Extended Versions of Polynomial Remainder Codes and Chinese Remainder Codes

Cheng Chen, Sian-Jheng Lin *Member, IEEE* and Yunghsiang S. Han *Fellow, IEEE*

***Abstract*—A polynomial remainder code, derived from the Chinese remainder theorem, is a class of linear block codes, where the Reed-Solomon code is a special case. In this letter, an extended version of polynomial remainder codes is introduced, where the class of doubly-extended Reed-Solomon codes is a special case. Furthermore, the extended version of Chinese remainder codes is also presented. The erasure decoding methods for both codes are proposed. Finally, an application of the extended polynomial remainder codes is discussed.**

I. Introduction

Polynomial remainder codes, derived from the Chinese remainder theorem, were introduced by Stone [1], and Reed-Solomon (RS) codes are a special case of polynomial remainder codes. Nowadays, the properties of these codes have been extensively discussed. [1] considered the codes with fixed symbol sizes that the moduli have the same degree. Mandelbaum [2] pointed out that using the moduli with various degrees, the polynomial remainder codes are suitable for error correction. Yu and Loeliger [3], [4] discussed the property of distances of the codes, proposed the corresponding decoding rules for them, introduced the partial-inverse problem for polynomials, and developed its application to decoding polynomial remainder codes [5], [6]. Xiao and Xia [7]–[9] considered a robust reconstruction problem for polynomial remainder codes with non-pairwise coprime moduli.

In contrast, the Chinese remainder codes were constructed over an integral domain [10]. Guruswani et al. [10] proposed a new algorithm for solving the soft-decision decoding of the Chinese remainder codes. The robust reconstruction of Chinese remainder codes were considered in [11]–[13].

As aforementioned, the singly-extended RS code (including the RS code) is a special case of polynomial remainder codes; however, the doubly-extended RS code [14] is not. To handle this issue, this paper introduces a class of codes, called extended polynomial remainder codes, to include the doubly-extended RS code as a special case. Furthermore, the extended version of Chinese remainder codes is also presented. The contributions of this paper are summarized as follows.

- The extended version of polynomial remainder codes is introduced to include the doubly-extended RS code as a special case. An erasure decoding method for this proposed class of codes is proposed. The minimum Hamming distance of this class of codes is determined.
- An error correction decoding approach for the extended polynomial remainder codes is proposed based on the decoding method given in [3].
- The extended-version Chinese remainder code is introduced, and an erasure decoding method for them is proposed.

The rest of this paper is organized as follows. Section II introduces the polynomial remainder codes and Chinese remainder codes, as well as their decoding procedures. In Section III, we introduce the new symbol and propose the definition of extended polynomial remainder codes as well as the decoding method for them. Section IV discusses some related issues. Section V concludes this work.

This work was partially supported by CAS Pioneer Hundred Talents Program, the Fundamental Research Funds for the Central Universities (No. WK2100000004), and the National Natural Science Foundation of China (No. 61671007). Chen and Lin are with the School of Information Science and Technology, University of Science and Technology of China, Heifei, 230026, China. (E-mail: yuleilei@mail.ustc.edu.cn, sjlin@u-stc.edu.cn). Y. S. Han is with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, Dongguan, China.(E-mail: yunghsiangh@gmail.com) Corresponding author: Sian-Jheng Lin.

II. Preliminaries

Let $\mathbb{F}_q$ denote a finite field with q elements $\{\alpha_i\}_{i=0}^{q-1}$, and $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$. Furthermore, let $\mathbb{Z}$ and $\mathbb{Z}_m$ denote the integral domain and the ring of integers modulo m, respectively. Let $\mathrm{Rem}(f_0, f_1)$ denote the residual of dividing f_0 by f_1.

A. Polynomial remainder codes

This subsection gives the definition of the polynomial remainder codes from [4]. An erasure decoding based on the Chinese remainder theorem is also introduced.

Let $\{m_i(x)\}_{i=0}^{n-1} \subseteq \mathbb{F}_q[x]$ denote a set of monic polynomials such that any two polynomials in it are pairwise relatively prime. The degree of $m_i(x)$ is denoted as $w_i = \deg(m_i(x))$ for $i = 0, 1, \ldots, n-1$, and we assume that $w_0 \leq w_1 \leq \cdots \leq w_{n-1}$. Given a message polynomial

$$S(x) = s_0 + s_1 x + s_2 x^2 + \ldots + s_{K-1} x^{K-1} \tag{1}$$

in $\mathbb{F}_q[x]$ and $\deg(S(x)) < K$, a set of polynomials is defined as $\{W_i(x)\}_{i=0}^{n-1}$, where

$$W_i(x) \triangleq \mathrm{Rem}(S(x), m_i(x)). \tag{2}$$

Equivalently, $W_i(x) \equiv S(x) \pmod{m_i(x)}$, and each $\deg(W_i(x)) < w_i$. A polynomial remainder code is defined as

$$\begin{aligned} \mathrm{C} \triangleq \{(c_0, \cdots, c_{n-1}) : & c_i = W_i(x), i = 0, 1, \ldots, n-1, \\ & S(x) \in \mathbb{F}_q[x], \deg(S(x)) < K\}, \end{aligned} \tag{3}$$

where each symbol $W_i(x)$ is defined in (2) and $K = \sum_{i=0}^{k-1} w_i$.

First, we assume that the decoder receives the first k symbols, $\{W_i(x)\}_{i=0}^{k-1}$, in the transmitted codeword. In this case, the message polynomial $S(x)$ can be uniquely determined via Chinese remainder theorem [15]. Precisely, we have

$$S(x) \equiv W_i(x) \pmod{m_i(x)} \tag{4}$$

for $i = 0, 1, \ldots, k-1$. As $\gcd(m_i(x), m_j(x)) = 1$ for any $i \neq j$, Chinese remainder theorem shows that $S(x)$ can be uniquely determined. The interpolation formula is expressed as $S(x) = \sum_{j=0}^{k-1} L_j(x)\Lambda_j(x)$, where $\Lambda_j(x) = \prod_{\substack{0\le i\le k-1 \\ i\neq j}} m_i(x)$, and $L_j(x)$ is determined by

$$L_j(x)\Lambda_j(x) \equiv W_j(x) \pmod{m_j(x)}. \tag{5}$$

Note that (5) can be solved via extended Euclidean algorithms. It can be seen that the above argument can be applied to the case when the decoder receives any k symbols, $\{W_{\ell_i}(x)\}_{\ell_i=0}^{k-1}$, in the transmitted codeword.

B. Chinese remainder codes

The Chinese remainder code is similar to the polynomial remainder code, instead of that it is constructed in $\mathbb{Z}$. Let $\{m_i\}_{i=0}^{n-1} \subset \mathbb{Z}$ denote a set of positive integers such that any two integers in it are pairwise relatively prime, and $m_0 \le m_1 \le \cdots \le m_{n-1}$. The Chinese remainder code is defined as

$$\begin{aligned}\hat{\mathrm{C}} \triangleq \{(c_0, \cdots, c_{n-1}) : & c_i = \mathrm{Rem}(s, m_i), \\ & i = 0, 1, \ldots, n-1, s \in \mathbb{Z}_{M_k}\},\end{aligned} \tag{6}$$

where $M_k = \prod_{i=0}^{k-1} m_i$.

Next we consider the erasure decoding of the Chinese remainder codes. Assume that the decoder receives the first k symbols, $\{c_i\}_0^{k-1}$, in the transmitted codeword, and $c_i = s \pmod{m_i}$, for $i = 0, 1, \cdots, k-1$. As $M_k \le \prod_{i=0}^{k-1} m_i$, s can be reconstructed uniquely via Chinese remainder theorem [15]. Then the interpolation formula is given by

$$s = \sum_{j=0}^{k-1} l_j \Lambda_j \mod M_k,$$

where each

$$\Lambda_j = \prod_{\substack{0\le i\le k-1 \\ i\neq j}} m_i,$$

and each l_j is determined by

$$l_j\Lambda_j \equiv c_j \pmod{m_j}. \tag{7}$$

Note that (7) can be solved via extended Euclidean algorithm and the decoding method can also be applied to the case when the decoder receives any k symbols.

III. Extended versions of codes

This section presents the extended polynomial remainder codes and their erasure decoding and error correction decoding. Extended Chinese remainder codes are also proposed.

A. Code constructions

Given a positive integer $w_\infty < K = \sum_{i=0}^{k-1} w_i$ and

$$K \le w_\infty + \sum_{i=0}^{k-2} w_i. \tag{8}$$

The message polynomial is divided by x^{K-w_∞}, resulting in

$$S(x) = W_\infty(x) \cdot x^{K-w_\infty} + R_\infty(x), \tag{9}$$

where $\deg(R_\infty(x)) < K - w_\infty$.

An extended polynomial remainder code is defined as

$$\begin{aligned}\mathrm{C}' \triangleq \{(c_0, \cdots, c_{n-1}, c_\infty) : & c_i = W_i(x), i = 0, 1, \ldots, n-1, \\ & S(x) \in \mathbb{F}_q[x], \deg(S(x)) < K, c_\infty = W_\infty(x)\},\end{aligned} \tag{10}$$

where $W_i(x)$, for $i \le n-1$, is defined in (2), $W_\infty(x)$ is defined in (9). Clearly, the code length of C' is $n+1$ by appending an extra symbol $W_\infty(x)$ to C.

It has been proved in [4] that the minimum Hamming distance of the polynomial code defined in Subsection II-A is $n-k+1$. Next we give the minimum Hamming distance of the extended polynomial code defined in (10).

Theorem 1. *The extended polynomial code C′ defined in* (10) *has minimum Hamming distance $n-k+2$. Hence, the error correction capability of this code is $\lfloor \frac{n-k+1}{2} \rfloor$.*

Proof. Note that the original and the extended polynomial remainder codes are linear. Hence, finding the minimum Hamming distance of the extended polynomial remainder code is equivalent to finding the minimum Hamming weight for nonzero codewords. We prove that, for any nonzero codeword in the original code with minimum Hamming weight, the appended symbol is never zero by contradictions.

Assume that $(c_0, \cdots, c_{n-1})$ is a nonzero codeword in the original code with minimum Hamming weight. Then there are $k-1$ zero symbols in it since its Hamming weight is $n-k+1$. Let $c_{i_1}, c_{i_2}, \ldots, c_{i_{k-1}}$ are zeros. Hence, the information polynomial corresponding to this codeword is $S(x) = q(x)\prod_{j=i_1}^{i_{k-1}} m_j(x)$. The degree of $S(x)$ is then

$$\deg(S(x)) \ge \sum_{j=i_1}^{i_{k-1}} w_j \ge \sum_{j=0}^{k-2} w_j. \tag{11}$$

Now assume that the symbol c_∞ appended to this codeword is zero. That is, $W_\infty(x) = 0$ and $S(x) = R_\infty(x)$. Recall that $\deg(R_\infty(x)) < K - w_\infty$. Hence, by (8), we have

$$\deg(S(x)) = \deg(R_\infty(x)) < K - w_\infty \le \sum_{j=0}^{k-2} w_j$$

which contradicts to (11). This completes the proof. □

B. Erasure decoding

As the definition of $W_\infty(x)$ is distinct from others $\{W_i(x)\}_{i=0}^{n-1}$, it is necessary to show that $S(x)$ can also be uniquely determined by $W_\infty(x)$ and $k-1$ other symbols.

The decoding procedure is now presented below. Assume that the decoder receives k symbols $\{W_j(x)\}_{j=0}^{k-2} \cup \{W_\infty(x)\}$

defined in (2) and (9). With any decoding method based on Chinese remainder theorem given in Section II-A, a polynomial $\underline{S}(x)$ can be determined by the $k-1$ symbols $\{W_j(x)\}_{j=0}^{k-2}$, and

$$\deg(\underline{S}(x)) < \sum_{j=0}^{k-2} \deg(m_j(x)). \tag{12}$$

Let

$$\underline{\Lambda}(x) = \prod_{i=0}^{k-2} m_i(x).$$

The above result conducts

$$S(x) \equiv \underline{S}(x) \pmod{\underline{\Lambda}(x)}. \tag{13}$$

That is, we have

$$S(x) = \underline{S}(x) + q(x)\underline{\Lambda}(x) \tag{14}$$

for some $q(x)$. According to (9), (14) becomes

$$R_\infty(X) = \underline{S}(x) - W_\infty(x)x^{K-w_\infty} + q(x)\underline{\Lambda}(x). \tag{15}$$

By (9) and the assumption (8), we have

$$\deg(R_\infty(x)) < K - w_\infty \le \deg(\underline{\Lambda}(x)). \tag{16}$$

Dividing both sides of (15) by $\underline{\Lambda}(x)$ and keep the remainders, we have

$$R_\infty(X) = \text{Rem}(\underline{S}(x) - W_\infty(x)x^{K-w_\infty}, \underline{\Lambda}(x)).$$

From (9), $S(x)$ is determined by

$$\begin{aligned} S(x) =& W_\infty(x) \cdot x^{K-w_\infty} \\ &+ \text{Rem}(\underline{S}(x) - W_\infty(x)x^{K-w_\infty}, \underline{\Lambda}(x)). \end{aligned} \tag{17}$$

Thus, the message polynomial $S(x)$ can be uniquely determined by $\{W_j(x)\}_{j=0}^{k-2} \cup \{W_\infty(x)\}$.

The major complexity of the erasure decoding is to determine $\underline{S}(x)$ in (14), which is similar to that of the classical algorithm with the Chinese remainder theorem. One extra step is required when the extra symbol is among the received k symbol. This step is given in (17), where the major complexity is to determine $\text{Rem}(\underline{S}(x) - W_\infty(x)x^{K-w_\infty}, \underline{\Lambda}(x))$. This step involves finding the remainder when a division between two polynomials is performed. This complexity is much smaller compared with solving $k-1$ congruences by the Chinese remainder theorem to determine $\underline{S}(x)$.

It can be seen that the first $k-1$ received symbols can be any symbols in the transmitted codeword except the last symbol in it. Furthermore, if the received k symbols do not contain $W_\infty(x)$, the erasure decoding procedure is the same as given in Section II-A.

C. Error correction decoding

This subsection proposes the error correction decoding approach for extended polynomial remainder codes, which is based on the decoding method given in [3], the Yu and Loeliger's method.

By Section III-A, we know that an extended polynomial remainder code is constructed by adding a new symbol $W_\infty(x)$ to the original code. From the definition (10), the extra symbol is different from other symbols. Therefore, in error correction decoding, calculating the information polynomial might ignore the added symbol such that we can directly apply Yu and Loeliger's method. Based on the construction of the code, the general process of error correction decoding method is as follows: first, obtain $S(x)$ by using Yu and Loeliger's method; then, evaluate the correctness of the added symbol. Next we give the detailed process of error correction decoding.

Let C' be an extended polynomial remainder code. The decoder receives $y = c + e$, where $c \in \mathrm{C}'$ is the transmitted codeword and e is an error pattern. The code lengths of y and e are $n+1$. The received polynomial $Y(x)$ can be obtained by Chinese remainder theorem from symbols y_i where $0 \le i \le n-1$. Then by using Yu and Loeliger's method, $S(x)$ can be uniquely determined. Next $W_\infty(x)$ can be recalculated by $S(x)$ to verify whether there is an error in this position or not. Note that, similar to the doubly-extended RS codes, the error correction capability of the above decoding method is the same as the original codes unless one extra error occurs in the appended symbol in the last position of the transmitted codeword.

D. Extended Chinese remainder codes

This subsection gives the definition of extended Chinese remainder codes, and their erasure decoding method. Given a positive integer $K' \le M_k = \prod_{i=0}^{k-1} m_i$, an extended Chinese remainder code is constructed by appending a new symbol

$$c_\infty = \left\lfloor \frac{s}{K'} \right\rfloor \tag{18}$$

to the Chinese remainder code, where $\lfloor x \rfloor$ denotes the largest integer that is less than or equal to x. The extended Chinese remainder code is defined as

$$\begin{aligned} \hat{\mathrm{C}}' \triangleq \{&(c_0, \cdots, c_{n-1}, c_\infty) : c_i = \text{Rem}(s, m_i), \\ &i = 0, 1, \ldots, n-1, s \in \mathbb{Z}_{M_k}, c_\infty = \left\lfloor \frac{s}{K'} \right\rfloor\}, \end{aligned} \tag{19}$$

where

$$M_k \le K'c_\infty + \prod_{i=0}^{k-2} m_i. \tag{20}$$

Since the erasure decoding of the extended Chinese remainder codes is similar to the extended polynomial remainder codes given in Section III-B, the erasure decoding is briefly explained below.

Assume that the decoder receives k symbols $\{c_j\}_{j=0}^{k-2} \cup \{c_\infty\}$ in the transmitted codeword in (19). Let

$$\underline{\Lambda} = \prod_{i=0}^{k-2} m_i.$$

Then we have

$$s \equiv \underline{s} \mod \underline{\Lambda}, \tag{21}$$

where $\underline{s}$ can be determined by $k-1$ symbols $\{c_j\}_{j=0}^{k-2}$ with Chinese remainder theorem. From (20), we have

$$s - K'c_\infty < \underline{\Lambda}. \tag{22}$$

Finally we have

$$s = K'c_\infty + \text{Rem}(\underline{s} - K'c_\infty, \Lambda). \tag{23}$$

IV. Discussions

In this section, some issues for the proposed codes are discussed. First, we show that the extended RS codes are special cases of extended polynomial remainder codes. Then an application of polynomial remainder codes to the weighted secret sharing is given.

A. Comparisons with extended RS codes

In this subsection, we show that the doubly-extended RS codes [14] is a subclass of extended polynomial remainder codes. The singly-extended RS code, which includes RS code [16], is defined as

$$RS(q,K) \triangleq \{(S(\alpha_i))_{i=0}^{q-1} : S \in \mathbb{F}_q[x], \deg(S) < K\}. \quad (24)$$

Clearly, $RS(q,K)$ is a subclass of polynomial remainder codes by letting $n = q$ and

$$m_i(x) = x - \alpha_i, \qquad \forall i = 0, 1, \ldots, q-1. \quad (25)$$

The definition of doubly-extended RS codes is given as

$$ERS(q+1,K) \triangleq \{(S(\alpha_0), S(\alpha_1), \ldots, S(\alpha_{q-1}), S(\infty)) : S \in \mathbb{F}_q[x], \deg(S) < K\}, \quad (26)$$

where $S(\infty)$ denotes the coefficient of x^{K-1} in S. When $w_\infty = 1$, (9) gives

$$W_\infty(x) = s_{k-1} = S(\infty).$$

Thus, $ERS(q+1,K)$ is a subclass of extended polynomial remainder codes given in (10) by setting $n = q+1$, $w_\infty = 1$ and (25).

B. Application to weighted secret sharing

This subsection introduces the application of the extended polynomial remainder codes to the weighted secret sharing scheme. We briefly reviewed the concept of the weighted secret sharing scheme [17]. Let $\{w_i\}_{i=0}^{n-1}$ denote the weights of n shares, and let K denote a threshold. Given $\{w_i\}_{i=0}^{n-1}$ and K, the weighted secret sharing scheme produces n shares as

$$\{S_i = (W_i(x), i, w_i)\}_{i=0}^{n-1}\},$$

where $W_i(x)$ is a polynomial of degree less than w_i. Suppose one has k shares $\{S_{l_j}\}_{j=1}^{k}$. If $K \leq \sum_{j=0}^{k-1} w_{l_j}$, the secret can be recovered.

The extended polynomial remainder code can be applied to the weighted secret sharing schemes as follows. In the secret sharing scheme, the secret is stored in s_0 of $S(x)$ in (1), and other coefficients of $S(x)$ are filled with random numbers. In the polynomial remainder code, let

$$m_i(x) = (x - \alpha_i)^{w_i} \quad (27)$$

in (2), such that $\deg(W_i) < w_i$ and $S(x)$ is uniquely determined according to Section II-A. Notably, $m_0(x)$ is inapplicable in secret sharing, as the constant term of $\mathrm{Rem}(S(x), m_0(x))$ is the secret s_0. This implies that the weight secret sharing supports $q-1$ users with polynomial remainder codes, where q denotes the size of the finite field.

We can add an extra share $S_\infty = (W_\infty(x), \infty, w_\infty)$ in the weighed secret sharing scheme. Similarly, if $W_\infty(x)$ satisfies (8), the secret can be successfully recovered according to Section III-B. The advantage of extended polynomial codes is to increase the length of the original codes without increasing the size of the finite field. Thus, when $n = q-1$, we can design a weighted secrete sharing scheme with $n+1$ users without increasing the size of the finite field.

V. Conclusions

In this letter, the extended versions of polynomial remainder codes and Chinese remainder codes are proposed by appending one more symbol to these codes. The erasure decoding for both codes are proposed. We also show that the class of the doubly-extended RS codes is a special case of the extended polynomial remainder codes. In the future work, We will investigate the efficient decoding algorithm of extended polynomial remainder codes based on [5], [6].

References

[1] J. J. Stone, "Multiple-burst error correction with the Chinese remainder theorem," *Journal of the Society for Industrial and Applied Mathematics*, vol. 11, no. 1, pp. 74–81, 1963.
[2] D. Mandelbaum, "On efficient burst correcting residue polynomial codes," *Information and control*, vol. 16, no. 4, pp. 319–330, 1970.
[3] J. Yu and H. Loeliger, "On irreducible polynomial remainder codes," in *Proceedings of 2011 IEEE International Symposium on Information Theory*, July 2011, pp. 1190–1194.
[4] ——, "On polynomial remainder codes," *CoRR*, vol. abs/1201.1812, 2012. [Online]. Available: http://arxiv.org/abs/1201.1812
[5] J.-H. Yu and H.-A. Loeliger, "Partial inverses mod $m(x)$ and reverse Berlekamp-Massey decoding," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 6737–6756, 2016.
[6] J.-H. Yu, "A partial-inverse approach to decoding Reed-Solomon codes and polynomial remainder codes," Ph.D. dissertation, ETH Zurich, 2014.
[7] L. Xiao and X. Xia, "Error correction in polynomial remainder codes with non-pairwise coprime moduli and robust Chinese remainder theorem for polynomials," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 605–616, March 2015.
[8] ——, "Minimum degree-weighted distance decoding for polynomial residue codes with non-coprime moduli," *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 558–561, Aug 2017.
[9] ——, "Robust polynomial reconstruction via chinese remainder theorem in the presence of small degree residue errors," *IEEE Transactions on Circuits and Systems II: Express Briefs*, pp. 1–1, 2018.
[10] V. Guruswami, A. Sahai, and M. Sudan, ""Soft-decision" decoding of Chinese remainder codes," in *Proceedings 41st Annual Symposium on Foundations of Computer Science*, Nov 2000, pp. 159–168.
[11] L. Xiao and X. Xia, "Frequency determination from truly sub-Nyquist samplers based on robust Chinese remainder theorem," *Signal Processing*, vol. 150, pp. 248 – 258, 2018.
[12] L. Xiao, X. Xia, and H. Huo, "Towards robustness in residue number systems," *IEEE Transactions on Signal Processing*, vol. 65, no. 6, pp. 1497–1510, March 2017.
[13] L. Xiao, X. Xia, and W. Wang, "Multi-stage robust Chinese remainder theorem," *IEEE Transactions on Signal Processing*, vol. 62, no. 18, pp. 4772–4785, Sept 2014.
[14] J. K. Wolf, "Adding two information symbols to certain nonbinary BCH codes and some applications," *Bell Labs Technical Journal*, vol. 48, no. 7, pp. 2405–2424, 1969.
[15] H. Krishna, K. Y. Lin, and B. Krishna, "Rings, fields, the Chinese remainder theorem and an extension-part ii: applications to digital signal processing," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 41, no. 10, pp. 656–668, Oct 1994.
[16] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the society for industrial and applied mathematics*, vol. 8, no. 2, pp. 300–304, 1960.
[17] M. Wang, "Secret sharing among weighted participants," *Journal of Beijing Electrenic Science and Technology Institute*, vol. 20, no. 4, pp. 481–485, 2005.