Recall RS codes last week. 4/25

Today: Introduce some hard problems in code-based cryptography

$C \subseteq \mathbb{F}_q^n$ code.

$\text{basis}(C) = \{v_1, v_2, \dots, v_k\}$

(1) $$G = \underbrace{\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}}_{n} \Big\} k$$

"Generator matrix"

$$C = \{ mG : m \in \mathbb{F}_q^k \}$$

(2) $$H = \underbrace{\begin{bmatrix} & & \\ & & \end{bmatrix}}_{n} \Big\} n-k$$

nullspace of G, i.e., $GH^T = 0$
"parity check matrix"

$$C = \{ y \in \mathbb{F}_q^n : Hy^T = 0 \}$$

Def ~~**Rmk**~~ Hy^T is called the syndrome.

$Hy^T = 0 \Rightarrow y =$ codeword
$Hy^T \neq 0 \Rightarrow ?$

Rmk $$G \xrightarrow[\text{elim}]{\text{Gaussian}} [I_k \mid A] = \underset{GL_k(\mathbb{F}_q)}{S}\, G\, \underset{\text{permutation}}{P}$$

$$\Rightarrow H = [-A^T \mid I_{n-k}]$$

Two equivalent problems

(1) (Naive codeword decoding)
Given generator matrix $G \in \mathbb{F}_q^{k \times n}$, $t \in \{0, 1, \ldots, n\}$
$y \in \mathbb{F}_q^n$ s.t. $y = c + e$ for some $c \in C$, $|e| = t$.
Find e.

(2) (Syndrome decoding)
Given parity check $H \in \mathbb{F}_q^{n-k \times n}$, $t \in \{0, 1, \ldots, n\}$
$s \in \mathbb{F}_q^{n-k}$ s.t. $He^T = s^T$ with $|e| = t$,
Find e.

Rmk (1) $\Leftrightarrow$ (2)

"$\Rightarrow$" H, s given.

- $\Rightarrow$ can find G (as $H =$ nullspace of G, Gaussian)
- $\exists$ solution y : $Hy^T = s^T$. (lin. alg.)
- Now $H(y-e)^T = 0$
  $\Rightarrow y - e = c \in C$.
  $\Rightarrow y = c + e$ $\overset{(1)}{\Longrightarrow}$ e found.

"$\Leftarrow$" G, y given

- $\Rightarrow$ can find H
- $Hy^T = Hc^T + He^T = He^T$ $\overset{(2)}{\Longrightarrow}$ e found.

McEliece cryptosystem / Niederreiter cryptosystem

Let $C = [n,k]$ code capable of correcting t errors & efficient decoding algorithm.

~~generator matrix~~

(decode $\leftrightarrow$ Patterson algorithm)

e.g. Goppa codes: $g \in \mathbb{F}_q[x]$, $\deg g = t$

$L_1, \dots, L_n \in \mathbb{F}_q$

$$\rightsquigarrow H = \begin{array}{c} 1 \\ x \\ \vdots \\ x^{t-1} \end{array} \begin{array}{c} \begin{array}{ccc} L_1 \; L_2 & \cdots & L_n \end{array} \\ \begin{bmatrix} 1 & \cdots & 1 \\ L_1 & \cdots & L_n \\ \vdots & & \vdots \\ L_1^{t-1} & \cdots & L_n^{t-1} \end{bmatrix} \end{array} \cdot \begin{bmatrix} \frac{1}{g(L_1)} & & \\ & \ddots & \\ & & \frac{1}{g(L_n)} \end{bmatrix}$$

$\rightsquigarrow G$ generator matrix $k \times n$ of C

say of systematic form, $G = [I_k \; A]$

$\hat{G} = SGP$ $\quad S \in GL_k(\mathbb{F}_q)$

P permutation matrix

public $(\hat{G}, t)$

private (S, G, P)

<u>encrypt:</u>
- write m as string of blocks of length k
- $c' = m\hat{G}$
- generate $|z| = t$ "error"
- $c = c' + z$

decrypt : · P^{-1} known

· $\hat{c} = cP^{-1} = (c' + z)P^{-1} = (m\hat{G} + z)P^{-1}$

$= (mSGP + z)P^{-1}$

$= mSG + zP^{-1}$

· decode $\hat{c}$ to get $\hat{m} = mS \iff m = \hat{m}S^{-1}$