DOI: 10.13718/j.cnki.xdzk.2015.05.016

二进制系统循环码的一个简化查表译码算法①

刘　旭，　包小敏，　武登杰，　李　梅，　袁治华

西南大学 数学与统计学院，重庆 400715

摘要：利用线性循环码的性质和伴随式的重量，给出了一个二进制系统循环码的查表译码算法. 本算法具有效率高，信息存储量少的特点.

关　键　词：循环码；查表译码；错误模式；伴随式；Hamming 重量

中图分类号：TN911　　**文献标志码**：A　　**文章编号**：1673－9868(2015)05－0102－06

本文采用文献[1]中的术语和符号.

域 F 上的一个(n, k)线性码 $\mathcal{C}$ 是 F 上的长为 n 的向量组成的一个 k 维向量空间. $\mathcal{C}$ 中的向量称为码字. 设 $\boldsymbol{c} \in \mathcal{C}$，$\boldsymbol{c}$ 的非零分量的个数称为 $\boldsymbol{c}$ 的 Hamming 重量，记为 $w(\boldsymbol{c})$. $\mathcal{C}$ 中两个码字差的重量称为这两个码字的 Hamming 距离. $\mathcal{C}$ 中任意两个码字的距离组成的集合中的最小值称为 $\mathcal{C}$ 的最小距离，用 d 表示. 此时我们也称 $\mathcal{C}$ 是一个(n, k, d)码. $\mathcal{C}$ 的纠错能力 $t=\left\lfloor \dfrac{d-1}{2} \right\rfloor$. 以 $\mathcal{C}$ 中 k 个线性无关的码字作成的 $k \times n$ 阶矩阵称为 $\mathcal{C}$ 的一个生成矩阵. $\mathcal{C}$ 的对偶码 $\mathcal{C}^{\perp}$ 的生成矩阵称为 $\mathcal{C}$ 的一个一致校验矩阵. 设 $\boldsymbol{H}$ 是 $\mathcal{C}$ 的一个一致校验矩阵，$\boldsymbol{r}$ 是一 n 维向量，$\boldsymbol{rH}^{\mathrm{T}}$ 称为 $\boldsymbol{r}$ 的伴随式. $\boldsymbol{r}$ 是码字当且仅当 $\boldsymbol{rH}^{\mathrm{T}}=\boldsymbol{0}$.

线性码的译码分为 3 步：首先计算伴随式，其次将伴随式与一个错误模式相联系，最后利用这个错误模式进行纠错. 将伴随式与错误模式相联系的最简单也是最直接的方法就是构造一个伴随式与错误模式的一一对应表，其主要思想是将纠错能力范围内的所有错误模式及对应的伴随式，按一个错误模式和与之对应的伴随式作为一行的格式作成一个译码表. 当收到一个向量 $\boldsymbol{r}$ 后，在这个表中找到其伴随式 $\boldsymbol{rH}^{\mathrm{T}}$，然后将与之对应的错误模式作为错误向量 $\boldsymbol{e}$，输出 $\boldsymbol{r}-\boldsymbol{e}$. 这种译码方式称为伴随式译码或查表译码. 同其它译码方法相比，伴随式译码具有结构简单，容易实现的优点. 在信息协调协议中伴随式译码算法也得到了应用[2]. 但当 n 很大时，伴随式译码的译码表会很大，因此占用的存储空间也会很大. 实际上，当纠错能力为 t 时，译码表有 N 行、$n+(n-k)=2n-k$ 列，其中

$$N=\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{t}$$

若对任意 $\boldsymbol{c}=[c_0, \cdots, c_{n-2}, c_{n-1}] \in \mathcal{C}$ 都有其右循环移位 $\boldsymbol{c}^R=[c_{n-1}, c_0, \cdots, c_{n-2}] \in \mathcal{C}$，则称 $\mathcal{C}$ 是一个循环码. 作为特殊的线性码，循环码的译码也分为 3 步. 但由于其循环特性，循环码的编码和译码都可通过电路来实现. Meggitt 译码器是循环码译码的一般方法[3]，它主要由 3 部分组成[4]：伴随式寄存器(syndrome register)、错误模式检测器(error－pattern detector)、存放接收向量的缓存器(buffer register to hold the received vector). 错误模式检测器是通过组合逻辑电路来实现查表的过程，这也是 Meggitt 译码器最复杂的部分. 随着码长 n 和纠错能力 t 的增加，其组合逻辑电路部分会变得很复杂，甚至难以实现. 因此简化译

① 收稿日期：2014－06－09
基金项目：国家自然科学基金项目(11471265).
作者简介：刘　旭(1989－)，男，河南商丘人，硕士研究生，主要从事编码理论，密码学的研究.
通信作者：包小敏，博士，教授.

码表就成了简化组合逻辑电路的一个突破口. 一个长为n的非零向量通过循环可以得到n个不同的向量，因此在循环码的译码表中，n个通过循环得到的错误模式可以只列出一个，从而将N减少为$\frac{N}{n}$[5]；文献[6－9]利用个别循环码((23，12，7)Golay码，(15，5，7)，(31，16，7)二进制BCH码和(47，24，11)二进制QR码)的特性和特殊结构，将这几个码的译码表从列出所有可能纠正的错误模式减少成只列出错误出现在信息部分的错误模式. i个错误出现在信息部分的k比特中，其可能性有$\binom{k}{i}$种，因此当错误个数不超过t且错误只出现在信息部分时，错误总数为$N'=\sum_{i=1}^{t}\binom{k}{i}$.

本文也是以减少译码表的行数为目的. 我们利用线性循环码的性质和伴随式的重量，给出了适用于所有二进制循环码的一个新的简化查表译码算法，并从理论上证明了这种算法的正确性.

1 系统循环码的生成矩阵和一致校验矩阵

设$\mathcal{C}$是一个$(n，k)$循环码. 多项式

$$\boldsymbol{c}(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$$

称为码字$\boldsymbol{c}=[c_0，c_1，\cdots，c_{n-1}]\in\mathcal{C}$的多项式. $\mathcal{C}$中码字多项式中次数最小的首一多项式称为$\mathcal{C}$的生成多项式. 设$\mathcal{C}$的生成多项式为

$$g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$$

则矩阵

$$\boldsymbol{G}_1=\begin{bmatrix}g(x)\\xg(x)\\x^2g(x)\\\cdots\\x^{k-1}g(x)\end{bmatrix}=\begin{bmatrix}g_0\\0\\0\\\vdots\\0\end{bmatrix}$$

是$\mathcal{C}$的一个生成矩阵. 对$\boldsymbol{G}_1$进行行初等变换，可以得到$\mathcal{C}$的如下的生成矩阵：

$$\boldsymbol{G}=[\boldsymbol{I}_k，\boldsymbol{A}_{k\times(n-k)}]$$

这里$\boldsymbol{I}_k$是k阶单位阵，$\boldsymbol{A}_{k\times(n-k)}$是一个$k\times(n-k)$阶矩阵. 由$\boldsymbol{G}$可得$\mathcal{C}$的一个一致校验矩阵：

$$\boldsymbol{H}=[-(\boldsymbol{A}_{k\times(n-k)})^{\mathrm{T}}，\boldsymbol{I}_{n-k}]$$

下面用$\boldsymbol{G}$和$\boldsymbol{H}$分别记二进制$(n，k)$循环码$\mathcal{C}$的生成矩阵和一致校验矩阵：

$$\boldsymbol{G}=[\boldsymbol{I}_k，\boldsymbol{A}_{k\times(n-k)}]，\boldsymbol{H}=[(\boldsymbol{A}_{k\times(n-k)})^{\mathrm{T}}，\boldsymbol{I}_{n-k}]$$

并分别简记为$\boldsymbol{G}=[\boldsymbol{I}，\boldsymbol{A}]$和$\boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}}，\boldsymbol{I}]$. 容易看出，信息向量$\boldsymbol{m}=[m_0，m_1，\cdots，m_{k-1}]$经过$\boldsymbol{G}$编码得到码字$\boldsymbol{c}$，其前$k$个分量恰为$\boldsymbol{m}$：

$$\boldsymbol{c}=\boldsymbol{m}\boldsymbol{G}=[\boldsymbol{m}\boldsymbol{I}，\boldsymbol{m}\boldsymbol{A}]=[\boldsymbol{m}，\boldsymbol{m}\boldsymbol{A}]$$

具有这种结构的码称为系统码. 在系统码的情况下，我们将一个二进制n维向量的前k个分量称为信息部分，后$n-k$个分量称为校验部分.

2 主要定理及证明

下面我们假设$\mathcal{C}$是二进制$(n，k，d)$循环码，$\boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}}，\boldsymbol{I}]$是$\mathcal{C}$的一个一致校验矩阵.

设$\boldsymbol{e}$是错误向量$\boldsymbol{e}=[\boldsymbol{e}_M，\boldsymbol{e}_P]=[e_0，e_1，\cdots，e_{n-1}]$，其中$\boldsymbol{e}_M=[e_0，e_1，\cdots，e_{k-1}]$是信息部分，$\boldsymbol{e}_P=[e_k，e_{k+1}，\cdots，e_{n-1}]$是校验部分，

$$w(\boldsymbol{e})\leqslant t，\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}$$

下面这个结论在后面的证明中多次用到：

定理1 若$\boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}}，\boldsymbol{I}]$，$\boldsymbol{e}=[\boldsymbol{e}_M，\boldsymbol{0}_{1\times(n-k)}]\neq\boldsymbol{0}_n$，则$w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\geqslant d-w(\boldsymbol{e}_M)$.

证 因为码字的重量至少是d，$\boldsymbol{e}_M[\boldsymbol{I}，\boldsymbol{A}]=[\boldsymbol{e}_M，\boldsymbol{e}_M\boldsymbol{A}]$是码字，所以

$$w(\boldsymbol{e}_M)+w(\boldsymbol{e}_M\boldsymbol{A})\geqslant d$$

而

$$\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}][\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}]^{\mathrm{T}}=\boldsymbol{e}_M\boldsymbol{A}$$

故

$$w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})=w(\boldsymbol{e}_M\boldsymbol{A})\geqslant d-w(\boldsymbol{e}_M)$$

在纠错范围内，定理 2 和定理 3 确定了错误只出现在校验部分的条件.

定理 2　若 $\boldsymbol{e}=[\boldsymbol{0}_{1\times k},\boldsymbol{e}_P]$，其中 $w(\boldsymbol{e}_P)\leqslant t$，则

$$w(\boldsymbol{s})=w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\leqslant t$$

证　由 $\boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}]$ 的结构可得

$$\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=[\boldsymbol{0}_{1\times k},\boldsymbol{e}_P][\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}]^{\mathrm{T}}=\boldsymbol{e}_P$$

故

$$w(\boldsymbol{s})=w(\boldsymbol{e}_P)\leqslant t$$

定理 3　若 $\boldsymbol{e}=[\boldsymbol{e}_M,\boldsymbol{e}_P]$，其中 $w(\boldsymbol{e}_M)\geqslant 1$，$w(\boldsymbol{e}_M)+w(\boldsymbol{e}_P)\leqslant t$，则

$$w(\boldsymbol{s})=w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\geqslant t+1$$

证　此时

$$\begin{aligned}w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})&=w([\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}+[\boldsymbol{0}_{1\times k},\boldsymbol{e}_P]\boldsymbol{H}^{\mathrm{T}})\geqslant\\&(d-w(\boldsymbol{e}_M))-w(\boldsymbol{e}_P)=\\&d-(w(\boldsymbol{e}_M)+w(\boldsymbol{e}_P))\geqslant\\&d-t\geqslant t+1\end{aligned}$$

故结论成立.

由定理 2 和定理 3 可得：

推论 1　若 $w(\boldsymbol{e})\leqslant t$，则 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\leqslant t$ 当且仅当 $\boldsymbol{e}=[\boldsymbol{0}_{1\times k},\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}]$.

当 $\boldsymbol{e}=[\boldsymbol{e}_M,\boldsymbol{e}_P]$ 时，下面的定理给出了 $\boldsymbol{e}_P$ 与 $\boldsymbol{e}$ 的伴随式和 $\boldsymbol{e}_M$ 的伴随式之间的一个关系.

定理 4　设 $\boldsymbol{e}=[\boldsymbol{e}_M,\boldsymbol{e}_P]$. 若 $[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{s}_M$，则

$$\boldsymbol{e}_P=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{s}_M$$

证　因为 $w(\boldsymbol{e}_P)\leqslant w(\boldsymbol{e})\leqslant t$，所以

$$\begin{aligned}\boldsymbol{e}_P&=[\boldsymbol{0}_{1\times k},\boldsymbol{e}_P]\boldsymbol{H}^{\mathrm{T}}=\\&(\boldsymbol{e}-[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}])\boldsymbol{H}^{\mathrm{T}}=\\&\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}-[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}=\\&\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{s}_M\end{aligned}$$

结论得证.

设 N' 个信息部分出错的错误向量为：

$$\boldsymbol{a}_1=[\boldsymbol{e}_M^1,\boldsymbol{0}_{1\times(n-k)}],\ \cdots,\ \boldsymbol{a}_{N'}=[\boldsymbol{e}_M^{N'},\boldsymbol{0}_{1\times(n-k)}]$$

其对应的伴随式分别为：

$$\boldsymbol{s}_1=\boldsymbol{a}_1\boldsymbol{H}^{\mathrm{T}},\ \cdots,\ \boldsymbol{s}_{N'}=\boldsymbol{a}_{N'}\boldsymbol{H}^{\mathrm{T}}$$

将向量 $\boldsymbol{s}_i$ 及 $\boldsymbol{e}_M^i$ 并置在第一行，得到一个 N' 行、n 列的表(表 1)，这个表称为信息部分伴随式与错误模式的对应表 MP-SET(Message Part-Syndrome Error Table)(表 1).

表 1　信息部分伴随式与错误模式的对应表

序号	伴随式	错误模式	序号	伴随式	错误模式
1	$\boldsymbol{s}_1=[\boldsymbol{e}_M^1,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}$	$\boldsymbol{e}_M^1$	i	$\boldsymbol{s}_i=[\boldsymbol{e}_M^i,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}$	$\boldsymbol{e}_M^i$
2	$\boldsymbol{s}_2=[\boldsymbol{e}_M^2,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}$	$\boldsymbol{e}_M^2$	⋮	⋮	⋮
⋮	⋮	⋮	N'	$\boldsymbol{s}_{N'}=[\boldsymbol{e}_M^{N'},\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}$	$\boldsymbol{e}_M^{N'}$

我们的译码算法就基于 MP-SET. 由于 $k<n$，所以 $N'<N=\sum_{i=1}^{t}\binom{n}{i}$，即表 MP-SET 的行数要比前

面提到的 $N\times(2n-k)$ 表的行数小很多，因此要减少很多存储空间. 下面的定理是我们的查表译码算法正确性的理论基础.

定理5 设 $w(\boldsymbol{e})\leqslant t$，$\boldsymbol{e}=[\boldsymbol{e}_M,\boldsymbol{e}_P]$，$w(\boldsymbol{e}_M)\geqslant 1$. 若 $\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{s}$，则存在唯一一个 $j\in\{1,\cdots,N'\}$，使得 $w([\boldsymbol{s}-\boldsymbol{s}_j,\boldsymbol{e}_M^j])\leqslant t$. 此时一定有 $\boldsymbol{e}=[\boldsymbol{e}_M^j,\boldsymbol{s}-\boldsymbol{s}_j]$.

证 由 MP-SET 的构造可知，存在 $1\leqslant j\leqslant N'$ 使得 $\boldsymbol{e}_M=\boldsymbol{e}_M^j$. 再由定理4知 $\boldsymbol{e}_P=\boldsymbol{s}-\boldsymbol{s}_j$，故 $w([\boldsymbol{s}-\boldsymbol{s}_j,\boldsymbol{e}_M^j])=w(\boldsymbol{e})$. 下面只需证当 $i\neq j$ 时必有 $w([\boldsymbol{s}-\boldsymbol{s}_i,\boldsymbol{e}_M^i])\geqslant t+1$. 实际上

$$\begin{aligned}w([\boldsymbol{s}-\boldsymbol{s}_i,\boldsymbol{e}_M^i])&=w([[\boldsymbol{e}_M,\boldsymbol{e}_P]\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{a}_i\boldsymbol{H}^{\mathrm{T}},\boldsymbol{e}_M^i])=\\&w([[\boldsymbol{e}_M+\boldsymbol{e}_M^i,\boldsymbol{0}]\boldsymbol{H}^{\mathrm{T}}+[\boldsymbol{0},\boldsymbol{e}_P]\boldsymbol{H}^{\mathrm{T}},\boldsymbol{e}_M^i])\geqslant\\&w([\boldsymbol{e}_M+\boldsymbol{e}_M^i,\boldsymbol{0}]\boldsymbol{H}^{\mathrm{T}})-w([\boldsymbol{0},\boldsymbol{e}_P]\boldsymbol{H}^{\mathrm{T}})+w(\boldsymbol{e}_M^i)\geqslant\\&d-(w(\boldsymbol{e}_M)+w(\boldsymbol{e}_M^i))-w(\boldsymbol{e}_P)+w(\boldsymbol{e}_M^i)=\\&d-w(\boldsymbol{e})\geqslant d-t\geqslant t+1\end{aligned}$$

3 新的译码算法

设 $\mathcal{C}$ 是纠错能力为 t 的 (n,k) 循环码，$g(x)=\sum_{i=0}^{n-k}g_ix^i$ 是它的一个生成多项式.

由 $g(x)$ 导出 $\mathcal{C}$ 的如下的生成矩阵和一致校验矩阵：

$$\boldsymbol{G}=[\boldsymbol{I}_k,\boldsymbol{A}],\ \boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}_{n-k}]$$

然后计算 MP-SET. 对于接收到的向量 $\boldsymbol{r}$，查表译码算法如下：

SimplifiedTableLookupDecoder($\boldsymbol{r}$, $\boldsymbol{H}$, MP-SET)

$\boldsymbol{s}\leftarrow\boldsymbol{r}\boldsymbol{H}^{\mathrm{T}}$

$\boldsymbol{e}\leftarrow[\boldsymbol{0}_{1\times k},\boldsymbol{s}]$

$i\leftarrow 1$

while $w(\boldsymbol{e})>t$ and $i\leqslant N'$

do $\begin{cases}\boldsymbol{e}\leftarrow[\text{MP-SET}(i,2),\boldsymbol{s}-\text{MP-SET}(i,1)]\\ i\leftarrow i+1\end{cases}$

if $w(\boldsymbol{e})>t$

then return ("failure")

else return $(\boldsymbol{r}+\boldsymbol{e})$ mod 2

注1 当算法输出"failure"时，表明在 MP-SET 中没有找到对应的错误模式，也就是说错误个数超出了纠错能力，因此算法此时实际上相当于检测到纠错能力范围之外的一个错误.

$(15,5)$ 循环码 $\mathcal{C}$ 的生成多项式为

$$g(x)=1+x^2+x^5+x^6+x^8+x^9+x^{10}$$

由此得到的生成矩阵

$$\boldsymbol{G}_1=\begin{bmatrix}g(x)\\xg(x)\\x^2g(x)\\x^3g(x)\\x^4g(x)\end{bmatrix}=\begin{bmatrix}1&0&1&0&0&1&1&0&1&1&1&0&0&0&0\\0&1&0&1&0&0&1&1&0&1&1&1&0&0&0\\0&0&1&0&1&0&0&1&1&0&1&1&1&0&0\\0&0&0&1&0&1&0&0&1&1&0&1&1&1&0\\0&0&0&0&1&0&1&0&0&1&1&0&1&1&1\end{bmatrix}$$

经初等行变换可化为

$$\boldsymbol{G}=\begin{bmatrix}1&0&0&0&0&1&0&1&0&0&1&1&0&1&1\\0&1&0&0&0&1&1&1&1&0&1&0&1&1&0\\0&0&1&0&0&0&1&1&1&1&0&1&0&1&1\\0&0&0&1&0&1&0&0&1&1&0&1&1&1&0\\0&0&0&0&1&0&1&0&0&1&1&0&1&1&1\end{bmatrix}$$

这时

$$\boldsymbol{A}=\begin{bmatrix}1&0&1&0&0&1&1&0&1&1\\1&1&1&1&0&1&0&1&1&0\\0&1&1&1&1&0&1&0&1&1\\1&0&0&1&1&0&1&1&1&0\\0&1&0&0&1&1&0&1&1&1\end{bmatrix}$$

$$\boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}_{10}]=\begin{bmatrix}1&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\0&1&1&0&1&0&1&0&0&0&0&0&0&0&0\\1&1&1&0&0&0&0&1&0&0&0&0&0&0&0\\0&1&1&1&0&0&0&0&1&0&0&0&0&0&0\\0&0&1&1&1&0&0&0&0&1&0&0&0&0&0\\1&1&0&0&1&0&0&0&0&0&1&0&0&0&0\\1&0&1&1&0&0&0&0&0&0&0&1&0&0&0\\0&1&0&1&1&0&0&0&0&0&0&0&1&0&0\\1&1&1&1&1&0&0&0&0&0&0&0&0&1&0\\1&0&1&0&1&0&0&0&0&0&0&0&0&0&1\end{bmatrix}$$

其中码 $\mathcal{C}$ 的最小距离 $d=7$，纠错能力 $t=3$，而 $N'=\binom{5}{1}+\binom{5}{2}+\binom{5}{3}=25$. MP-SET 见表 2.

假设发送的码字是 $\boldsymbol{c}=[001101110000101]$，接收到的向量是 $\boldsymbol{r}=[100101100000101]$. 计算伴随式得 $\boldsymbol{s}=[1111110000]$，其重量大于 3，进入 while 循环，在第 7 次得到的错误向量是

$$\boldsymbol{e}=[10100,\boldsymbol{s}-[1101110000]]=[10100,0010000000]=[1010000010000000]$$

其重量是 3，故译码输出为 $\boldsymbol{y}=\boldsymbol{r}+\boldsymbol{e}=[001101110000101]$.

与 $N=\sum_{i=1}^{3}\binom{n}{i}=575$ 相比，MP-SET 少了 550($575-25=550$) 行.

表 2　(15, 5) 循环码的 MP-SET

序号	伴随式										错误模式				
1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	0
2	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0
3	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0
4	1	0	0	1	1	0	1	1	1	0	0	0	0	1	0
5	0	1	0	0	1	1	0	1	1	1	0	0	0	0	1
6	0	1	0	1	0	0	1	1	0	1	1	1	0	0	0
7	1	1	0	1	1	1	0	0	0	0	1	0	1	0	0
8	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0
9	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1
10	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
11	0	1	1	0	1	1	1	0	0	0	0	1	0	1	0
12	1	0	1	1	1	0	0	0	0	1	0	1	0	0	1
13	1	1	1	0	0	0	0	1	0	1	0	0	1	1	0
14	0	0	1	1	0	1	1	1	0	0	0	0	1	0	1
15	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1
16	0	0	1	0	1	0	0	1	1	0	1	1	1	0	0
17	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0
18	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1
19	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0
20	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
21	0	1	1	1	0	0	0	0	1	0	1	0	0	1	1
22	0	0	0	1	0	1	0	0	1	1	0	1	1	1	0
23	1	1	0	0	0	0	1	0	1	0	0	1	1	0	1
24	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1
25	1	0	1	0	1	1	0	0	1	0	0	0	1	1	1

4 结束语

文献[6－9]中的译码算法正确性是通过程序对所有可能的错误模式进行纠错来验证的. 定理5则从理论上保证了本文算法的正确性. 本文给出的译码算法简单明了，容易理解和实现. 除了能纠正所有纠错能力范围内的错误外，还能检测到部分纠错能力范围外的错误. 同传统的查表译码算法中的表的行数 $\sum_{i=1}^{t}\binom{n}{i}$ 相比，本算法只需 $\sum_{i=1}^{t}\binom{k}{i}$ 行，极大地减少了存储量和译码的复杂性.

参考文献：

[1] MCELIECE R J. The Theory of Information and Coding(Second Edition) [M]. 北京：电子工业出版社，2002：140.

[2] 瞿云云，包小敏，童新安. 基于(24，12)扩展 Golay 码的信息协调协议 [J]. 西南大学学报：自然科学版，2010，32(5)：26－29.

[3] MEGGITT J E. Error Correcting Codes and Their Implementation for Data Transmission Systems [J]. IRE Trans on Information Theory，1961，7(4)：234－244.

[4] LIN Shu，COSTELLO D J. Error Control Coding [M]. 2nd Edition. Englewood Cliffs：Pearson Prentice Hall，2004：156.

[5] WICKER S B. Error Control Systems for Digital Communication and Storage [M]. Englewood Cliffs：Prentice Hall，1995：118.

[6] CHANG H C，LEE H P，LIN T C，et al. A Weight Method of Decoding the (23，12，7) Golay Code Using Reduced Table Lookup [C]// Proceedings of the Sixth International Conference on Communications，Circuits and Systems (ICCCAS'08). Chengdu：UESTC Press，2008：1－5.

[7] CHEN Y H，TRUONG T K，HUANG C H，et al. A Lookup Table Decoding of Systematic (47，24，11) Quadratic Residue Code [J]. Information Sciences，2009，179：2470－2477.

[8] LEE H P，CHANG H C. A Weight Method of Decoding the Binary BCH Code [C]// Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications(ISDA'08). Piscataway：IEEE Press，2008：545－549.

[9] LIN T C，LEE H P，CHANG H C，et al. High Speed Decoding of the Binary (47，24，11) Quadratic Residue Code [J]. Information Sciences，2010，180：4060－4068.

A Simplified Table Lookup Decoding Algorithm for Systematic Binary Cyclic Codes

LIU Xu，BAO Xiao-min，WU Deng-jie，
LI Mei，YUAN Zhi-hua

School of Mathematics and Statistics，Southwest University，Chongqing 400715，China

Abstract：By utilizing the properties of linear cyclic codes and the weights of syndromes，we derive a table lookup decoding algorithm for binary cyclic codes. The algorithm has the advantages of high efficiency and low memory requirement.

Key words：cyclic code；table lookup decoding；error pattern；syndrome；Hamming weight

责任编辑 张 枸