Decoding linear codes

H: parity check mtx (e.g. $H = \begin{pmatrix} 1&1&0&1&0 \\ 1&0&1&0&1 \end{pmatrix}$ $\}n-k$, n columns)

Recall: $x \in C \iff x H^T = 0$

Def. $s(x) = x H^T$ is called the syndrome of x. $s(x) \in GF(q)^{n-k}$

Ex. $x = (11011)$, $s(x) = (1,0)$

Prop. $s(x) = s(y) \iff x - y \in C \iff x, y \in u + C$ (for some u)

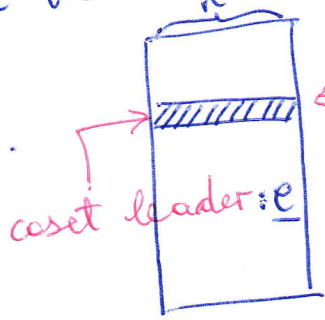
$u + C = \{u + c : c \in C\}$

Pf. $x H^T = y H^T \iff (x-y) H^T = 0$

Def. coset leader: smallest wt vector in $u+C$

Decoding with syndromes:

Build an array of size $q^{n-k} \times n$.



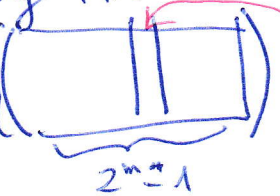
c was sent, x received

1) Compute $s(x)$
2) Look up the corresponding e ($e = e_s$) from array
3) $c = x - e$

Prop. If $w(e) \le t$ and C is t-error corr., then e is a coset leader

Pf. Can there be an e' with wt $< w(e)$ in the same coset?
Then $e - e' \in C$ with $w(e - e') \le 2t$ $\Rightarrow d \ge 2t+1$.

Binary HAMMING codes

$H = m \{$  $2^m - 1$

i-th column: binary expansion of "i"

$s(x) = ?$ $x = c + e$ $w(e) \le 1$

$GF(2^m)$ $s(x) = 0 \Rightarrow x \in Ham(m)$

$s(x) =$ "i-th column" $\Rightarrow e = (0, \dots 0, \underset{i}{1}, 0 \dots 0)$.

Def. $x \preccurlyeq y \overset{def}{\iff} \forall i \; [x_i = y_i \text{ or } x_i = 0]$

Thm. If y is a coset leader and $x \preccurlyeq y$ then x is also a coset leader.

Remark. NP complete: given H (an $m \times n$ mtx), $s \in GF(q)^m$, $w_0 > 0$
Is there vector $v \in GF(q)^n$, $w(v) \le w_0$, so that $v H^T = s$?
(BERLEKAMP, MCELIECE, VAN TILBORG)