

Error correcting code

Math21b, O.Knill

We try out the error correcting code as in the book (problem 53-54 in 3.1).

I) Encoding.

To do so, we encode the letters of the alphabet by pairs of three vectors containing zeros and ones:

$A = (0, 0, 0, 1), (0, 0, 0, 1)$	$B = (0, 0, 0, 1), (0, 0, 1, 0)$	$C = (0, 0, 0, 1), (0, 0, 1, 1)$
$D = (0, 0, 0, 1), (0, 1, 0, 1)$	$E = (0, 0, 0, 1), (0, 1, 1, 0)$	$F = (0, 0, 0, 1), (0, 1, 1, 1)$
$G = (0, 0, 0, 1), (1, 0, 0, 1)$	$H = (0, 0, 0, 1), (1, 0, 1, 0)$	$I = (0, 0, 0, 1), (1, 0, 1, 1)$
$J = (0, 0, 0, 1), (1, 1, 0, 1)$	$K = (0, 0, 0, 1), (1, 1, 1, 0)$	$L = (0, 0, 0, 1), (1, 1, 1, 1)$
$M = (0, 0, 1, 0), (0, 0, 0, 1)$	$N = (0, 0, 1, 0), (0, 0, 1, 0)$	$O = (0, 0, 1, 0), (0, 0, 1, 1)$
$P = (0, 0, 1, 0), (0, 1, 0, 1)$	$Q = (0, 0, 1, 0), (0, 1, 1, 0)$	$R = (0, 0, 1, 0), (0, 1, 1, 1)$
$S = (0, 0, 1, 0), (1, 0, 0, 1)$	$T = (0, 0, 1, 0), (1, 0, 1, 0)$	$U = (0, 0, 1, 0), (1, 0, 1, 1)$
$V = (0, 0, 1, 0), (1, 1, 0, 1)$	$W = (0, 0, 1, 0), (1, 1, 1, 0)$	$X = (0, 0, 1, 0), (1, 1, 1, 1)$
$Y = (0, 0, 1, 1), (1, 0, 0, 1)$	$Z = (0, 0, 1, 1), (1, 0, 1, 0)$	$? = (0, 0, 1, 1), (1, 0, 1, 1)$
$! = (0, 0, 1, 1), (1, 0, 0, 1)$	$. = (0, 0, 1, 1), (1, 0, 1, 0)$	$, = (0, 0, 1, 1), (1, 0, 1, 1)$

Choose a letter

Look up in the above table the pair (x, y) which belongs to this letter.

$$x = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}, \quad y = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

Now we build (Mx, My) , where M is the matrix $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Use $1 + 1 = 0$ in the matrix multiplications which follow! Let's go:

$$Mx = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

$$My = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

Now, fold this page at the prescribed fold and show the two vectors Mx, My to your friend, who writes down on the top of the second page.

II) Transmission.

You obtain now the vectors Mx, My from your neighbor. Copy the two vectors (Mx, My) of him or her but add one error. To do so, switch one 1 to 0 or one 0 to 1 in the above vectors.

$$u = Mx + e = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} \quad v = My + f = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

III) Detect the error e and f.

Detect errors by forming

$$Hu = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

$$Hv = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

Now look in which column Hu or Hv is. Put 0's everywhere in e except at that place, where you put a 1. For example if Hu is the second column, then put a 1 at the second place. We obtain e and f :

$$e = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}, \quad f = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

IV) Decode the message.

Let $P \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \end{bmatrix} = \begin{bmatrix} d \\ e \\ f \\ g \end{bmatrix}$. Determine $Pe = P \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}, Pf = P \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$. In an error-free transmission (Pu, Pv) would give the right result back. Now

$$Pu = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}, \quad Pv = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

satisfy $Pu = x + Pe, Pv = y + Pf$. We recover the original message by subtracting Pe, Pf from that

$$x = Pu - Pe = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}, \quad y = Pv - Pf = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

(In the subtraction like addition, use $1 + 1 = 0, -1 - 1 = 0, 1 - 1 = 0, -1 = 1$.)

The letter belonging to (x, y) (look it up) is .