第 17 卷 第 3 期　　自 动 化 学 报　　Vol. 17, No. 3
1991 年 5 月　　ACTA AUTOMATICA SINICA　　May, 1991

伪随机遥控指令码集的选择

周廷显　匡载华　王　静
(哈尔滨工业大学)

摘　　要

本文论述了所有达到 Baumert-王-welch (BWW) 下界的伪随机序列可用于构成遥控指令码;推导出这类码集最大容错数的一般公式. 得出了达到 BWW 界的伪随机序列的平移等价序列构成的指令码集在抗干扰性能上是最佳循环码集的结论. 给出了序列及其反序列的平移等价序列共同做为遥控指令码集的条件.

关键词: 遥控指令码集,伪随机序列,容错数目.

在对遥控系统的抗干扰性能要求较高的场合,往往对指令进行抗干扰编码,使之具有容错能力. 据此,文献[1,2]论述了用m序列的平移等价序列做为遥控指令码集的原理及实现方法;文[6]提出了用m序列及其反序列实现遥控指令编码的设想. 它们的共同特点是这种码集本身具有容错能力,省去了一次专门的抗干扰编码,致使设备简单. 本文试图从更一般的角度出发,论述所有达到 BWW 下界的伪随机序列用于遥控指令编码的可行性及其一般性结论.

一、理 论 依 据

设一个伪随机序列为 $A = a_0a_1\cdots a_{P-1}$ (其中 P 为周期), 如果其周期自相关特性良好,则下列编码组成的码集具有良好的容错性能:

$$\left.\begin{array}{c} a_0a_1a_2\cdots a_{P-2}a_{P-1} \\ a_1a_2a_3\cdots a_{P-1}a_0 \\ \cdots \qquad \cdots \\ a_{P-1}a_0a_1\cdots a_{P-3}a_{P-2} \end{array}\right\}, \tag{1}$$

由 (1) 式可以看出,这个码集中的码字互为平移等价序列. 在相关译码时, 码字间的互相关值即为序列 A 异相时的自相关值. 由编码理论知,码集最小码距越大, 则此码集纠错能力越强. 而序列的周期自相关特性又是(1)式码集码矩的另一种表征.所以如果一个序列其周期自相关异相最大值越小,则用此序列的平移等价序列形成的码集,其纠错能力越强.

文[4]给出了任何长大于 2 的序列都遵循的自相关函数的精确下界, 即对周期 $P>2$ 的序列,设其异相自相关最大值为 $\theta_{a\max}$ 时,有

$$\left.\begin{aligned} P &\equiv 0\bmod 4,\ \theta_{a\max} \geqslant 0, \\ P &\equiv 1\bmod 4,\ \theta_{a\max} \geqslant 1, \\ P &\equiv 2\bmod 4,\ \theta_{a\max} \geqslant 2, \\ P &\equiv 3\bmod 4,\ \theta_{a\max} \geqslant -1. \end{aligned}\right\} \tag{2}$$

(2) 式所表示的下界被称为 Baumert-王-welch 界[3],简称 BWW 界. (2) 式表明不可能找到这样的序列:其异相周期自相关函数值(最大值)小于(2)式给出的值. 因此当用达到 BWW 界的序列的平移等价序列做为码集时,其纠错性能必定是优良的.

二、最佳循环码

达到 BWW 界的伪随机序列,当用其平移等价序列做为码集时，此码集实质上是一种循环码，这种循环码从抗扰性能的角度考虑是最佳循环码，因为此时对应的最小码矩在循环码中达到了上界.

三、最大容错数

设一序列,其周期自相关的异相最大值为 $\theta_{a\max}$,用其平移等价序列做为码集,其容错数的计算方法见图 1(P 为码字长度). 当接收来的码字发生 x 位错时，和此码字本身的

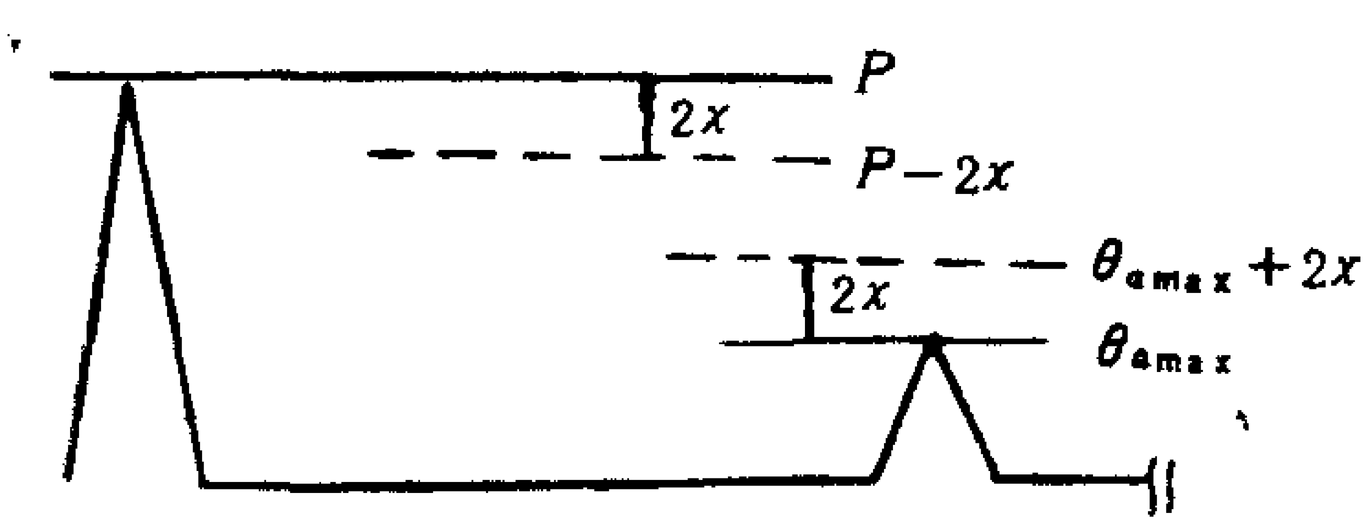

图 1　相关峰值变化示意图

参考码字相关运算时,峰值下降 $2x$,变为 $P-2x$. 而和其它码参考图样相关运算时，最坏的情况是相关函数值上升 $2x$,最大值变为 $\theta_{a\max}+2x$. 当主峰和异相最大值相接近时，码字就无法识别了,即

$$P-2x=\theta_{a\max}+2x,\quad x=\frac{P-\theta_{a\max}}{4}.$$

只要把译码判决门限取成 $P-2[x]$ 时,则得最大容错数为

$$D=\left[\frac{P-\theta_{a\max}}{4}\right], \tag{3}$$

其中 $[x]$ 表示小于 x 值的最大整数.

对于达到 BWW 下界的伪随机序列,其下界 θ_a 分别为 0,1,2,—1,所以当取 $(P-\theta_a)/4$ 为整数时,最大容错数可简化为

$$D'=\frac{P-\theta_a}{4}-1, \tag{4}$$

其中 θ_a 表示P所对应的 BWW 下界.

当发生 $D'+1=(P-\theta_a)/4$ 位错时,验证可知

$$P-2(D'+1)=\theta_a+2(D'+1),$$

所以在不能纠正错误时,能检测出错误来.

(3)式给出了任何序列、其平移等价序列做为码集时,抗扰性能所能达到的上限;(4)式则是表征了所有达到 BWW 界的序列,其平移等价序列做为码集时,抗扰性能所能达到的上限.

四、达到 BWW 界的伪随机序列

前已指出,用达到 BWW 界的伪随机序列形成如(1)式的循环指令时,是最佳循环码,而达到 BWW 界的伪随机序列是广泛的,因而具有很大的选择余地.

1. $P\equiv 0\bmod 4$, $\theta_{a\max}=0$ 的情况

文[4]中列举的所有非正自相关序列就属于此类. 这种序列的存在是无限的,目前已找到其代数结构的有两类: 一类是阴阳序列[4]; 另一类是 f-序列[5]中周期为 4 的倍数的情况. 这类序列由于是 4 的倍数,易于与计算机字节相配.

2. $P\equiv 1\bmod 4$, $\theta_{a\max}=1$ 的情况

达到此界的序列已知的有 $P=5$, 13 的巴克序列.

3. $P\equiv 2\bmod 4$, $\theta_{a\max}=2$ 的情况

目前已找到其代数结构的有两类: 一类是文[3]中由 $GF(q)$(q 为奇素数)上广义m序列通过平方剩余变换得到的长不为 4 的倍数的情况;另一类则是文[5]中长不为 4 的倍数的 f-序列.

4. $P\equiv 3\bmod 4$, $\theta_{a\max}=-1$ 的情况

达到此界的序列有m序列、L序列、H序列和 TP 序列等. 所列举的这几种序列都具有双值特性,而且异相自相关函数值正是 BWW 界(−1).

利用上述的任何一种序列的平移等价序列做为遥控指令码集,都有很好的纠错性能. 不难证明,对于 $P\equiv 3\bmod 4$, $\theta_{a\max}=-1$ 的情况所对应的各序列,用其平移等价序列做为遥控指令码集时,不仅是最佳循环码集,而且是最佳码集[7].

五、序列与反序列

设序列 $A=a_0a_1\cdots a_{P-1}$, 则定义反序列 $\bar{A}=\bar{a}_0\bar{a}_1\cdots\bar{a}_{P-1}$.

文[6]提出m序列及其反序列的平移等价序列共同做为指令码集,同样具有很好的抗干扰性能,编码效率还提高了一倍. 其实,不仅是m序列, 任何序列只要其周期自相关旁瓣峰值的绝对值足够小,就可用此序列的平移等价序列及其反序列做为指令码集,而且有良好的纠错能力,编码效率可提高一倍,还便于实现.

六、结　　论

1）用达到 BWW 界的所有伪随机序列的平移等价序列做为指令码集是可行的，而且是最佳循环指令码.

2）任一序列，当它的异相自相关最大值为 θ_{amax} 时，用此序列的平移等价序列构成的码集的最大容错数为 $D=[(P-\theta_{amax})/4]$，其中 P 为序列长，$[x]$ 为小于 x 值的最大整数. 当此序列为达到 BWW 界的伪随机序列时 $D=[(P-\theta_{amax})/4]-1$.

3）达到 BWW 界的伪随机序列很广泛，具有很大的选择余地，其中 $P\equiv 3\bmod 4$，$\theta_{amax}=-1$ 的序列的平移等价序列构成的码集，不仅是最佳循环码，而且是最佳码.

4）一序列及其反序列的平移等价序列能共同做为遥控指令码集的充要条件是此序列的异相自相关正负峰值都很小.

参　考　文　献

[1] 周延显、徐炳星，m 序列指令遥控系统研究初步，自动化学报，**10**(1984)，No. 3.
[2] 周延显，m 序列指令系统的研究，遥测遥控，**8**(1987)，No. 5.
[3] 王可、尹小维，扩频通信中的伪随机序列及一类新的 CDMA 码，电子学报，1987，No. 5.
[4] 王可、Welch, L. R.，具有非正自相关函数二进制序列，电子学报，1982，No. 5.
[5] ABRAHAM. LENPEL et al. A class of balanced binary sequences with optimal autocorrelation properties, *IEEE Tran. on infor. theory*, (1977),No. 1, 38—51.
[6] 姚育东、陈仲津，用 m 序列及其反序列实现遥控指令，自动化学报，**13**(1987)，No. 1,
[7] 钟义信，伪噪声编码通信，人民邮电出版社，(1979).

THE CHOICES OF REMOTE-CONTROL COMMANDING CODE SET OF PSEUDO RANDOM

Zhou Tingxian　Kuang Zaihua　Wang Jing
(Harbin Institute of Technology)

Abstract

In this paper, it is proved that all pseudo-random sequences with Baumer-Wang-Welch's (BWW) lower bound can be used to construct remote-control commanding codes, and a general formula of maximum fault tolerant number for this kind of code set is given. It is proved that the code set of command, which reaches the equivalent translating sequences of a pseudo-random sequence with BWW's lower bound construct, is an optimal "cyclic" code set on the interference-free performance. Full essential condition is given, under which a sequence and its inverse sequence together with their equivalent translating sequences can be used to construct remote-control command code set.

Key words: Remote-control command code set; pseudo-random sequences; maximum fault tolerant number.