第12卷 第5期 电子科学学刊 Vol. 12, No. 5
1990年9月 JOURNAL OF ELECTRONICS Sept., 1990

复数旋转码及其对偶码的超限译码* **

袁 毅 靳 蕃
(西南交通大学,成都)

摘要 本文讨论了复数旋转码及其对偶码的超限译码能力,得到了 $t=(p+1)/2$ 时复数旋转码可以纠 $C^{t+1}_{p^2+p(p-1)}-p^2C^t_{p+1}$ 个 $t+1$ 错;其对偶码可以纠 $C^{t_1+1}_{p^2+2t_1p}-2tpC^{t_1+1}_{p+1}$ 个 t_1+1 错,这里 $t_1=[(p+1)/2]-1$, p 为素数.

关键词 复数旋转码;对偶码;超限译码

一、引 言

码的纠错能力由其最小距离 d 决定,即若最小距离为 d,则码能纠 $\lfloor(d-1)/2\rfloor=t$ 个错. Berlekamp[1] 讨论了纠 t 错 BCH 码纠多于 t 个错的方法. Hartmann[2] 研究了超 BCH 限的译码,作为例子给出了纠2错31长 BCH 码纠某些3错的方法,纠5错 BCH 码纠某些6错的方法. 本文着重讨论了 $p\geqslant 3$, $t=(p+1)/2$ 时复数旋转码[3-5](复转码)的超限译码,证明了可以纠 $C^{t+1}_{p^2+p(p+1)}-p^2C^t_{2t+1}$ 个 $t+1$ 错; 以及复数旋转码对偶码 $\lceil p^2+2pt, 2pt, p+1\rceil$ 的超限译码,证明了可以纠 $C^{t_1+1}_{p^2+2t_1p}-2tpC^{t_1+1}_{p+1}$ 个 t_1+1 错,这里 $t_1=[(p+1)/2]-1$.

二、复数旋转码的超限译码

一般如码字能纠所有不超过 t 的随机错,是指以不超过 t 重的矢量(错误图样)作为陪集首在相应的陪集中重量最小,且是唯一的,故根据最大似然原则译码. 能够纠这样的错. 对 $t+1$ 个错,一般有:

引理1 文献[6]中的 C 是具有最小重量 $d=2t+1$ 的 $[n,k]$ 线性码,则至少存在一种重量为 $t+1$ 的错误图样是不可纠的.

事实上,码 C 中存在一个码字 c_i, $\mathrm{wt}(c_i)=2t+1$, 存在一个错误图样 e_i, $\mathrm{wt}(e_i)=t$, 它使得 $\mathrm{wt}(e_i+c_i)=t+1$, 即 e_i 的陪集中至少包含有一个重为 $t+1$ 的矢量,该 $t+1$ 错就被认为是不可纠的. 显然, $\mathrm{wt}(e)<t$ 的 e 所对应的陪集中都没有 $t+1$ 重的矢量.一般情况下,以下两类 $t+1$ 错是不可纠的: 一是 $c_i\in C$, $\mathrm{wt}(c_i)=2t+1$,刚

* 1988年9月20日收到,1990年4月1日修改定稿.
** 国家自然科学基金资助课题.

好在 c_i 的某 t 位上发生错，这样以该 t 错为陪集首的陪集中，包含有 $t+1$ 重矢量；二是某些 $t+1$ 错发生在 c_i，$c_i \in C$，$\mathrm{wt}(c_i)=2t+2$ 的某 $t+1$ 位上，使得在其陪集中有重 $t+1$ 的矢。

由复转码的编码可知，纠 t 错，每个信息元与监督矩阵中 $2t$ 个位置相对应，故每个信息元为 1 时产生的码重是 $2t+1$；若记 A_i 表示重 i 的所有码字的个数，下面将证明：$A_{2t+1}=p^2$。以下的 p 都是素数。

信息元中有 k 个 1，$1<k<2t+1$，每个 1 出现 $2t$ 次，至多同另外的 $k-1$ 个 1 分别只在一个方程中见面，即在监督元矩阵至少产生共 $2t-(k-1)=2t+1-k$ 个 1，k 个 1 至少产生 $k(2t+1-k)$ 个 1，k 个 1 对应的码重至少是

$$k+k(2t+1-k)=2(t+1)k-k^2 \tag{1}$$

注意到

$$(2t+1)-[2(t+1)k-k^2]=(2t+1-k)(1-k)<0 \tag{2}$$

有 $2(t+1)k-k^2>2t+1$，所以 k 个 1（信息元中）其码重至少是 $2t+1$。在 $k=2t+1$ 时，信息元部分有奇数个 1，由于监督元阵每一列之模二和等于信息元阵的模二和，故监督元阵中每一列上至少有一个 1，共 $2t$ 列，即码重至少是 $2t+1+2t$；在 $k>2t+1$ 时，自不待言。因此，码中重为 $2t+1$ 的那些码字都是 $k=1$ 时生成的，共 p^2 个，即

引理 2 $A_{2t+1}=p^2$。事实上，

$$(2t+2)-[(2t+1)k-k^2]=[(2t+1)-k](1-k)+1 \tag{3}$$

若 $1<k<2t+1$，即 $1-k\leqslant -1$；$2t+1-k\geqslant 1$，(3) 式为零的充要条件是

$$\left.\begin{aligned} 2t+1-k&=1\\ 1-k&=-1\end{aligned}\right\} \tag{4}$$

得 $t=1$，$k=2$；即当 $t\geqslant 2$ 时，恒有 $(2t+1-k)(1-k)+1<0$。于是证明了：

引理 3 若 $t\geqslant 2$，$1<k\leqslant 2t+1$，k 个信息元为 1 所得码字其码重至少是 $2t+3$。

一般要证明 $2t+2$ 个信息元为 1 在监督元阵中不产生全零是比较困难的，但对 $p\geqslant 3$，$t=(p+1)/2$，有

引理 4 $p\geqslant 3$，$t=(p+1)/2$，则 $A_{2t+2}=0$。

证明 用反证法。假设存在 $2t+2$ 个信息元，其编码结果为全零，对该 $2t+2$ 个元中的任意一个，每次仅仅能同其中奇数个见面（i 次为 t_i 个）才会使其编码结果为零，共出现 $2t$ 次，因而与其见面的元素共是 $\sum_{i=1}^{2t} t_i=$ 偶数。而 $t=(p+1)/2$。每个元要同另外的 $2t+1$ 个中的每一个见面一次，$2t+1=$ 奇数；奇数＝偶数，故矛盾，即至少有一次编码不为零。因此，$A_{2t+2}=0$。 *Q. E. D.*

进一步，显然有复转码的监督元阵中 1 的个数必为偶数，可以证明：

推论 1 $t=(p+1)/2$，则 $A_{2t+3}=0$。

引理 5 $p\geqslant 3$，$t=(p+1)/2$，复转码可以纠 $C_{p^{t+1}+p(p+1)}^{t+1}-p^2C_{2t+1}^{t}$ 个 $t+1$

错。

证明　由引理 4 的证明知，仅在 p^2 个 $2t+1$ 重的码字中错 t 位才会产生一个重 $t+1$ 的矢。因为码字重为 $2t+1$，$2t$ 个 1 都在一条错检线上，而每条错检线只同其它的有一次相交，$t(>1)$ 个错，只有发生在这条错检线和相应的信息元上才会产生一个重 $t+1$ 的矢量，共 C_{2t+1}^{t} 个。故这 t 个错就不能使其它的码字与之相加变成另一个 $t+1$ 重的。共 p^2 条错检线，因此共有 $p^2C_{2t+1}^{t+1}$ 个 $t+1$ 错在 t 错的陪集中，所以共有 $C_{p^2+p(p+1)}^{t+1}-p^2C_{2t+1}^{t}$ 个 $t+1$ 错是可纠的。　　$Q.\ E.\ D$

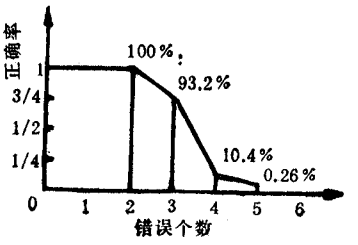

图 1　纠错能力图

注意到

$$\lim_{p\to\infty}\frac{C_{p^2+p(p+1)}^{t+1}-p^2C_{2t+1}^{t}}{C_{p^2+p(p+1)}^{t+1}}=1$$

即当 p 比较大时，几乎所有的 $t+1$ 错都是可纠的。$p=3$，$t=2$ 时的纠错能力图如图 1 所示。

三、复数旋转码对偶码的超限译码

定义　C 是数域 F 上的 $[n,k]$ 线性码，其对偶码或正交码 $C^{\perp}$ 是所有与 C 的全部码字都正交的矢量作成的集合。

$$C^{\perp}=\{u\mid u\cdot v=0,\ \forall v\in C\}$$

记 $C(C^{\perp})$ 的监督矩阵为 $H(H^{\perp})$，生成矩阵为 $G(G^{\perp})$，复转码的对偶码为 $CR^{\perp}$，显然有 $G^{\perp}=H$，$G=H^{\perp}$。$p=3$，$t=1$，复转码由其编码方法可得其 H 阵：

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

由复转码的编码方法知，p 个信息元一组被监督一次，$x_{i1}+x_{i2}+\cdots+x_{ip}=x_{ip+1}$。因而其 H 阵的每行共 $p+1$ 个 1，而每个信息元被 $2t$ 个监督元监督，即说 H 阵中信息元部分每列都仅有 $2t$ 个 1；因为每两个信息元至多有一次同在一个监督方程中出现，所以 H 的任何两行都满足至多有一个元素是公共的，共 $2pt$ 行。显然，与 H 阵的行矢量线性无关，$G^{\perp}=H$，$G^{\perp}$ 具有这些性质，$G^{\perp}$ 生成 $CR^{\perp}$ 的全部码字。

定理 1　$\forall c\in CR^{\perp}$，$\mathrm{wt}(c)\geqslant p+1$。

证明：　从 $G^{\perp}$ 知，任何两行相加至多抵消 2 个 1，任何 l 行相加至多抵消 $2(l-1)$ 个 1，于是就有任何 l 行相加生成码字中 1 的个数至少是 $l(p+1)-2(l-1)$。注意到 $[l(p+1)-2(l-1)]-(p+1)=(l-1)(p+1)>0$。在 $l\geqslant 2$ 时，上式成立，故 $CR^{\perp}$ 中仅有 $2tp$ 个码重为 $p+1$ 的码字，其它码字的码重都大于 $p+1$。$Q.\ E.\ D.$

即复转码的对偶码为 $[p^2+2pt, 2pt, t+1]$.

推论 2 $A_{p+1}=2tp$.

进一步可以证明

定理 2[7] $\forall p$, $1\leqslant t\leqslant\dfrac{p+1}{2}$, $A_{2k+1}=0$, 其中 $0\leqslant k\leqslant(p^2+2pt-1)/2$, 即 $CR^{\perp}$ 中无奇数码重.

定理 3 $\forall p$, $1\leqslant t\leqslant\dfrac{p+1}{2}$, $CR^{\perp}$ 可纠 $C_{p^2+2tp}^{t_1+1}-2tpC_{p+1}^{t_1+1}$ 个 t_1+1 错, 且

$$\lim_{p\to\infty}\frac{C_{p^2+2tp}^{t_1+1}-2tpC_{p+1}^{t_1+1}}{C_{p^2+2tp}^{t_1+1}}=1$$

这里 $t_1=[(p+1)/2]-1$.

证明 一般地, $CR^{\perp}$ 可纠 $t_1=[(p+1)/2]-1$ 错, 由前述 $A_{2t_1+1}=0$. 显然, $t_2\leqslant t_1$ 个错的陪集中矢量的重量都大于 t_1+1, 仅当 t_1+1 错发生在码重为 $p+1(=2t_1+2)$ 的码字之 $p+1$ 个上的任何 t_1+1 位上, 共 $C_{p+1}^{t_1+1}$ 个, 在其陪集中才会有 t_1+1 重的矢量, 故有 $2tpC_{p+1}^{t_1+1}$ 个 t_1+1 错是不可纠的, 可纠的共 $C_{p^2+2tp}^{t_1+1}-2tpC_{p+1}^{t_1+1}$ 个 t_1+1 错.

Q. E. D.

复数旋转码是一类新的纠错码, 它具有较好的组合特性, 编译码方法简单, 速度快, 曾经成功地在铁路电报系统中试运行, 经受了检验. 它的许多特性有待于进一步认识.

王新梅教授曾在本文的写作过程中提出过许多有价值的意见和建议, 信息工程专业的不少同志给了作者许多有益的启示, 在此一并表示感谢.

参 考 文 献

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Company, (1968).
[2] C. R. P. Hartmann, *IEEE Trans. On IT*, **IT-26** (1972), 441—444
[3] Jin Fan, An Investigation on New Complex-Rotary Code, A paper presented at IEEE 1985 International Symposium On Information Theory, Brighton, England, (1985), 1—8.
[4] 靳蕃, 通信学报, 1986 年, 第 2 期, 62—69.
[5] 靳蕃, 铁道学报, 1986 年, 第 1 期 56—64.
[6] S. Lin 著, 陈太一译, 纠错码入门, 人民邮电出版社, 1976 年.
[7] 袁毅, 复数旋转码性能的研究及计算机模拟分析, 西南交通大学硕士论文, 1988 年.

DECODING BEYOND THE BOUND OF THE COMPLEX-ROTARY CODES AND ITS DUAL CODES

Yuan Yi　　Jin Fan

(Southwest Jiaotong University, Chengdu)

Abstract　The capabilities of decoding beyond the bound of the complex-rotary codes and its dual codes are analysed. It is obtained that the complex-rotary codes with $t=(p+1)/2$ can correct $C_{p^{t+1}+p(p-1)}^{t+1}-p^2C_{p+1}^{t}$ errors of $(t+1)$ and its dual codes can correct $C_{p^{t_1+1}+t_1,p}^{t_1+1}-2tpC_{p+1}^{t_1+1}$ errors of (t_1+1), where $t_1=[(p+1)/2]-1$ and p is a prime.

Key words　Complex-rotary codes; Dual codes; Decoding beyond the bound