

האקדמיית סיומן

נתן סוף

$$F: \{0,1\}^n \rightarrow \mathbb{C}$$

סדר קדום מלא מנה
מ'א? ; צמצם

מבטחן להפוך F
מ'א? ; צמצם
מ'א?

$$\forall x \in \{0,1\}^n \quad F(x+L) = F(x)$$

וגם כן, נ"מ
מ'א? ; צמצם

$$F(x) = F(y) \Rightarrow x \in \{y, y+L\}$$

מ'א? ; צמצם
מ'א? ; צמצם

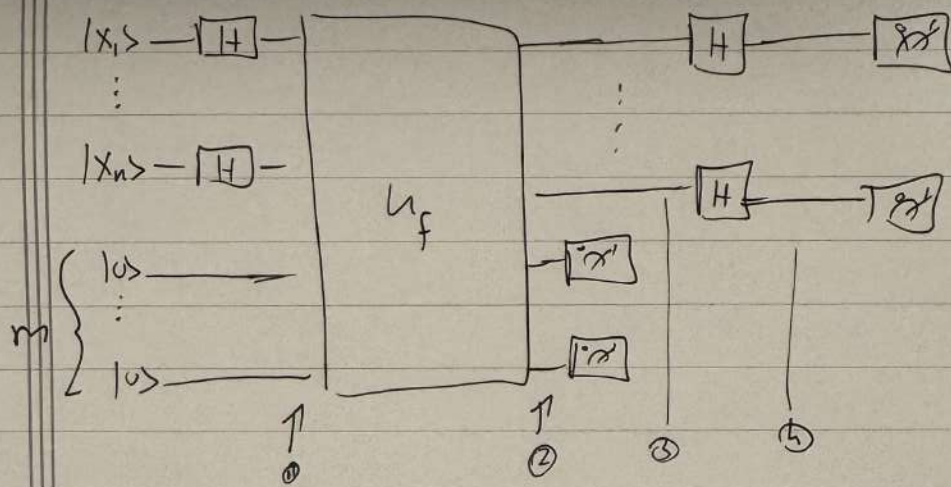
מ'א? ; צמצם
מ'א? ; צמצם
מ'א? ; צמצם

$$\sqrt{2}^n \sim 1.4^n$$

מ'א? ; צמצם

מ'א? ; צמצם
מ'א? ; צמצם
מ'א? ; צמצם

מ'א? ; צמצם



רענ:

$$① \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

$$② U_f ① = \sum_x |x\rangle |f(x)\rangle$$

$$F^{-1}(c^*) = \{x^*, x^* + L\}$$

המקרה הזה, $c^* \in C \subseteq \{0,1\}^m$ הוא איננו יחיד, כלומר יש לנו שני פתרונות, x^* ו- $x^* + L$.
 ?

$$③ = \frac{1}{\sqrt{2}} \left[|x^*\rangle |c^*\rangle + |x^* + L\rangle |c^*\rangle \right]$$

המקרה הזה, c^* הוא איננו יחיד, כלומר יש לנו שני פתרונות, x^* ו- $x^* + L$.

אם x^* ו- $x^* + L$ הם שני פתרונות, אז $x^* + L = x^*$ (mod 2).
 כלומר, $L = 0$.
 זה אומר שיש לנו שני פתרונות, x^* ו- $x^* + L$, שונים זה מזה.
 זה אומר שיש לנו שני פתרונות, x^* ו- $x^* + L$, שונים זה מזה.

המקרה הזה, c^* הוא איננו יחיד, כלומר יש לנו שני פתרונות, x^* ו- $x^* + L$.

$$④ = \frac{1}{\sqrt{2}} (H |x^*\rangle + H |x^* + L\rangle) =$$

