几类格的快速译码 [1]

马建峰 王育民

(西安电子科技大学 西安 710071)

摘 要 本文通过研究 16 维 Barnes-Wall 格和基于构造 A 的二元线性分组码、四元线性分组码的导出格的代数结构，将这些格的译码问题转化为在相应码的格图上求最短路径的问题，从而提出了这些格的快速译码算法，并分析了译码算法的时间复杂性。

关键词 线性分组码，格图， Barnes-Wall 格，构造 A, 译码

中图号 TN911.22

1 前 言

格在矢量量化，限带信道的分组编码调制等领域有广泛的应用 [1,2] 。这些应用均涉及格的译码问题，格的译码问题可叙述为任给空间一个点，求与该点有最小欧氏距离的格点。如果将格用作 Gauss 信道的分组码，则格的译码算法按最大似然译码规则找到一个与接收序列最近的格点；如果将格用于均匀分布的数据的矢量量化，则格的译码算法给出一个具有最小失真的格点。本文首先讨论基于构造 A 的二元线性分组码和四元线性分组码的导出格的代数结构，结果将这类格的译码问题转化为二元码或四元码的译码问题，并给出了快速的译码算法。其次讨论了 16 维 Barnes-Wall 格的译码问题。

2 基于构造 A 的二元码的导出格的译码

构造A 设 C 是二元 (n,k,d) 分组码，由码 C 导出的格 $\wedge(C)$ 包含 R^n 中满足 $2^{1/2}x \bmod 2 \in C$ 的所有点 $x=(x_1,\cdots x_n)$[3] 。

由构造 A 的定义可知：格 $\wedge(C)$ 的所有矢量均可通过给码 C 的码字的分量添加任意个偶数，然后用 2 来除得到。基于构造 A 的二元码 C 的导出格 $\wedge(C)$ 的译码问题可转化为码 C 的译码问题。

设 $r=(r_1,\cdots,r_n)$ 是 R^n 中的任意矢量， $R_0 \triangleq \{(1/\sqrt{2})x | x \in Z, 2|x\}$ ， $R_1 \triangleq \{(1/\sqrt{2})x | x \in Z, 2\nmid x\}$ ，其中 Z 为整数集。设 x 是格 $\wedge(C)$ 中某个矢量的分量。如果 $x \in R_0$ ，则 x 对应于 GF(2) 的元素 0 ；如果 $x \in R_1$ ，则 x 对应于 GF(2) 中的元素 1 。

格 $\wedge(C)$ 的译码算法 (1) 对于矢量 $r=(r_1,\cdots r_n)$ 中的每个分量 r_i ，计算 R_0 、 R_1 中距 r_i 最近的点，分别记为 $r_i(0)$ ， $r_i(1)$ ，对应的平方距离分别为 $\mathrm{dist}_i^2(0)$ ， $\mathrm{dist}_i^2(1)$ ， $1 \le i \le n$ ； (2) 利用 Wolf[4] 的方法构造二元码 C 的 n 段格图，对于第 i 段，设 GF(2) 中的元素 0 、 1 分别对应于费用 $\mathrm{dist}_i^2(0)$ ， $\mathrm{dist}_i^2(1)$ ， $1 \le i \le n$ ； (3) 用 Viterbi 译码算法或 Dijkstra 最短路径算法 [5] 所求二元码 C 的加权格图上的最短路径所对应的 $\wedge(C)$ 中的矢量即为所求格点。

容易证明上述算法的正确性 [6] 。

[1] 1994-09-23 收到， 1995-05-24 定稿
国家自然科学基金资助项目

因为对于任意 $r \in \boldsymbol{R}$，求 R_0， R_1 中离 r 最近的点是非常容易的，而且这一步，可放在预计算步来完成，所以，可以认为二元码 C 的导出格 $\wedge(C)$ 的译码复杂性与该二元码的译码复杂性相同，可以证明，如果用 Wolf 格图译码算法 [4] ，则最坏情况下的译码复杂性为

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

所以格 $\wedge(C)$ 的译码复杂性可用 N 来衡量。

例 1 设 $H_8(8,4,4)$ 为扩展汉明码，利用构造 A 可得 $\boldsymbol{R}^8$ 中的最稠密格 $\wedge(H_8)=E_8=2\boldsymbol{Z}^8+(8,4,4)$，用上面的译码算法可对格 E_8 进行译码，译码的最坏复杂性为 39 次二元运算。对于格 $D_4=2\boldsymbol{Z}^4+(4,3,2)$，$D_8=2\boldsymbol{Z}^8+(8,7,2)$，$D_{16}=2\boldsymbol{Z}^{16}+(16,15,2)$，$H_{16}=2\boldsymbol{Z}^{16}+(16,11,4)$，相应的译码复杂性分别为 7 次， 15 次， 31 次， 199 次二元运算。

3 四元线性分组码的导出格的快速译码

本节研究的格为复空间 $\boldsymbol{C}^n$ 上的格。

设 $E=\{a+b\omega|a,b\in\boldsymbol{Z},\omega=e^{2\pi i/3}\}$ 是 Eisentein 整数集。易证 $2E$ 是 E 的素理想，于是存在划分 $E/2E$，并且可选 0， 1， ω， ω^2 为陪集代表元；所以 $E/2E$ 与 GF(4) 之间存在同构映射 $E/2E\to$GF(4)： $2E\to 0$， $1+2E\to 1$， $\omega+2E\to\omega$， $\omega^2+2E\to\omega^2$；因而也存在映射 σ： $E\to E/2E\to$GF(4) 使得 $\omega^r\in E$ 映射为 $\omega^r\in$GF(4)(r=0, 1, 2)。

构造A 设 C 是 (n,k,d) 分组码，格 $\wedge(C)$ 由所有满足 $\sigma(\sqrt{2}\boldsymbol{x}\in C$ 的矢量 $\boldsymbol{x}=(x_1,\cdots,x_n)\in C^n$ 构成 [3]。

例 2 设 T_n 是生成矩阵为 I_n， $k=n$ 的平凡四元码，则 T_n 生成的格 $\wedge(T_n)=(1/\sqrt{2})E^n$。设 $C=\{00,11,\omega\omega,\omega^2\omega^2\}$，则码 C 生成的格 $\wedge(C)=E^2$。

与二元码的导出格的译码问题一样，四元码的导出格的译码问题也可转化为码 C 的译码问题。

设 $\boldsymbol{u}=(u_1,\cdots,u_n)\in C$，则格 $\wedge(C)$ 中对应于 $\boldsymbol{u}$ 的点集为 $\wedge(\boldsymbol{u})=(1/\sqrt{2})\sigma^{-1}(\boldsymbol{u})=\{(y_1,\cdots,y_n)|y_r\in(1/\sqrt{2})u_r+\sqrt{2}E,1\le r\le n\}$。于是格 $\wedge(C)$ 中的格点的分量 y 属于四个集合 R_0、R_1、R_ω、R_{ω^2} 之一，其中 $R_0=\sqrt{2}E$， $R_1=1/\sqrt{2}+\sqrt{2}E$， $R_\omega=(1/\sqrt{2})\omega+\sqrt{2}E$，$R_{\omega^2}=(1/\sqrt{2})\omega^2+\sqrt{2}E$。

格 $\wedge(C)$ 的译码算法 (1) 对于复空间 $\boldsymbol{C}^n$ 中的给定矢量 $\boldsymbol{r}=(r_1,\cdots,r_n)$ 的每一分量 r_i，计算 R_0， R_1， R_ω， R_{ω^2} 中离 r_i 最近的点， $1\le i\le n$，于是得四个点 $r_i(0)$， $r_i(1)$，$r_i(\omega)$， $r_i(\omega^2)$ 及相应的平方欧氏距离 (SED) $\mathrm{dist}_i^2(0)$， $\mathrm{dist}_i^2(1)$， $\mathrm{dist}_i^2(\omega)$， $\mathrm{dist}_i^2(\omega^2)$；(2) 构造码 C 的 n 段格图，该格图的第 i 段的标号 0， 1， ω， ω^2 分别对应权值 $\mathrm{dist}_i^2(0)$， $\mathrm{dist}_i^2(1)$，$\mathrm{dist}_i^2(\omega)$， $\mathrm{dist}_i^2(\omega^2)$，从而得到一个赋权有向图；(3) 利用 Viterbi 译码算法或 Dijkstra 最短路径算法 [5] 求该格图上具有最小权值的码字 $\mathbf{c}=(c_1,\cdots,c_n)$，其所对应的格点 $(r_1(c_1),\cdots,r_n(c_n)$ 即为所求格点。

容易证明上述算法的正确性 [6]。

类似与二元码的导出格的情况，四元码的导出格的最坏译码的时间复杂性为

$$N=\begin{cases}(14k-7n+4)4^{n-k}-7, & n-k\le k;\\ (7n-14k+4)4^{k}-7, & n-k>k.\end{cases}$$

例 3 GF(4) 上的矩阵

$$\begin{pmatrix}1&0&0&1&\omega&\omega\\0&1&0&\omega&1&\omega\\0&0&1&\omega&\omega&1\end{pmatrix}$$

生成自对偶码 $Q_6(6,3,4)$ 。可以证明 Q_6 的导出格 $\wedge(Q_6)$ 是自对偶格，在实空间 $\boldsymbol{R}^{12}$ 中的对应格为 K_{12} 格，即由 Coxeter 和 Todd 构造的格。格 K_{12} 是空间 $\boldsymbol{R}^{12}$ 中已知的最稠密格 [3] 。用上面的译码算法译 $\wedge(Q_6)$ 的最坏时间复杂性为 249 次实运算 (加法，比较) 。

4 16 维 Barnes-Wall 格的译码算法及进一步的结果

Barnes-Wall 格具有良好的代数结构，是一类重要的稠密格。 16 维 Barnes-Wall 格是 16 维空间中的最稠密格。 Forney[7] 利用二次结构的概念证明了 16 维 Barnes-Wall 格 $\mathrm{BW}_{16}=4\boldsymbol{Z}^{16}+2(16,15,2)+(16,5,8)$ ，其中 (16, 15, 2)=RM(3, 4) ， (16, 5, 8)=RM(1, 4) 。这里我们利用 RM(2, 4)=(16, 11, 4) 来构造格 BW_{16} 。首先用 Ungerboeck[1] 的方法将一个 2 维格划分为 8 个子集，每个子集都有一个固定的标号，划分 1 次， 2 次， 3 次后的 64 点星座如图 1 所示。用这样的星座及其复制可以不交地填满整个 2 维空间，即 2 维格。这时 A_{ij} 和 B_{ij} 均代表一类点的集合， i ， j =0 ， 1 。

A	B	A	B	A	B	A	B
B	A	B	A	B	A	B	A
A	B	A	B	A	B	A	B
B	A	B	A	B	A	B	A
A	B	A	B	A	B	A	B
B	A	B	A	B	A	B	A
A	B	A	B	A	B	A	B
B	A	B	A	B	A	B	A

A_0	B_0	A_0	B_0	A_0	B_0	A_0	B_0
B_1	A_1	B_1	A_1	B_1	A_1	B_1	A_1
A_0	B_0	A_0	B_0	A_0	B_0	A_0	B_0
B_1	A_1	B_1	A_1	B_1	A_1	B_1	A_1
A_0	B_0	A_0	B_0	A_0	B_0	A_0	B_0
B_1	A_1	B_1	A_1	B_1	A_1	B_1	A_1
A_0	B_0	A_0	B_0	A_0	B_0	A_0	B_0
B_1	A_1	B_1	A_1	B_1	A_1	B_1	A_1

A_{00}	B_{00}	A_{11}	B_{11}	A_{00}	B_{00}	A_{11}	B_{11}
B_{10}	A_{01}	B_{01}	A_{10}	B_{10}	A_{01}	B_{01}	A_{10}
A_{11}	B_{11}	A_{00}	B_{00}	A_{11}	B_{11}	A_{00}	B_{00}
B_{01}	A_{10}	B_{10}	A_{01}	B_{01}	A_{10}	B_{10}	A_{01}
A_{00}	B_{00}	A_{11}	B_{11}	A_{00}	B_{00}	A_{11}	B_{11}
B_{10}	A_{01}	B_{01}	A_{10}	B_{10}	A_{01}	B_{01}	A_{10}
A_{11}	B_{11}	A_{00}	B_{00}	A_{11}	B_{11}	A_{00}	B_{00}
B_{01}	A_{10}	B_{10}	A_{01}	B_{01}	A_{10}	B_{10}	A_{01}

图 1 64 点星座

16 维 Barnes-Wall 格 BW_{16} 可定义为所有 8 个点的序列的集合 [1] ，每个点取自 2 维格，并且满足： (1) 8 个点或全属 A 类集合，或全属 B 类集合； (2) 8 个点所在集合的下标 (ij) 构成的 0 ， 1 序列为 RM(2, 4)=(16, 11, 4) 一个码字。

利用前面的译码思想可将 16 维 BW_{16} 格的译码问题转化为在 RM(2, 4) 的 8 段赋权格图上求最短路径的问题。最坏译码时间复杂性为 399 次实运算。详细的论述参见文献 [6] 。

上面讨论了二元码及四元码的导出格的译码问题。证明了导出格的译码问题可转化为相应码的译码问题。如 $\wedge(C)=2\boldsymbol{Z}^n+C$ 的译码问题可转化为二元码 C 的译码问题。如果用 +1 ， -1 分别代替码元 0 ， 1 ，则格 $\wedge(C)=4\boldsymbol{Z}^n+C$ 。同样可以证明 $\wedge(C)$ 的译码也可转化为码 C 的译码，此时，由 Conway 和 Sloane[2] 提出的译码方法仅是本文提出的方法的特例。本文仅讨论了二元及四元线性分组码的导出格的译码问题，但是显然所提的算法也适用于非线性分组码的导出格的译码。此外，这里的译码思想稍加修改也可用于基于构造 B[3] 的二元码的导出格的译码。

设 $\boldsymbol{r}=(r_1,\cdots,r_n)\in\boldsymbol{R}^n$ ，求 R_0 ， R_1 中离 r_i 最近的点，分别设为 $r_i(0)$ ， $r_i(1)$ ，其对应的平方欧氏距离分别为 $\mathrm{dist}_i^2(0)$ ， $\mathrm{dist}_i^2(1)$ 。对码 C 的 n 段格图的第 i 段标号为 0 和 1 的边分别赋值 $\mathrm{dist}_i^2(0)$ ， $\mathrm{dist}_i^2(1)$ 。设 $(c_1,\cdots,c_j)$ 是某条路径所对应的码元序列，定义其得分为

$\sum_{i=1}^{j} r_i(c_i) \bmod 4$ 。用 Viterbi 译码算法或 Dijkstra 最短路径算法[5] 对码 C 译码时，保留其格图上第 1 段至 $n-1$ 段的得分为 0， 1， 2， 3 的最佳路径，为了保证 $\sum_{i=1}^{j} r_i(c_i) \bmod 4=0$，在第 n 段必须选择这些路径的适当延伸，最后经比较得最佳路径，其所对应的格点即为所求。

显然，二元码和四元码的导出格的译码思想也可推广到 q 元码的基于构造 A 的导出格的译码，如三元码的基于构造 A[3] 的导出格的译码。

参 考 文 献

[1] Forney Jr G D, *et al.* Efficient modulation for band-limited channels. IEEE J. of Selected Areas in Comm., 1984, SAC-2(5): 632–647.

[2] Conway J H, Sloane N J A. Soft decoding techniques for codes and lattices, including the Golay codes and the Leech lattices. IEEE Trans. on IT, 1986, IT-32(1): 41–50.

[3] Conway J H, Sloane N J A. Sphere Packing, Lattices and Groups. New York: Springer-Verlag, 1988, Chapters 5, 7, 20.

[4] Wolf J K. Efficient maximum likelihood decoding of linear block codes using a trellis. IEEE Trans. on IT, 1978, IT-24(1): 76–80.

[5] 阿霍 A V, 霍普克罗夫特 J E, 厄尔曼 J D 著, 唐守文译. 数据结构与算法. 北京：科学出版社， 1987, 256–261.

[6] 马建峰. 分组码快速译码算法的研究： [博士论文]. 西安：西安电子科技大学， 1994. 12.

[7] Forney Jr G D. Coset codes-Part II: Binary lattices and related codes.IEEE Trans. on IT, 1988, IT-34(5): 1152–1187.

FAST DECODING OF SOME KINDS OF LATTICES

Ma Jianfeng Wang Yumin

(*Xidian University, Xi'an* 710071)

Abstract By studying the structure of 16 dimension Barnes-Wall lattice and lattices resulting from binary linear block codes and quaternary linear block codes based on Construction A, decoding problem of the lattices can be transformed into the problem of finding the shortest path of trellises accordingly. The time complexities of the decoding algorithms are analyzed.

Key words Linear block code, Trellis, Barnes-Wall lattice, Construction A, Decoding

马建峰： 男， 1963 年生，博士，副教授，现从事编码理论，容错计算的教学与研究.

王育民： 男， 1936 年生，教授，博士生导师，现从事通信理论的教学与研究.