The Error-Correcting Codes of The m-Sequence

ZHOU TINGXIAN, HOU LIKUN, XU BINGXING
Harbin Institute of Technology
Harbin, China

Abstract

The paper analyses the properties of m-sequence error-correcting codes when adapting the correlation detection decoding method, deduces the error-tolerant number formula of binary sequence with a good auto-correlation property being used as error-correcting codes, provides with a method to increase the efficiency of the m-sequence error-correcting codes and make its coding and decoding procedures in the form of framed figures.

1. Theoretical Analysis:

Suppose u equals the m-sequence with a period p= 2^r -1, (r refers to primitive polinomial power of the m-sequence), thus, all the motion of translation equivalent sequence form the set u, shown as follows,

\[ u = \{u, Tu, \cdots, T^{p-1}u\} \]

Suppose \( N \) stands for all “0” sequence, the error-correcting code set \( u_c \) consists of definition m-sequence. It is given

\[ u_c = \{\phi, u, Tu, \cdots, T^{p-1}u\} \]

To add optional two sequence mod 2 among set \( u_c \), the result is a certain motion of translation equivalent sequence of m-sequence \( u \). Therefore, the cross-correlation properties in the code words of set \( u_c \) are the same as the auto-correlation properties in m-sequence \( u \).

Figure I is the error-correction coding and decoding diagram of the m-sequence. The coding function is to take error-correcting set for information group. Decoding code, in fact, is a correlation detector. The auto-correlation properties of the m-sequence is shown in (1), on condition that there is nothing wrong with the code words in the channel.
Thus, \( \hat{u} = u \), and \( p_{a,u} = p \) (1) whenever there happens to be a wrong position in code words, between \( p_{a,u} \) and \( p \) (I) is a difference value \( \pm \frac{2}{p} \). That is, \( \rho_{\hat{u},u} = \left\{ \begin{array}{ll} 1 - \frac{2}{p} & (u = \text{the reference code of } \hat{u}) \\ - \frac{1}{p} + \frac{2}{p} & \text{or } - \frac{1}{p} - \frac{2}{p} & (u \neq \text{the reference code of } \hat{u}) \end{array} \right. \)

when something is wrong with \( t \) digit errors, if the correlation detecting codes go smoothly, it is required as follows:

\[
1 - \frac{2}{p} t > - \frac{1}{p} + \frac{2}{p} t
\]

We define the digital number \( t \) of errors which the m-sequence of length \( p \) can correct as the error-correcting power. It is obtained from (2)

\[
t = 2^{m-2} - 1
\]

II. The Error-Correcting Performance

Owing to the fact that adding the optional two code word mod 2 in the code set or its result is still a certain code word in \( u_c \), the code distance and slightest weight of the code word in \( u_c \) is the same. That is,

\[
d_{\text{min}} = 2^{m-1}
\]
Judging from the theory of linear block code, the formula (4) indicates the code of code distance. Its power to correct errors is,

\[ t \leq \left[ \frac{d_{\text{min}} - 1}{2} \right] = 2^{m-2} - 1 \]  

(5)

It is seen that formula (4) reaches the superior limit of formula (5). That means that the correlation detection decoding method has given full scope to the potentiality of the random error-correction of the m-sequence.

The correlation detection decoding code has a very striking character, that is, all the errors can be corrected together. From the above theoretical analysis, no matter the error properties are random or burst, formula (3) is always found right. This indicates that the correlation detection decoding code of the m-sequence is capable to correct the burst errors. As for the single burst error of length \( l \leq 2^{m-2} - 1 \), several burst errors which the sum of their lengths is no more than \( 2^{m-2} - 1 \), all can be corrected. Furthermore, in the case of more burst errors, there is no requirement for burst intervals.

When the random and the burst errors appear at the same time, it is requested that the sum of the random error digits and the burst length is no more than \( 2^{m-2} - 1 \). From formula (3), \( m=3,4,5, t=1,3,7 \), we can see the error-correcting power of the m-sequence is much stronger.

III The Auto-correlation Properties and The Error-tolerant Number in The Binary Sequences

The m-sequence can correct errors by using the correlation detection decoding code. The essence is due to a certain difference which exists between the in phase auto-correlation function value and out of phase auto-correlation function value. When several digital errors appear, there remains a difference of the kind, which makes the correlating detection go in a right way. We call the property of the m-sequence error-tolerant property. That the m-sequence can correct the random and the burst errors at the same time is the inevitable result of the error-tolerant properties.

The error-tolerant properties are not only possessed by the sequences with double value auto-correlation property. As long as the out of phase auto-correlation function value is small enough, this kind of sequence will have a good error-tolerant property.

In the document (5), the precise inferior limit of auto-correlation function is given, which must be followed by any sequence longer than two. It is supposed that the peak value of the out of phase auto-correlation function of the sequence is \( \theta_{\text{amax}} \). It has,
The inferior limit expressed by formula (6) is called Baument-Wang-Welch Limit. We’ll simplify it as BWW limit in the following. Fromula (6) indicates that it is impossible to find such sequences, the function value of the out of phase auto-correlation is smaller than the value given by formula (6). So, in order to gain a good error-tolerant property, we must find the sequence which reaches BWW limit, for the peak value of the out of phase auto-correlation function among the sequences is just the possible minimum value.

As for binary sequence, when the received code word happens to be in the wrong position with t digits and when the reference code word itself is used in the relevant operation, the peak-value drops 2t and changes into p-2t. While, it is used in the operation of other code’s reference graphs, the worst condition is that the correlation function value arises 2t, the peak value changes into \( \theta_{\text{max}} + 2t \). If the correlation detection goes on in a right way, it has

\[
p - 2t > \theta_{\text{max}} + 2t
\]

namely

\[
 t < \frac{p - \theta_{\text{max}}}{4}
\]

In the four cases shown by formula (6), the binary sequences with period p have error-tolerant power, shown separately as below,

\[
\begin{align*}
 t &< \frac{p}{4} \\
 t &< \frac{p-1}{4} \\
 t &< \frac{p-2}{4} \\
 t &< \frac{p+1}{4}
\end{align*}
\]

Evidently, among the four cases, the fourth one \( t < \frac{p+1}{4} \) is the best, namely, choosing periodical kind \( p=3 \mod 4 \), the available maximal out of phase auto-correlation function value comes to \( \theta_{\text{max}} = -1 \), whose sequence forms error-correcting code set. Its error-tolerant property is the best of all. As the m-sequence is due to the correlation of \( p=3 \mod 4 \).
4, \( \theta_{\text{amax}} = -1 \), its error-tolerant property is the best. Those reaching the limit are the sequences L, H and TP.

IV. The Coding Efficiency of The m-Sequence

One of the shortcomings of the m-sequence error-correcting code is have a lower coding efficiency,

\[
\eta = \frac{m}{2^n - 1} \quad (8)
\]

When the error-correcting code set consists of the m-sequence and the inverse sequence, the efficiency may be raised, and there is no effect on other properties.

Suppose \( u = (u_0, u_1, \cdots, u_{p-1}) \) is the m-sequence with the period \( p = 2^r - 1 \), thus, we regard \( \bar{u} = (\bar{u}_0, \bar{u}_1, \cdots, \bar{u}_{p-1}) \) the inverse sequence of the m-sequence. The auto-correlation function of the inverse sequence \( \bar{u} \) has a double value property,

\[
\rho_{\bar{u}}(i) = \begin{cases} 
1 & i = 0 \pmod{p} \\
-\frac{1}{p} & i \neq 0 \pmod{p}
\end{cases} \quad (9)
\]

The cross-correlation function of the m-sequence \( u \) and its inverse sequence \( \bar{u} \) s shown bellow,

\[
\rho_{u,\bar{u}}(i) = \begin{cases} 
-1 & i = 0 \pmod{p} \\
\frac{1}{p} & i \neq 0 \pmod{p}
\end{cases} \quad (10)
\]

Consequenty, the cross-correlation function peak value of the code word in the code set having been enlarged \( 1 / p \), the error-tolerant power of the set can be deduced as follows,

\[
1 - \frac{2}{p} > \frac{1}{p} + \frac{2}{p} t \\
t < \frac{p - 1}{4}
\]

Hence,

\[ t = 2^{m-2} - 1 \quad (11) \]
That is to say, on condition that the error-correcting power is not lost, the coding efficiency can rise up to,

$$\eta = \frac{\Lambda}{2^n + 1}$$  \hfill (12)

V. Realize The Error-correction Coding and Decoding Code of The m-Sequencen

The $2^{m+1}$ matched filter hardware, required to the correlation detection decoding code, is rather complex to be realized. Whereas, it has been proved right to realize the error-correction coding and decoding code of the m-sequence by using computer on-slice and software procedure. The following is the procedure framed diagram of m-sequence with period $p=15$ error-correction coding and decoding code, which is realized on the 8031 computer on-slice of the series MCS-51.

VI. Summary

1) By using the correlation detection decoding code, the random error-correcting power of the m-sequence comes to the superior limit of random error-correcting power of block code. In this sense, it is the best.

2) by using the correlation detection decoding code, the m-sequence need not distinguish the error properties, namely, no matter whether it is the random errors or the burst errors, all can be corrected. There is no need for burst intervals in operation.

3) The m-sequence is a special example of a binary sequence which has a good error-tolerant property. In the binary sequence reaching BWW limit, the sequences, such as $p = 3 \mod 4$, $\theta = -1$ have got a better error-tolerant property.

4) The binary sequence with error-tolerant property has a general formula of error-tolerant number as shown as follow,

$$t < \frac{p - \theta_{\text{max}}}{4}$$

5) Since the integrated circuits have appeared on a large scale at present days, it is both simple and possible to use computer on-slice to realize the error-correcting coder and decoder of the m-sequence. Because of making full use of software, the hardware circuits become quite simple.
Fig. 2 coding procedure framed diagram
Fig. 3 decoding procedure framed diagram

References