第 14 卷 第 6 期　　电 子 科 学 学 刊　　Vol. 14, No. 6
1992 年 11 月　　JOURNAL OF ELECTRONICS　　Nov., 1992

并元加性群的陪集划分与 RM 码的小数逻辑译码算法

陆正福　胡正名　阮传概
（北京邮电学院，北京 100088）

摘要　本文首次提出了并元加性群陪集划分中的两个新概念，给出了它们的充分必要条件，并给予证明．籍此解决了对 RM 码实施的小数逻辑译码算法的可行性问题．

关键词　并元群；陪集；编码；RM 码

一、引　言

在 RM 码中，大数逻辑译码算法(即 Reed 算法)在理论上相对比较成熟．1989 年，刘玉君[1]对 Reed 译码算法提出改进，提出了小数逻辑译码算法，以求减少译码计算量及提高译码速度．本文提出了并元加性群正则可分(交)性两个新概念，并给出了它们的充要条件．在这基础上，推广了文献[1]中的结论，并解决了 RM 码在实施小数逻辑译码算法时的纠错能力问题．从理论上完善了 RM 码的小数逻辑译码算法．这是与小数逻辑译码算法意义下的 RM 码的实际应用密切相关的重要问题．

二、并元加性群的陪集划分

文献[2]中提出了并元加性群．我们设 $G_m \triangleq \{0,1,2,\cdots,2^m-1\}$，$\oplus$ 为并元和，表示数的二进制表达下的逐位模 2 加，则 $(G_m, \oplus)$ 构成并元加性群．鉴于并元加性群具有如下基本特征：(1)所含元素的个数是 2^r（r 是非负整数，称为该群的阶)；(2) 两个同阶的并元加性群必同构．所以我们只研究 $(G_m, \oplus)$，其结论不难推广到一般情形．在下面的叙述中，凡提及群(子群)的地方均指并元加性群(子群)．

引理 1　任意 r 阶并元加性群必可由该群某 r 个元素通过并元加法生成，且有 $\prod_{p=0}^{r-1}(2^r-2^p)$ 种生成方式(对应于 r 个元素的选择)．

证略．

例如 G_4 可由 $\{1,2,4,8\}$，也可由 $\{3,5,7,9\}$ 生成．一般地，G_m 可由 $R_m \triangleq \{1,2,2^2,\cdots,2^{m-1}\}$ 生成．同时，由 R_m 的任意 r $(0 \leqslant r \leqslant m)$ 个元素生成 G_m 的 $\binom{m}{r}$ 个子群（r —

1991.09.20 收到，1992.03.11 定稿．

0 时，以 G_m 的零元单独构成子群），称这些子群为 r-正则子群。当该 r-正则子群可由 $\{2^{i_1},2^{i_2},\cdots,2^{i_r}\}$ 生成时，记为 $S_{i_1i_2\cdots i_r}$。

根据引理 1　G_m 的任意元素 x 可表示成 R_m 中的元素的并元和式。当该和式的各项两两互不相同时，称此和式为元素 x 的正则表示式。若再考虑和式中各项按数的由小到大顺序排列，则 G_m 的任意元素的正则表示式是唯一的。例如，7 的正则表示式为 $1\oplus2\oplus4$。显然，r-正则子群 $S_{i_1i_2\cdots i_r}$ 的元素的正则表示式的各项必来自 $\{2^{i_1},2^{i_2},\cdots,2^{i_r}\}$。

因为每个 r-正则子群均导致一个等价类划分——G_m 的陪集划分（2^{m-r} 个等价类），称此划分为 G_m 的 r-正则划分。当此划分由正则子群 $S_{i_1i_2\cdots i_r}$ 导致时，记为 $D_{i_1i_2\cdots i_r}$。至此，我们以 R_m 作为参考元素系统，获得了 $\binom{m}{r}$ 种划分 G_m 的特殊方式（$r=0,1,\cdots,m$）。

定义 1　设 $X_t\triangleq\{x_i:1\leqslant i\leqslant t,\ i\neq j\Longleftrightarrow x_i\neq x_j,\ x_i\in G_m\}$ 是 G_m 的任意 t 元子集，若存在 G_m 的 r-正则划分 $D_{i_1i_2\cdots i_r}$ 使得 X_t 中的元素属于 t 个两两互不相同的陪集，则称 G_m 具有 (r,t)-正则可分性。

对于具体确定的 X_t，满足定义 1 的条件的 r-正则划分不一定唯一，将这样的 r-正则划分统称为实现 X_t 分离的 r-正则划分。

定义 2　若 G_m 具有 (r,t)-正则可分性，且满足对任意 $X_t\subset G_m$，有

$$\bigcap_{S\in S_{X_t}}\bigcup_{x\in X_t}(x\oplus S)=X_t \tag{1}$$

式中 S_{X_t} 是实现 X_t 分离的 r-正则划分所对应的 r-正则子群，对称 G_m 具有 (r,t)-正则可交性。

引理 2　$\forall x,\ y\in G_m$，$D_{i_1i_2\cdots i_r}$ 是任意确定的 r-正则划分，则 x 与 y 属于同一个陪集的充分必要条件是 $x\oplus y$ 的正则表示式中的各项为 $\{2^{i_1},2^{i_2},\cdots,2^{i_r}\}$ 的元素。

证略。

命题 1　G_m 具有 (r,t)-正则可分性，当且仅当 $r+t\leqslant m+1$。

证明　*必要性*　不妨考虑 $X_t=\{2^i:0\leqslant i\leqslant t-1\}$，由于 G_m 具有 (r,t)-正则可分性，所以存在 r-正则划分实现 X_t 分离，设该正则划分为 $D_{i_1i_2\cdots i_r}$，则由引理 2 可分两种情形：

(1) $\{i_1,i_2,\cdots,i_r\}\cap\{0,1,\cdots,t-1\}=\phi$，（空集）

(2) $\{i_1,i_2,\cdots,i_r\}\cap\{0,1,\cdots,t-1\}=\{i_k\},(1\leqslant k\leqslant r)$

对情形(1)有 $m-t\geqslant r$，从而 $r+t\leqslant m$；对情形(2)有 $m-t+1\geqslant r$，从而 $r+t\leqslant m+1$。总之有 $r+t\leqslant m+1$。

充分性　注意到，由正则可分性定义，若 G_m 具有 (r,t)-正则可分性，且 $s<t$，$q\leqslant r$，则 G_m 具有 (q,s)-正则可分性。因此，只证 $r+t=m+1$ 情形即可，此时 $(r,t)=(m+1-t,t)$，$t=1,2,\cdots,m+1$。

对 t 用归纳法。首先，$t=1$ 时，为平凡情形。事实上，$(r,t)=(m,1)$，$(0,m+1)$ 均为平凡情形。其次，假定 $t=k$ 时，G_m 具有 $(m+1-k,k)$-正则可分性，则可证 $t=k+1$ 时 G_m 具有 $(m-k,k+1)$-正则可分性。事实上，任取 G_m 的 $(k+1)$-子集 X_{k+1}，由归纳法假设，存在 $(m-k+1)$-正则划分 $D_{i_1i_2\cdots m-k+1}$ 实现 X_k 的分离。下面

分两种情形讨论：

(1) X_{k+1} 中的元素属于 $k+1$ 个两两互不相同的陪集，则 $D_{i_1\cdots i_{\alpha-1}i_{\alpha+1}\cdots i_{m-k+1}}$，$(\alpha=1,2,\cdots,m-k+1)$ 可实现 X_{k+1} 的分离(由引理 2)。

(2) x_{k+1} 与 X_k 中某元素(不妨设为 x_k) 属于同一个陪集。令 $x=x_k\oplus x_{k+1}$，则由引理 2，其正则表示式为

$$x=2^{l_1}\oplus\cdots\oplus 2^{l_\beta},\ \text{其中}\ \{l_1,\cdots,l_\beta\}\subseteq\{i_1,i_2,\cdots,i_{m-k+1}\}$$

令 $$\{j_1,j_2,\cdots,j_{m-k}\}=\{i_1,i_2,\cdots,i_{m-k+1}\}\backslash\{l_\alpha\},(1\leqslant\alpha\leqslant\beta)$$

则 $D_{j_1j_2\cdots j_{m-k}}$ 可实现 X_{k+1} 的分离。

综合(1),(2)两种情形可知，G_m 具有 $(m-k,k+1)$-正则可分性。

由归纳法原理，命题的充分性获证。

命题 2 G_m 具有 (r,t)-正则可交性，当且仅当 $r+t\leqslant m$，$(0\leqslant r\leqslant m-1)$。

证明 *必要性* 按定义，若 G_m 具有 (r,t)-正则可交性，则 G_m 具有 (r,t)-正则可分性，从而由命题 1 得 $r+t\leqslant m+1$。注意到命题 1 的必要性证明过程，不难证明 $r+t=m+1$ 不成立，故而 $r+t\leqslant m$。

充分性 注意到，由正则可交性定义，若 G_m 具有 (r,t)-正则可交性，且 $s\leqslant t$，$q\leqslant r$，则 G_m 具有 (q,s)-正则可交性。因此只证 $r+t=m$ 时的情形即可。又因为，由命题 1 知，$r+t=m\Rightarrow G_m$ 具有 (r,t)-正则可分性。所以由正则可交性定义知，只需证明

$$r+t=m\Rightarrow(1)\text{式} \tag{2}$$

成立。当 $(r,t)=(m,0)$ 时；(1)式显然成立，但其它情形均不明显。我们对 t 用归纳法证明结论(2)式。首先 $t=1$ 时，$r=m-1$，(1)式为

$$\bigcap_{\{j_1j_2\cdots j_{m-1}\}}(x\oplus S_{i_1i_2\cdots i_{m-1}})=x\oplus\bigcap_{\{i_1i_2\cdots i_{m-1}\}}S_{i_1i_2\cdots i_{m-1}}=x\oplus 0=x$$

其中的交运算是针对 $\{0,1,\cdots,m-1\}$ 的所有 $(m-1)$-子集 $\{j_1,j_2,\cdots,j_{m-1}\}$ 进行的。因此 $(r,t)=(m-1,1)$ 时，结论(2)式成立。其次，假定 $t=k$ 时，结论(2)式成立，则可证 $t=k+1$ 时结论(2)式成立。事实上，在归纳法假设的基础上，根据实现 k 个点分离的 $(m-k)$-正则划分与实现 $k+1$ 个点分离的 $(m-k-1)$-正则划分的联系(参见命题 1 的充分性证明部分)，即可实施证明，细节从略。

由归纳法原理，命题 2 的充分性得到证明。

注 1 改变参考元素系统 R_m，可以获得 G_m 的另外$\binom{m}{r}$种陪集划分，显然可获得类似于定义 1,2 的概念和类似于命题 1,2 的结论。

注 2 如果考虑多并元加性群，则具有与命题 1,2 类同的结论。此时的 R_m 换成 $\{1,q,q^2,\cdots,q^{m-1}\}$，($q$ 为素数幂)，其定义和叙述是平行的，不再赘述。

三、RM 码的小数逻辑译码问题的完善

$R(r,m)$ 的生成矩阵定义为

$$G = [G_0^{tr}, G_1^{tr}, \cdots, G_l^{tr}, \cdots, G_r^{tr}]^{tr}$$

其中 tr 表示矩阵的转置，G_0 是长为 2^m 的全"1"行向量，G_l 是 $\binom{m}{l} \times 2^m$ 阶矩阵，对应于 GF(2) 上的 $\binom{m}{l}$ 个形如 $f(x_0, x_1, \cdots, x_{m-1}) = x_{i_1} x_{i_2} \cdots x_{i_l}$ 的多项式函数的向量 $\boldsymbol{f} = \boldsymbol{x}_{i_1} \boldsymbol{x}_{i_2} \cdots \boldsymbol{x}_{i_l}$，$(0 \leqslant i_1 < i_2 < \cdots < i_l \leqslant m-1;\ 1 \leqslant l \leqslant r)$.

若信息矢量的分段表示式为 $\boldsymbol{u} = (\boldsymbol{I}_0, \boldsymbol{I}_1, \cdots, \boldsymbol{I}_l, \cdots, \boldsymbol{I}_r)$，则编码表示式为 $\boldsymbol{C} = \sum_{l=0}^{r} \boldsymbol{I}_l G_l$. 对于 $\boldsymbol{I}_l$ 段，若对应于 $\boldsymbol{f} = \boldsymbol{x}_{i_1} \boldsymbol{x}_{i_2} \cdots \boldsymbol{x}_{i_l}$ 的信息位表示为 $u_{i_1 i_2 \cdots i_l}$，则由文献[3]的定理 14，用并元加性群的说法，可得下述引理.

引理 3　对于 $R(r,m)$，无差错接收矢量 $\boldsymbol{R} = \boldsymbol{C} = (c_0, c_1, \cdots, c_p, \cdots, c_{2^m-1})$，有结论：

(1) $u_{i_1 i_2 \cdots i_l} = \sum_{p \in S_{i_1 i_2 \cdots i_l}} c_p$，$(l \leqslant r)$

(2) $u_{i_1 i_2 \cdots i_l} = \sum_{p \in T} c_p$，其中 T 为子群 $S_{i_1 i_2 \cdots i_r}$ 的 2^{m-r} 个陪集中的任一个.

引理 3 的结论(2)中的 2^{m-r} 个等式称为 $u_{i_1 i_2 \cdots i_r}$ 的监督和式. 小数逻辑译码算法改进了 Reed 算法，根据 $u_{i_1 i_2 \cdots i_r}$ 的 2^{m-r} 个监督和式，通过择多逻辑判决确定 $u_{i_1 i_2 \cdots i_r}$ 的值，通过择少逻辑判决确定错误码元的位置. 记出现在少数监督和式（和式值与 $u_{i_1 i_2 \cdots i_r}$ 不一致）中的码元位置标号的全体为集合 $L_{i_1 i_2 \cdots i_r}$，故对 $\boldsymbol{I}_r$ 段，这样的 $L_{i_1 i_2 \cdots i_r}$ 共有 $\binom{m}{r}$ 个，记

$L_r = \{L_{i_1 i_2 \cdots i_r} : \{i_1, i_2, \cdots, i_r\} \subset \{0, 1, 2, \cdots, m-1\},\ i_1, i_2, \cdots, i_r$ 两两互不相等$\}$

文献[1]通过具体例子阐述了小数逻辑译码思想，总结文献[1]的分析，从理论上可概括为：

$R(r,m)$是小数逻辑可译码，当且仅当对任意 $t \leqslant 2^{m-r-1}-1$ 个错误，能从 L_r 中选择若干合适的元素，作为交运算的对象，运算的结果是且仅是错误码元的位置标号全体，即存在 L_r 的子集 L_r'，使得 $\bigcap_{L \in L_r'} L$ = 错误码元的位置标号全体所构成的集合.

定义 3　给定码系统 C，A 为 C 的译码算法，若(1)对 C 实施 A，可纠任意 $k \leqslant t$ 个错误，(2)T 是满足(1)中的 t 的最大值，则称 C 在译码算法中的纠错能力为 T.

命题 3　当 C 为 $R(r,m)$，A 为小数逻辑译码算法时，

$$T = \begin{cases} m-r, & \text{当 } m-r \geqslant 3 \\ 2^{m-r-1}-1, & \text{当 } m-r \leqslant 3 \end{cases}$$

即 $R(r,m)$ 在小数逻辑译码算法中可以纠不多于 T 个错

证明　第一部分　首先由于 L_r 的存在受到择少(多)辑逻判决的制约，所以 $T \leqslant 2^{m-r-1}-1$. 其次，$T \leqslant m-r$，事实上，设 $t \geqslant m-r+1$，t 个错误码元的位置标号集合 L_E 为 $\{2^{i_1}, 2^{i_2}, \cdots, 2^{i_\alpha}\}$ 的扩集，但不含有元素 0，其中 α 满足：

$$m-r+1\leqslant\alpha\leqslant\min(t,m)$$

于是由命题1的必要性证明过程可见，对于 G_m 的任意 r-正则划分 $D_{i_1i_2\cdots i_r}$，成立

$$\#(\{i_1,i_2,\cdots,i_r\}\cap\{j_1,j_2,\cdots,j_\alpha\})\geqslant 1$$

即 $L_E\cap S_{i_1i_2\cdots i_r}$ 不为空集，至少有1个错误码元的位置标号在 $S_{i_1i_2\cdots i_r}$ 中。因此 L_r 的任一元素 $L_{i_1i_2\cdots i_r}$ 必具有下列两种互斥的性质之一：

(1) $0\notin L_{i_1i_2\cdots i_r}$，此时偶数个错误码元出现在以 $S_{i_1i_2\cdots i_r}$ 为位置标号的监督和式中。

(2) $0\in L_{i_1i_2\cdots i_r}$，此时奇数个错误码元出现在以 $S_{i_1i_2\cdots i_r}$ 为位置标号的监督和式中。

选择 L_r 的子集 L'_r 构成集合交运算表达式：

$$L_I\triangleq\bigcap_{L\in L'_r}L$$

显然，当且仅当存在 L'_r，使得 $L_I=L_E$，才能找到译码方案使得译码错误不会产生。但是，这样的 L'_r 是不存在的。

事实上，(1)如果 L'_r 的某元素(设为 $L_{i_1i_2\cdots i_r}$) 具有性质(1)，则 $L_E\cap S_{i_1i_2\cdots i_r}$ 不是 L_I 的子集，所以 $L_I\neq L_E$；(2) 如果 L'_r 的所有元素都具有性质(2)，则 $0\in L_I$，但 $0\notin L_E$，所以 $L_I\neq L_E$。故而所希求的 L'_r 不存在。

因此，当 $t\geqslant m-r+1$ 时，译码错误的产生不可避免，所以 $T\leqslant m-r$。

总结第一部分的证明，即可得 $T\leqslant\min\{m-r,\ 2^{m-r-1}-1\}$。

第二部分 对于任意 $t\leqslant\min\{m-r,\ 2^{m-r-1}-1\}$，因为 $r+t\leqslant m$，所以由命题2知，G_m 具有 (r,t)-正则可交性。因此由正则可交性的定义易知，若选择 L_r 的子集 L'_r，使得 L'_r 是 L_r 中所有基数最大(等于 $t\cdot 2^r$) 的元素，则必有 $L_E=L_I=\bigcap_{L\in L'_r}L$。

综合第一、二两部分的证明可知，

$$T=\min\{m-r,2^{m-r-1}-1\}=\begin{cases}m-r, & \text{当 } m-r\geqslant 3\\ 2^{m-r-1}-1, & \text{当 } m-r\leqslant 3\end{cases}$$

推论1 $m-r\geqslant 4$ 时，$R(r,m)$ 不是小数逻辑可译码。当对 $R(r,m)$ 实施小数逻辑译码算法时，$R(r,m)$ 可纠任意 $t\leqslant m-r$ 个错，可检 $t'\leqslant 2^{m-r}$ 个错。

推论2 $m-r\leqslant 3$ 时，$R(r,m)$ 是小数逻辑可译码，即可纠 $t\leqslant 2^{m-r-1}-1$ 个错，可检 $t'\leqslant 2^{m-r}$ 个错。

至此，我们从理论上完善了 RM 码的小数逻辑译码问题。

四、结 束 语

本文所做的工作是对并元加性群[2]研究的深化和推进，对 RM 码的小数逻辑译码算法[1]的理论完善，后者解决了下述问题：对于任意 r 和 m，小数逻辑译码算法是否行之有效？有效情形(例如文献[1]不加证明地给出 $t=1,3$ $(m-r=2,3)$ 时，$R(r,m)$ 是小数逻辑可译码)为什么有效？无效情形纠错情况如何？

参　考　文　献

[1] 刘玉君，电子学报，17(1989)1，14－19.
[2] 胡正名，电子学报，8(1980)1，69－78.
[3] F. J. Macwilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, (1977), pp.370—405.

COSET PARTITION OF DYADIC ADDITIVE GROUPS AND MINORITY-LOGIC DECODING ALGORITHM FOR RM CODES

Lu Zhengfu　Hu Zhengming　Ruan Chuangai

(*Beijing University of Posts and Telecommunications, Beijing* 100088)

Abstract　Two new notions for coset partition of the dyadic additive goups are proposed, and their sufficient and necessary cond itions are also given. On the basis of these works, the feasibility problem of implementing minority-logic decoding algorithm for RM codes is solved.

Key words　Dyadic additive goup; Coset; Coding; RM code