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

Yuan Yi(袁 毅) Jin Fan(靳 蕃)
(*Southwest Jiaotong University, Chengdu*)

Abstract The capabilities of decoding beyond the bound of the Complex-Rotary code (CR codes)[1] and its dual code are analyzed. It is obtained that the CR codes with normal error-correcting ability $t = (p+1)/2$ can correct $(t+1)$-errors up to $C^{t+1}_{p^2+p(p+1)} - p^2 C^{t}_{2t+1}$ and its dual code can correct (t_1+1)-errors up to $C^{t_1+1}_{p^2+2tp} - 2tpC^{t_1+1}_{p+1}$ where $t_1 = (p+1)/2 - 1$ and p is a prime.

Key words Complex-Rotary code; Dual code; Decoding beyond the bound

I. Introduction

It is well known that a code can correct t random errors if its minimum distance is $2t+1$. Berlekamp[2] and Tzeng[3] discussed the question of decoding some patterns of more than $[(d_0-1)/2]$ errors even if the minimum distance of cyclic code is d_0, where d_0 denotes the BCH bound. Hartmann[4] made an investigation on decoding beyond the BCH bound and gave an example that the two-error-correcting BCH code of length 31 can correct some three-errors. In this paper we investigate the decoding capabilities of t-error-correcting CR codes and the dual of CR codes.

II. Decoding Beyond the CR Codes

Lemma 1 If C is a [n,k,d] linear code, then there exists at least one error of weight $t+1$ which cannot be corrected, where $d = 2t+1$.

In fact,vectors of weight $t+1$, that cannot be corrected, are just contained in the two kinds of cosets. One is that the coset of its leader has weight t, and the other is that the coset of its leader has weight $t+1$. From its coding rule it is easy to show that each information bit in t-error-correcting CR codes corresponds to $2t$ check symbols. Thus if only one information bit is 1, the weight of corresponding codewords is $2t+1$.

Lemma 2 $A_{2t+1} = p^2$,
where A_i denotes the number of codewords of weight i and p is a prime.

Proof There exist k ones in the information square matrix, $1 < k < 2t+1$, and in the worst case every one meets another $k-1$ ones in an equation separately, such that the check symbol equals to 0, that is, at least $2t-(k-1)$ ones appear in the parity-check-symbol matrix for each one. In total, for all k ones, we have $k(2t+1-k)$ ones in whole parity-symbol matrix and the weight of a codeword is at least

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

or

$$(2t+1) - [(2t+1)k - k^2] = (2t+1-k)(1-k) < 0$$

and thus

$$(2t+1)k - k^2 > 2t+1$$

While $k = 2t+1$,there are odd ones in the information square matrix. Because the sum of each column in parity-check-symbol matrix and the sum of the information square matrix is congruent modulo 2,each column in parity-check-symbol matrix has a one. So the weight is more than $2t+1+2t$.

Therefore the codewords of weight $2t+1$ correspond to $k=1$, and the total number of codeword is p^2.

In fact

$$(2t+2) - [(2t+1)k - k2] = [(2t+1) - k][1-k] + 1 \tag{2}$$

If $1 < k < 2t+1$ then $1-k \le -1$, $2t+1-k \ge 1$.

The sufficient and necessary conditions such that (2) equals to zero are

$$\begin{cases} 2t+1-k=1 \\ 1-k=-1 \end{cases}$$

Hence we get $t=1$ and $k=2$. That is while $t \ge 2$, we always have $(2t+1-k)(1-k)+1 < 0$. Thus the following lemma is obviously valid.

Lemma 3 If $t \ge 2$ and $1 < k < 2t+1$, the weight of the codeword which has k ones in the information square matrix is at least $2t+3$.

Generally it is difficult to prove that if there are $(2t+2)$ ones in the information square matrix, the corresponding parity-check-symbol matrix is not a zero matrix, but for $p > 2$, $t = (p+1)/2$, we have

Lemma 4 If $p > 3$, $t = (p+1)/2$, then $A_{2t+2} = 0$.

Proof Suppose that there exist $(2t+2)$ information bits such that the check-symbol matrix is zero matrix. Then when any of the $(2t+2)$ bits can just meet odd bits of the rest in an equation, the check bit is zero and each information bit occurs $2t$ times, and thus the total bits which met by this one are even.

Since $t = (p+1)/2$, from the coding rule, this bit must meet any of the $(2t+1)$ bits just one time. $2t+1$ is odd number,and odd=even makes a contradiction. Therefore there exists at least one time that the coding result is not zero, and hence we have $A_{2t+2} = 0$.

Theorem 5 For $p \ge 3$, $t = (p+1)/2$, the CR codes can correct

$$C^{t+1}_{p^2+2pt} - p^2 C^t_{2t+1}$$

$t+1$ random errors.

Proof It is pointed out in the proof of Lemma 3 that the error vectors of weight $t+1$, that cannot be corrected, are derived from p^2 codewords of weight $2t+1$ when any t errors appear on any of $2t+1$ bit. The total number of error vectors is $p^2 C^t_{2t+1}$, and thus the rest $C^{t+1}_{p^2+2pt} - p^2 C^t_{2t+1}$ $(t+1)$-errors can be corrected.

It is also easy to obtain that

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

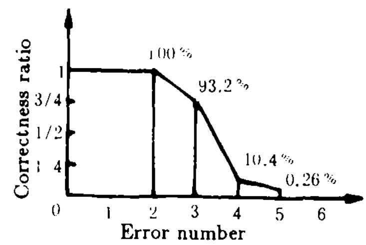

Fig.1 The error-correcting capability of CR code [21,9,5]

It shows that almost all $t+1$ errors can be corrected when p is large enough. For example, when $p=3$, $t=2$, and the CR codes is a [21,9,5] linear code, we have the error-correcting capability as shown in Fig.1

III. Decoding the Bound of the Dual of CR Codes

The sign $C^{\perp}$ denotes the dual of C. $H(H^{\perp})$, $G(G^{\perp})$ are the parity check matrix, generator matrix of $C(C^{\perp})$, respectively. There obviously exists

$$G^{\perp}=H, \qquad H^{\perp}=G$$

For example, $p=3$, $t=1$. From the coding rule, we have the following H matrix

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

According to the coding rule of the CR code,each group of p information bits is checked one time, and each row in H has $(p+1)$ ones. And each information bit is checked by $2t$ check bits, and each column in information part of H has $2t$ ones. Any two rows just have at most one common symbol. The total rows of H is $2pt$. So $G^{\perp}$ generates all codewords of $CR^{\perp}$.

Theorem 1 $\forall c \in CR^{\perp}$, $wt(c) \geq p+1$.

Proof At most 2 ones may eliminate in the sum of any two rows, because any two rows do not have more than one common symbol. For any l rows, at most $2(l-1)$ ones will be vanished. Thus codewords from the combination of l rows have weight no less than

$$l(p-1)-2(l-1)$$

For all $l \geq 2$

$$[l(p-1)-2(l-1)]-(p+1)=(l-1)(p+1)>0$$

Thus, there are $2tp$ codewords having weight $p+1$ in $CR^{\perp}$, the rest of which having weight larger than $p+1$.

The dual code of the CR code $[p^2+2pt,\ p^2,\ 2t+1]$ is a $[p^2+2pt,\ 2pt,\ p+1]$, linear code and its minimum distance is free of t.

Similarly, we have

Theorem 2 $A_{p+1} = 2tp$.

Furthermore, we can prove

Theorem 3 If $1 \le t \le (p+1)/2$, then $A_{2k+1} = 0$, where $0 < k \le (p^2 + 2pt - 1)/2$. i.e. there are no codewords of odd weight in $CR^{\perp}$.

Theorem 4 If $1 \le t \le (p+1)/2$, then $CR^{\perp}$ can correct

$$C_{p^2+2pt}^{t_1+1} - 2ptC_{p+1}^{t_1+1}$$

t_1 errors and

$$\lim_{p\to\infty} \frac{C^{t_1+1}p^2 + 2pt - 2ptC_{p+1}^{t_1+1}}{C_{p^2+2pt}^{t_1+1}} = 1$$

where $t_1 = (p+1)/2 - 1$.

Proof Generally, $CR^{\perp}$ can correct all $t_1 = (p+1)/2 - 1$ errors. Obviously, the weight of any vector in the coset with the coset leader's weight $\le t_1$ is larger than $t_1 + 1$. Therefore error vectors of weight $t_1 + 1$, that cannot be corrected, are derived from $2tp$ codewords of weight $p+1$ when any $t_1 + 1$ errors appear on any of the $p+1$ bit. The total number of error vectors is $2tpC_{p+1}^{t_1+1}$. Thus the rest $C^{t_1+1}p^2 + 2pt - 2ptC_{p+1}^{t_1+1}$ can be corrected.

References

[1] Jin Fan, An Investigation on New Complex-Rotary Codes, A paper presented at IEEE 1985 International Symposium on Information Theory, Brigton, England, 1985 pp. 1–8.

[2] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[3] K. K. Tzeng, C. R. P. Hartmann, and Chien, Some Notes on iterative decoding, Proc. 9th Ann. Allerton Conf. Circuit and System Theory, Oct. 1971.

[4] C. R. P. Hartmann, *IEEE Trans. Inform. Theory*, **IT-18**(1972), 441–444.