

ד"ר מייקל א. ריאן
Ryan O'Donnell

בסוף קונסי

קצת היסטוריה: את היציון של קונסי היצ' סטיבן ויזנר (Stephen Wiesner) ויזנר דמיטרי יוז' - undergraduate עם מיועץ צ'ארס קר ברייזיס, והם השכיחו לעיתים מתקנה קר ברייזיס וויזנר בקולומביה דדוקטור של ויזנר את קר הוא סיפרו על היציון שהיו ראו שצאו בין היה את היציון של בסוף קונסי. זה 15-10 שנה לפני שפיין וצ'ארס התחילו למשל על מחקר קונסי (1969). היציון של ויזנר קרם זה למשל אי-השלכא שמהל מוסיקליה (בדדוקטור) בסוף קונסי. ויזנר כתב את המאמר שניה של ויזנר ויזנר צא את הווקציה והיציון של בסוף קונסי נותר ח' בדדוקטור קר לסיום של זה לעולם המחקר השנים.

ב-1979 קרם דדוקטור (FOCS) שמה ראו פוסטדוק המוסק בקרייבס - צ'ארס דמיטרי (Gilles Brassard) בלסטאמ נצל אור אחר לראש קר ויזנר ראו על היציון של ויזנר. דמיטרי התייחס לזה כאל "The most bizarre and certainly the most magical moment in my professional life."

זה ברם לפני ודמיטרי למשל על דריפטציה קונסי - כד - 1979 (דמיטרי ויזנר - RSA - 78). ויזנר הציג דמיטרי של דמיטרי דמיטרי - מאמר על בסוף קונסי וקירל הכרה דדוקטור. דמיטרי דדוקטור (וזה אק מקבול - מתי קונסי דאון של) אלא פים גודליק דמיטרי ויזנר. הוא נפטר - 2021.

את מה זה בסוף קונסי?

הקצ'ה הרעיון הוא לייצר סדרה ע"י מזה קוונט יחיד לא סדר
 (למשל קוונטים שמוכנים בזווית מסוימת) עם מזהב קלאסי. הרעיון
 הוא להבדיל את (סדר) מזהב אי-השכלה שומר את אפס
 להצגת מזהב קוונט לא ידוע כי יהיה אותו. באותו, לא ניתן
 לייצר את הסימנים מזהב יוצא דופן.

הדבר מאוד שונה מזהב קלאסי שבו ניתן למנות מאותה מסומנות
 בסיס יחידה לא ניתן לשלול הרעיון א וצדד הוא להשתמש בקיוון
 טיפול יחיד בסיס יחידה אחרת. למרות, מבחינה סטטיסטית
 הרעיון התאמת מקרים לא ניתן עם יחיד.

הסכומה המקורית א וצדד

לסכומה יש פרמטר ביטוי — (security parameter) n .
 בבסיס ליצור סדר חזק ה"ק"ה דומה $s \in \{0,1\}^n$ באקראי
 - s היא המזהב של הסדר (serial number) שמזהב q הסדר
 ובנוסף הוא כזה באקראי $q \in \{0,1,+,-\}^n$ ומזהב קוונט

$$|\psi\rangle = |q_1\rangle \otimes |q_2\rangle \otimes \dots \otimes |q_n\rangle$$

הסדר הוא הציג

$$\text{coin} = (s, |\psi\rangle)$$

והקצ'ה שזה ברשומה
 שיהי $a \rightarrow (s, q)$.

בבסיס לייצר אם סדר חזק: בהנחת s הקצ'ה שולף את q
 מהרשומה המאומת (אם אין רשומה המאומתת s הסדר קלאסי)
 מציג, ומזהב את $|\psi\rangle$ (קוונט - קוונט) עפי הקסם המתאים:
 צדדי $[n] \in s$ את $\{0,1\}^n$ המזהב נצטרך את $\{0,1\}^n$
 ומזהב את $\{|\pm\rangle\}$.

ה'צ"א מסתים בה'ת"ת ה' כאלו ע"ה [חלש] מוצא
 במקרה של הקוים ה' - > 14 / מחזיקה ע"ה. ה'
 תבאר שאלו ה' תבין תבין ה'צ"א עזר בה'ת"ת
 (הסתברות 1) - > 14 / נלא נלמה.

המין אלו - מעורר במחזיקים למשך ע"ה מחזק ה'ת'
 בה'ת"ת, ונצ"ח בה'ת"ת אלו הא' ע"ה נכח בה'ת'
 ע"ה תבין - הא' נ'ת ע"ה ע"ה?

בכ"ה ל"ה א"ה ה'ת"ת ע"ה נכח כ' א"ה נכח ע"ה, ונצ"ח
 באקראי ויש ל' ע"ה ה'ת"ת א"ה תבין ה'ת"ת ע"ה
 ה' - ע"ה ע"ה ע"ה ע"ה - ה'ת"ת א"ה ע"ה ע"ה
 ע"ה ה'ת"ת - $(\frac{1}{4})^n$. א"ה כ' - נ'ת ע"ה ע"ה א"ה
 ה'ת"ת נכח א"ה ע"ה ע"ה ע"ה ע"ה ע"ה ע"ה.

התבין ה'ת"ת ה'ת"ת - $(\frac{5}{8})^n$
 תבין ה'ת"ת: ה'ת"ת ע"ה חוקי (5, 14) נכח ע"ה
 ע"ה ע"ה * (ע"ה חוקי ל"ה חוקי) שיעור ע"ה
 ונ' א"ה ה'ת"ת ע"ה ה'ת"ת ה'ת"ת ע"ה
 ע"ה. תבין, ה'ת"ת ע"ה ע"ה ע"ה ע"ה ע"ה
 ע"ה ע"ה ע"ה. א"ה, ה'ת"ת ה'ת"ת ע"ה ע"ה
 האקראי ע"ה ע"ה ע"ה ע"ה ע"ה ע"ה ע"ה
 ונ' - ה'ת"ת (5, 14).

התבין נכח ע"ה ע"ה > 14 / ה'ת"ת ה'ת"ת. ה'ת"ת
 נכח ע"ה ע"ה ע"ה ע"ה ע"ה ע"ה ע"ה

$$2 \times (5, 14 \otimes 14 \otimes \dots \otimes 14 \otimes 14, 5)$$

יחידה. נקבע $i \in [n]$. ההסתברות $(\frac{1}{2})^i$ (היא $\frac{1}{2}$ עבור $i=1$)
 ה- $\{1, \dots, \frac{1}{2}\}$ היא $\frac{1}{2}$ והסתברות $\frac{1}{2}$

$$Pr[r_i = q_i] = 1$$

ההסתברות $\frac{1}{2}$ עבור $q_i \in \{ \pm 1 \}$
 ובמקרה $\frac{1}{4}$, כשהסתברות $\frac{1}{4}$ עבור $q_i \in \{ \pm 1 \}$ ו- $\frac{1}{4}$ עבור $q_i = 0$.
 בהסתברות $\frac{1}{4}$ עבור $q_i = 0$, בהסתברות $\frac{1}{4}$ עבור $q_i = 1$ ו- $\frac{1}{4}$ עבור $q_i = -1$.
 בהסתברות $\frac{1}{4}$ עבור $q_i = 0$, בהסתברות $\frac{1}{4}$ עבור $q_i = 1$ ו- $\frac{1}{4}$ עבור $q_i = -1$.

ובסך הכול,

$$Pr[i \text{ הולך סדרה עם } i] = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}$$

הסתברות $\frac{1}{4}$ עבור $q_i \in \{ \pm 1 \}$ (היא $\frac{1}{4}$ עבור $q_i = 1$ ו- $\frac{1}{4}$ עבור $q_i = -1$)
 הסתברות $\frac{1}{2}$ עבור $q_i = 0$ (היא $\frac{1}{2}$ עבור $q_i = 0$)

ואם n הוא מספר זוגי, ה- $\frac{5}{8}$ הוא הסתברות $\frac{5}{8}$

הערה: מספר שיש לו אסימטריות תהיה הסתברות $\frac{3}{4}$ או $\frac{1}{4}$ היא אסימטריות. שני $\frac{3}{4}$ כי
 "יש" ערכו כזה שהוא שווה הערך האסימטרי (אם n הוא
 האישי של n ...

יש רק ההסתברות! כאמור, מרכז שמותיהם לחשוב על המושג
 צדד - המושג שאנו: האם ח"כ "לכת" עדיין או רמת-העסק
 אינו על ערך קוואנטי? האם עדיין עדיין בהסתברות גדולה
 יותר בהתאם שנים או יותר מזה? מה נעשה - חשיבה
 והסתברות התורה במסגרת? מה נעשה באשר התורה שחיה תהיה?
 מה אם נרצה למצוא משהו (מסקנות) בתוספת) ואם.

השאלה היא: כיצד ניתן להשתמש ב- $\mathcal{H}$ כדי להוכיח את הטענה.

לפי כמות המידע של המערכת

נניח שיש לנו מערכת עם n קוביות. כל קוביה יכולה להיות במצב 0 או 1 . המערכת כולה יכולה להיות במצב אחד מתוך 2^n מצבים. אם אנחנו רוצים לדעת את המצב של המערכת, אנחנו צריכים לשאול שאלות. כל שאלה שאנחנו עושים, אנחנו מקבלים תשובה 0 או 1 . אנחנו רוצים לדעת את המצב של המערכת, אבל אנחנו לא יכולים לשאול ישירות. אנחנו צריכים להשתמש ב- $\mathcal{H}$ כדי להוכיח את הטענה.

$$(\mathcal{H}, |0\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle)$$

"המקרה" של $n=1$. במקרה זה, $q_1 = 0$ או 1 . אם $q_1 = 0$, אז המערכת היא במצב 0 . אם $q_1 = 1$, אז המערכת היא במצב 1 . אנחנו רוצים לדעת את המצב של המערכת, אבל אנחנו לא יכולים לשאול ישירות. אנחנו צריכים להשתמש ב- $\mathcal{H}$ כדי להוכיח את הטענה.

נניח שיש לנו מערכת עם n קוביות. כל קוביה יכולה להיות במצב 0 או 1 . המערכת כולה יכולה להיות במצב אחד מתוך 2^n מצבים. אם אנחנו רוצים לדעת את המצב של המערכת, אנחנו צריכים לשאול שאלות. כל שאלה שאנחנו עושים, אנחנו מקבלים תשובה 0 או 1 . אנחנו רוצים לדעת את המצב של המערכת, אבל אנחנו לא יכולים לשאול ישירות. אנחנו צריכים להשתמש ב- $\mathcal{H}$ כדי להוכיח את הטענה.

$$\Sigma = 2^n$$

אם n הוא מספר שלם, אז 2^n הוא מספר שלם. לכן, Σ הוא מספר שלם.

$$n \cdot \log\left(\frac{n}{\Sigma}\right)$$

אם n הוא מספר שלם, אז 2^n הוא מספר שלם. לכן, Σ הוא מספר שלם. אנחנו רוצים לדעת את המצב של המערכת, אבל אנחנו לא יכולים לשאול ישירות. אנחנו צריכים להשתמש ב- $\mathcal{H}$ כדי להוכיח את הטענה.

מקרה א' $q_1 = +$ כלומר 1 באותו צד, המילוי, ק"ק
 המקרה ב' $q_1 = -$ במקרה $1 \rightarrow \varepsilon$, $-$ בדיוק, $CNOT$:

$$CNOT |1 \rightarrow \varepsilon\rangle \otimes |q_1\rangle = \cos \theta CNOT |0\rangle \otimes |+\rangle + \sin \theta CNOT |1\rangle \otimes |+\rangle$$

$\frac{|0\rangle + |1\rangle}{2} \Rightarrow \frac{1}{\sqrt{2}} CNOT$

$$= \cos \theta |0\rangle \otimes |+\rangle + \sin \theta |1\rangle \otimes |+\rangle$$

$$= |1 \rightarrow \varepsilon\rangle \otimes |+\rangle$$

כלומר, $CNOT$ לא משפיע
 כעת, המקרה ג' 3 ומקרה א' $|4\rangle$ להבנת המקרה
 בדיוק $\{1, 2\}$, המקרה ג' $|4\rangle$ ומהק"ק $|4\rangle$ בדיוק המקרה
 שבו $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 ובסוף המקרה $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 נמצא המקרה $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$

מה שקרה המקרה דאמרי, ואם $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 יס"ס"ן $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 שבו $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 בק"ק $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$
 מה $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$ $|4\rangle$ $|1 \rightarrow \varepsilon\rangle$