·计算机工程与应用·

二进制QR码的一个简化查表译码算法

包小敏[1]，瞿云云[2]，武登杰[1]，袁治华[1]，刘 旭[1]，李 梅[1]

(1. 西南大学数学与统计学院 重庆 北碚区 400715；2. 贵州师范大学数学科学学院 贵阳 550001)

【摘要】基于QR码的特点和伴随式的重量，给出了二进制QR码的一个新的简化查表译码算法。译码表的行是形如($\boldsymbol{e}$, $\boldsymbol{eH}$)的向量，其中$\boldsymbol{e}$是错误仅出现在信息部分且错误个数不超过码的纠错能力一半的错误模式，$\boldsymbol{eH}$是$\boldsymbol{e}$的伴随式。该算法适用于所有的二进制QR码。其译码表的行数在目前已知的二进制QR码的查表译码算法中是最小的。因此该算法不仅有一定的理论意义，也有一定的实用价值。

关 键 词 错误模式； Hamming 重量； QR码； 伴随式； 查表译码

中图分类号 TP391 文献标志码 A doi:10.3969/j.issn.1001-0548.2016.05.014

A Simplified Table Lookup Decoding Algorithm for Binary QR Codes

BAO Xiao-min[1], QU Yun-yun[2], WU Deng-jie[1], YUAN Zhi-hua[1], LIU Xu[1], and LI Mei[1]

(1. School of Mathematics and Statistics, Southwest University Beibei Chongqing 400715;

2. School of Mathematics Science, Guizhou Normal University Guiyang 550001)

Abstract A new simplified table lookup algorithm for decoding binary QR codes is presented. The algorithm is based on the properties of QR codes and the weights of syndromes. The decoding table is composed of the vectors of the form ($\boldsymbol{e}$,$\boldsymbol{eH}$), where $\boldsymbol{e}$ is an error pattern, of which the error bits are located only in the information part and the number of errors is no more than half of the error-correcting capability of the code, and $\boldsymbol{eH}$ is the syndrome of $\boldsymbol{e}$. The algorithm can be applied to decoding any binary QR code. Moreover, the number of rows of the lookup table in this algorithm is the smallest one among all known lookup table decoding algorithms for binary QR codes. So this algorithm not only has certain theoretical significance, but also has certain practical value.

Key words error pattern; Hamming weight; QR codes; syndrome; table lookup decoding

QR码是一类循环码。著名的 (23,12,7) Golay码就是一个QR码，它的扩展码是 (24,12,8) 扩展Golay码，二十世纪80年代在NASA的Voyager spacecraft program中被用于传输木星(Jupiter)和土星(Saturn)的彩色照片。在美国政府的两个标准中也指定使用 (24,12,8) 扩展Golay码[1-2]。

QR码是在1958年被提出的[3]。从那时起，人们对QR码的研究就一直没有停止过[4-8]。

QR码是一类译码比较困难的“好”码[9]；而对于Q译R码的码，文献[10]认为QR码类的译码算法通常不具有规范的结构，针对不同的QR码，采用不同的译码算法[10]。因此对QR码的译码算法研究具有一定的理论意义和实际意义。

本文针对所有二进制QR码给出一个通用的简化查表译码算法。目前已有的二进制QR码的查表译码算法一般都是针对特定的QR码，本文给出的算法不仅具有适用性广的特点，而且译码表的行数也是最小的。

1 QR码及QR码的查表译码算法

本文采用文献[11]中的术语和符号。域 F 上的一个 (n,k) 线性码 C 是 F 上的长为 n 的向量作成的一个 k 维向量空间。C 中的向量称为码字。设 $\boldsymbol{c}\in C$，$\boldsymbol{c}$ 的非零分量的个数称为 $\boldsymbol{c}$ 的(Hamming)重量，记为 $w(\boldsymbol{c})$。C 中两个码字差的重量称为这两个码字的(Hamming)距离。C 中任意两个码字的距离构成的集合中的最小值称为 C 的最小距离，用 d 表示。此时称 C 是一个 (n,k,d) 码。C 的纠错能力 $t=\lfloor (d-1)/2 \rfloor$。以 C 中 k 个线性无关的码字作成的 $k\times n$ 矩阵称为 C 的一个生成矩阵。C 的对偶码 $C^{\perp}$ 的生成矩阵称为 C

收稿日期：2014－07－21；修回日期：2016－03－21

基金项目：国家自然科学基金(61462016)；贵州省科学技术基金(黔科合J字[2014]2125号)

作者简介：包小敏(1959－)，男，博士，教授，主要从事编码理论和密码学方面的研究.

的一致校验矩阵。设 $\boldsymbol{H}$ 是 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 $\boldsymbol{rH}^{\mathrm{T}}=\boldsymbol{0}$。

设 p 是一个奇素数，$GF(q)$ 是一个有限域，其中 q 是另一素数，且是 mod p 的二次剩余。令：

$Q_p=\{$所有mod p的二次剩余$\}$，$N_p=\{$所有mod p的二次非剩余$\}$。

设 α 是包含 $GF(q)$ 的某个域中的一个 p 次本原单位根，则多项式：

$$q(x)=\prod_{r\in Q_p}(x-\alpha^r) \text{ 和 } n(x)=\prod_{r\in N_p}(x-\alpha^r)$$

都属于 $GF(q)[x]$ [12]。分别以多项式 $q(x)$，$(x-1)q(x)$，$n(x)$ 和 $(x-1)n(x)$ 作为生成多项式的循环码称为二次剩余码(quadratic residue codes，QR码)。设 C 是一个二进制 (n,k) 线性码。下面的集合作成一个二进制 $(n+1,k)$ 码：

$$\{[c_1,c_2,\cdots,c_n,\sum_{i=1}^{n}c_i]\,|\,[c_1,c_2,\cdots,c_n]\in C\}$$

称为 C 的扩展码。

QR码的译码分为两类：代数译码[13-14]和查表译码。查表译码的大致过程如下：

事先构造一个译码表，该表中一个错误模式与一个伴随式对应。对接收到的向量 $\boldsymbol{r}$，按下面的步骤进行译码：

1) 计算 $\boldsymbol{r}$ 的伴随式 $\boldsymbol{s}=\boldsymbol{rH}^{\mathrm{T}}$；

2) 通过译码表找到 $\boldsymbol{s}$ 对应的错误模式；

3) 通过错误模式进行纠错，然后将纠错后的向量输出。

查表译码最直接的做法是在译码表中将纠错能力范围内的所有错误模式和其对应的伴随式一一全部列出，这时译码表的行数为 $\sum_{i=1}^{t}\binom{n}{i}$。由于译码表的大小直接影响查表译码算法的效率和实用性，所以长期以来有很多学者都致力于减少译码表的行数的研究。

文献[15]利用循环码的循环特性，将译码表的行数减少为 $\sum_{i=1}^{t}\binom{n}{i}\Big/n$。由二项式系数的单峰性可知，当$t<n/2$时，$\binom{n}{1}<\binom{n}{2}<\cdots<\binom{n}{t}$。因此减少 $\sum_{i=1}^{t}\binom{n}{i}$ 中求和的项数t，对和的减小影响是非常大的。正因为如此，文献[16]为了将 (47,24,11) QR码的译码表的行数从 $\sum_{i=1}^{5}\binom{47}{i}$ 减少为 $\sum_{i=1}^{4}\binom{47}{i}$，不得不单独处理错误个数为5的情形：逐个反转接收码字 $\boldsymbol{r}$ 的每个分量，然后计算其伴随式，该伴随式与译码表中的伴随式相比。如果与译码表中的某个伴随式相同，那将该伴随式对应的错误模式在反转位置的比特反转后得到的向量就是错误向量。即从47个位置中逐个去搜索。这种搜索最多有可能要进行43次才能找到一个错误位置。文献[17]也采取了同样的方法来减少 (41,21,9) QR码的译码表的行数。文献[18]给出了 (47,24,11) QR码的一个查表译码算法，译码表的行数从文献[16]的 $\sum_{i=1}^{t-1}\binom{n}{k}$ 减少为 $\sum_{i=1}^{t-1}\binom{n}{k}\Big/n$。文献[19]给出了 (23,12,7) Golay码的一个查表译码算法，其译码表的简化是通过将和中项 $\binom{n}{i}$ 的n换成k：在译码表中只列出错误个数不超过 $t=3$，且错误只出现在信息部分的错误模式及其对应的伴随式。因此译码表的行数为 $\sum_{i=1}^{t}\binom{k}{i}=298$，错误只出现在校验部分时的情况单独处理。沿用此思路，文献[4]给出了 (73,37,13) QR码的一个查表译码算法，在译码表中只列出信息部分出现1～3个错误的错误模式及其对应的伴随式。其译码表的行数为 $\sum_{i=1}^{\lceil t/2\rceil}\binom{k}{i}=8\ 473$。当接收向量 $\boldsymbol{r}$ 的伴随式在表中查不到时，表明 $\boldsymbol{r}$ 信息部分的错误超过3。当信息部分出现至少4个错误时，校验部分就最多出现2个错误，故循环移位36位后，信息部分最多只有3个错误。继续文献[4]的这种思路，文献[5]给出了 (41,21,9) QR码的一个查表译码算法，译码表的行数为 $\sum_{i=1}^{\lceil t/2\rceil}\binom{k}{i}=231$；而文献[6]则给出了 (47,24,11) QR码的一个查表译码算法，其译码表的行数为 $\sum_{i=1}^{\lceil t/2\rceil}\binom{k}{i}=2\ 324$。文献[7]给出了 (23,12,7) Golay码的一个查表译码方法，将求和的项数从 $\lceil t/2\rceil$ 减少为 $\lfloor t/2\rfloor$，故其译码表的行数为 $\sum_{i=1}^{\lfloor t/2\rfloor}\binom{k}{i}=12$。

以上这些算法大多数都是针对单个具体的QR码来给出的，且译码表的行数都大于 $\sum_{i=1}^{\lfloor t/2\rfloor}\binom{k}{i}$。

通过研究，本文发现了QR码的一些性质，利

用这些性质，给出一个针对所有二进制 (n,k,d) QR码的通用的查表译码算法，译码表的行数都为 $N_h=\sum_{i=1}^{\lfloor t/2\rfloor}\binom{k}{i}$。该算法不仅能纠正小于或等于 t 个的错误，而且还可以检测出部分多于 t 个的错误。

2　循环码的生成矩阵和一致校验矩阵

设 C 是一个 (n,k) 循环码。多项式：

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

称为码字 $\boldsymbol{c}=[c_0,c_1,\cdots,c_{n-1}]\in C$ 的多项式。C 中非零码字的多项式中次数最小的首一多项式称为 C 的生成多项式。设 C 的生成多项式为：

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

则矩阵：

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

$$\begin{bmatrix}g_0&g_1&g_2&\cdots&g_{n-k}&0&\cdots&0\\ 0&g_0&g_1&\cdots&g_{n-k-1}&g_{n-k}&\cdots&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\ 0&0&\cdots&g_0&g_1&g_2&\cdots&g_{n-k}\end{bmatrix}$$

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

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

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

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

分别简记为 $\boldsymbol{G}=\left[\boldsymbol{I},\boldsymbol{A}\right]$ 和 $\boldsymbol{H}=\left[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}\right]$。

容易看出，信息向量 $\boldsymbol{m}=[m_1,m_2,\cdots,m_k]$ 经过 $\boldsymbol{G}$ 编码得到码字 $\boldsymbol{c}$，其前 k 个分量恰为 $\boldsymbol{m}$：

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

具有这种结构的码称为系统码。在系统码的情况下，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。

3　主要定理及证明

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

设 $\boldsymbol{e}=\left[\boldsymbol{e}_M,\boldsymbol{e}_P\right]$，其中 $\boldsymbol{e}_M=[e_1,\cdots,e_k]$ 是信息部分，$\boldsymbol{e}_P=[e_{k+1},\cdots,e_n]$ 是校验部分，$\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}$。

为了得到一个适用于所有QR码的通用算法，本文对QR进行研究，发现QR码都具有一些性质，利用这些性质可以得到一个通用的简化查表译码算法。将结果用6个定理的形式给出。

定理　1　若 $\boldsymbol{e}=\left[\boldsymbol{e}_M,\boldsymbol{e}_P\right]$，$w(\boldsymbol{e}_M)\geqslant 1$，则 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\geqslant d-w(\boldsymbol{e})$。

证明：因为码字的重量至少是 d，而 $\boldsymbol{e}_M\left[\boldsymbol{I},\boldsymbol{A}\right]=\left[\boldsymbol{e}_M,\boldsymbol{e}_M\boldsymbol{A}\right]$ 是非零码字，所以 $w(\boldsymbol{e}_M)+w(\boldsymbol{e}_M\boldsymbol{A})\geqslant d$。由于 $\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{e}_M\boldsymbol{A}+\boldsymbol{e}_P$，而 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})=w(\boldsymbol{e}_M\boldsymbol{A}+\boldsymbol{e}_P)\geqslant w(\boldsymbol{e}_M\boldsymbol{A})-w(\boldsymbol{e}_P)$，故 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\geqslant d-w(\boldsymbol{e}_M)-w(\boldsymbol{e}_P)=d-w(\boldsymbol{e})$。

因为 $d\geqslant 2t+1$，所以由定理1可得：

定理　2　若 $\boldsymbol{e}=\left[\boldsymbol{e}_M,\boldsymbol{e}_P\right]$，其中 $w(\boldsymbol{e}_M)\geqslant 1$，$w(\boldsymbol{e})\leqslant t$，则 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\geqslant t+1$。

由 $\boldsymbol{H}=\left[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}\right]$ 的结构及矩阵的乘法容易看出：

定理 3　若 $\boldsymbol{e}=\left[\boldsymbol{0}_{1\times k},\boldsymbol{e}_P\right]$，则 $\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{e}_P$。

由定理2和定理3可得：

定理 4　若 $w(\boldsymbol{e})\leqslant t$，则 $w(\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})\leqslant t$ 当且仅当 $\boldsymbol{e}=\left[\boldsymbol{0}_{1\times k},\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}\right]$。

定理4给出了一个如何判别错误只出现在校验部分的方法及如何确定错误模式的方法。因此当错误只出现在校验部分时就可统一处理，而不必将每个错误模式和其对应的伴随式一一列出。下面只须考虑信息部分一定有错误出现的情形。

当 $\boldsymbol{e}=\left[\boldsymbol{e}_M,\boldsymbol{e}_P\right]$ 时，定理5给出了 $\boldsymbol{e}_P$ 与 $\boldsymbol{e}$ 的伴随式和 $[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}]$ 的伴随式之间的关系。

定理 5　设 $\boldsymbol{e}=\left[\boldsymbol{e}_M,\boldsymbol{e}_P\right]$。若 $[\boldsymbol{e}_M,\boldsymbol{0}_{1\times(n-k)}]\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{s}_M$，则 $\boldsymbol{e}_P=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{s}_M$。

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

由定理5可知，在错误向量的伴随式及其信息部分对应的伴随式已知的情况下可以得到错误向量的校验部分。

当错误仅出现在信息部分，且错误个数不超过 t 时，错误向量的总数为 $N_f=\sum_{i=1}^{t}\binom{k}{i}$。设 N_f 个信息部分出错的错误向量为：

$$\boldsymbol{a}_1=[\boldsymbol{e}_M^1,\boldsymbol{0}_{1\times(n-k)}],\boldsymbol{a}_2=[\boldsymbol{e}_M^2,\boldsymbol{0}_{1\times(n-k)}],\cdots,\boldsymbol{a}_{N_f}=[\boldsymbol{e}_M^{N_f},\boldsymbol{0}_{1\times(n-k)}]$$

其对应的伴随式分别为：

$$\boldsymbol{s}_1=\boldsymbol{a}_1\boldsymbol{H}^{\mathrm{T}},\boldsymbol{s}_2=\boldsymbol{a}_2\boldsymbol{H}^{\mathrm{T}},\cdots,\boldsymbol{s}_{N_f}=\boldsymbol{a}_{N_f}\boldsymbol{H}^{\mathrm{T}}$$

将向量 $\boldsymbol{s}_i$ 及 $\boldsymbol{e}_M^i$ 并置在一行，得到一个 N_f 行、n 列的表，这个表称为信息部分伴随式与错误模式的

对应表MPSET(message part syndrome error table)：

表1 MPSET表

伴随式	错误模式
$\boldsymbol{s}_1$	$\boldsymbol{e}_M^1$
$\boldsymbol{s}_2$	$\boldsymbol{e}_M^2$
⋮	⋮
$\boldsymbol{s}_{N_f}$	$\boldsymbol{e}_M^{N_f}$

在实际译码时并不知道错误向量的信息部分，所以定理5的结果不具可操作性。定理6则从理论上保证由错误向量的伴随式和表MPSET，通过比较向量的汉明重量就可确定错误向量。因为错误向量的伴随式可通过接收到的向量得到，而表MPSET可事先做好，所以定理6的结果可实际操作。

定理 6 设 $\boldsymbol{e}=[\boldsymbol{e}_M,\boldsymbol{e}_P]$，$w(\boldsymbol{e})\leqslant t$。若 $w(\boldsymbol{e}_M)\geqslant 1$，$\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}$，则存在唯一一个 i $(1\leqslant i\leqslant N_f)$，使得 $w([\boldsymbol{s}-\boldsymbol{s}_i,\boldsymbol{e}_M^i])\leqslant t$。此时一定有 $\boldsymbol{e}=[\boldsymbol{e}_M^i,\boldsymbol{s}-\boldsymbol{s}_i]$。

证明：由MPSET的构造可知，存在 $1\leqslant i\leqslant N_f$ 使得 $\boldsymbol{e}_M=\boldsymbol{e}_M^i$。再由定理5知 $\boldsymbol{e}=[\boldsymbol{e}_M^i,\boldsymbol{s}-\boldsymbol{s}_i]$，故 $w([\boldsymbol{s}-\boldsymbol{s}_i,\boldsymbol{e}_M^i])=w(\boldsymbol{e})$。

下面只需证当 $j\neq i$ 时必有：

$$w([\boldsymbol{s}-\boldsymbol{s}_j,\boldsymbol{e}_M^j])\geqslant t+1$$

实际上由定理1可得：

$$w([\boldsymbol{s}-\boldsymbol{s}_j,\boldsymbol{e}_M^j])=w([(\boldsymbol{e}+\boldsymbol{a}_j)\boldsymbol{H}^{\mathrm{T}},\boldsymbol{e}_M^j])=$$
$$w((\boldsymbol{e}+\boldsymbol{a}_j)\boldsymbol{H}^{\mathrm{T}})+w(\boldsymbol{e}_M^j)\geqslant$$
$$d-w(\boldsymbol{e}+\boldsymbol{a}_j)+w(\boldsymbol{e}_M^j)\geqslant$$
$$d-w(\boldsymbol{e})-w(\boldsymbol{a}_j)+w(\boldsymbol{e}_M^j)\geqslant d-w(\boldsymbol{e})\geqslant t+1$$

4 新的译码算法

保留MPSET中重量 $\leqslant\lfloor t/2\rfloor$ 的错误模式和其对应的伴随式，得到的表记作SMPSET(simplified MPSET)，其行数为 $N_h=\sum_{i=1}^{\lfloor t/2\rfloor}\binom{k}{i}$。

译码时，当用 $\boldsymbol{r}$ 的伴随式在SMPSET中找不到错误向量时，则 $\boldsymbol{r}$ 信息部分的错误个数 $\geqslant\lfloor t/2\rfloor+1$，因此校验部分的错误个数 $\leqslant\lfloor t/2\rfloor$。将 $\boldsymbol{r}$ 右循环移位 $n-k$ 位，得到 $\boldsymbol{r}^{R^{(n-k)}}$，再用 $\boldsymbol{r}^{R^{(n-k)}}$ 的伴随式在SMPSET中查找错误向量。若用 $\boldsymbol{r}^{R^{(n-k)}}$ 的伴随式在SMPSET中仍找不到错误向量时，则 $\boldsymbol{r}$ 的第一个比特是错的。将其反转，然后再用得到的向量的伴随式查找错误向量。

设 C 是纠错能力为 t 的 (n,k) QR码，$g(x)=\sum_{i=0}^{n-k}g_ix^i$ 是它的一个生成多项式。由定理4和定理6，本文给出一个 C 的查表译码方法。

预处理：由 $g(x)$ 导出 C 的一个生成矩阵和一个一致校验矩阵：

$$\boldsymbol{G}=[\boldsymbol{I},\boldsymbol{A}],\quad \boldsymbol{H}=[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}]$$

然后计算SMPSET。

对于接收到的向量 $\boldsymbol{r}$，本文的译码算法如下：

Algorithm：SimplifiedTLD
{
input SMPSET, $\boldsymbol{H},\boldsymbol{r},t$;
$N_h\leftarrow$ number of rows in SMPSET;
$n\leftarrow$ number of columns in $\boldsymbol{H}$;
$k\leftarrow n-$ number of rows in $\boldsymbol{H}$;
$\text{testVec}\leftarrow\begin{bmatrix}\boldsymbol{r}=[r_1,r_2,\cdots,r_n]\\(\boldsymbol{r}<<k)\vee(\boldsymbol{r}>>n-k)\\[(r_1+1)\bmod 2,r_2,\cdots,r_n]\end{bmatrix}$;
testedNo $\leftarrow 1$;
$\boldsymbol{e}\leftarrow\overbrace{[1,1,\cdots,1]}^{n}$;
while ($w(\boldsymbol{e})>t$ and testedNo $\leqslant 3$){
$\boldsymbol{s}\leftarrow$ testVec(testedNo)$\boldsymbol{H}^{\mathrm{T}}$;
if ($w(\boldsymbol{s})\leqslant t$)
$\boldsymbol{e}\leftarrow[\boldsymbol{0}_{1\times k},\boldsymbol{s}]$;
else {
$i\leftarrow 1$;
while ($w(\boldsymbol{e})>t$ and $i\leqslant N_h$){
$\boldsymbol{e}\leftarrow[\text{SMPSET}(i,2),\boldsymbol{s}-\text{SMPSET}(i,1)]$;
$i\leftarrow i+1$;
}
}
if testedNo = 2
$\boldsymbol{e}\leftarrow(\boldsymbol{e}<<n-k)\vee(\boldsymbol{e}>>k)$;
if testedNo = 3
$\boldsymbol{e}\leftarrow[(e_1+1)\bmod 2,e_2,\cdots,e_n]$;
testedNo $\leftarrow$ testedNo $+1$;
}
if $w(\boldsymbol{e})>t$
output (“failure”);
else
output $(\boldsymbol{r}+\boldsymbol{e})\bmod 2$;
}

当算法输出“failure”时，表明在SMPSET中没有找到对应的错误模式，即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模式。

利用SimplifiedTLD，可以得到QR码 C 的扩展码 C^* 的一个译码算法如下：

设 $\boldsymbol{r}^*=[r_1,\cdots,r_n,r_{n+1}]$ 是接收到的向量。

1) 用算法SimplifiedTLD对 $\boldsymbol{r}=[r_1,r_2,\cdots,r_n]$ 进行译码，设其输出为 $\boldsymbol{y}=[y_1,y_2,\cdots,y_n]$。

2) 计算校验和 $y_{n+1}=\sum_{i=1}^{n}y_i \bmod 2$，然后输出 $\boldsymbol{y}^*=[y_1,y_2,\cdots,y_{n+1}]$。

按照这个算法译码，不仅可以纠正码 C^* 纠错能力范围内(即错误个数$\leqslant t$)的所有错误模式，而且还能纠正最后一位出错、错误个数为 $t+1$ 的错误模式。

5　结 束 语

本文利用QR码的特点及伴随式的重量，给出了QR码的一个简化译码算法。该译码算法简单明了，容易理解和实现。其译码表的行数为 $\sum_{i=1}^{\lfloor t/2\rfloor}\binom{k}{i}$，是目前QR码的查表译码算法中最少的。

从本文的讨论可以看出，这个数目还可进一步减少。在SMPSET中，错误模式经过循环移位可以得到的所有错误模式中只需保留一个，其他的均可删去。比如对 (23,12,8) Golay码，SMPSET的12行可以只保留第一行 $\boldsymbol{s}_1,\boldsymbol{e}_M^1$，这个行数是最小的。

参　考　文　献

[1] MIL-STD-188-141B. Interoperability and performance standards for medium and high frequency radio equipment[S]. Washington DC, USA: Army Information Systems Engineering Command, 1988.

[2] FED-STD-1045. Telecommunications: HF radio automatic link establishment[S]. Washington DC, USA: General Services Administration, 1990.

[3] PRANGE E. Some cyclic error-correcting codes with simple decoding algorithms[R]. Cambridge, MA: Tech Rep of Air Force Cambridge Research Center, AFCRC-TN-58-156, 1958.

[4] LEE H P, CHANG H C. An efficient decoding algorithm for the (73,37,13) quadratic residue code[C]//CSE 2011, Part I. Qingdao, China: Springer, 2011.

[5] LEE H P, CHANG H C. A memory improvement on decoding of the (41,21,9) quadratic residue code[J]. International Journal of Computer Theory and Engineering, 2012, 4(4): 590-594.

[6] LIN T C, LEE H P, CHANG H C, et al. A cyclic weight algorithm of decoding the (47,24,11) quadratic residue code[J]. Information Sciences, 2012, 197: 215-222.

[7] LEE H P, CHANG C H, CHU S I. High-speed decoding of the binary golay code[J]. Journal of Applied Research and Technology, 2013, 11: 331-337.

[8] WANG L, LI Y, TRUONG T K, et al. On decoding of the (89,45,17) quadratic residue code[J]. IEEE Trans Commun, 2013, 61(3): 832-841.

[9] 肖国镇, 卿斯汉. 编码理论[M]. 北京: 国防工业出版社, 1993.
XIAO Guo-zhen, QING Si-han. Coding theory[M]. Beijing: National Defense Industry Press, 1993.

[10] 赵晓群. 现代编码理论[M]. 武汉: 华中科技大学出版社, 2008.
ZHAO Xiao-qun. Modern coding theory[M]. Wuhan: Huazhong University of Science and Technology Press, 2008.

[11] MCELIECE R J. The theory of information and coding [M]. 2nd ed. Beijin: Publishing House of Electronics Industry, 2002.

[12] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. Amsterdam: North-Holland Publishing Company, 1977.

[13] CHANG Y, TRUONG T K, REED I S, et al. Algebraic decoding of (71,36,11), (79,40,15), and(97,49,15)quadratic residue codes[J]. IEEE Transactions on Communications, 2003, 51(9): 1463-1473.

[14] REED I S, YIN X, TRUONG T K. Algebraic decoding of the (32,16, 8) quadratic residue code[J]. IEEE Trans Inform Theory, 1990, 36: 876-880.

[15] WICKER S B. Error control systems for digital communication and storage[M]. Englewood Cliffs NJ: Prentice-Hall, 1995.

[16] 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.

[17] CHEN Y H, CHIEN C H, HUANG C H, et al. Efficient decoding of systematic (23,12,7) and (41,21,9) quadratic residue codes[J]. Journal of Information Science and Engineering, 2010, 26(5): 1831-1843.

[18] 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.

[19] 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]//2008 International Conference on Communication, Circuits and Systems (ICCCAS 2008). Xiamen: IEEE, 2008.

编　辑　税　红