The Choices of The Remote-Control Commanding Code Set of The Pseudo Random

ZHOU TINGXIAN, KUANG ZAIHUA, WANG JING

Harbin Intitute of Technology
Harbin, China

Abstract

In this paper, it is described that all of these pseudo-random sequences with Baumert-Wang-Welch's tow limits can be used to construct remote-control commanding codes; some general conclusions are got, a general formula of maximum fault tolerant number of this kind of code set is given. It is proved that the code set of command, which all of this equivalent translating sequences of a pseudorandom sequence with Baumert-Wang-Welch's low limit construct, is an optimal "Cyclic" code set oil interference-free performance. In particular, these equivalent translating sequences of a sequence with period p = 3 mod4, auto-correlation limit & = -1, construct an optimal code set. It's given that the full essential condition of which a sequence and its inverse sequence together with their equivalent translating sequences can be used to construct remote-control command code set is that the peak value of the absolute values of out of phase periodic auto-correlation of the sequence is little. It is pointed that this constructing way makes coding more effective, easy to carry out, and there are many suitable sequences that can be broadly seleted.

In the cases where a high level of interference-free function is required in a remote control system, we usually enforce the commanding into interference-free coding, so that it will posses certain fault-tolerance. The coding and decoding circuits should be simple in equipment and easy to realise. But the efficiency of coding may be quite low. According to the requirements and characteristics, the principles of using the equivalent translating squences m as the remote-control commanding code set, its realization and characteristics are described [1] [2]. A scheme of realising the remote-control commanding by using the sequence m and its inverse-sequence is given [6]. In this paper from the more general point of view, the possibility and the general result of all the pseudo-random sequence reached Baument-Wang-Welch's inferior limit that is used in remote control commanding code is discussed.

The Condition which one sequence and the equivalent translating sequence of its inverse sequence can be used together as the command-code set is given.

I. Theoretical Basis:

Suppose one sequence is $A=a_0\ a_1 \cdots a_{p-1}$ (p is period), if it has a good periodic auto-correlation property, then the code set consisting of the following codings has very good function of fault-tolerance.

$$\begin{array}{l} a_0\ a_1\ a_2 \cdots a_{p-2}\ a_{p-1} \\ a_1\ a_2\ a_3 \cdots a_{p-1}\ a_0 \\ \qquad \cdots\ \cdots\ \cdots \\ a_{p-1}\ a_0\ a^1 \cdots a_{p-3}\ a_{p-2} \end{array} \qquad (1)$$

From (1) we can see, the code words of the code set are mutually equivalent translating sequences. In interelated decoding, the cross-correlating value between the code words is the auto-correlating value of sequence A out of phase. According to the theory of decoding to the theory of coding, the bigger the minimum code distance in a code set is, the greater competence of error correction it has. Meanwhile the periodic auto-correlation feature of a sequence is another characteristic of the code distance of the code set of Formula 1. So, if the smaller peak value of a sequence's out of phase auto-correlation has, the greater the competence of error-correction the code set has, which is formed by the equivalent translating sequence of the sequence.

The precise inferior limit of auto-correlation function is given which must be followed by any sequence longer than two [4]. It is supposed the peak value of out of phase correlation of the period sequence is Q It has:

$$\begin{array}{l} p \equiv 0 \bmod 4,\ Q_{QMQX} \geq 0 \\ p \equiv 1 \bmod 4,\ Q_{QMQX} \geq 1 \\ p \equiv 2 \bmod 4,\ Q_{QMQX} \geq 2 \\ p \equiv 3 \bmod 4,\ Q_{QMQX} \geq -1 \end{array} \qquad (2)$$

The inferior limit expeessed by Formula (2) is called Baument-Wang-Welch limit [3]. We'll simplify it as BWW limit in the following. Formula (2) indicates that it is impossible to find such sequence, the function value of the out of phase periodic auto-correlation is smaller than the value given by Formula 2. So when the equivalent translating sequence reached BWW limit is used as code set, its competence of error-correction must be good. In this way, the pseudo-random sequences reached BWW limit is what we are interested in.

II. The Best "Cyclic" Code

The pseudo-random seached BWW limit, when its equivalent translating sequence is used as code set, the code set is actually a kind of cyclic code. From the viewpoint of interference-free faculty, this cyclic code is the best cyclic code. Because the corresponding minimum code distance has reached the superior limit in the cyclic code.

III. The maximal Fault-Tolerant Number

Suppose we've one sequence, the peak value of the out-of-phase periodic auto-correlation is Q_{QMQX} , using its equivalent translating sequence as the code set, its fault-tolerant number may be calculated as the following. As graph 1. p is the length of the code word.

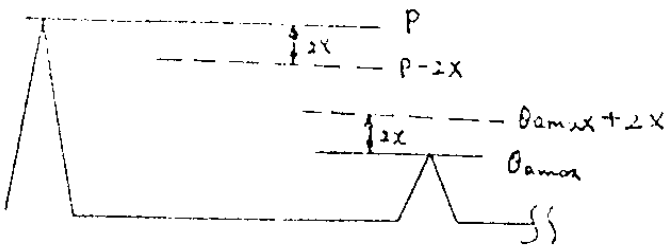

Figure 1

When the received code word happens to be in the wrong position of X, When the referent code word of the code set itself is used in the relevant operation, the peak value drops 2X, and changing into p-2x. While it is used in the operation of other code's referent graphs, the worst condition is that the relevant function value arises 2x, the peak value changes into Q_{QMQX} +2x. When the peak approcaximates to the extreme value of the out of phase correlation, it's difficult to distinguish the code wordes. That is,

$$p - 2x = Q_{\cdots} + 2x$$

$$x = \frac{p - Q_{\cdots}}{4}$$

As long as taking the door limit of deciding the decoding as p-2x, the available maximal fault-tolerant number is

$$D = \left[\frac{p - Q_{\cdots}}{4}\right] \tag{3}$$

in which [x] expresses the biggest integer, which is smaller than the value of X.

For the pseudo-random sequences reached the BWW limit, its inferior limit Q_Q is respectively o,1,1,-1, so D is an integer. In this way the maximal fault-tolerant number can be simplified as:

$$D' = \frac{p - Q_o}{4} - 1 \qquad (4)$$

Where Q_Q espresses p's corresponding BWW inferior limit.

When the wrong positions $D'+1 = \frac{p-Q_o}{4}$ happens , we can know through demonstration, $p-2(D'+1) = Q_Q+2(D'+1)$ So when it cannot be corrected, the error can be checked out. Formula (3) gives the superior limit of interference-free competene, when its equivalent translating sequences are used as code set.

Formula (4) expresses the superior limit of interference-free compentence that can be reached by all the sequences reached BWW limit, when its equivalent translating sequence is used as code set.

IV. The Pseudo-random Sequences Reach BWW Limit

As we've already pointed out, when psuedo-random sequence reached BWW limit forms the cyclic commanding as Formula (1), it's the best cyclic code. But the pseudorandom sequence reached BWW limit is general, so it has a large room for choice.

1) The condition of $p \equiv 0 \bmod 4$, $Q_{QMQX} = 0$. All the non-positive auto-correlation sequences enumerated in paper [4], belong to this kind. The existence of this kind of sequence is limitless. So far, we've found two kinds of its algebraic structure. One is Ying-Yang sequence [4], the other is the condition that the period is the multiple of 4 in f-sequence [5]. Because this kind of sequence is the multiple of 4, It's easy to match with the word syllables of computer.

2) The condition of $p \equiv 1 \bmod 4$, $Q_{QMQX} = 1$, we've known the Bark sequence of P which is equivalent to 3 and 13, that is the kind of the sequence.

3) The condition of $p \equiv 2 \bmod 4$, $Q_{QMQX} = 2$, up to now, we've found two kinds of its algebraic structure. One is the generalized sequence M in G=F(q) (q is odd prime number) which changes into the condition whose length is not the multiple of four, by square-surplas conversion. The other is the f-sequence in [5] whose length is not the multiple of four.

4) The condition of $p \equiv 3 \bmod 4$, $Q_{QMQX} = -1$, sequences which reached the limit are sequence m,L,H,TP, etc. All the enumerated sequences have the feature of two values. Also the function value of the out of phase correlation is exactly the BWW limit (-1).

The remote-control commanding code set, using the equivalent translating sequences of any of the abve enumerated sequence has a good capacity of error-correction. It's worthwhile to point out that is on the condition $p \equiv 3 \bmod 4$, $Q_{QMQX} = -1$. For this kind of sequence, using the equivalent translating sequence as the remote-control commanding code set, which is not only the best cyclic code set, but also the best code set.

Because of the theorem (7) the cross-correlation number is $p(C_1, C_0)$, then we have

$$\underset{\text{any code}}{0 \leq \text{Min Max}} \rho(C_i, C_j) \geq \begin{cases} \dfrac{-1}{n-1} & \text{when } n \text{ is even} \\ -\dfrac{1}{n} & \text{when } n \text{ is odd} \end{cases} \qquad (5)$$

The code set reached the inferior limit of formula (5) is the best code set. For the sequence of $p \equiv 3 \bmod 4$, $Q_{QMQX} = -1$, the code set put forward by its equivalent translating sequences include P code words, that is n=P.

But Max $P(C_1, C_0) = -1$ / P=3 mod 4

According to formula (5), obviously we have

Min Max $P(C_1, C_0) = -1$ / P P=3 mod 4

For the sequence of P=3 mod 4, $Q_{QMQX} = -1$, the code set formed by its equivalent translating sequences is the best code set.

So in the coding of remote-control commanding, choosing this kind of sequence is the best choice, which has the superior interference-free competence.

V. Sequence and Inverse Sequence

Suppose sequccne $A=a_o\ a_1 \cdots a_{p-1}$ then the inverse sequence is defined as $A=a_o\ a_1 \cdots a_{p-1}$

Sequence m and the equivalent translating sequence of its inverse sequence are used together as commanding code set [6], so that it possesses great advantage of interference-free competence. The effiency of codings is also raised by two times. Actually, not only sequence m, an sequence, as long as the absolute value of the periodic auto-correlation

sidelobe peak value of any sequence is small enough, then the equivalent translating sequence of the sequence and its inverse sequence can be used as commanding code set, and it has a very good competence of error-correction, the efficiency of coding is also raised by two times, and it's quite easy to realize.

Suppose sequence $A=a_o\ a_1 \cdots a_{p-1}$ the inverse code set $A=a_o\ a_1 \cdots a_{p-1}$ constructure is

$$(A_o , A_1 \cdots , A_{p-1} , A_o , A_1 \cdots , A_{p-1})^{\tau} \tag{6}$$

Suppose the cross-correlation of code set (6), that is A's periodic auto-correlation function with the code word A_1 , A_j (i, j ∈ [0, p)) is

$$Q_A(\tau) = \begin{cases} p & \text{when } \tau = 0, \text{ where } p \text{ is perid} \\ 0(\tau) \quad |0(\tau)| \leqslant \varepsilon, & \text{when } \tau \neq 0 \text{ where } \varepsilon \text{ is constant} \end{cases} \tag{7}$$

Let's deduce the cross-correlation function of code set (6)

First of all let's have a look of value of cross-correlation funtion of inverse sequence A's equivalent translating sequence that is A's auto-correlation funceion value.

$$\begin{aligned} \bar{A} &= \bar{a}_0 \bar{a}_1 \cdots \bar{a}_{p-1} \qquad a_i \in (0, 1) \\ &= (a_0 \oplus 1)(a_1 \oplus 1) \cdots (a_{p-1} \oplus 1) \\ \bar{A}\tau &= \bar{a}_{\langle \tau \rangle_p} \bar{a}_{\langle 1+\tau \rangle_p} \cdots \bar{a}_{\langle p-1+\tau \rangle_p} \\ &= (a_{\langle \tau \rangle_p} \oplus 1)(a_{\langle 1+\tau \rangle_p} \oplus 1) \cdots (a_{\langle p-1+\tau \rangle_p} \oplus 1) \\ \bar{A} \oplus \bar{A}_\tau &= (\bar{a}_0 \oplus \bar{a}_{\langle \tau \rangle_p})(\bar{a}_1 \oplus \bar{a}_{\langle \tau+1 \rangle_p}) \cdots (\bar{a}_{p-1} \oplus \bar{a}_{\langle \tau+p-1 \rangle_p}) \\ &= (a_0 \oplus a_{\langle \tau \rangle_p})(a_1 \oplus a_{\langle 1+\tau \rangle_p}) \cdots (a_{p-1} \oplus a_{\langle \tau+p-1 \rangle_p}) \\ &= A \oplus A_\tau \end{aligned}$$

So $Q_A(\tau) = Q_A(\tau)$

That's to say A and A have the same periodic auto-correlation function. The question left is the calculation of cross-correlation value of

$$\begin{aligned} \bar{A}_\tau &= A_\tau \oplus I \qquad I = 1\,1\,1 \cdots 1 \\ A_{\tau_1} \oplus \bar{A}_{\tau_2+\tau} &= A_{\tau_1} \oplus \overline{A_{\tau_2+\tau} \oplus I} \\ &= A_{\tau_1} \oplus A_{\tau_2+\tau} \end{aligned}$$

$$Q_{A_{\tau_1} \bar{A}_{\tau_2}}(\tau) = \begin{cases} -p, & (\tau_2 + \tau)_p = \tau_1 \\ -Q(\tau) & (\tau_2 + \tau)_p \neq \tau_1, \ |Q(\tau)| \leqslant \varepsilon \end{cases} \tag{8}$$

The footnote p in formula (8) indicates modul p.

From formulas (7), (0), the mark of A's out of phase auto-correlation is just the opposite with the cross correlation of A and A, the absolute value doesn't change. When code set (6) can be used efficiently as remote-control commanding coding, $Q(\tau)$, $-Q(\tau)$ have to be very small. That's the positive and negative peak value of a sequences out of phase correlation are all very small i.e. $|Q(\tau)|$ is very small. It's appropriate to use the equivalent translating sequence as the remote-control commanding code set. For example, sequence M, L, H, and TP. Though the Ying-Yang sequence [4] reaches the BWW inferior limit, its negative peak is very high. It's not suitable to add its inverse sequence into the code set, otherwise it will greatly reduce its own error-correction competence.

VI. Summary:

1. Commanding code set using the equivalent translating sequence of all the pseudorandom sequences reached BWW limit, is the best cyclic commanding code.

2. Any sequence, when the peak value of its out of phase correlation is Q_{QMQX}, the biggest fault-tolerant number of the code set formed by its equivalent translating sequence is

$D = [\frac{p - Q_{QMQX}}{4}]$, in which P is the length of the sequence [X] indicates the biggest integer which is small than the value of X. When the sequence is the pseudorandom sequence reached BWW limit,

$D = \frac{p - Q_{QMQX}}{4} - 1$

3. All the equivalent translating sequence of any sequence reached BWW limit can be used as commanding code set. But the pseudorandom sequence which reaches BWW limit is very general, and has large room for choices, in which the code set formed by the equivalent translating sequence of $p = 3 \bmod 4$, $Q_{QMQX} = -1$ sequences is not only the best cyclic code, but also the best code.

4. The necessary and sufficient condition of which one sequence and its equivalent translating sequence and their inverse sequence can be used together as the remote-control commanding code set, is that both the positive and negative peak value of the out of phase correlation of the sequence are all very small.

REFERENCES

[1] ZHOU TINGXIAN, XIU BINXING, “The initial research on m sequences commanding remote-control system”. The Chinese Automation Journal, Vol. 10, No. 3, 1984.

[2] ZHOU TINGXIAN, “The research on m sequences commanding remot-control systemm” Telemetry and remote control, China, Vol. 8, No. 5, 1987

[3] WANG KE et al, “On PN sequneces for spread spectrum communication and a new class of CDMA codes” Acta Electronica sinica, China, No. 5, 1987.

[4] WANG KE, L.R. WELCH, “Binary sequences with non-positive autocorrelation values” Acta Electronica sinica, China, No. 5, 1987.

[5] ABRAHAM, LEMPEL et al “A class of balanced binary sequences with optimal autocorrelation properties” IEEE Tran. On info. Theory pp. 38-51 No. 1 1977.

[6] YIAO YUDONG, CHENG ZHONG JING, “Remote commanding is reliazed with m-sequences and their, inverse sequences” China Automation Journal No. 1, 1987.

[7] ZHONG YIXING, “psendo Radom coding communication” The post and Telecommunication organization of China, 1979.