

like up in P3p

$[n, k]_2$  code  
 $C \subseteq \mathbb{F}_2^n$

$[n, k]_2$  code  
 $C \subseteq \mathbb{F}_2^n$

$[3, 1]_2$  code

$$C_4 = \text{span} \{ |1000\rangle, |1111\rangle \}$$

$[9, 1]_2$  code

$$|0_L\rangle = \frac{1}{\sqrt{2}} \left( |1000\rangle + |1111\rangle \right)$$

$$|1_L\rangle = \frac{1}{\sqrt{2}} \left( |1000\rangle - |1111\rangle \right)$$

$$C_2 = \text{span} \{ |0_L\rangle, |1_L\rangle \}$$

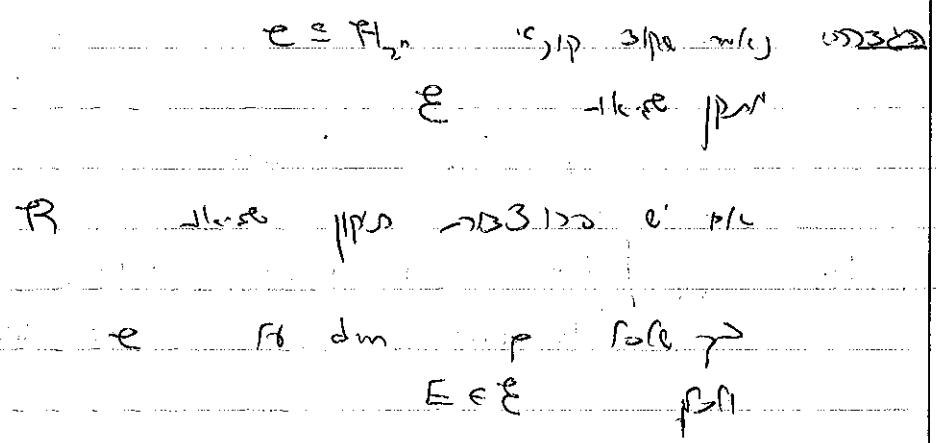
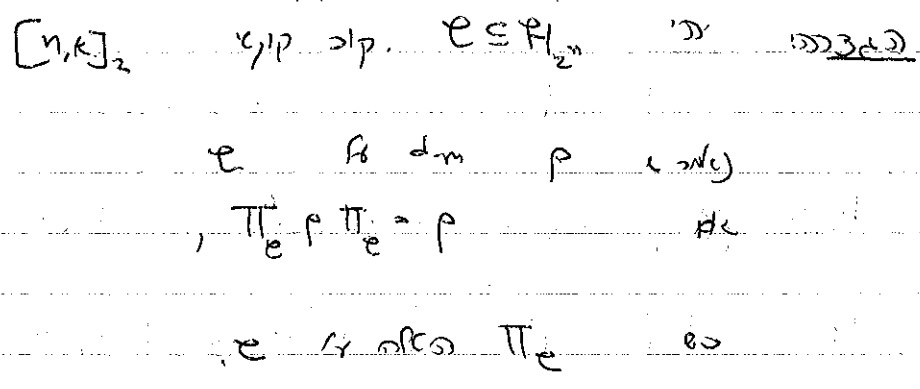
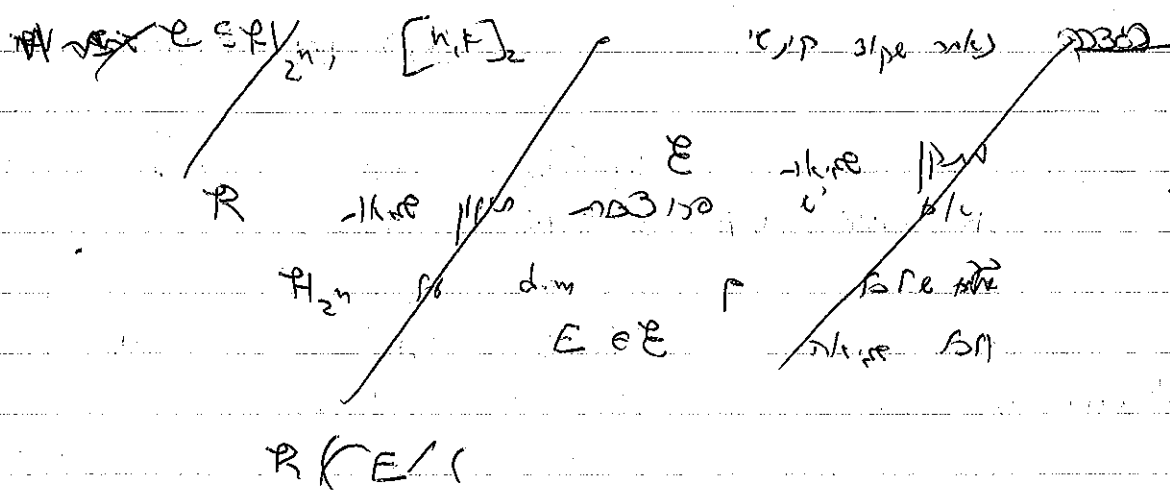
$[7, 1]_2$  Steane's code

$$|0_C\rangle = \frac{1}{\sqrt{8}} \left[ |1000100\rangle + |1010101\rangle + |1011001\rangle + |1100100\rangle + |1001111\rangle + |1011010\rangle + |1011100\rangle + |1101001\rangle \right]$$

$$|1_C\rangle = \frac{1}{\sqrt{8}} \left[ |1111\rangle + |1010101\rangle + |1001100\rangle + |1011001\rangle \right]$$

$|1_C\rangle = \frac{1}{\sqrt{2}} \left( |0_C\rangle + |1_C\rangle \right)$

$$C_3 = \text{span} \{ |0_C\rangle, |1_C\rangle \}$$



$$\mathbb{R}(E(p)) = p$$

הצגת המרחב הריבועי

יש להניח כי  $E_1, \dots, E_T$  הם פרויקטורים

כאלו ש-  $\Psi_j = \Psi_j \circ E_j$  ו-  $\Psi_j \circ E_j = \Psi_j$

הריבועי  $R$  הוא

$$R(E_j(\Psi_j)) = \Psi_j \otimes |i\rangle$$

כאן  $|i\rangle$

$$R\left(\sum \alpha_i E_i(\sum \beta_j \Psi_j)\right)$$

$$= \sum \alpha_i R(E_i(\sum \beta_j \Psi_j))$$

$$= \sum \alpha_i \beta_j R(E_i(\Psi_j)) = \sum \alpha_i \beta_j \Psi_j \otimes |i\rangle$$

$$= \sum \beta_j \Psi_j \otimes \sum \alpha_i |i\rangle$$

כלומר  $R$  הוא פרויקטור

$$E_1 = \text{span}\{H_1, H_2, H_3\}$$

span  $E_1$  is linear

1. 906.4 6. 0.0 - 0.17  $H_1$

$$E_1 = \text{span}\{1000, 1111\}$$

span

$$R_2(E_1, (\psi_j)) = |m, m, m\rangle \otimes |1\rangle$$

$$m = \text{maj}\{b_1, b_2, b_3\}$$

$\downarrow$   
 $H_1, H_2, H_3$

$0, 1, 2 \rightarrow$  for  $100, 101, 110, 111$

$$R(1000) = 100, 0 \otimes 107$$

$$R(001) = 1000 \otimes 3$$

$$010 \quad 000 \quad 2$$

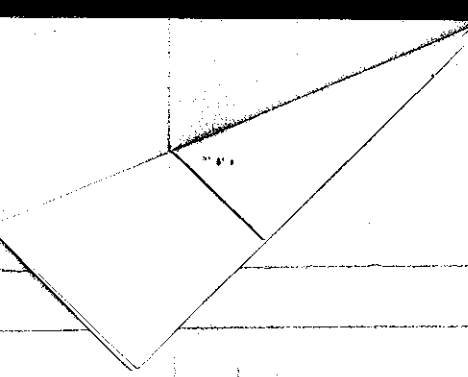
$$100 \quad 000 \quad 1$$

$$110 \quad 111 \quad 3$$

$$101 \quad 111 \quad 2$$

$$011 \quad 111 \quad 1$$

$$111 \quad 111 \quad 0$$



$E_i$

2 lines

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

X - bit flip

$$\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

Z - phase flip

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

XZ - bit & phase flip

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

I - none

$H_{2^n}$

for  $2^n$

$$E = E_1 \otimes \dots \otimes E_n$$

over  $2^n$

$$E_i \in \{X, Z, XZ, I\} \quad \text{BP} \Rightarrow$$

$$E_i \neq I \quad \text{for } i \in \{1, \dots, n\} \quad \text{BP}$$

work +  $2^n$  BP for  $2^n$  bits  $E$

$E_i$  part share code length

for  $2^n$  bits

...  $2^n$  bits  $2^n$  bits  $2^n$  bits

bit flip  $2^n$  bits  $2^n$  bits  $2^n$  bits

$$|m_1, m_2, m_3\rangle \otimes |m_1, m_2, m_3\rangle \otimes |m_1, m_2, m_3\rangle \quad \text{for } 2^n \text{ bits}$$

$$|m_1, m_2, m_3\rangle$$

...  $H^{\otimes 3}$   $2^n$  bits

... bit flip  $2^n$  bits  $2^n$  bits  $2^n$  bits

$E = E_1 \otimes \dots \otimes E_n$   
 $E_i \in \{I, X, Z, XZ\}$   
 $\forall i \in \{1, 2, \dots, n\}$

bit flip  $\rightarrow$  phase flip  
 phase flip  $\rightarrow$  bit flip

$|0\rangle = (|+\rangle)^{\otimes 3}$   
 $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$   
 $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|+\rangle \otimes |0\rangle \otimes |0\rangle$   
 $|0\rangle \otimes |0\rangle \otimes |0\rangle$

$\Delta$   $\rightarrow$  phase flip

Proof PDP for GN

$k$  זמין  $n \times k$   $C \in \mathbb{F}_2^n$   $n \times n$

מב' מב' ג'

$C = \text{Im}(G) \rightarrow \tilde{C} \quad G: \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n \quad e', k$

$$\begin{pmatrix} G \end{pmatrix}_{n \times k}$$

מב' מב' ג'  
מב' ג' ר

ר מב' ג' מב' ג' ג' ג'  
ג' ג'

$$C^\perp = \{y \in \mathbb{F}_2^n \mid \forall c \in C \quad c \cdot y = 0\}$$

parity check matrix

$n-k$  זמין  $n \times (n-k)$   $C^\perp \subseteq \mathbb{F}_2^n$

parity check matrix  $H$   $n \times (n-k)$

מב' ג' ג' ג' ג'

$$H_{(n-k) \times n}$$

$$\forall c \in C \quad Hc = 0 \quad \rightarrow$$

$$C = \{y \mid Hy = 0\} \quad \text{:-k-sr sru}$$

$$C = \{y \mid Hy = 0\} \quad \rightarrow$$

$k$  זמין  $n-k$

Syndrom de-codage

1. ~~calculer~~ ~~produit~~

2.  $c \in C$   $\rightarrow$   $\exists$   $p \in \mathbb{F}_q^n$   $\rightarrow$   $c = p + e$

$$d = \min_{x_1 \neq x_2} d(c, x_1) + d(x_1, x_2)$$

$\underbrace{\qquad\qquad\qquad}_{\text{syndromes}} \quad \underbrace{\qquad\qquad\qquad}_{\text{syndromes}}$

$w(e) \leq d \rightarrow p, e \in \mathbb{F}_q^n$   $\rightarrow c \in C$   $\rightarrow$   $d(c, c) = d(0, 0) = 0$

$$H(c+e) = H(c) + H(e)$$

syndromes  $\rightarrow$   $H(c) = 0$

$w(e_1), w(e_2) \leq \frac{d-1}{2}, e_1 \neq e_2 \rightarrow H(e_1) \neq H(e_2)$

syndromes  $\rightarrow$   $H(e_1) = H(e_2) \rightarrow$

$$H(e_1 + e_2) = H(e_1) + H(e_2) = 0$$

$w(e_1 + e_2) < d$

syndromes  $\rightarrow$   $e_1 + e_2 \in C$   $\rightarrow$



Hamming code

$$C_1 = [7, 4, 3]_2$$

1101112

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

p.c.m + 6

$$k = 7 - 3 = 4, n = 7$$

es c:  $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$  ...

des p5, ...  $H_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

$$C_2 = C_1^+$$

$$C_2 = [7, 3, ?]_2$$

$$G_2 = H_2^t$$

$$H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\left[ I \mid A \right]$$

$$H_2 G_2 = 0$$

$$H_2 = \dots$$

$$H_2 \text{ is } II+III$$

$$\dots I+III$$

$$\boxed{C_2 \subseteq C_1} \Leftrightarrow H_1 = 0 \Leftrightarrow H_2 = 0$$



Calderbank, Sham, Sterne

CSF codes

dim  $C_1 = k_1$

$$C_2 = \left[ \begin{array}{c} C_1 \\ 0 \end{array} \right] \quad \text{dim } C_2 = n$$

alle  $t$  in  $C_2^\perp$ ,  $C_1$  ist ein  $\perp$  zu  $C_2^\perp$  (siehe S. 100 in [1])

$$C_1 \rightarrow C_2 \text{ isosomorph } \frac{|C_1|}{|C_2|} = 2^k$$

also  $\frac{|C_1|}{|C_2|} = 2^k$

$$|C_2| = 2^{n-k}$$

$$|C_2^\perp| = \frac{1}{|C_2|} \sum_{g \in C_2} |g + C_2|$$

~~...~~  $\Rightarrow \text{Span} \{ |g + C_2| \mid g \in C_1 \}$

$$\text{Sp} \{ |g + C_2| \} = [n, n-k]_2 \quad (10)$$

$$\frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = 2^{k_1 - k_2} \quad \text{also BNL } \Rightarrow$$



1. Discrete Random Variable

Let \$X\$ be a discrete random variable with probability mass function \$p(x)\$ and cumulative distribution function \$F(x)\$.

$$\frac{1}{\sqrt{c_2}} \sum_{c \in C_2} (-1)^k (y+c) \cdot e_2 \quad \text{as } y \in \mathbb{R}$$

Discrete Random Variable

$$\frac{1}{\sqrt{c_2}} \sum_{c \in C_2} (-1)^k (y+c) \cdot e_2 \quad \sum_{z} (-1)^k (y+c) \cdot z \quad |z \in \mathbb{Z}$$

$$= \frac{1}{\sqrt{c_2}} \sum_{z} \left( \sum_{c \in C_2} (-1)^k (y+c) (e_2+z) \right) |z \in \mathbb{Z}$$

$$(-1)^k y (e_2+z) \sum_{c \in C_2} (-1)^k c (e_2+z)$$

\$C\_2\$ is a subset of \$\mathbb{Z}\$, \$C\_2 = \{2k+2\}\$, \$C\_2 = \{2k\}\$

\$\alpha \in C\_2\$

$$\alpha (e_2+z) \neq (\alpha+c) (e_2+z)$$

Let \$y \in \mathbb{R}\$, \$z \in \mathbb{Z}\$, \$c \in C\_2\$

$$\frac{0}{\sqrt{c_2}}$$

$\forall c_n \quad c(e_2+z)=0 \quad \forall z > 2 \quad \text{for } p \text{ bigger } p^p$

$$e_2 + z \in C_n^+$$

$$z \in C_n^+ + e_2$$

$$\forall \sum (-1)^{|\lambda|} \quad |\lambda| >$$

$$z \in C_n^+ + e_2$$

is it?

$$C_n^+ \quad \text{for } p^p \text{ and } \textcircled{2}$$

$$e_2 \quad \text{for } p^p$$

$$p^p \text{ and } p^p$$

$$\forall \sum (-1)^{|\lambda|} \quad |\lambda| >$$

$$w \in C_n^+$$

$$w = z + e_2$$

is it?

$$\sum_{\lambda \in \mathcal{P}_n} (-1)^{|\lambda|} \quad |\lambda| >$$

$$\text{for } p^p \text{ and } \textcircled{4}$$

$$\text{for } p^p$$

E