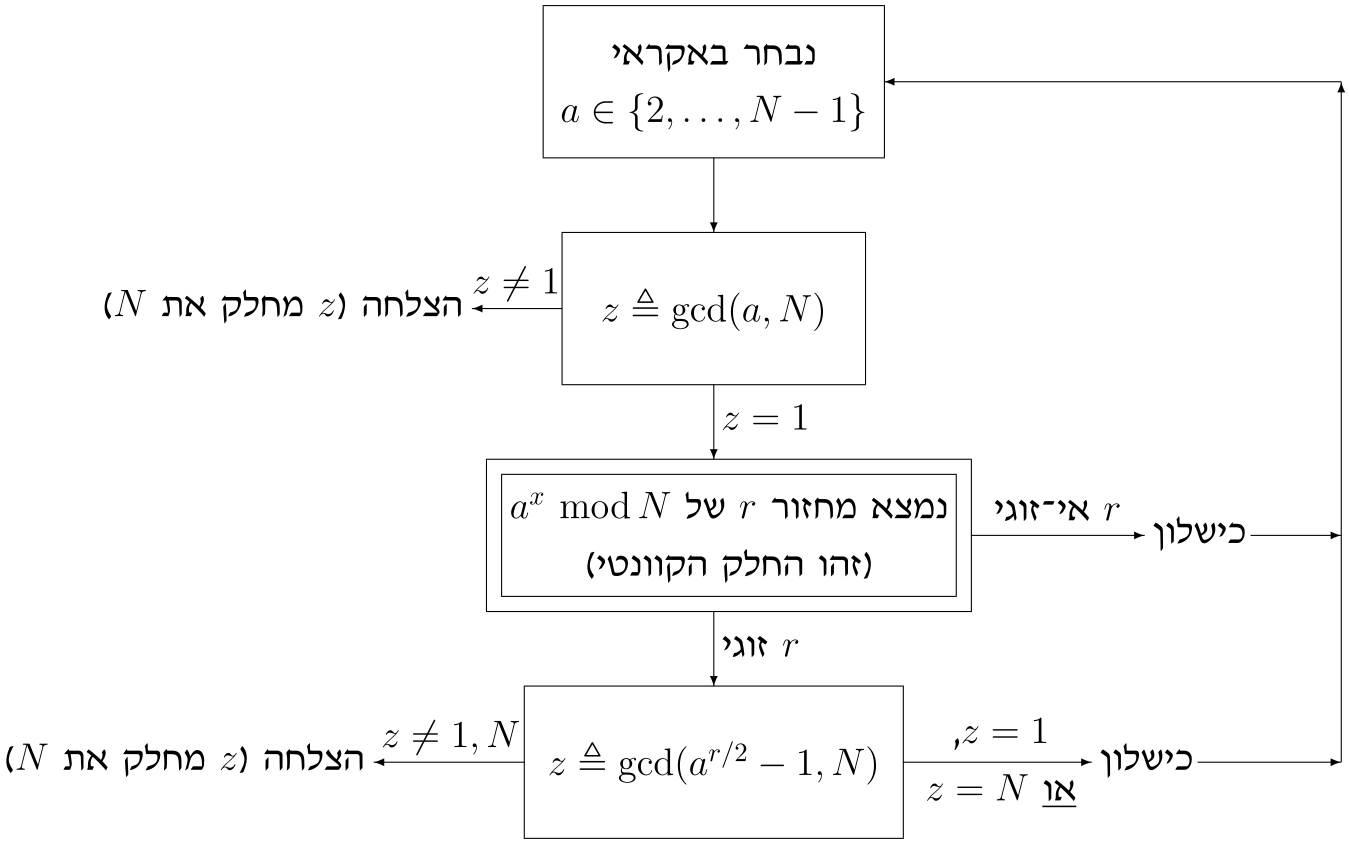
אלגוריתם הפירוק לגורמים של שור: מבט כללי

נתון מספר $N=PQ$ בן m ביטים, P ו־Q ראשוניים. המטרה: למצוא את P ואת Q.



מונחים נדרשים בתורת המספרים

בהינתן שני מספרים שלמים a ו־b:

- נאמר ש־a מחלק את b (ונסמן $a \mid b$) אם קיים מספר שלם c כך ש־$b = a \cdot c$.
- המחלק המשותף המקסימלי של a ו־b (המסומן $\gcd(a,b)$) הוא המספר השלם הגדול ביותר שמחלק את שניהם.
- a ו־b ייקראו זרים (co-prime) אם המחלק המשותף המקסימלי שלהם הוא 1.

כמו כן, בהינתן מספר טבעי k, חישוב מבוצע מודולו k (ומסומן $\bmod k$) אם לאחר ביצועו מחלקים ב־k עם שארית, ותוצאת החישוב היא השארית שהתקבלה.

תוצאות החישוב האפשריות הן: $\{0, 1, \ldots, k-1\}$

עקרונות האלגוריתם של שור

- המחזור (המינימלי) של $f(x) = a^x \bmod N$ נקרא <u>הסדר</u>, וכאשר הוא זוגי, לעיתים קרובות ניתן ללמוד ממנו את הגורמים של N.
- כמו האלגוריתמים הקודמים שלמדנו, גם חלקו הקוונטי של האלגוריתם של שור כולל שלושה מרכיבים:
  - יצירת סופרפוזיציה של כל ערכי x, בעזרת שערי הדמארד.
  - הפעלת הפונקציה $f(x)$ במקביל על כל ערכי x.
  - התאבכות בונה של הפתרונות הרצויים, הפעם לא על ידי הדמארד, אלא על ידי התמרת פורייה הקוונטית.

  תוצאת המדידה הקוונטית, שנקרא לה y, אינה הסדר של הפונקציה, אך כפי שנראה בהמשך, ניתן ללמוד ממנה את הסדר של הפונקציה.
- נשים לב שלחישוב $f(x) = a^x \bmod N$ קיים אלגוריתם קלאסי יעיל, ולכן אין כאן צורך באורקל. זה הופך את אלגוריתם הפירוק לגורמים לאלגוריתם שיעילותו הפולינומיאלית היא אמיתית.

ממציאת הסדר לפירוק לגורמים

כמעט תמיד a זר ל־N, ואז מתקיים: $a^r \equiv a^0 = 1 \bmod N$. לכן:

$$a^r - 1 = kN$$

מתוך ידיעת r, ואם r זוגי, לעיתים קרובות ניתן למצוא את הפירוק לגורמים של $N = PQ$.

נניח שהסדר r הוא זוגי. כיוון ש־$(b-1)(b+1) = b^2 - 1$, נקבל:

$$a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1) = kN = 0 \bmod N$$

בהכרח מתקיים $a^{r/2} - 1 \neq 0 \bmod N$, כי r הוא המחזור המינימלי, ולכן $r/2$ אינו מחזור.
כעת, עבור $a^{r/2} + 1$ ייתכנו שני מקרים:

- אם מתקיים $a^{r/2}+1 \equiv 0 \bmod N$, אז האלגוריתם נכשל (כי $a^{r/2}+1$ הוא כפולה של N, ואז החישוב $\gcd(a^{r/2} - 1, N)$ נותן 1), ולכן נתחיל את ריצת האלגוריתם מההתחלה.
- אם מתקיים $a^{r/2}+1 \neq 0 \bmod N$, אז האלגוריתם מצליח: שני הגורמים אינם כפולות של N, ולכן, כיוון שמתקיים $N = PQ$, מתקיים בהכרח $k_Q Q = a^{r/2}-1$ ו־$k_P P = a^{r/2}+1$. במקרה זה, חישוב $\gcd(a^{r/2} - 1, N)$ ייתן את אחד הגורמים של N (למשל, Q). כעת, כמובן, ניתן למצוא בקלות את הגורם השני ($P = \frac{N}{Q}$).

רכיבי האלגוריתם של שור

נחלק את הדיון באלגוריתם של שור לחלקים הבאים:

1. סקירת האלגוריתם לפירוק לגורמים.
2. חישוב קלאסי יעיל של הפונקציה $f(x) = a^x \bmod N$.
3. חישוב קוונטי פרקטי ויעיל של $f(x)$ הנ"ל, העובד גם עבור ערך בודד של x, וגם עבור סופרפוזיציה של x-ים.
4. אלגוריתם קוונטי יעיל למציאת מחזור (מינימלי) של פונקציה כללית $f(x)$.
האלגוריתם משתמש ב"התמרת פורייה קוונטית" (Quantum Fourier Transform, או בקיצור QFT) וב"שיטת השבר המשולב" (Continued Fraction Method, או CFM).
   (א) תיאור כללי של האלגוריתם הקוונטי.
   (ב) חישוב קוונטי יעיל של "התמרת פורייה קוונטית" (QFT).
   (ג) המדידה הקוונטית y והסדר r.
   (ד) יישום "שיטת השבר המשולב" (Continued Fraction Method) כדי למצוא, באופן קלאסי, את הסדר r מתוך המדידה הקוונטית y.

סקירת האלגוריתם לפירוק לגורמים (.1)

בחלק הקוונטי נסביר כיצד למצוא, בהסתברות גבוהה, את המחזור r של הפונקציה $f(x) = a^x \mod N$ (כאשר $1 < a < N$ זר ל-N).

כלומר, נמצא את המספר השלם r המינימלי, כך שמתקיים לכל J שלם:

$$a^{x+Jr} = a^x \mod N$$

מסיבה שתתבהר בהמשך (סעיף ד4, טענה a), בוחרים את n כך ש-$N^2 < 2^n < 2N^2$.
לכן הפונקציה $f(x) = a^x \mod N$ היא $f : \{0,1\}^n \to \{0,1\}^n$, ולמעשה $f : \{0,1\}^n \to \{0, \ldots, N-1\}$.

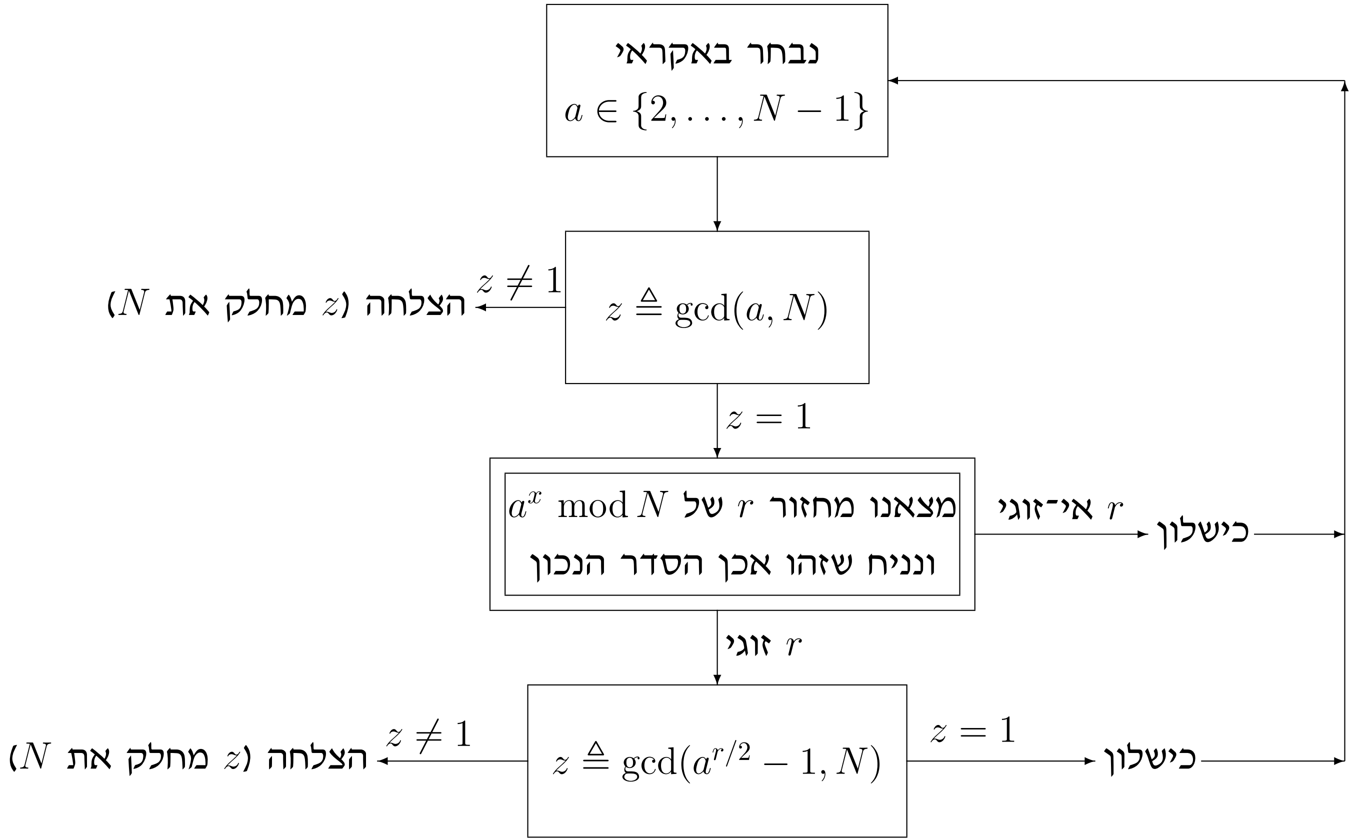
נוכיח שהפונקציה $f(x) = a^x \mod N$ היא אכן מחזורית, עם מחזור r המקיים $1 \le r < N$:
כיוון שיש בסך הכל $N-1$ מספרים מודולו N שאינם אפס (והם $1, \ldots, N-1$), נובע שלפחות אחד המספרים יצטרך להופיע יותר מפעם אחת ב-N החזקות הבאות (מודולו N):

$$a^0, a^1, a^2, \ldots, a^{N-1}$$

(0 לא יופיע כחזקה של a, כי a זר ל-N.)

במקרה של כישלון האלגוריתם, נפעיל אותו מחדש (שוב ושוב), עם מספרים אקראיים חדשים.
בהסתברות גבוהה, האלגוריתם יצליח כעבור מספר הפעלות.

נסביר את שלבי תרשים הזרימה, אבל הפעם עבור תרשים פיקטיבי — תחת ההנחה שהאלגוריתם הקוונטי למציאת הסדר תמיד מוצא את הסדר הנכון:



הסבר שלבי תרשים הזרימה:

מגרילים a באקראי ($1 < a < N$). קיים סיכוי (קטן באופן אקספוננציאלי) שהוא אינו זר ל־N. כדי לאתר מקרה זה, בודקים את ה־gcd: חישובו מבוצע ביעילות (על מחשב קלאסי) בעזרת האלגוריתם של אוקלידס.

(נשים לב שהמחלקים של $N = PQ$ הם בדיוק $1, P, Q, N$. לכן ה־gcd של כל מספר עם N הוא אחד המחלקים הללו. אם ה־gcd של מספר עם N שונה גם מ־1 וגם מ־N, אז מצאנו את אחד הגורמים P או Q, כפי שרצינו.)

אם a אינו זר ל־N, כלומר $\gcd(a, N) \neq 1$, אז מצאנו פירוק לגורמים של N, כי $\gcd(a, N) = P$ או $\gcd(a, N) = Q$. במקרה זה האלגוריתם מצליח בקלות.

אך לרוב a זר ל־N: כעת נוכל לחשב את המחזור r (על מחשב קוונטי), ואז מתקיים:

$$a^r \equiv a^0 = 1 \bmod N$$

לכן:

$$a^r - 1 = kN$$

מתוך ידיעת המחזור המינימלי (הנכון) r, ניתן (בהסתברות גבוהה מ־$\frac{1}{4}$) למצוא את הפירוק לגורמים של $N = PQ$.

ראינו שלבים אלו בפירוט בשקף 4, וכעת רק נחזור עליהם בקצרה, תוך ציון ההסתברויות.

בהסתברות גדולה מ־$\frac{1}{2}$, המחזור המתקבל r הוא זוגי, ונקבל:

$$kN = a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$$

בהכרח $a^{r/2} - 1 \neq 0 \bmod N$, ועבור $a^{r/2} + 1$ ייתכנו שני מקרים:

- בהסתברות קטנה מ־$\frac{1}{2}$ מתקיים $a^{r/2} + 1 \equiv 0 \bmod N$, ובמקרה זה האלגוריתם נכשל כי $\gcd(a^{r/2} - 1, N) = 1$.
- בהסתברות גדולה מ־$\frac{1}{2}$ מתקיים $a^{r/2} + 1 \neq 0 \bmod N$, ובמקרה זה האלגוריתם מצליח כי P מחלק את אחד מהם ואילו Q מחלק את השני, ופיקטרנו את N.

שאלה למחשבה: מה קורה בתרשים הזרימה אם האלגוריתם הקוונטי מצא r שגוי?

(2.) חישוב יעיל של הפונקציה $f(x) = a^x \bmod N$

לכל $x < 2^n$ ניתן לכתוב את הפיתוח הבינרי שלו:

$$x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \ldots + x_1 2^1 + x_0 2^0$$

ואז נקבל:

$$\begin{aligned} a^x \bmod N &= a^{x_{n-1}2^{n-1}} \cdots a^{x_1 2^1} a^{x_0 2^0} \bmod N \\ &= \left[a^{2^{n-1}}\right]^{x_{n-1}} \cdots \left[a^{2^1}\right]^{x_1} \left[a^{2^0}\right]^{x_0} \bmod N \end{aligned}$$

את $a \bmod N, a^2, \ldots, a^{2^j} \ldots$ קל לחשב ברקורסיה, באופן הבא:

$$a^{2^j} \bmod N = \left[a^{2^{j-1}}\right]^2 \bmod N$$

תוצאות אלה נותנות לנו אלגוריתם פשוט (קלאסי, וניתן למימוש קוונטי) לחישוב $a^x \bmod N$:
מחשבים את כל הערכים $a^{2^j} \bmod N$, וכופלים את החזקות המתאימות שלהם.

חישוב קוונטי יעיל ופרקטי של הפונקציה (.3)

$$f(x) = a^x \mod N$$

כיום ובעתיד הנראה לעין, אין טעם לחשב את החזקות של a על מחשב קוונטי, לכן אותן נחשב מראש, כלומר על מחשב קלאסי.

כעת, על מחשב קלאסי או קוונטי, נוכל להכניס כקלט את המספר 1, ואז נכפיל אותו בחזקה המתאימה כאשר הביט המתאים מהמספר x משמש כביט בקרה (קונטרול) לביצוע ההכפלה, וכך החל מהביט הראשון, ביט אחר ביט, ועד הביט האחרון.

המחשב הקוונטי יוכל לבצע זאת במקביל, לכל ערכי x, דבר שאותו המחשב הקלאסי כמובן אינו יודע לעשות.

תיאור האלגוריתם למציאת מחזור של פונקציה (א4.)

(גולת הכותרת של החישוב הקוונטי)

נניח שנתונה לנו פונקציה בעלת מחזור r, כלומר, פונקציה המקיימת לכל J שלם:

$$f(x + Jr) = f(x)$$

כך ש־r הוא המספר המינימלי המקיים תכונה זו.

מחשב קוונטי יודע למצוא ביעילות את המחזור r של הפונקציה. נלמד את האלגוריתם למציאת מחזור של פונקציה בעזרת השוואה לאלגוריתם של סיימון.

האלגוריתם עובד בתנאי שניתן לחשב את f ביעילות או שנתון אורקל לפונקציה. באלגוריתם של סיימון, היה נתון אורקל לפונקציה f; ואילו באלגוריתם של שור, הפונקציה היא:

$$f(x) = a^x \mod N$$

וכבר ראינו שהיא מחזורית ושהיא ניתנת לחישוב יעיל.

האלגוריתם משתמש בהתמרת פורייה הקוונטית (QFT), המוגדרת באופן הבא:

$$|x\rangle \overset{QFT}{\longrightarrow} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle$$

זוהי מעין הכללה של אופרטור הדמרד (למעשה, עבור $n = 1$ מקבלים בדיוק את אופרטור הדמרד), עבורו קיימת הנוסחה:

$$|x\rangle \overset{H}{\longrightarrow} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

ב־QFT, הפעולה במעריך היא כפל מספרים רגיל (ולא מכפלה סקלרית כמו בהדמרד).

באלגוריתם של שור, מספר ביטי הקלט והפלט של הפונקציה f, שיסומן ב־n, נבחר כך שמתקיים $N^2 < 2^n < 2N^2$. כלומר:

$$n = \lceil \log_2(N^2) \rceil$$

כמו כן, כפי שראינו קודם, המחזור r מקיים $1 \leq r < N$.

סיימון	שור
$f:\{0,1\}^n \to \{0,1\}^n \quad ; \quad f \text{ is } 2\ \textit{to}\ 1$	$f:\{0,1\}^n \to \{0,1\}^n \quad ; \quad f \text{ is } A\ \textit{to}\ 1$ [למעשה $f:\{0,1\}^n \to \{0,\ldots,N-1\}$]
$f(x)=f(y)$ אם ורק אם $y=x\oplus s$	$f(x_j)=f(x_0)$ אם ורק אם $x_j=x_0+jr$

$$|0\rangle_n|0\rangle_n \overset{H_n\otimes I_n}{\longrightarrow} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle \overset{f(x)}{\longrightarrow} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$$

כעת נמדוד את $f(x)$, נקבל ערך מסוים $f(x_0)$, ואז נותר מצב (מנורמל) של הרגיסטר השמאלי:

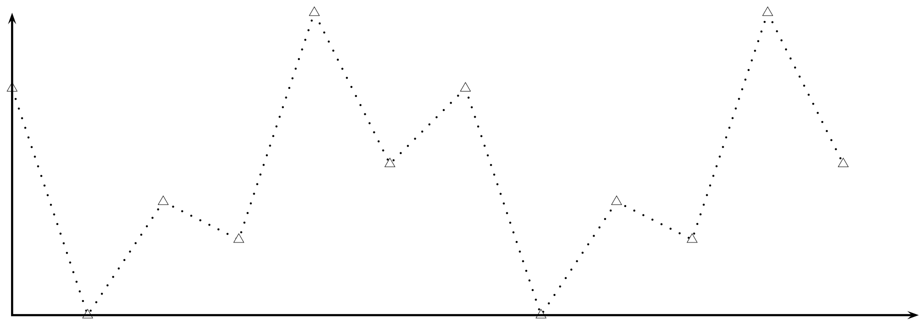
סיימון:

$$\frac{1}{\sqrt{2}}\left(|x_0\rangle+|x_0\oplus s\rangle\right) \overset{H}{\longrightarrow}$$
$$\frac{1}{\sqrt{2\cdot 2^n}}\sum_{y=0}^{2^n-1}\left[(-1)^{x_0\cdot y}+(-1)^{(x_0\oplus s)\cdot y}\right]|y\rangle$$
$$=\frac{1}{\sqrt{2\cdot 2^n}}\sum_{y=0}^{y=2^n-1}(-1)^{x_o\cdot y}\left[1+(-1)^{s\cdot y}\right]|y\rangle$$
$$=\frac{2}{\sqrt{2\cdot 2^n}}\sum_{\{y|s\cdot y=0\}}(-1)^{x_o\cdot y}|y\rangle$$

שור:

$$\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle \overset{QFT}{\longrightarrow}$$
$$\frac{1}{\sqrt{A\cdot 2^n}}\sum_{y=0}^{2^n-1}\left[\sum_{j=0}^{A-1}e^{\frac{2\pi i(x_0+jr)y}{2^n}}\right]|y\rangle$$
$$=\frac{1}{\sqrt{A\cdot 2^n}}\sum_{y=0}^{2^n-1}e^{\frac{2\pi i x_0 y}{2^n}}\left[\sum_{j=0}^{A-1}e^{\frac{2\pi i j r y}{2^n}}\right]|y\rangle$$
$$= \qquad ?$$

למעשה, המדידה של $f(x)$ פירושה שנשארים רק עם נקודות הנמצאות על אותו קו אופקי באיור:



נמדוד y. איזה y נקבל?

כדי למצוא את ההסתברויות של ערכי y השונים, נמצא מתי ההתאבכות בונה ומתי היא הורסת.

אם $ry = d2^n$ ($ry \equiv 0 \mod 2^n$), אז נקבל מה־j־ים התאבכות בונה לגמרי (כי כל המקדמים $e^{\frac{2\pi ijry}{2^n}}$ שווים ל־$e^{2\pi ijd} = 1$).

אם $ry = \left(d + \frac{1}{2}\right) 2^n$ (כלומר, $ry \equiv \frac{1}{2}2^n \mod 2^n$), אז נקבל התאבכות הורסת לגמרי (כי כל המקדמים $e^{\frac{2\pi ijry}{2^n}}$ שווים ל־$e^{2\pi ij\left(d+\frac{1}{2}\right)} = e^{\pi ij} = (-1)^j$).

עבור $-\frac{r}{2} \leq ry \mod 2^n \leq \frac{r}{2}$ נקבל התאבכות די בונה (כלומר, הסתברות די גבוהה לקבל ערך y המקיים את אי־השוויון: בתרגול יוסבר מדוע).

אחרת – נקבל התאבכות די הורסת (כלומר, הסתברות די נמוכה).

כל אחד מערכי y המקיימים $y \cdot s = 0$ יתקבל בהסתברות שווה.

חישוב קוונטי יעיל של QFT (ב4.)

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi ixy}{2^n}} |y\rangle$$

צריך מטריצה $2^n \times 2^n$ (שגדולה מ־$N^2 \times N^2$) כדי לייצג את QFT, ובאופן נאיבי צריך $O(2^{2n})$ פעולות כדי לבצע חישוב של QFT עבור מצב כללי כלשהו.

נוכל לממש להלן אלגוריתם קוונטי יעיל, אם נכתוב את x ו־y כמספרים בינריים:

$$x: \quad x_{n-1}x_{n-2}x_{n-3}\ldots x_1x_0$$

$$y: \quad y_{n-1}y_{n-2}y_{n-3}\ldots y_1y_0$$

(כאשר $x_i \in \{0,1\}$.)

לפי הפיתוח הבינרי, נוכל לכתוב את x ו־y כסכום חזקות של 2^i:

$$\begin{aligned} x &= x_{n-1}\cdot 2^{n-1} + x_{n-2}\cdot 2^{n-2} + x_{n-3}\cdot 2^{n-3} + \ldots + x_1\cdot 2^1 + x_0 \\ y &= y_{n-1}\cdot 2^{n-1} + y_{n-2}\cdot 2^{n-2} + y_{n-3}\cdot 2^{n-3} + \ldots + y_1\cdot 2^1 + y_0 \end{aligned}$$

$$
\begin{aligned}
x &= x_{n-1} \cdot 2^{n-1} + x_{n-2} \cdot 2^{n-2} + x_{n-3} \cdot 2^{n-3} + \ldots + x_1 \cdot 2^1 + x_0 \\
y &= y_{n-1} \cdot 2^{n-1} + y_{n-2} \cdot 2^{n-2} + y_{n-3} \cdot 2^{n-3} + \ldots + y_1 \cdot 2^1 + y_0
\end{aligned}
$$

בגלל המחזוריות ב־2^n, ניתן להתחשב רק בחלק השבר של $\frac{xy}{2^n}$, כלומר, ב־$\frac{xy \mod 2^n}{2^n}$:

$$
\begin{aligned}
\frac{xy \mod 2^n}{2^n} = \mathrm{frac}\left(\frac{xy}{2^n}\right) &= y_{n-1}(0.x_0) + y_{n-2}(0.x_1x_0) + y_{n-3}(0.x_2x_1x_0) + \\
&\ldots + y_1(0.x_{n-2}x_{n-3}\ldots x_0) + y_0(0.x_{n-1}\ldots x_0)
\end{aligned}
$$

לכן נוכל להציג את המקדם $e^{\frac{2\pi ixy}{2^n}}$ באופן הבא:

$$
e^{\frac{2\pi ixy}{2^n}} = e^{2\pi i\cdot\frac{xy \mod 2^n}{2^n}} = e^{y_{n-1}\cdot 2\pi i(0.x_0)} e^{y_{n-2}\cdot 2\pi i(0.x_1x_0)} \cdots e^{y_0\cdot 2\pi i(0.x_{n-1}\ldots x_0)}
$$

ומכאן נובע שנוכל להציג את פעולת QFT באמצעות הנוסחה הבאה:

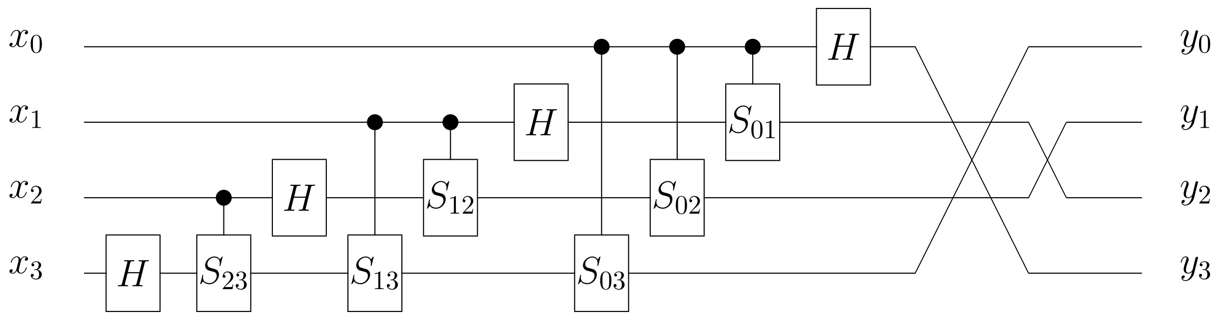
נשים לב שווקטור $|x\rangle$
עובר למצב שאינו שזור
אך תלוי בהרבה ביטים

$$
\begin{aligned}
|x\rangle \;\rightarrow\; & \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi ixy}{2^n}} |y\rangle \\
= \; & \frac{1}{\sqrt{2^n}} \left[|0\rangle + e^{2\pi i(0.x_0)}|1\rangle\right] \otimes \left[|0\rangle + e^{2\pi i(0.x_1x_0)}|1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{2\pi i(0.x_{n-1}\ldots x_1x_0)}|1\rangle\right]
\end{aligned}
$$

מעגל לביצוע QFT

נבחין ששער הדמרד מבצע $H|x_k\rangle = \frac{1}{\sqrt{2}}[|0\rangle + e^{2\pi i(0.x_k)}|1\rangle]$ (זכרו: $0.1 = \frac{1}{2}$ בכתיב בינרי)

ונגדיר שער פאזה $S_{jk} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2^{k-j}} \end{pmatrix}$. אז המעגל הבא מממש QFT ביעילות:



בסך הכל נדרשים $O(n^2) = \frac{n(n+1)}{2}$ שערים. המעגל מממש, עבור $n = 4$:

$$|x\rangle \;\rightarrow\; \frac{1}{\sqrt{2^4}}\left[|0\rangle + e^{2\pi i(0.x_0)}|1\rangle\right] \otimes \left[|0\rangle + e^{2\pi i(0.x_1x_0)}|1\rangle\right]$$
$$\otimes\left[|0\rangle + e^{2\pi i(0.x_2x_1x_0)}|1\rangle\right] \otimes \left[|0\rangle + e^{2\pi i(0.x_3x_2x_1x_0)}|1\rangle\right]$$

ג4.) המדידה הקוונטית y והסדר r

באלגוריתם הקוונטי מדדנו, בסיכוי גבוה, ערך y המקיים $-\frac{r}{2} \leq ry \bmod 2^n \leq \frac{r}{2}$.

נרשום $ry = d2^n + w$, ואז $ry \bmod 2^n = w = ry - d2^n$, ונקבל:

$$-\frac{r}{2} \leq ry - d2^n \leq \frac{r}{2}$$

נחלק ב־$r \cdot 2^n$, ונקבל:

$$-\frac{1}{2 \cdot 2^n} \leq \frac{y}{2^n} - \frac{d}{r} \leq \frac{1}{2 \cdot 2^n}$$

מתוך ידיעת y ו־2^n ניתן למצוא את $\frac{d}{r}$ (כלומר, גם את d וגם את r) ע"י **עיגול**, בשיטת השבר המשולב (Continued Fraction Method, או בקיצור CFM).

המטרה היא לעגל את השבר הרציונלי $\frac{y}{2^n}$ ל־$\frac{d}{r}$, לכן נדרוש שהמכנה יהיה קטן מ־N (כי נזכור $1 \leq r < N$) וכן נדרוש שיתקיים אי־השוויון $-\frac{1}{2 \cdot 2^n} \leq \frac{y}{2^n} - \frac{d}{r} \leq \frac{1}{2 \cdot 2^n}$.

נזכור שמתקיים $2^n > N^2$: זה אומר שאנחנו מקטינים את מספר הספרות במכנה לפחות פי 2 במהלך העיגול.

(ד4.) יישום "שיטת השבר המשולב" למציאת המחזור

להלן נוכיח את שלוש הטענות הבאות:

a. קיים שבר יחיד $\frac{d}{r}$ בעל מכנה $1 \le r < N$ המקיים את אי־השוויון:

$$-\frac{1}{2 \cdot 2^n} \le \frac{y}{2^n} - \frac{d}{r} \le \frac{1}{2 \cdot 2^n}$$

b. קיים אלגוריתם יעיל למציאת השבר (שיטת השבר המשולב).

c. ההסתברות שאכן ה־y שקיבלנו עונה לאי־השוויון הנ"ל היא:

$$\mathrm{Prob}(y) \gtrsim \frac{4}{\pi^2} > 0.4 \quad \text{(יוכח בתרגול)}$$

ואם y אכן עונה לאי־השוויון הנ"ל, ההסתברות שנצליח למצוא את r היא:

$$\frac{\phi(r)}{r} = \frac{\text{constant}}{\log \log r}$$

(כאשר ההגדרה של פונקציית אוילר $\phi(r)$ היא כמות המספרים הטבעיים הקטנים מ־r וזרים לו.)

לכן, אם נחזור על האלגוריתם מספיק פעמים, נקבל y בתחום הנכון, ונקבל ממנו את r ואת d.

(.a) נראה ש־$\frac{d}{r}$ הוא השבר היחיד בעל מכנה $1 \le r < N$ המקיים את אי־השוויון:

$$-\frac{1}{2\cdot 2^n} \le \frac{y}{2^n} - \frac{d}{r} \le \frac{1}{2\cdot 2^n}$$

נניח בשלילה שקיימים שני פתרונות שונים $\frac{d}{r}$, $\frac{d'}{r'}$ בעלי מכנים $1 \le r < N$ ו־$1 \le r' < N$ המקיימים שניהם את אי־השוויון. אזי:

$$\left|\frac{dr' - d'r}{rr'}\right| = \left|\frac{d}{r} - \frac{d'}{r'}\right| \le \left|\frac{d}{r} - \frac{y}{2^n}\right| + \left|\frac{y}{2^n} - \frac{d'}{r'}\right| \le \frac{1}{2\cdot 2^n} + \frac{1}{2\cdot 2^n} = \frac{1}{2^n}$$

לכן $\left|\frac{dr'-d'r}{rr'}\right| \le \frac{1}{2^n}$. אבל $r, r' < N$, והמונה $dr' - d'r$ שונה מאפס (כי $\frac{d}{r} \neq \frac{d'}{r'}$), לכן $\frac{|dr'-d'r|}{rr'} \ge \frac{1}{rr'} > \frac{1}{N^2} > \frac{1}{2^n}$, וזוהי סתירה. לכן $\frac{d}{r}$ הוא השבר היחיד המקיים את שני התנאים הנדרשים.

להזכירכם, אי השיוויון $\frac{1}{N^2} > \frac{1}{2^n}$ נובע ישירות מהבחירה של n:

$$N^2 < 2^n$$

לכן בחירה זו חשובה לאלגוריתם.

אנו בוחרים את ה־n הקטן ביותר האפשרי שעדיין מקיים את אי־השוויון $N^2 < 2^n$:
כלומר, אנו בוחרים $n = \left\lceil \log_2(N^2) \right\rceil$. זו הסיבה לדרישה השנייה, $2^n < 2N^2$.

b.) האלגוריתם למציאת השבר (CFM) (לא נדון כאן ביעילותו):

$$\frac{5}{11}=\frac{1}{11/5}=\frac{1}{2+\frac{1}{5}}\equiv[2,5]\overset{\text{עיגול}}{\rightsquigarrow}[2]=\frac{1}{2}$$

$$\frac{5}{12}=\frac{1}{12/5}=\frac{1}{2+\frac{2}{5}}=\frac{1}{2+\frac{1}{5/2}}=\frac{1}{2+\frac{1}{2+\frac{1}{2}}}\equiv[2,2,2]\rightsquigarrow[2,2]=\frac{1}{2+\frac{1}{2}}=\frac{2}{5}$$

בצד שמאל מבצעים פיתוח של השבר הפשוט לשבר משולב. התהליך מסתיים כאשר המונה של השבר האחרון הוא 1.

בצד ימין משמיטים כמה מהמספרים האחרונים במכנה שבפיתוח, וכך מבצעים עיגול לשבר קרוב בעל מונה ומכנה קטנים יותר. באופן הזה נוכל למצוא שבר $\frac{d}{r}$ שמקיים את שני התנאים הדרושים ($1\le r<N$ ו־$\left|\frac{y}{2^n}-\frac{d}{r}\right|\le\frac{1}{2\cdot2^n}$). כיוון שהוכחנו ששבר זה הוא יחיד, אנו יכולים למצוא באופן הזה את השבר הדרוש.

כל עוד משמיטים פחות מדי מספרים, נשארים עם מכנה גדול מדי $r>N$; ואם משמיטים יותר מדי מספרים, מקבלים שבר $\frac{d}{r}$ רחוק מדי, $\left|\frac{y}{2^n}-\frac{d}{r}\right|>\frac{1}{2\cdot2^n}$.

(c.) ההסתברות שמתוך y העונה לאי־שוויון נקבל את r היא $\frac{\phi(r)}{r}$. נסביר זאת:
מצאנו את השבר הפשוט $\frac{d}{r}$, כלומר, את המונה והמכנה:

- אם $\gcd(d,r)=1$, אז המונה והמכנה הם d ו־r, ובפרט מצאנו את r.
- ואולם, אם $\gcd(d,r)=k\neq 1$, אז נוכל לסמן $r=kr_1$ ו־$d=kd_1$, ואז שיטת ה"עיגול" תיתן לנו את השבר המצומצם $\frac{d_1}{r_1}$ (השווה ל־$\frac{d}{r}$), ולכן נקבל את המחלק r_1 של r. במקרה זה האלגוריתם נכשל, ונצטרך לבחור ערכים אקראיים חדשים ולנסות שוב.

המחזור r קבוע (נובע מבחירת a). לעומת זאת, d הוא אקראי־למדי, כי הוא נובע ממדידת y. לכן ההסתברות ש־$\gcd(d,r)=1$ נתונה ע"י $\frac{\phi(r)}{r}$. במקרה זה, שהסתברותו גבוהה למדי, אכן נצליח למצוא את r.

למידע נוסף על האלגוריתם מומלץ לקרוא את פרקים 6.9 ו־6.10 אצל פרסקיל
`http://www.theory.caltech.edu/people/preskill/ph229/notes/chap6.ps`.