

message

                      
v

=

codeword

                      
vC

C = generator matrix for linear (over  $GF(2)$ )  
error-correcting code.

Every vector in RowSpace(C) has weight  
(i.e. # 1's) at least  $k+1$ .

Enables error detection up to  $k$  errors.

correction up to  $\lfloor \frac{k}{2} \rfloor$  errors.

$$\boxed{M} = \boxed{0}$$

$M =$  parity check matrix for  $C$

$$wM = 0 \iff w \in \text{Rowspace}(C) \iff w \text{ is a codeword}$$

$$\left. \begin{array}{l} \text{Every vector in} \\ \text{Rowspace}(C) \text{ has} \\ \text{weight} \geq k+1 \end{array} \right\} \iff \left\{ \begin{array}{l} \text{Every } k \text{ rows of } M \\ \text{are linearly independent} \end{array} \right.$$

# Linear and Statistical Independence

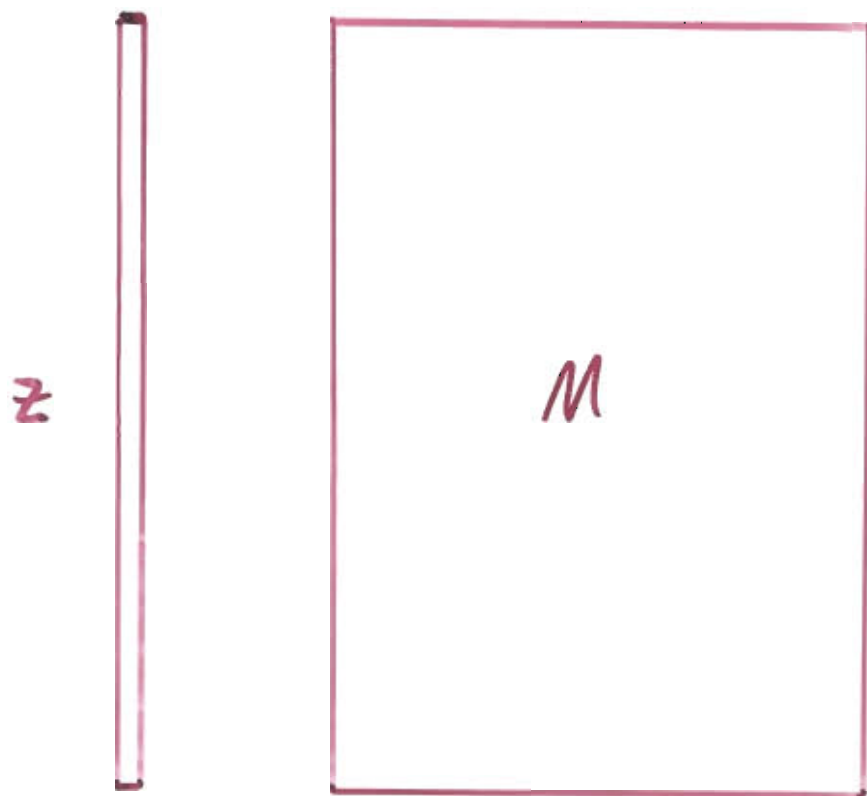
$B = k \times l$  matrix over  $GF(2)$

Full row rank.

$x \in (GF(2))^l$  random. (All bits statistically independent)

$$y = Bx$$

$\Rightarrow$  All bits of  $y$  stat. ind.



Every  $k$  rows of  $M$  lin. ind.

$\Rightarrow$  Every  $k$  bits of  $z$  stat. ind.

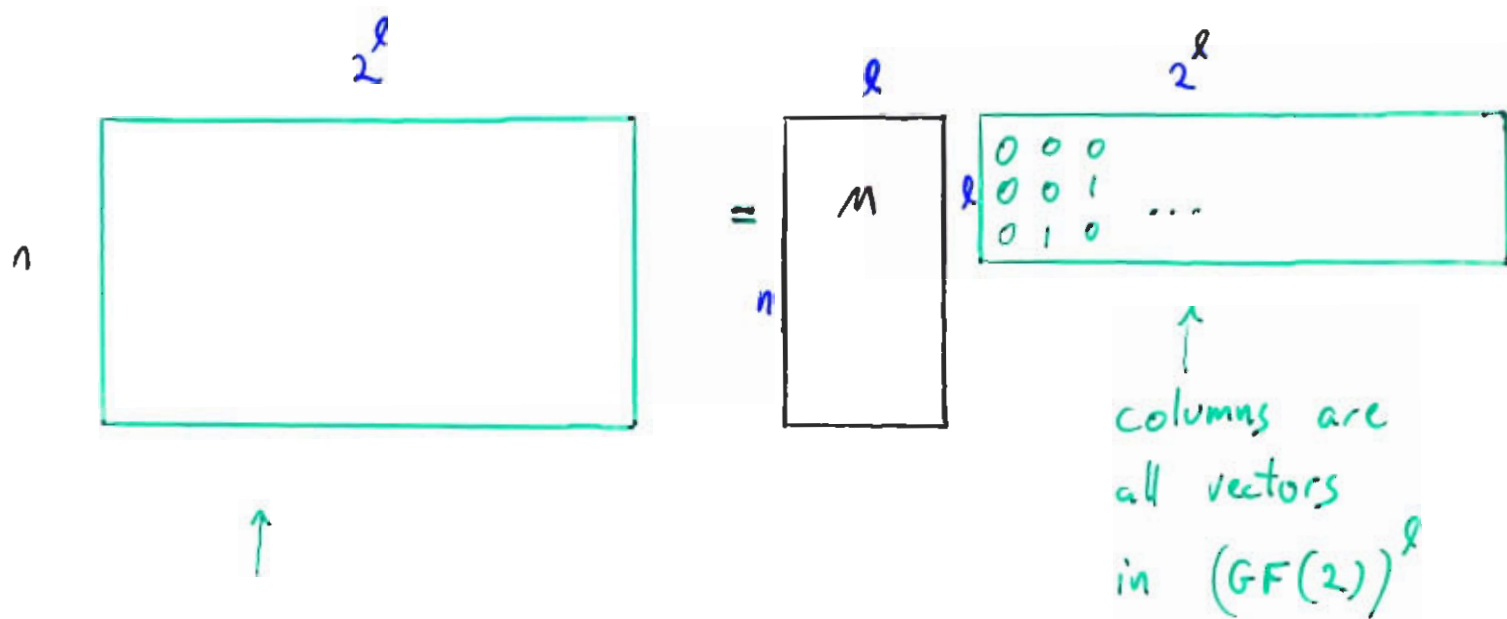
# Dual Applications of the Parity Check Matrix:

$$\overline{\text{codeword}} \quad M = \overline{0}$$

$$\begin{array}{l} \text{k-wise} \\ \text{independent} \\ \text{(uniform)} \\ \text{bits} \end{array} \quad \begin{array}{|c|} \hline \\ \hline \end{array} = \begin{array}{|c|} \hline M \\ \hline \end{array} \quad \begin{array}{|c|} \hline \\ \hline \end{array} \begin{array}{l} \text{independent} \\ \text{(uniform)} \\ \text{bits} \end{array}$$

Every  $k$  rows of  $M$  linearly independent.

$k$ -wise independent sample space:



Each column is an element (with weight  $2^{-k}$ ) in the  $k$ -wise independent sample space  $S$ .

How big does  $S$  have to be?

Maximizing the transmission rate  $\frac{n-k}{n}$  of a binary,  $k$ -error-detecting linear code, is equivalent to minimizing the size  $2^k$  of a linear  $k$ -wise independent binary sample space.

Answer: for binary, uniform,  $k$ -wise independent  
random variables  $z_1, \dots, z_n$ ,  
 $|S| \approx n^{\lfloor k/2 \rfloor}$ .

Construction for upper bound:

Round  $n$  up to  $n = 2^r - 1$ .

Let  $a_1, \dots, a_n$  be the nonzero elts of  $GF(2^r)$ .

~~Let~~ In the van der Monde matrix

$$M_1 = \begin{bmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{k-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{k-1} \end{bmatrix} \quad \begin{array}{l} \text{matrix} \\ \text{over} \\ GF(2^r) \end{array}$$

every  $k$  rows are linearly independent over  $GF(2^r)$ .