Monday, October 17, 2022 10:24 AM

* Summary: Polynomial-based construction

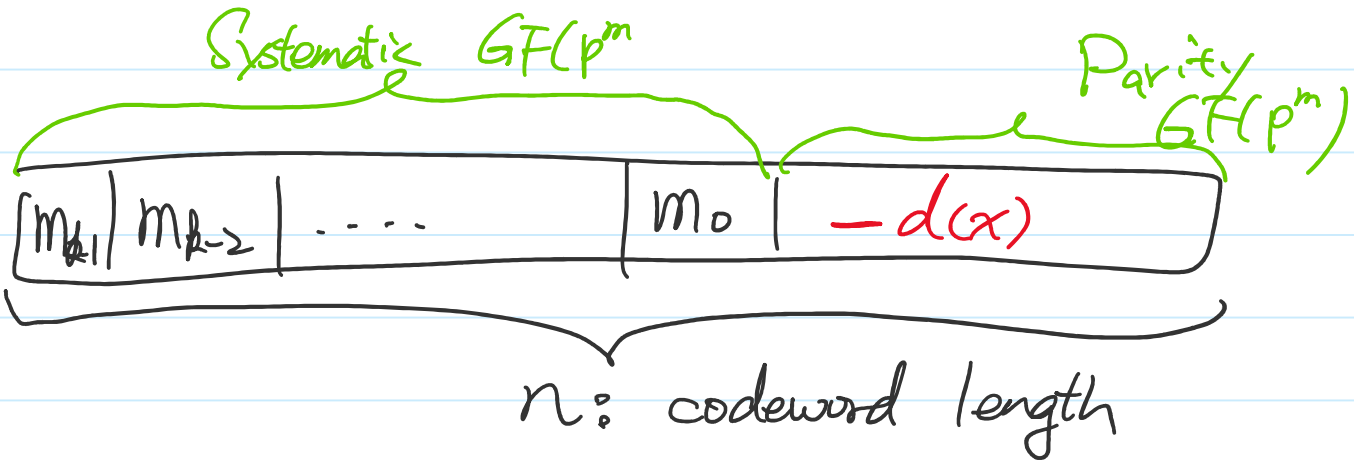
$$c(x) = m(x) \cdot g(x)$$

Encoding #1: By multiplication

Encoding #2: By long-division

$g(x)$ ⟌ $m_{k-1}, \cdots, m_0, 0, 0, 0, 0$

) $d(x)$



* If $g(x)$ happens to divide $x^n - 1$

* If $g(x)$ happens to divide $x^n - 1$

$\Rightarrow$ We have several new properties

① The linear code is cyclic.

② The parity polynomial is $g(x) \cdot h(x) = x^n - 1$

③ The dual code $C^{\perp}$ is cyclic.

---

* Cyclic Redundancy Codes

* Error Detection Only

* Almost always use division-based systematic encoding

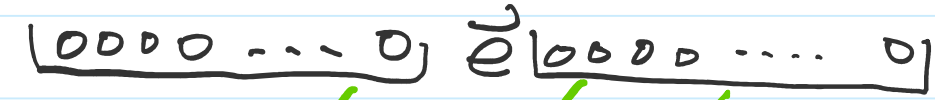
* No constraint on the length of $m(x)$. That is $\deg(g(x)) = r$ is fixed. But $\deg(m(x))$ can be arbitrary

$\Rightarrow n = \deg(m(x)) + r$ can be arbitrary.

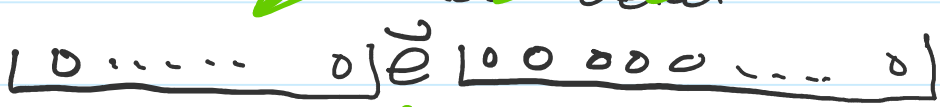
* Technically NOT a cyclic code.

I.e. The "detection capability" is always linear-shift-invariant but not necessarily cyclic-shift-invariant.

That is, if it can detect



then it can also detect



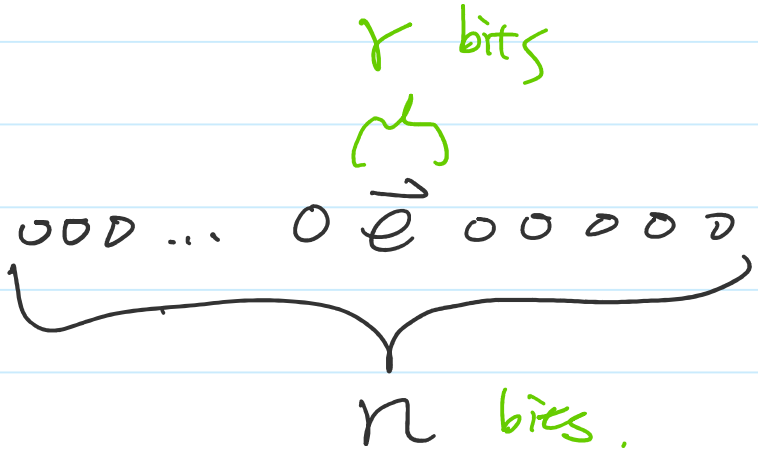
But may not detect cyclically shifted version

where $\vec{e} = \vec{e}_L \vec{e}_R$

Corollary: If $\deg(g(x)) = r$, then the corresponding CRC ... "burst error"

CRC can detect any "burst error" pattern of length $\leq r$.

i.e. can deted any $\text{dim}(\vec{e}) \leq r$ that are embedded in a zero vector



* Common CRC:

CRC-16: $g(x) = x^{16} + x^{15} + x^2 + 1$ (USB)

being cyclic if $n = 2^{15} - 1$ bits

CRC-16 Dect: $x^{16} + x^{10} + x^8 + x^7 + x^3 + 1$

being cyclic if $n = 254 = 2^8 - 2$ bits.

CRC-32 (ethernet) $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11}$

CRC-32 (ethernet)

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

being cyclic if $n = 2^{32} - 1$ bits.

this $g(x)$ is primitive