

① Revisit the matrix identity in the context of codes

$$\begin{aligned}\langle(I_k|A)\rangle &= \\ \langle(E^T|I_{m-k})\rangle^+ &\end{aligned}$$

Regarding the upper matrix as a systematic encoder for an  $(n, k)$  code with the lower as the check matrix,

the identity tells us that the check values are positioned opposite the weight-one columns (of  $H$ ).

Example:  $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$  has rank 3

$C = \langle H \rangle^\perp$  is  
a  $(7, 4, 3)$  code

$$\underbrace{a_1 \ a_2 \ a_3 \ a_4}_{4 \text{ data bits}} \mapsto \begin{cases} a_1 + a_2 + a_4, a_1 + a_3 + a_4, a_1, \\ a_2 + a_3 + a_4, a_2, a_3, a_4 \end{cases}$$

$(1001) \mapsto (0011001) = \vec{c}$ . If  $\vec{r} = (0001001)$ , then  $H\vec{r}^T = (011)$ , which is taken as binary index of error

with this formula for encoding  $H\vec{r}^T = \begin{cases} (000), \text{ if } r \in \langle H \rangle^\perp = C \\ \text{binary index of error, if } \text{wt}(e) = 1. \end{cases}$

② Variation on Hamming Code (see "shortened codes")

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \text{ has rank 4} \Rightarrow \langle H \rangle^\perp \text{ is a } (10, 6, 3) \text{ code}$$

$$\underbrace{a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a_6}_{\text{data bits}}$$

Derive a systematic encoder directly from  $H$

As before  $H\vec{r}^T = \begin{cases} (00000), \text{ if } r \in \langle H \rangle^\perp \\ \text{binary index of error, if } \text{wt}(e) = 1 \end{cases}$

This  $(10, 6, 3)$  code is not a perfect code.

If  $H\vec{r}^T$  does not match any column of  $H$ , then  $\text{wt}(e) > 1$ .

Example:  $H\vec{r}^T = (1101)$  must involve two or more errors.

$$\left. \begin{array}{l} (00000001001) \\ (0001000010) \\ (0000100100) \end{array} \right\} \text{Equally-likely weight-two errors with } H\vec{e}^T = (1101)$$

Often, one declares "Decoding Farther" in such situations

③  $n-k$  "small"  $\rightarrow$  build a syndrome table, size  $|F|^{n-k}$   
 (make decoding almost as simple as Hamming codes)

Suppose we have a check matrix  $H$  for  $(n, k, d)$   
 linear code. Set  $\lfloor \frac{d-1}{2} \rfloor = t$  (correction capacity)

Principle: If  $t \geq \begin{cases} \text{wt}(\vec{v}) \\ \text{wt}(\vec{u}) \end{cases}$ , then  $H\vec{v}^T \neq H\vec{u}^T$

This means we can construct a syndrome  $\leftrightarrow$  error table by pairing each  $\vec{v}$  of weight  $\leq t$  with its syndrome  $H\vec{v}^T$ . In effect, this assumes an all-0 codeword. [Reprove Hamming bound]

If  $d$  is unknown, build the table using one weight "class" at a time. When a "collision" occurs, the correction capacity is exceeded.

④ Technical property of syndrome table / systematic codes

Suppose  $G = (I_k | A)$

$H = (-A^T | I_{n-k})$  associated with  $(n, k, d)$  code

Set  $t = \lfloor \frac{d-1}{2} \rfloor$ , and assume  $\vec{r} = \vec{c} + \vec{e}$ , with  $\text{wt}(\vec{e}) \leq t$

then data values in  $\vec{r}$  are correct iff  $\text{wt}(H\vec{r}^T) \leq t$

Sketch of Proof: Observe for  $\vec{e} = (00\dots 0 e_{k+1} e_{k+2} \dots e_n)$

we have  $H\vec{e}^T = (e_{k+1} e_{k+2} \dots e_n)$

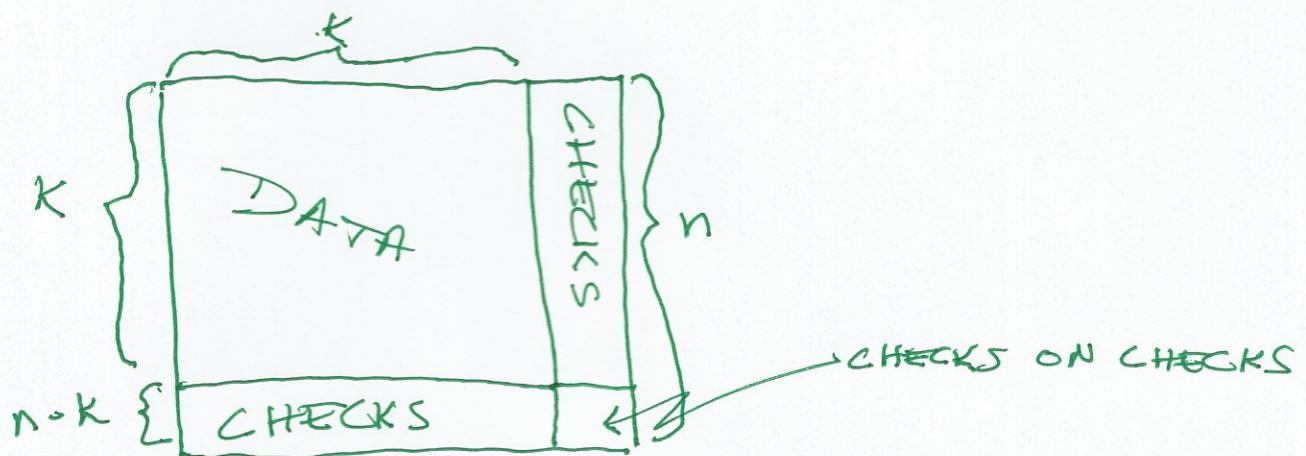
(Binary) # syndromes of weight  $\leq t$ :  $\sum_{i=0}^t \binom{n-k}{i}$

#  $\vec{e} = (00\dots 0 e_{k+1} \dots e_n)$  of weight  $\leq t$ :  $\sum_{i=0}^t \binom{n-k}{i}$

The claim follows.

⑤ Start with an  $(n, k, d)$  code,  $G$ , that allows simple decoding. A Z-D Product Code creates an  $(n^2, k^2, d^2)$  which can be decoded by iterated application of the  $(n, k, d)$  decoder.

Expand a  $K \times K$  array of data values by encoding "across" and "down" to create a  $n \times n$  array / codeword



transmit one row at a time, and store in a  $n \times n$  buffer.

For cases of practical interest  $G$  is not perfect

ONE ITERATION { Decode columns, skipping "Decoding failures"  
Decode rows, skipping "Decoding failures"

the number of iterations required is determined empirically

often the minimum distance  $d^2$  significantly underestimates number of correctable errors.