Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 234–239*

On syndrome decoding of Chinese remainder codes

Wenhui Li wenhui.li@uni-ulm.de
Institute of Communications Engineering, University Ulm

Abstract. A unique decoder for the Chinese remainder codes was stated in [1] in 2000. In this paper, we present a decoder which gives the same error correction radius by introducing syndromes of the Chinese remainder codes. The error positions can be found using a so–called *error–locator* integer Λ which appears in the proposed key equation. To find Λ, this key equation can be solved by the extended Euclidean algorithm. The sent message can be obtained from the error free positions by the Chinese remainder theorem.

1 Introduction

The Chinese remainder code is an error correction code based on the Chinese remainder theorem. Each symbol of the codeword is defined to be the residue of some number over different congruences $(p_1, p_2, \ldots, p_n)$. Therefore, the Chinese remainder code is a polyalphabetic code, that is, every codeword's component belongs to its own alphabet. To decode such a code, there are two kinds of unique decoders which have been investigated by Mandelbaum ([2], [3]) and Goldreich et.al. [1]. Mandelbaum gave a decoding algorithm when the number of errors is within half the minimum distance provided p_i's do not differ much. In this paper, we present another decoder which reaches the same error correction radius $(n-k)\log p_1/(\log_{p_1} + \log p_n)$ as in [1]. The authors of [1] find directly the sent codeword under some conditions. A salutary lesson drawn from classical decoding Reed–Solomon codes is to separate decoding into two steps. The first step is to find the error locations, and the second is to figure out the error values. According to this experience, we can decode the Chinese remainder code in two steps as well. Therefore, in this paper, we first define the syndrome of the code and then use our syndrome–based decoder to find the error positions, and finally we correct errors.

The paper is organized as follows. In the first section, we recall the Chinese remainder theorem and give the definition of the Chinese remainder code. Some properties which will be used later are also pointed out. Then we introduce the syndrome in the second section, and a syndrome–based decoding algorithm follows. In Section 4, we come to the conclusion and look into the future work.

2 Chinese remainder code

In this section, we give the definition of the Chinese remainder code and introduce the error–locator Λ to analyze some properties of the Chinese remainder codes. Similar to Reed–Solomon codes, a transformation between domain of integer numbers and vectors over integers is proposed. Before defining the Chinese remainder code, we recall the Chinese remainder theorem (CRT).

Theorem 1 (Chinese Remainder Theorem)**.** *If $p_1, p_2, \ldots, p_\ell$ are positive integers which are relatively prime in a Euclidean domain $\mathbb{R}$, and $a_1, a_2, \ldots, a_\ell$ is any given integer sequence in the Euclidean domain, let $[X]_{p_i} \forall i$ denote the remainder when X is divided by p_i, then there exists an integer X solving the following system of simultaneous congruences*

$$[X]_{p_1} = a_1, [X]_{p_2} = a_2, \ldots, [X]_{p_\ell} = a_\ell.$$

Furthermore,

$$X = \sum_{i=1}^{\ell} a_i \cdot \frac{P}{p_i} \cdot \left[\left(\frac{P}{p_i} \right)^{-1} \right]_{p_i},$$

where $P = \prod_{j=1}^{\ell} p_i$. The integer X is unique when $X < P$.

The Chinese remainder theorem gives a construction of Chinese remainder codes.

Definition 1 (Chinese Remainder Code)**.** *Let $p_1 < p_2 < \cdots < p_n$ be relatively prime integers, and $k < n$ an integer. An integer message C smaller than $K = \prod_{i=1}^{k} p_i$ can be mapped to a codeword vector $\mathbf{c}$ of length n:*

$$C \mapsto \mathbf{c} = \{(c_i = [C]_{p_i}, i = 1, \ldots, n) : C \in \mathbb{N} \text{ and } C < K\}.$$

Obviously, the Chinese remainder code is a polyalphabetic code with cardinality K. It has length n, and the minimum Hamming distance is $d = n - k + 1$ since at most $k - 1$ coordinates of different codewords can be the same by the Chinese remainder theorem.

Consider integer $X < N = \prod_{i=1}^{n} p_i$ and vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, then by CRT there is a one-to-one mapping from a number X to a vector $\mathbf{x}$. We denote this mapping by $X \bullet\!\!-\!\!\circ\, \mathbf{x}$, and vice versa $\mathbf{x} \circ\!\!-\!\!\bullet\, X$. If a codeword $\mathbf{c}$ is transmitted over an additive noise channel, then at the receiver side we get a received word $\mathbf{r} = \mathbf{c} + \mathbf{e}$ where $\mathbf{e}$ is an error word. Here each coordinate r_i is abtained by $[c_i + e_i]_{p_i}$. The same relation holds between the message C and the received number R in the numerical domain, which is $R = C + E$. The integer numbers R and E can be calculated from the vector $\mathbf{r}$ and $\mathbf{e}$ respectively

according to the CRT, so $0 \leq R, E \leq N-1$.

Let

$$\Lambda := \prod_{j \in \mathcal{J}} p_j \tag{1}$$

where $\mathcal{J}$ is the set of error positions. We call Λ the *error–locator*. According to the definition of Λ (1), if we transform Λ into a vector λ, then the entries where errors occur are zero, i.e., $\lambda_i = 0$ for $c_i \neq r_i, \forall i = 1, \ldots, n$. Thus, we have the following lemma:

Lemma 1. *The product of the error–locator and the error value is a multiple of N, i.e.,*

$$\Lambda \cdot E \equiv 0 \mod N.$$

Proof. Let $\Gamma = \prod_{\substack{j=1 \\ j \notin \mathcal{J}}}^{n} p_j$. The error word $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ has zero entries at error free positions, that is $\Gamma | E$. Since $\Lambda \cdot \Gamma = N$, it is straightforward to obtain $N | (E \cdot \Lambda)$ which is stated by the lemma. □

Corollary 1 (Convolution Property)**.** *The product of two integer numbers modulo N corresponds to elementary multiplication of two vectors:*

$$\mathbf{a} \circ\!\!-\!\!\bullet\ A, \qquad \mathbf{b} \circ\!\!-\!\!\bullet\ B$$
$$c_i = a_i b_i \mod p_i, \quad \mathbf{c} \circ\!\!-\!\!\bullet\ C = AB \mod N.$$

Corollary 2. *The product of the error–locator and $[E]_K$ is a multiple of K:*

$$\Lambda \cdot [E]_K \equiv 0 \mod K. \tag{2}$$

Proof. The integer $[E]_K < K$ is the remainder of E modulo K, i.e., $[E]_K = E - mK$ where m is some integer factor. Therefore,

$$[E - mK]_{p_i} = [E]_{p_i} \tag{3}$$

for $i = 1, \ldots, k$. For $i = k+1, \ldots, n$, we can not guarantee that (3) holds. In the vector form, $\mathbf{e}$ and $\mathbf{e}_K (:= \circ\!\!-\!\!\bullet\ [E]_K)$ have the same error position(s) in the first k positions. Therefore, the vector form of $\Lambda \cdot [E]_K$ has all zero in the first k positions, and (2) holds by Corollary 1. □

One can compare Chinese remainder codes with Reed–Solomon codes in a perspektive of the transform between two domains or the convolution property. And for the Reed–Solomon codes, we define an error–locoter polynomial $\Lambda(x)$ which has roots at all error positions, whereas all the factors of the error-locator Λ for the Chinese remainder codes indicate error positions as well. For more details of the Reed–Solomon codes, we refer to [4].

3 Syndrome–based decoding

Equipped with the results mentioned in the previous section, we now define the syndrome of the Chinese remainder codes and later on the key equation to decode Chinese remainder codes.

3.1 Syndrome

We define the syndrome S of a received word $\mathbf{r} \multimap\!\bullet\ R$ as follows:

$$S = \frac{R - [R]_K}{K}. \tag{4}$$

Remark:

1. The syndrome of a codeword $\mathbf{c}$ is zero, because $(C - [C]_K)/K = 0$.
2. The syndrome is an integer and depends only on the error word E, and does not depend on the codeword C:

$$S = \frac{R - [R]_K}{K} = \begin{cases} \frac{C+E-[C]_K-[E]_K}{K} & \text{if } 0 \le [E]_K < K - C; \\ \frac{C+E-[C]_K-[E]_K+K}{K} & \text{otherwise.} \end{cases}$$

We denote it as $S = \frac{E-[E]_K+\delta_K(C,E)K}{K}$ where

$$\delta_K(C, E) = \begin{cases} 0 & \text{if } 0 \le [E]_K < K - C; \\ 1 & \text{otherwise.} \end{cases}$$

3.2 Decoding algorithm

The inspiration of the algorithm comes from decoding Reed–Solomon codes by the key equation [4]. The proposed decoder finds the error–locator Λ given parameters (N, K) of the code and the syndrome S. Up to $(n-k)\log p_1/(\log p_1 + \log p_n)$ errors can be always corrected. The decoding radius is the same as the one for the unique decoder in [1]. In contrast to [1] which finds the codeword directly, our decoder finds the number of errors and their positions.

The multiplication of Λ and the syndrome S can be written as

$$\Lambda \cdot S = \Lambda \left(\frac{E - [E]_K + \delta_K(C, E)K}{K} \right).$$

With Lemma 1 and Corollary 2, we obtain

$$\Lambda \cdot S = \frac{iN - jK + \delta_K(C, E)\Lambda K}{K} = i\frac{N}{K} - j + \delta_K(C, E)\Lambda. \tag{5}$$

where $i \triangleq \Lambda E/N$ and $j \triangleq \Lambda[E]_K/K$ are some integer factors. We know from (2) that $1 \leq j < \Lambda$. Let $\Omega = -j + \delta_K(C, E)\Lambda$, then there are two cases we have to consider:

1. $\Omega = -j < 0$. Since $\Omega + \Lambda = -j + \Lambda > 0$, we obtain $-\Lambda < \Omega < 0$.
2. $\Omega = -j + \Lambda > 0$. Furthermore, $\Omega - \Lambda = -j < 0$, hence, $0 < \Omega < \Lambda$.

In both cases, the absolute value of Ω should be smaller than Λ. Note that, if $\Omega = 0$, then the received word is error free.

Using $\Lambda R = \Lambda C + \Lambda E = \Lambda C \mod N$, one can find the decoding radius is $\Lambda < \sqrt{N/(K-1)}$ which corresponds to the number of correctable errors is at most $(n-k)\log p_1/(\log p_1 + \log p_n)$. For the proof, see [1].

Rewrite (5) as

$$\Lambda \cdot S \equiv \Omega \mod \frac{N}{K} \quad \text{with } |\Omega| < \Lambda < \sqrt{\frac{N}{K-1}}. \tag{6}$$

As a result, we have the *key equation* (6). Given S, N and K, one can solve the key equation and obtain Λ, using the following Algorithm 1.

Algorithm 1: Syndrome–Based Decoding Chinese Remainder Codes

Input: Syndrome S calculated by (4), N, K
Output: Error–locator Λ

1. Solve $\Lambda \cdot S \equiv \Omega \mod N/K$ by extended Euclidean algorithm iteratively to find the greatest common divisor of S and N/K, which is $\Lambda_i S + t_i(N/K) = \Omega_i$;
2. Stop when $\Lambda_i < |\Omega_i|$ and $\Lambda_{i+1} > |\Omega_{i+1}|$;
3. Output $\Lambda = \Lambda_i$ and by factorization we know the error positions and the number of errors.

The error–locator is needed to be factorized, so we still need to analyze the complexity for factorization and then for the whole algorithm. This can be done as the future work. When the set $\mathcal{J}$ of error positions was found, the message C can be obtained from the error free positions by the CRT.

4 Conclusion

To decode the Chinese remainder codes, we introduce the error–locator, the syndrome, and derive the key equation. We propose to solve the key equation by the extended Euclidean algorithm and as a result to find the error locator and hence positions of errors. The message C can be obtained from the error

free positions by the CRT.

This approach allows to decode interleaved Chinese remainder codes where a number of codewords of same length are corrupted by the errors at the same error locations. We can decode all the words collaboratively beyond half the minimum distance.

Acknowledgments

The author would thank Dr. Vladimir Sidorenko for his valuable comments and suggestions.

References

[1] O. Goldreich, D. Ron and M. Sudan, *Chinese Remaindering with Errors,* IEEE Transactions on Information Theory, Vol. 46, NO. 4, July 2000, 1330–1338.

[2] D. Mandelbaum, *On a class of arithmetic codes and a decoding algorithm,* IEEE Transactions on Information Theory, Vol. IT–22, Jan. 1976, 85–88.

[3] D. Mandelbaum, *Further results on decoding arithmetic residue codes (Corresp.),* IEEE Transactions on Information Theory, Vol. IT–24, Sept. 1978, 643–644.

[4] Blahut, Richard E. *Algebraic Codes for Data Transmission,* Cambridge University Press, 2002.