(q) 上以 $\alpha_1,\cdots,\alpha_s$ 为根的循环码，则 C_0 是 C 的循环子域子码，C_0 的扩展码也是 C 的扩展码的子域子码。

定理 1 设 C 是 GF(q^m) 上以 $\alpha_1,\cdots,\alpha_s$ 为根的循环码，C_0 是 GF(q) 上以 $\alpha_1,\cdots,\alpha_s$ 为根的循环码，则 $dB(C)$ 包含直和子码 $\oplus\sum_{i=1}^{m}C_0$。

对定理作适当修改也适用于扩展码。

由上面的讨论可知：一般应选尽可能大的子域子码，这样线性码的映象才包含一个较大的直和子码，从而有利于映象码的译码。下面讨论 QR 码和 RS 码的映象码。

设 p 是形如 $8\lambda+3$ 的素数，则可在 $GF(2^2)$ 上定义码长为 p 的二次剩余码。

当 $p=3$ 时，得到的扩展二次剩余码为 QR(4, 2, 3)，它包含直和子码 $C_0(4,1)\oplus C_0(4,1)$，如果取适当的 GF(4) 关于 $G(2)$ 的基 $\boldsymbol{B}$，所得的二元码 dB(QR(4,2,3)) =Hamming(8, 4, 4)。

当 $p=11$ 时，扩展二次剩余码在 GF(4) 关于 GF(2) 适当的基下，dB(QR(12,6,6)) =Golay(24, 12, 8)$\supset C_0(12,1)\oplus C_0(12,1)$.

当 $p=19$ 时，在 $GF(4)$ 关于 GF(2) 的适当基底 $\boldsymbol{B}$ 下，$dB(\mathrm{QR}(20,10,8))=C(40,20,8)\supset C_0(20,1)\oplus C_0(20,1)$.

对于 RS 码，由上面的定理可知：RS(q^m-1,K,q^m-K) 包含直和子码 $\oplus\sum_{i=1}^{m}$BCH($q^m-1,k,d\geq q^m-K$)。

可以证明，在适当的 GF(2^m) 关于 GF(2) 的基底 $\boldsymbol{B}$ 下，dB(RS(8, 4, 5)) =Golay(24, 12, 8)，因此 Golay(24, 12, 8)$\supset\oplus\sum_{i=1}^{3}$BCH(8, 1)，而 $dB(\mathrm{RS}(16,9,8))=C(64,36)\supset\oplus\sum_{i=1}^{4}$BCH(16, 5, 8)。如果选取适当的 GF(2^4) 关于 $GF(2)$ 的基，可得 $dB(\mathrm{RS}(16,8,9))=C(64,32,12)\supset C_0(32,4)\oplus C_0(32,4)$，其中 $C_0(32,4)\supset$BCH(16, 1) $\oplus$BCH(16, 1)。

GF(q^m) 上的线性码 C 都存在上述直和划分，可用陪集译码或 Viterbi 译码算法进行译码。设译子域子码 C_0 的时间复杂性为 Ω，则译 C 的时间复杂性为 $N_1=[m\Omega+m]q^{m(K-k)}$。可以证明基于传统的 Wolf 格图的 Viterbi 译码算法的时间复杂性为

$$N_2=\begin{cases}\dfrac{2(q^{m(N-K)+2}-q^2}{q-1}+(2K-N-1)(2q-1)q^{m(N-K)}+(q-1), & N\leq 2K;\\ \dfrac{2(q^{mK+2}-q^2}{q-1}+(2K-N-1)(2q-1)q^{mK}+(q-1), & N>2K.\end{cases}$$

因此，基于直和划分结构的 L 段格图的分组码 Viterbi 译码算法的计算增益为 N_2/N_1，如对映象 dB(RS(16,9,8)) 码的计算增益为 21.71，而 dB(RS(8, 4, 5) =Golay(24, 12, 8) 的计算增益为 1.66，因此，利用码的直和划分结构译码总能获得一定的计算增益，对于有的码甚至可获得较大的计算增益。

4 结束语

分组码的格图理论是设计分组码的译码算法的有效工具，而有效的译码算法依赖于分组码较小的格图尺寸和规则的格图结构。Kasami 等 [3] 讨论了置换意义下某些线性分组码的绝对最小格图尺寸，对分组码的 Viterbi 译码算法的设计和实现在理论上具有一定的指导意义，但是怎样求解线性分组码的最佳置换仍然没有解决。Vardy 等 [4] 对于设计距离与实际最小距离相等的本原 BCH 码和某些合数长 BCH 码给出了其规则的 L 段格图结构，从而得到了有效的 Viterbi 译码算法，但采用穷举搜索的办法，工作量比较大。本文简化了 Vardy 等求解本原 BCH 码的直和划分的过程，利用某些 BCH 码的包含关系，将直和划分结构推广到其他的设计距离与实际最小距离不等的 BCH 码中去，获得了理想的 L 段格图，从而给出了快速的译码算法。最后讨论了 q^m 元线性分组码的 q 元映象的直和划分结构和基于该划分的译码的有效性问题。但怎样求一般 p(p 为素数) 元线性分组码的直和划分结构的问题仍有待研究，这个问题等价于怎样判断一个码为可分码的问题。

参 考 文 献

[1] Wolf J. IEEE Trans. on IT, 1978, IT-24(1): 76–80.

[2] Forney Jr G D. IEEE Trans. on IT, 1988, IT-34(5): 1152–1187.

[3] Kasami T, *et al.* IEEE Trans. on IT, 1993, IT-39(3): 1057–1064.

[4] Vardy A, Be'ery Y. IEEE Trans. on IT, 1994, IT-40(2): 546–554.

[5] 马建峰. 线性分组码快速译码算法研究：[博士论文]. 西安电子科技大学通信工程学院，1995. 3.

[6] Mouaha C. Applicable algebra in engineering, communication and computing, 1992, AAECC-3(4): 311–319.

TRELLIS STRUCTURES OF BLOCK CODES AND DECODING

Ma Jianfeng　　Wang Yumin

(*Xidian University, Xi'an* 710071)

Abstract　Trellis structures of block codes are discussed. L-section trellis structures of some BCH codes are presented. A fast maximum likelihood decoding algorithm for BCH codes is proposed correspondingly, Decoding porblem of q-ary images of q^m-ary block codes is also discussed. The direct sum partition and the associated decoding algorithms are given for the images.

Key words　Trellis, Decoding, BCH code, RS code, q-ary image, Direct sum partition

马建峰：　男，1963 年生，博士，副教授，主要从事编码理论，信息论，容错网络设计，并行处理等方面的研究工作.

王育民：　男，1936 年生，教授，博士生导师，主要从事编码理论，信息论，密码学，通信理论等方面的研究工作.