A concatenated binary locally repairable codes with locality 2 using puncturing

Zhi Jing, Gangsan Kim, and Hong-Yeop Song

Yonsei University

2019

IWSDA

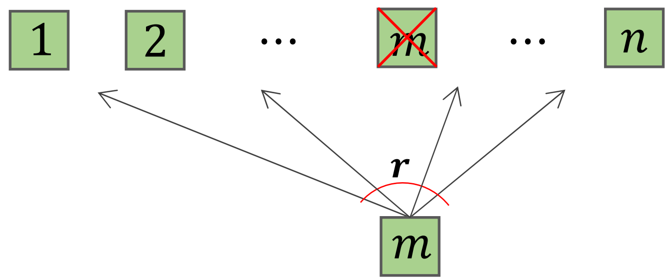
Contents

Locally Repairable Code (LRC)

- $[n, k, r]$ LRC is:

  $[n, k]$ linear block code with ***locality r***

- **Symbol locality:**
  the smallest number of symbols needed to repair the failed symbol.



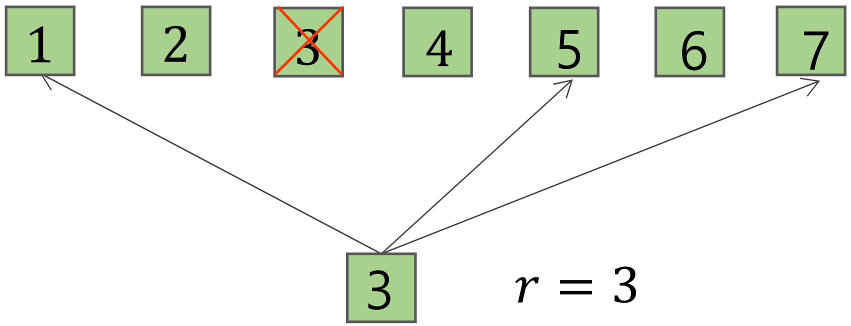
- **Code with locality r:**
  each symbol has the locality at most r.

Locally Repairable Code (LRC)

It's easy to get the locality from the parity check matrix $\boldsymbol{H}$.

[7,4] Hamming code:

$$H \cdot \boldsymbol{c} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{pmatrix} = 0$$



$r = 3$

Concatenated LRC

- Concatenated $[n, k]$ code:

H: the parity check matrix of the concatenated code
H_{in}: the parity check matrix of the inner code

We have known

$$H \cdot \boldsymbol{c} = 0.$$

Because of the concatenated structure,

$$H_{in} \cdot \boldsymbol{c} = 0.$$

Concatenated LRC

From the paper "*New constructions of binary and ternary locally repairable codes using cyclic code*" by C. Kim, the concatenated BLRC with locality 2 is proposed as following:

Outer code: shortened *expurgated Hamming code*.

- $[2^m-1, 2^m-m-2]$ expurgated Hamming code with generator polynomial $g(x)=(x+1)g_1(x)$, where $\frac{2n}{3} \le 2^m-1$ and g_1 is the primitive polynomial of order m over F_2.
- shortening the first $(2^m-1-\frac{2n}{3})$ information bits of the above expurgated Hamming code.

Inner code: *binary* $[n, \frac{2n}{3}]$ *cyclic code* with parity check polynomial $h_{in}(x)=x^{\frac{2n}{3}}+x^{\frac{n}{3}}+1$.

Concatenated LRC

From the paper "*New constructions of binary and ternary locally repairable codes using cyclic code*" by C. Kim, the concatenated BLRC with locality 2 is proposed as following:

Inner code: a binary $[n, \frac{2n}{3}]$ cyclic code with parity check polynomial $h_{in}(x) = x^{\frac{2n}{3}} + x^{\frac{n}{3}} + 1$.

$$H_{in} = \left[\underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{\frac{n}{3}} \;\middle|\; \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} \;\middle|\; \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} \right]$$

Motivation

Shortening: decrease the length and dimension simultaneously.

Puncturing: decrease the length and keep the same dimension.

For the given length and locality, the system want the larger dimension.

Shortening → Puncturing

Cyclic code

Let u be an odd integer ≥ 3;

v be any positive integer;

β be a primitive u^{th} root of unity in some extension field of F_2.

$$uv = (\frac{2n}{3} + 1) \text{ or } \frac{2n}{3}$$
$$\gcd(u, v) = 1$$

C_{cyc} be a binary $[n_{cyc}, k]$ cyclic code with the generator polynomial

$$g(x) = (x^v + 1)g_1(x),$$

where $g_1(x)$ is the minimal polynomial of β over F_2.

$n_{cyc} = uv$;

$k = vu - v - \deg[g_1(x)]$.

Proposed concatenated LRC

Let $n \geq 9$ and $3|n$;

C_{cyc} be a binary $[n_{cyc}, k]$ cyclic code, where $n_{cyc} = (\frac{2n}{3} + 1)$ or $\frac{2n}{3}$.

Outer code:

1) $n_{cyc} = (\frac{2n}{3} + 1)$: **puncturing** any one bit of C_{cyc};

2) $n_{cyc} = \frac{2n}{3}$: C_{cyc}.

Inner code (the same inner code by Kim):

a systematic binary $[n, \frac{2n}{3}]$ cyclic code with parity check polynomial $h_{in}(x) = x^{\frac{2n}{3}} + x^{\frac{n}{3}} + 1$.

Then, a binary $[n, k, r = 2]$ can be constructed.

Comparison

Construction by Kim

Outer code:

shortening the first $(2^m - 1 - \frac{2n}{3})$ information bits of the expurgated Hamming code.

Inner code:

a systematic binary $[n, \frac{2n}{3}]$ cyclic code with parity check polynomial $h_{in}(x) = x^{\frac{2n}{3}} + x^{\frac{n}{3}} + 1$.

Proposed Construction

Outer code:

1) $n_{cyc} = (\frac{2n}{3} + 1)$:

puncturing any one bit of C_{cyc};

2) $n_{cyc} = \frac{2n}{3}$: C_{cyc}.

Inner code:

a systematic binary $[n, \frac{2n}{3}]$ cyclic code with parity check polynomial $h_{in}(x) = x^{\frac{2n}{3}} + x^{\frac{n}{3}} + 1$.

Proposition

Let $[n, k_1]$ C_1 be constructed by proposed construction;

Let $[n, k_2]$ C_2 is constructed by [1].

If $n = 3(2^{t-1} - 1)$, where t is a positive integer.

Then $\boldsymbol{k_1 = k_2 + 1}$.

[1]. C. Kim and J.-S. No, "New constructions of binary and ternary locally repairable codes using cyclic code," IEEE Communications Letter, vol. 22, no. 2, pp. 228–231, Feb. 2018.

Proposition

Proof: Let $v = 1$ and $u = 2^t - 1$.

For C_1, $n_{cyc} = uv = 2^t - 1 \Longrightarrow n = \frac{3}{2}\left(n_{cyc} - 1\right) = 3(2^{t-1} - 1)$

So, $k_1 = vu - v - \deg[g_1(x)] = u - 1 - t = 2^t - 2 - t$

$g_1(x)$ is the minimal polynomial of β over F_2, and β be a primitive u^{th} root of unity in some extension field of F_2.

$\because u = 2^t - 1$

$\therefore \deg[g_1(x)] = t$

Proposition

Proof:

For C_2, $k_2 = \frac{2n}{3} - \left\lceil \log_2\left(\frac{2n}{3} + 1\right)\right\rceil - 1$

$$= (2^t - 2) - \lceil \log_2(2^t - 2 + 1)\rceil - 1$$

$$= 2^t - 2 - t - 1$$

$$= 2^{\mathrm{t}} - 3 - \mathrm{t} = \mathrm{k}_1 - 1$$

Proposition

Proposed construction	(9,3)	(21,10)	(30,15)	(45,25)	……
Construction in [1]	(9,2)	(21,9)	(30,14)	(45,24)	……

[1]. C. Kim and J.-S. No, "New constructions of binary and ternary locally repairable codes using cyclic code," IEEE Communications Letter, vol. 22, no. 2, pp. 228–231, Feb. 2018.

Conclusion

In this paper,

- propose a construction for LRC using the punctured code
- increase the dimension at some length of n.

In the future, …

We will

- try to find other outer code, which can provide better k and n based on the concatenated structure.
- use concatenated structure to construct the LRC with other properties, such as, joint locality, availability.