

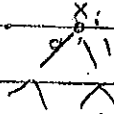
5/12/13

ECG to P-5/12/13 2

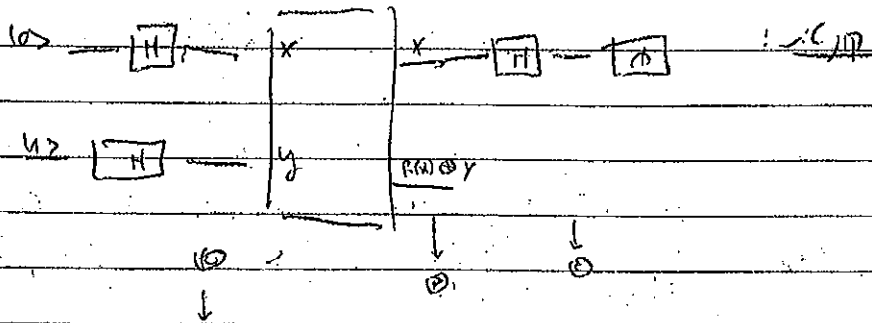
(The message is 4 bits)

$f_1: 1011 \rightarrow 1011$ 1011
 $f_2: 0101 \rightarrow 1011$ 1011

Decision trees to find output



6/10/13



$$\textcircled{1} \quad \frac{1}{2} [(00+11) \oplus (01+10)] = \frac{1}{2} [00+10+01+11]$$

$$\textcircled{2} \quad \frac{1}{2} [0, f(x) + 1, f(x) - 0, f(x) - 1, \bar{f}(x)]$$

$$= \frac{1}{2} [10 \oplus (f(x) = \bar{f}(x)) + 11 \oplus (f(x) = \bar{f}(x))]$$

$$\textcircled{3} \quad = \frac{1}{2} [10+11] \oplus \frac{1}{2} [f(x) = \bar{f}(x)] \quad f(x) = f(x), \quad f(x) \oplus f(x) = 0 \quad \text{ms}$$

$$\textcircled{4} \quad = \frac{1}{2} [10+11] \oplus \frac{1}{2} [f(x) = \bar{f}(x)] \quad f(x) = f(x), \quad f(x) \neq f(x), \quad f(x) \oplus f(x) = 1$$

$$f(x) = \bar{f}(x) = - [f(x) = \bar{f}(x)]$$

⑤

Black-box (BND)

Blackbox $(f: \{0,1\}^n \rightarrow \{0,1\})$...

Yes $\{0,1\}^n$
No $\{0,1\}^n$

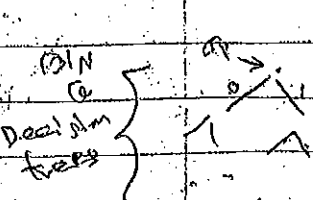
... $\{0,1\}^n$...

$f: \{0,1\}^n \rightarrow \{0,1\}$

| | |
|-------------------|-----------------|
| $\sum_x f(x) = 0$ | Yes $\{0,1\}^n$ |
| ... | No $\{0,1\}^n$ |

Yes \cup No $\neq \{0,1\}^n$...
 Promise problem ...
 $f \in \text{Yes} \cup \text{No}$...

... Yes \cup No $= \{0,1\}^n$...

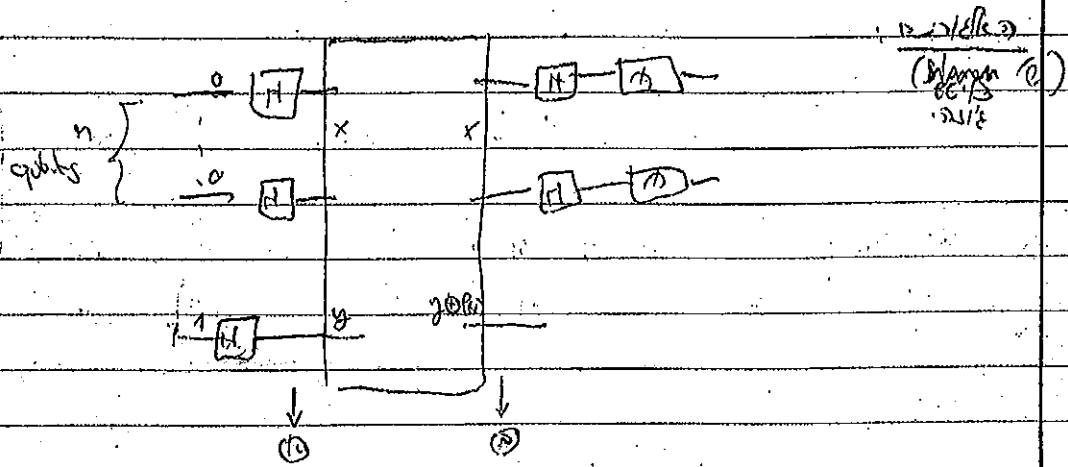
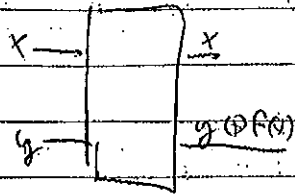


... 2^n ...

... 2^n ...

ישו המערכת - קיבל 0.0 פ-1/2 כל הזמן
 זמן ה-1/2 + 1/2

קיבל פ-1/2 : קיבל 0.0 פ-1/2
 קיבל 0.0 פ-1/2 : קיבל



"מקבל פ" קיבל 0.0 קיבל 1/2 כל הזמן
 "מקבל פ" " מקבל 1/2 " " "

$$\textcircled{1} \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \textcircled{2} \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle] = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_x [|x, 0\rangle - |x, 1\rangle]$$

$$\textcircled{2} \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_x [|x, f(x)\rangle - |x, \bar{f}(x)\rangle]$$

$$= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \textcircled{3} |0\rangle - |1\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_x (-1)^{f(x)} |x\rangle \textcircled{3} |0\rangle - |1\rangle$$

למקבל פ-1/2
 $\sum_x (-1)^{f(x)} |x\rangle$ ברור מקבל פ-1/2 כל הזמן

? Had " 1st p. Proves n/p an

62 y: (1)

$$H(y) = \frac{1}{\sqrt{2}} [|0\rangle + (-1)^y |1\rangle]$$

$$= \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{y \cdot z} |z\rangle$$

$$H^{\otimes n} |y_1 \dots y_n\rangle = H|y_1\rangle \otimes H|y_2\rangle \otimes \dots \otimes H|y_n\rangle \quad \text{nc 1) (2)}$$

$$= \frac{1}{\sqrt{2}^n} \sum_{z \in \{0,1\}^n} (-1)^{y_1 z_1} (-1)^{y_2 z_2} \dots (-1)^{y_n z_n} |z\rangle$$

$$= \frac{1}{\sqrt{2}^n} \sum_{z \in \{0,1\}^n} (-1)^{y \cdot z} |z\rangle$$

$$y \cdot z = \sum_{i=1}^n y_i z_i \quad (\text{mod } 2)$$

(1) (2)

o B > 0 > 6 b/c

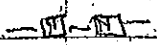
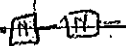
$$H^{\otimes n} (H^{\otimes n} |0\rangle) = (H^{\otimes n})^2 |0\rangle = I^{\otimes n} |0\rangle = |0\rangle \quad \text{Sp}$$

$$\frac{1}{\sqrt{2}} \sum_x |x\rangle$$



$$H^{\otimes n}$$

H = H†, cyclic H



$$\frac{1}{\sqrt{2}} \sum_x (-1)^{F(x)} |x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}} \sum_x (-1)^{F(x)} \frac{1}{\sqrt{2}} \sum_z (-1)^{x \cdot z} |z\rangle \quad \text{inserted f b/c}$$

$$= \frac{1}{\sqrt{2}^2} \sum_z \left[\sum_x (-1)^{F(x)} (-1)^{x \cdot z} \right] |z\rangle$$

for the input 0, the output is $\sum_x (-1)^{F(x)} |x\rangle$ is 0. 12/21 1, 10/11 0 (3)

Simon C. 2-7/1976

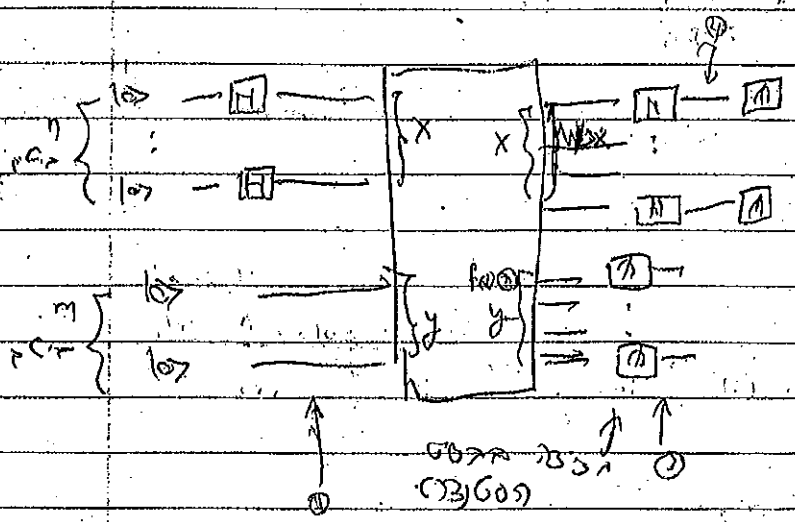
$f: \mathbb{Z}/n^h \rightarrow \mathbb{Z}/n^m$ ICP
מפתח

$f(x) = (f_1(x), \dots, f_p(x))$ $\in \mathbb{Z}/n^m$

(מפתח של f הוא (f_1, \dots, f_p))

$f_1(x) = \dots = f_p(x)$ $\in \mathbb{Z}/n^m$

(Simon) 'GIP' מפתח



מפתח של f הוא (f_1, \dots, f_p)

$\sum_{x \in \mathbb{Z}/n^h} f(x) = \sum_{x \in \mathbb{Z}/n^h} (f_1(x), \dots, f_p(x))$

$\sum_{x \in \mathbb{Z}/n^h} f(x) = \sum_{x \in \mathbb{Z}/n^h} (f_1(x), \dots, f_p(x))$

$\sum_{x \in \mathbb{Z}/n^h} f(x) = \sum_{x \in \mathbb{Z}/n^h} (f_1(x), \dots, f_p(x))$

$\alpha \sum_{k=0}^{\infty} (4 \cdot 1^k x + 1 \cdot 0^k x) \otimes |z\rangle$

...

$H^{\otimes n}$

$$\sum_{k=0}^{\infty} \frac{\alpha}{2^k} \left[\sum_{z \in \mathbb{F}_2^n} (-1)^{x \cdot z} |z\rangle + \sum_{z \in \mathbb{F}_2^n} (-1)^{(x+D) \cdot z} |z\rangle \right]$$

$$\alpha \sum_{k=0}^{\infty} \sum_{z \in \mathbb{F}_2^n} \left[(-1)^{x \cdot z} + (-1)^{(x+D) \cdot z} \right] |z\rangle$$

$$(1 + (-1)^{D \cdot z}) (-1)^{x \cdot z}$$

$1 + (-1)^{D \cdot z} = 2$ if $D \cdot z = 0$
 $1 - 1 = 0$ if $D \cdot z = 1$

$$= 2 \alpha \sum_{z \in \mathbb{F}_2^n} \sum_{z \in \mathbb{F}_2^n} |z\rangle$$

...

$$\sum_{i=1}^n z_i \cdot s_i + z_2 \cdot s_2 + \dots + z_n \cdot s_n = 0$$

...

...

$$f(x) = x + D$$

$$f(x) = f(x+D)$$