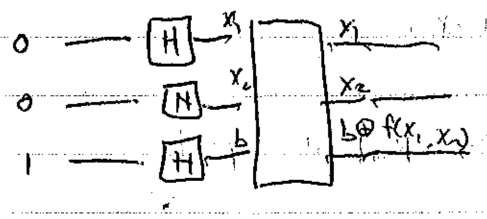
תרגיל 3.

1. (בן סימון) אפשר בשאלה אחת.

נסתכל על



ומצאנו,

ולפי המצב הקודם: עבור 4 פונק' ה f האפשריות תמיד הקבוע.
במקרה מראה שהם בלתי אורתוגונלים.
ולכן ניתן להבחין ביניהם,
ועשינו את ההבחנה בשאלה אחת!

2. א) $\pi(x_1\ldots x_N)=x_{\pi(1)}\ldots x_{\pi(N)}$, $\tilde{p}=\sum_{\pi\in S_N} p(\pi(x_1\ldots x_N))$

ב. כל פולינום סימטרי ניתן להצגה כפולינום בפונק' הסימטריות הבסיסיות $Q_0,\ldots,Q_N$

$$Q_k(x_1\ldots x_N)=\sum_{i_1<\ldots<i_k} x_{i_1}\cdots x_{i_k}$$

$$p(x_1\ldots x_N)=\sum_{I=(i_0,\ldots,i_N)} c_I\cdot Q_0^{i_0}\cdots Q_N^{i_N}$$

עכשיו אנו רק מסתכלים על ערכים בוליאנים. מה ערך הנ"ל:
[illegible]

$$Q_\ell(x_1\ldots x_N)=\binom{\sum x_i}{\ell}$$

ולכן מעל ערכים בוליאניים $p(x_1\ldots x_n)=q(\sum x_i)$
ו $\deg(q)\le\deg(p)\le k$.

ג. ל-OR יש את הייצוג הפולינומי הבא:

$$OR(x_1 \ldots x_N) = 1 - \prod_{i=1}^{N} (1 - x_i)$$

ולכן $\deg(OR_N) = N$

ד. לפי ב׳ יש q $q(\sum x_i) = f(x_1 \ldots x_N)$

יש לפחות $\frac{N}{2}$ ערכים שבהם q מתאפס (או q הוא 1, ואז נסתכל על $1-q$)

ולכן ל-q יש $\frac{N}{2}$ שורשים

ולכן $\deg(f) \geq \deg(q) \geq \frac{N}{2}$

<u>שאלה 3</u> נניח שיש אלגוריתם קוונטי Q_1 שפותר את OR עם T שאילתות,
אז קיים פולינום W מדרגה $\leq 2T$

כך:

$OR(a_1 \ldots a_N) = 1 \Rightarrow W(a_1, \ldots, a_N) = 1$

$a_1 = \ldots = a_N = 0 \Rightarrow W(a_1 \ldots a_N) < 1$

<u>סימטריזציה</u>

ולכן $1 - W$ פולינום שאינו אפס.
נסמן ב-Z הפולינום המתאים לו

$Z(i) = 0 \quad \forall i > 0$

$Z(0) \neq 0$

ולכן $2T \geq \deg(W) \geq \deg(Z) \geq N$

ו- $T \geq \frac{N}{2}$.

4. ש.ל. החשוב פ' גדולה שישנו דרך השקבולות את הפעולה כיוון G N,R.

ד. i. בחר $M=\sqrt[3]{N}$ אברים, של ערכים, ובדוק אם יש שם התנגשות (אם כן סיימנו).

אחרת נגדיר

$g:[N]\to\{0,1\}$

$g(i)=1 \Leftrightarrow$ יש ערך בסט ה- i שמתנגש עם O_i.

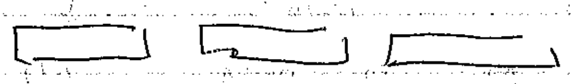
אז לפי g, נבדוק M ערכים שמחזירים 1

הפעלת אלגוריתם Grover על g.

ג. Simon פ ~ $O(\lg N)$ שאילתות

כלל, לכל המקרה המצב יהיה קיים s כך ש $O_x = O_{x\oplus s}$.

ב. קבוע ליניק $O(\sqrt{N})$, birthday paradox.

5. רקורסיה, 3 שלשה 

מחזיק 2 רקורסיות

אם ערכים שווים - סיימנו (אין צורך לפתור את השלישית)

אם שונים - פותרים את השלישית רקורסיבית.

6. עובדת יסוד

אם $A = Med(X_1 \dots X_n)$

$B = Med(Y_1 \dots Y_n)$

ו- $A < B$

ונקח $M = Med(X_1 \dots X_n Y_1 \dots Y_n)$

אז

$\boxed{A \le M \le B}$

לא המשכתי.

אלגוריתם

A,B משפט על ה med שלהם

הם ממוינים וזהו כי כן, החל מהמקום הנ"ל משמאל ;

אם שווים - הבא - ממשיכים ולא הבא

אם שונים - אז ה med הקטן, צריך את ה G האיברים

שלו שקטנים מה med שלו,

ובשביל ה med הגדול, צריך את G האיברים שלו

שגדולים מה med שלו (כמו [illegible] שנשארים [illegible] עם מספר שווה של איברים) זה med הגדול לא הפסיד.

ממשיכים על ה med שנבחר וממשיכים

בכל שלב - או מספר האיברים הקטן בחצי n,m

או שהאורך קטן בחצי: [m]

[illegible]

בכל חישוב ה med ממוצע בכל שלב,

ולכן: $O(\lg n \cdot \lg m)$

- הערה: כשמשתמש על ה med ממוצע

נניח ש med_A קטן מ med_B

אז A צריך את הקטנים שלו, וה med_A הופך רק אחד

[illegible] med_B [illegible]

לכן - [illegible] יכול לשלוח את אם ה med שלו הצריך prefix

ה[illegible] שלחו עד כה.

אם לא אפשר להמשיך [illegible] k+1 [illegible].

אם כן - [illegible] יוצאים מ[illegible] ומי קטן.

מרצת את הסתברות ל $O(\lg n)$.