On Syndrome Decoding of Chinese Remainder Codes

Wenhui Li

Institute of Communications Engineering, Ulm University

June 16, 2012

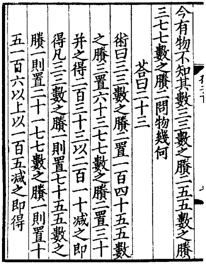
Thirteenth International Workshop on
Algebraic and Combinatorial Coding Theory (ACCT 2012)
Pomorie, Bulgaria

Outline

Outline

1. Chinese Remainder Codes
   - Chinese Remainder Theorem
   - Chinese Remainder Codes
2. Decoding Algorithms
   - Error–Locator
   - Syndrome
3. Conclusion and Future Work

Chinese Remainder Theorem


今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

圖二：《孫子算經》書影

$$[x]_3 = 2$$
$$[x]_5 = 3$$
$$[x]_7 = 2$$

$$\Rightarrow x?$$

Denote $x \equiv a_i \mod p_i$ by $[x]_{p_i} = a_i$.

Chinese Remainder Theorem (CRT)

Let $0 < p_1 < p_2 < \cdots < p_n$ be the set $\mathcal{P}$ of relatively prime integers. If $a_1, a_2, \ldots, a_n$ $(0 \leq a_i < p_i)$ is a sequence of integers, then there exists a positive integer x solving

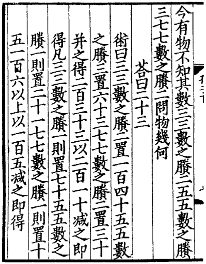
$$[x]_{p_1} = a_1, [x]_{p_2} = a_2, \ldots, [x]_{p_n} = a_n.$$

Furthermore,

$$x = \sum_{i=1}^{n} a_i \cdot \frac{N}{p_i} \cdot \left[\left(\frac{N}{p_i} \right)^{-1} \right]_{p_i}.$$

The integer x is unique when $x < N = \prod_{i=1}^{n} p_i$.

Chinese Remainder Theorem


今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

圖二：《孫子算經》書影

$$[x]_3 = 2$$
$$[x]_5 = 3$$
$$[x]_7 = 2$$

$$\Rightarrow x?$$

Denote $x \equiv a_i \mod p_i$ by $[x]_{p_i} = a_i$.

Chinese Remainder Theorem (CRT)

Let $0 < p_1 < p_2 < \cdots < p_n$ be the set $\mathcal{P}$ of relatively prime integers. If $a_1, a_2, \ldots, a_n$ $(0 \le a_i < p_i)$ is a sequence of integers, then there exists a positive integer x solving

$$[x]_{p_1} = a_1, [x]_{p_2} = a_2, \ldots, [x]_{p_n} = a_n.$$

Furthermore,

$$x = \sum_{i=1}^{n} a_i \cdot \frac{N}{p_i} \cdot \left[\left(\frac{N}{p_i} \right)^{-1} \right]_{p_i}.$$

The integer x is unique when $x < N = \prod_{i=1}^{n} p_i$.

Chinese Remainder Codes

Definition

Given $\mathcal{P}$ and integer $k < n$, a Chinese remainder code $\mathcal{CR}(\mathcal{P}; n, k)$ having cardinality $0 \leq K = \prod_{i=1}^{k} p_i \leq N$ and length n over alphabets $\mathcal{P}$ is defined as follows:

$$\mathcal{CR}(\mathcal{P}; n, k) = \{([C]_{p_1}, \ldots, [C]_{p_n}) : C \in \mathbb{N} \text{ and } C < K\} .$$

The Chinese remainder code ..

- .. is constructed by the Chinese remainder theorem.
- .. is exploited in theoretical computer science.
- .. is used for computation reduction.

Chinese Remainder Codes

Definition

Given $\mathcal{P}$ and integer $k < n$, a Chinese remainder code $\mathcal{CR}(\mathcal{P}; n, k)$ having cardinality $0 \leq K = \prod_{i=1}^{k} p_i \leq N$ and length n over alphabets $\mathcal{P}$ is defined as follows:

$$\mathcal{CR}(\mathcal{P}; n, k) = \{([C]_{p_1}, \ldots, [C]_{p_n}) : C \in \mathbb{N} \text{ and } C < K\}.$$

The Chinese remainder code ..

- .. is constructed by the Chinese remainder theorem.
- .. is exploited in theoretical computer science.
- .. is used for computation reduction.

Properties

Parameters

Length: n,

Hamming distance: $d = n - k + 1$.

Transform

Numerical domain: $C, E, R = C + E \in \mathbb{N}$, and $0 \leq E, R < N$

Vector form: $\mathbf{c}, \mathbf{e}, \mathbf{r}$, and $r_i = [c_i + e_i]_{p_i}$ for $i = 1, \ldots, n$

Convolution Property

The product of two integer numbers modulo N corresponds to elementwise multiplication of two vectors:

$$\mathbf{a} \circ\!\!-\!\!\bullet\; A, \qquad \mathbf{b} \circ\!\!-\!\!\bullet\; B$$

$$c_i = a_i b_i \mod p_i, \quad \mathbf{c} \circ\!\!-\!\!\bullet\; C = AB \mod N.$$

Outline

Toy Example

The word we receive:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

If r_i, r_j are erroneous:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

Consider the polyalphabetic set $\mathcal{P}$ for allocation.
Unique representation:

$$\Lambda = p_i p_j.$$

Toy Example

The word we receive:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

If r_i, r_j are erroneous:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

Consider the polyalphabetic set $\mathcal{P}$ for allocation.

Unique representation:

$$\Lambda = p_i p_j.$$

Toy Example

The word we receive:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

If r_i, r_j are erroneous:

$$\mathbf{r} = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$$

Consider the polyalphabetic set $\mathcal{P}$ for allocation.
Unique representation:

$$\Lambda = p_i p_j.$$

Error–Locator

Let $\mathcal{J}$ be the set of error positions $(c_j \neq r_j, \ \forall j \in \mathcal{J})$, the *error–locator* Λ is defined as follows

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

$$\begin{array}{c} \Lambda \bullet\!\!-\!\!\circ \ \lambda \\ E \bullet\!\!-\!\!\circ \ \mathbf{e} \end{array} \Rightarrow \begin{cases} \lambda_i = 0, e_i \neq 0 & \text{if } i \in \mathcal{J}, \\ \lambda_i \neq 0, e_i = 0 & \text{Otherwise.} \end{cases}$$

The product of the error–locator and the error value is a multiple of N:

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

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

$$\Lambda \cdot [E]_K \equiv 0 \mod K$$

The GRS Decoder

An error correction decoder was proposed by Goldreich, Ron and Sudan, given a parameter $D < \sqrt{N/(K-1)}$.

Algorithm 1: The GRS Decoder for Error Correction

Input: The set $\mathcal{P}$, the received word $(r_1, \ldots, r_n)$, N, K, D

Output: The message C

1. Using the CRT compute $0 \leq R < N$ such that $r_i = [R]_{p_i}$.
2. Find integers Λ, Ω such that

$$\begin{aligned} &1 \leq \Lambda \leq D, \\ &0 \leq \Omega < N/D, \\ &\Lambda R \equiv \Omega \mod N. \end{aligned}$$

3. Output Ω/Λ if it is an integer.

Properties

- The GRS decoder gives the transmitted message C directly.
- The logarithm of the integer parameter D is the error correcting radius in the weighted metric.

Decoding Radius

If $D = \sqrt{\frac{N}{K}}$,

$$t \leq \left\lfloor (n-k)\frac{\log p_{k+1}}{\log p_{k+1} + \log p_n} \right\rfloor,$$

or less precisely,

$$t \leq \left\lfloor (n-k)\frac{\log p_1}{\log p_1 + \log p_n} \right\rfloor.$$

Syndrome

Similar to decoding Reed–Solomon codes, we decode the Chinese remainder codes in two steps.

- Find the error positions,
- Estimate the error values.

Syndrome

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

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

The syndrome can be also written as

$$S = \frac{E - [E]_K + \delta_K(C, E)K}{K}$$

where

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

Syndrome

Similar to decoding Reed–Solomon codes, we decode the Chinese remainder codes in two steps.

- Find the error positions,(difficult)
- Estimate the error values.(easy)

Syndrome

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

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

The syndrome can be also written as

$$S = \frac{E - [E]_K + \delta_K(C, E)K}{K}$$

where

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

Syndrome

Similar to decoding Reed–Solomon codes, we decode the Chinese remainder codes in two steps.

- Find the error positions,(difficult)
- Estimate the error values.(easy)

Syndrome

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

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

The syndrome can be also written as

$$S = \frac{E - [E]_K + \delta_K(C, E)K}{K}$$

where

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

Key Equation

The Syndrome ..

- .. of a codeword $\mathbf{c}$ is zero.
- .. depends only on the error word.
- .. reduces computation.

The *key equation* is defined as follows:

Key Equation

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

Given S, N and K, one can solve the key equation and obtain Λ.

Decoding Algorithm

Algorithm 2: The Syndrome–based Decoder for Error Correction

Input: The set $\mathcal{P}$, the received word $(r_1, \ldots, r_n)$, N, K

Output: The message C

1. Using the CRT compute $0 \leq R < N$ from $\mathbf{r}$, then compute S.
2. Find integers Λ such that

$$|\Omega| < \Lambda < \sqrt{\tfrac{N}{K-1}},$$
$$\Lambda S \equiv \Omega \mod \tfrac{N}{K}.$$

3. Factorize Λ to obtain error positions.
4. Reconstruct the massage C from non–error positions by CRT.

Decoding Radius

The key equation and the condition is equivalent to

$$\Lambda R = \Lambda C \mod N$$

(from Algorithm 1).

$\Rightarrow$ Same error correcting radius

The number of correctable errors t is at most

Decoding Radius

$$t \leq (n-k)\frac{\log p_1}{\log p_1 + \log p_n}.$$

Syndrome–based Decoding

We can solve the key equation by extended Euclidean algorithm.

Algorithm 3: On Syndrome Decoding by Extended Euclidean Algorithm

Input: Syndrome S calculated by, 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 Λ we know the error positions and the number of errors.

Outline

Conclusion and Future Work

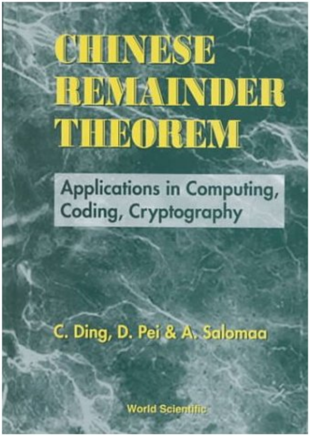
Conclusion

- The error–locator and the syndrome for the Chinese remainder codes are introduced.
- A key equation is derived.
- An algorithm for solving the key equation is proposed.

Future work

- Analysis of complexity of the decoding algorithm.
- Extension to interleaved Chinese remainder codes, which allows collaboratively decoding beyond half the minimum distance.

Thank you!


CHINESE
REMAINDER
THEOREM
Applications in Computing,
Coding, Cryptography
C. Ding, D. Pei & A. Salomaa
World Scientific