L11.2

Tuesday, August 9, 2022 9:46 AM

* What is an error correcting code?

* We deliberately limit the legitimate codewords from $\{0,1\}^n$ to $\{0,1\}^k$.

  when $k = n \cdot R < n$

* One way is to consider the "vector subspace"

  E.g. $\vec{y} = A\vec{m}$ $\underline{A: n \times k \text{ matrix}}$

* The second way is as follows.

* Consider all elements $\alpha \in GF(p^n)$

  Totally how many elements? Ans: p^n

  - Each element roughly represent

- Each element ... represent an n-dim vector with each coordinate in $GF(p)$

- Each element can also be represented as a degree $\leq n-1$ polynomial in $f(x) \in F_p[x]$ and $\deg(f(x)) \leq n-1$

* A codebook is a subset of $f(x)$ such that $f(x) = m(x)g(x)$ for some generator polynomial $g(x)$ s.t. $\deg(g(x)) \leq n-k$

($m(x)$ is the message polynomial.)

$\deg(m(x)) \leq k-1$

For any finite set of polynomials $\{f_1(x), \ldots, f_n(x)\}$.

Let $d(x)$ denote the g.c.d. of

Let $d(x)$ denote the g.c.d. of all $f_i(x)$

Then we can always write

$$d(x) = \lambda_1(x) f_1(x) + \lambda_2(x) f_2(x) + \cdots + \lambda_n(x) f_n(x)$$

for some polynomials $\lambda_1(x), \cdots, \lambda_n(x)$

proof: omitted by reversing the long-division method.