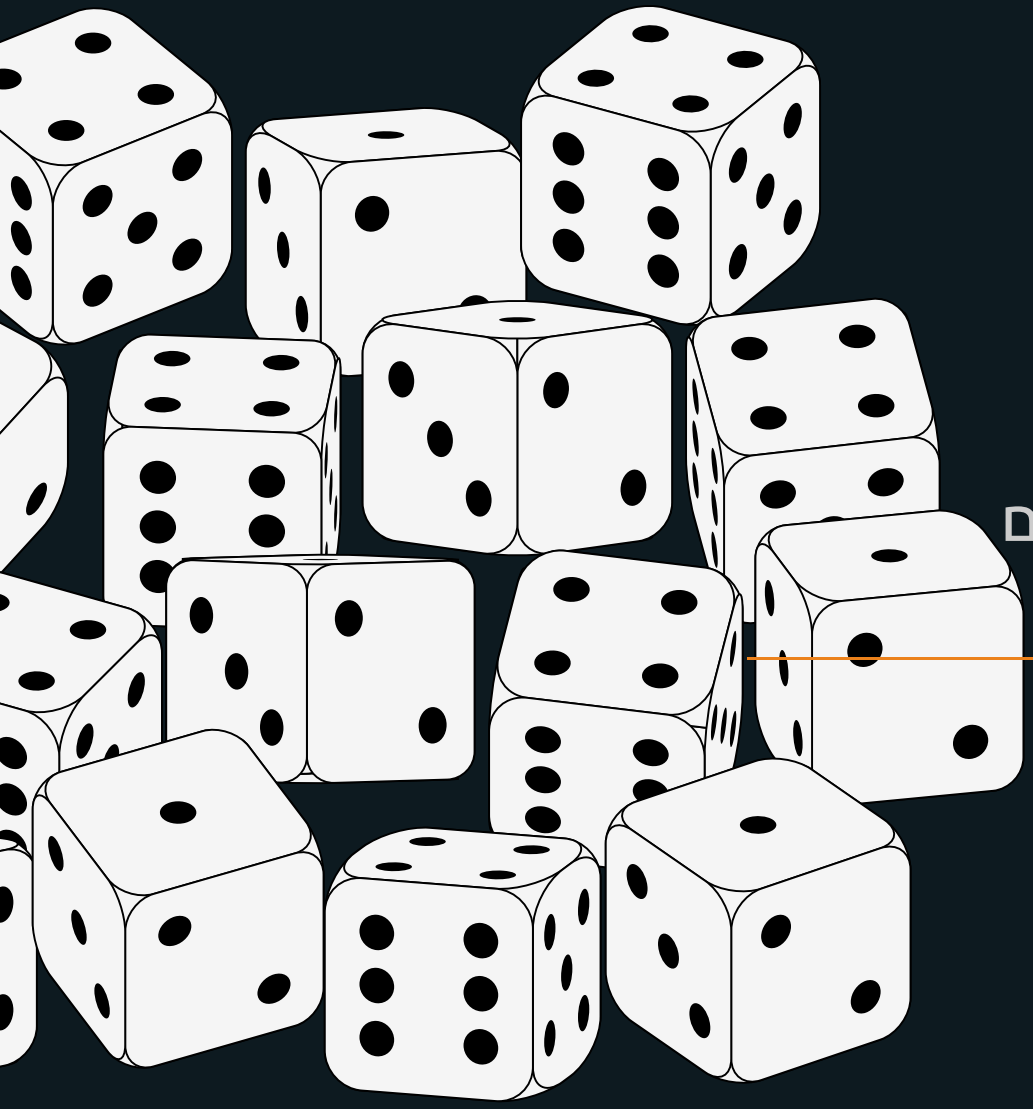


תרגול 5 - דגימה 2

שיטת הקבלה-דחייה
ומחוללי מספרים פסאודו-אקראיים

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

על סדר היום

מוטיבציה - איך מחשב דטרמיניסטי מייצר אקראיות?

מחוללים פסאודו-אקראיים

Linear Congruential Generator - LCG

Linear Feedback Shift Register - LFSR

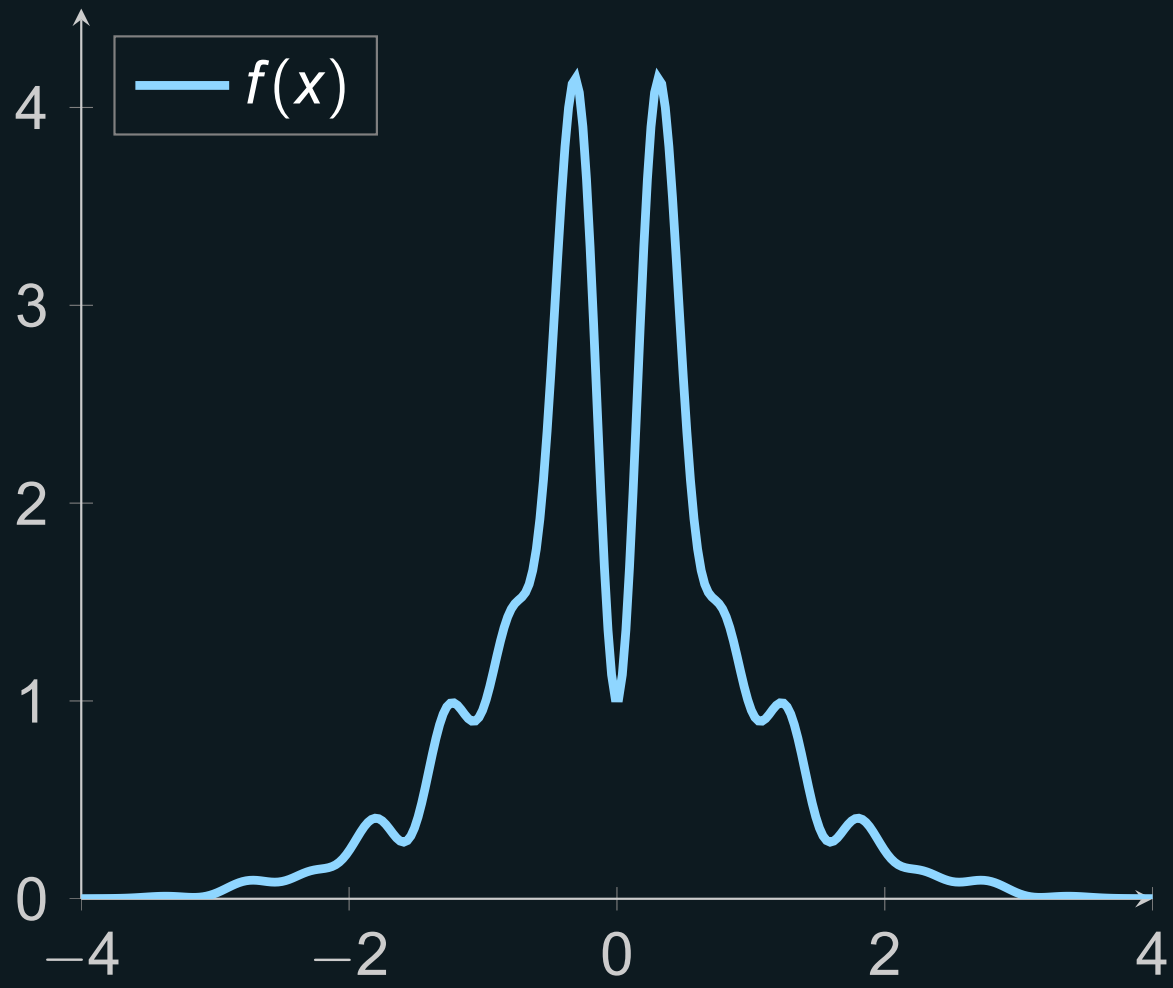
מעבר מביטים אקראיים למספר ב-$[0, 1]$

קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$

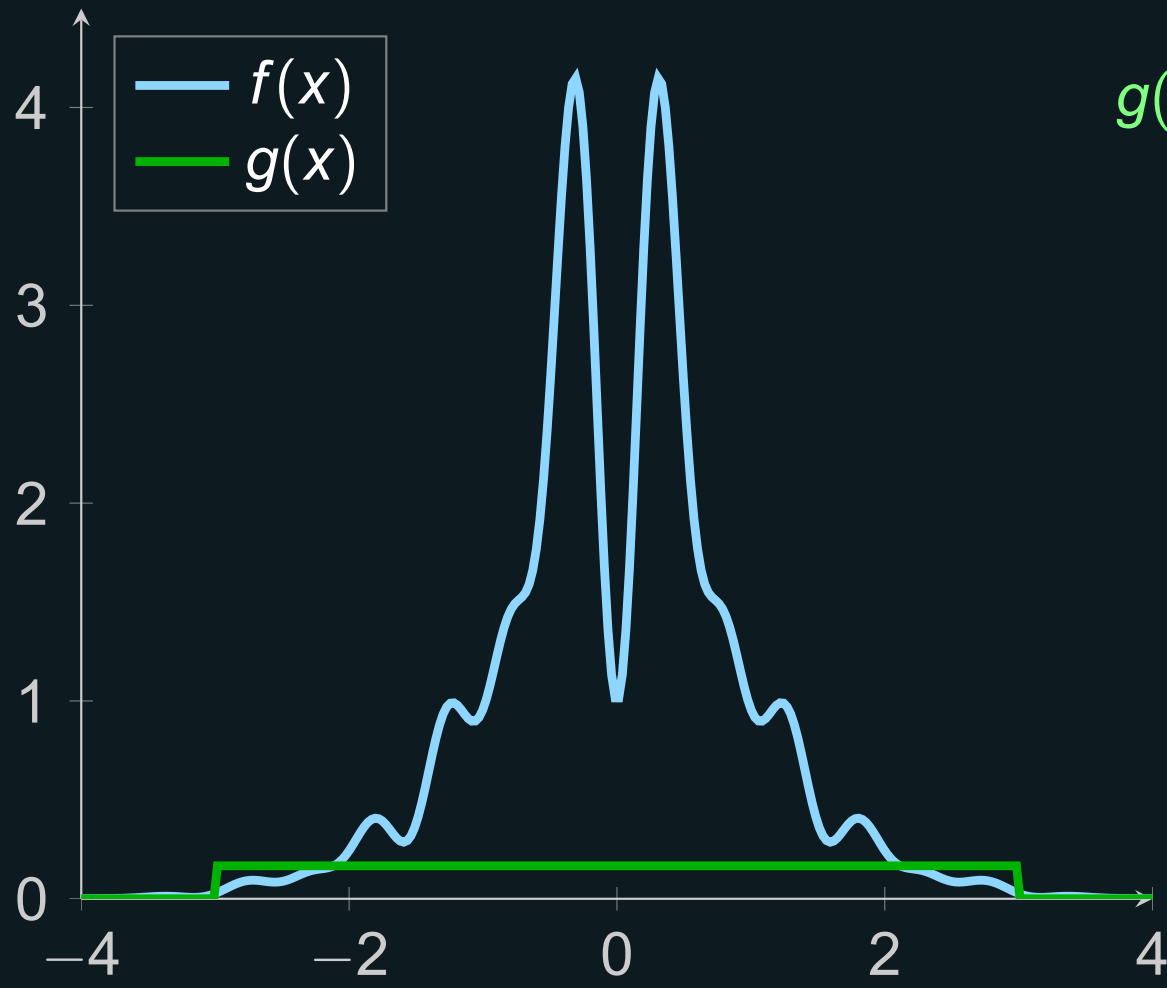
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



קבלה-דחייה

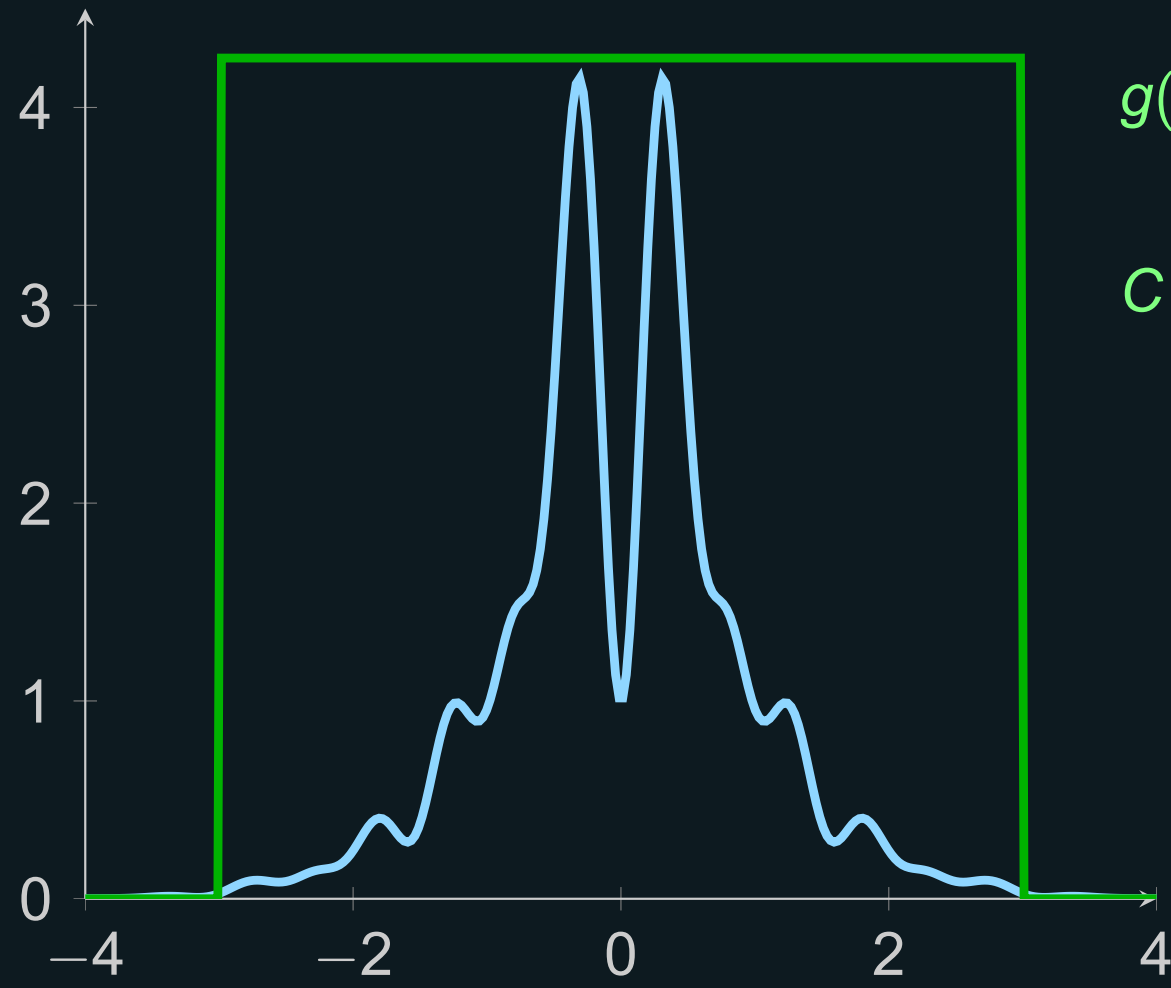
$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



$g(x) \sim U(-3, 3)$

קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$

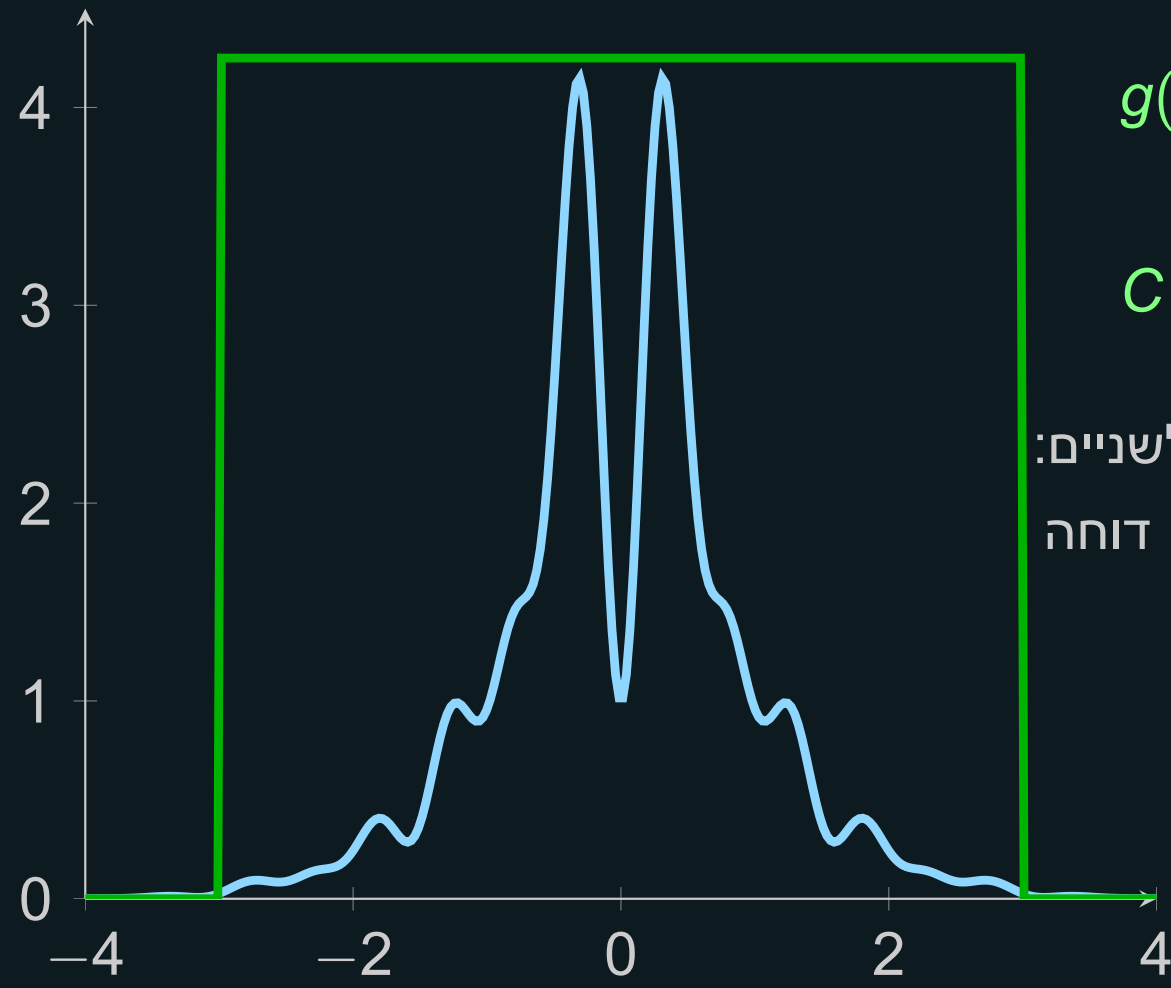


$g(x) \sim U(-3, 3)$

$C \cdot g(x) \geq f(x)$

קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



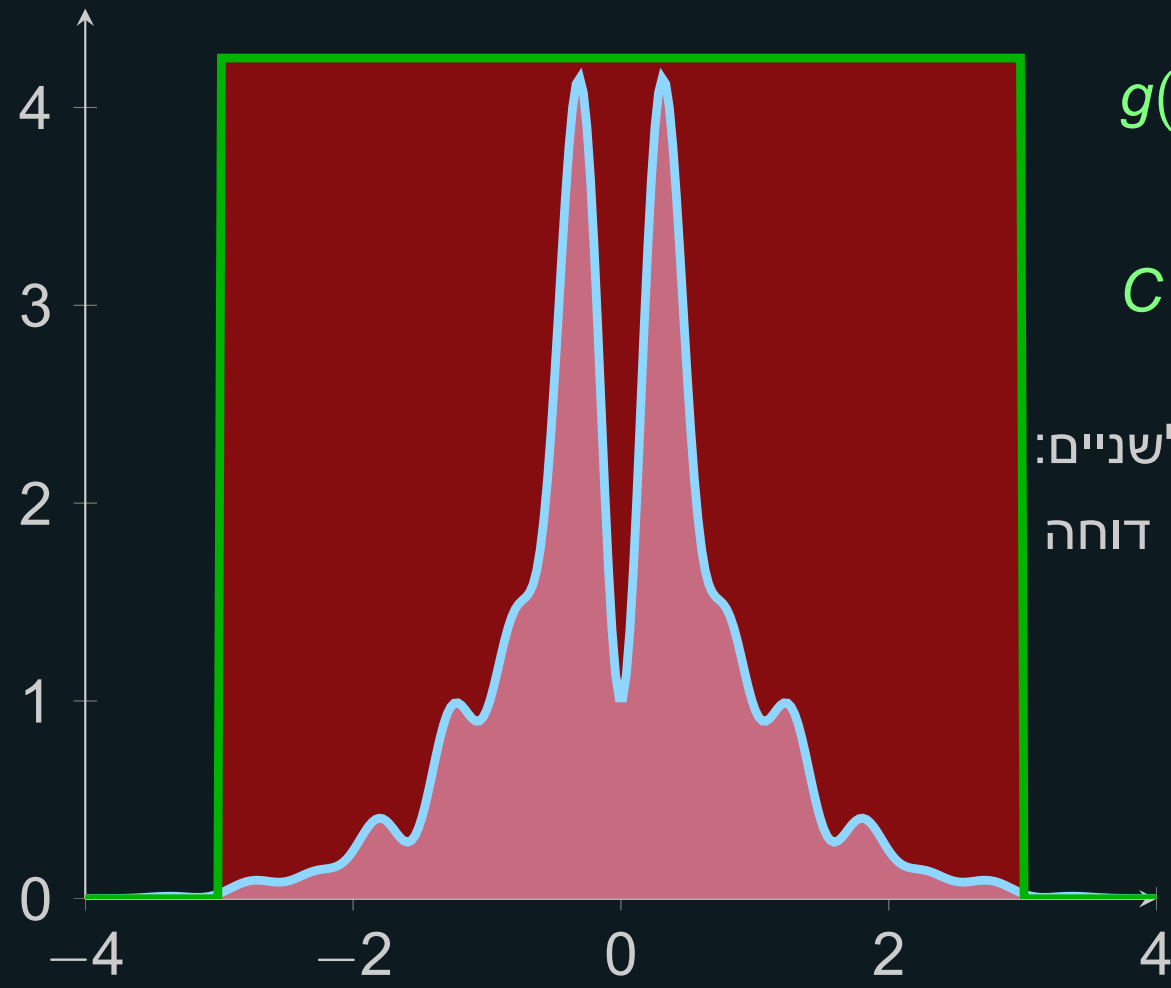
$g(x) \sim U(-3, 3)$

$C \cdot g(x) \geq f(x)$

נחלק את התחום לשניים:
תחום מקבל ותחום דוחה

קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



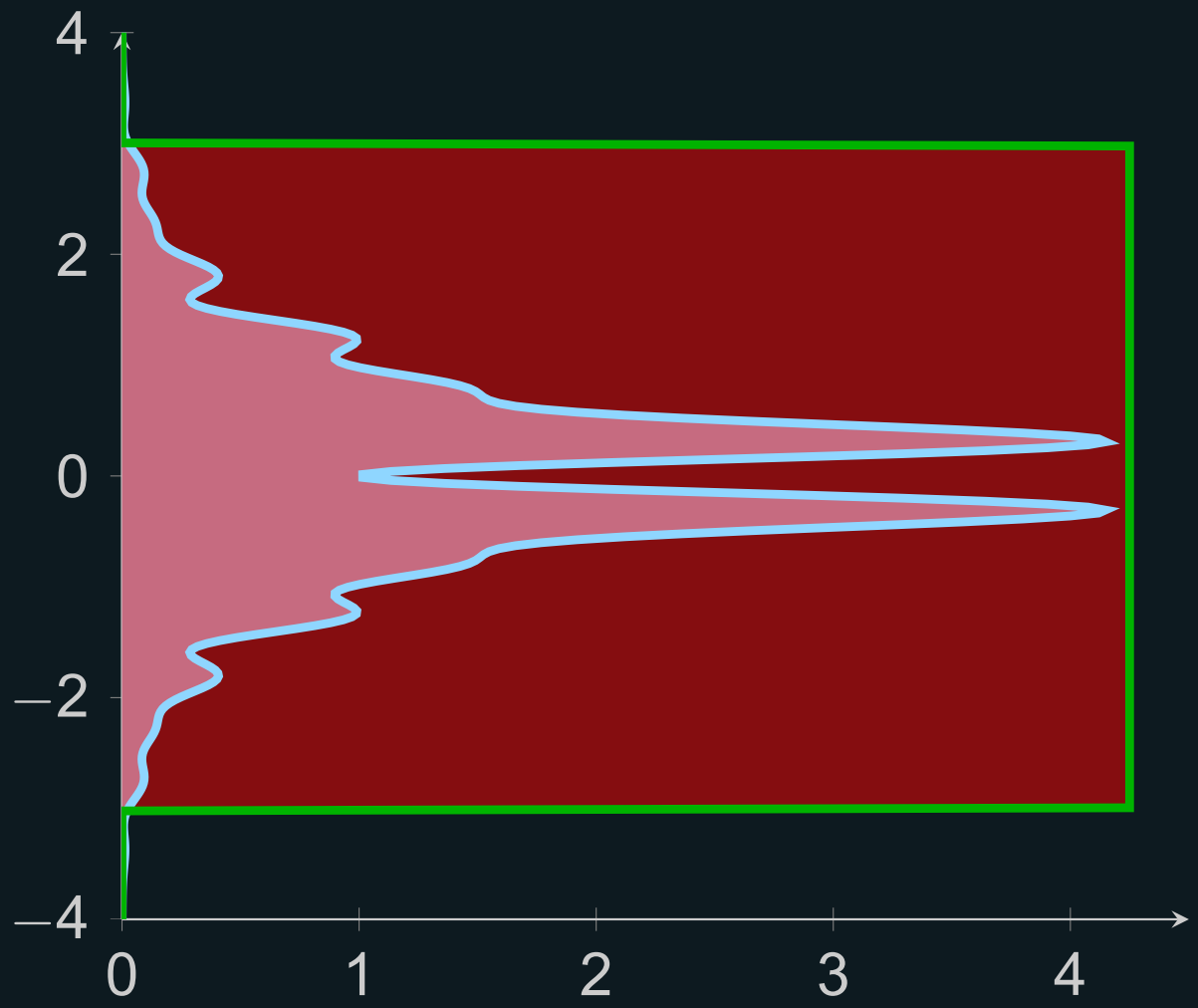
$g(x) \sim U(-3, 3)$

$C \cdot g(x) \geq f(x)$

נחלק את התחום לשניים:
תחום מקבל ותחום דוחה

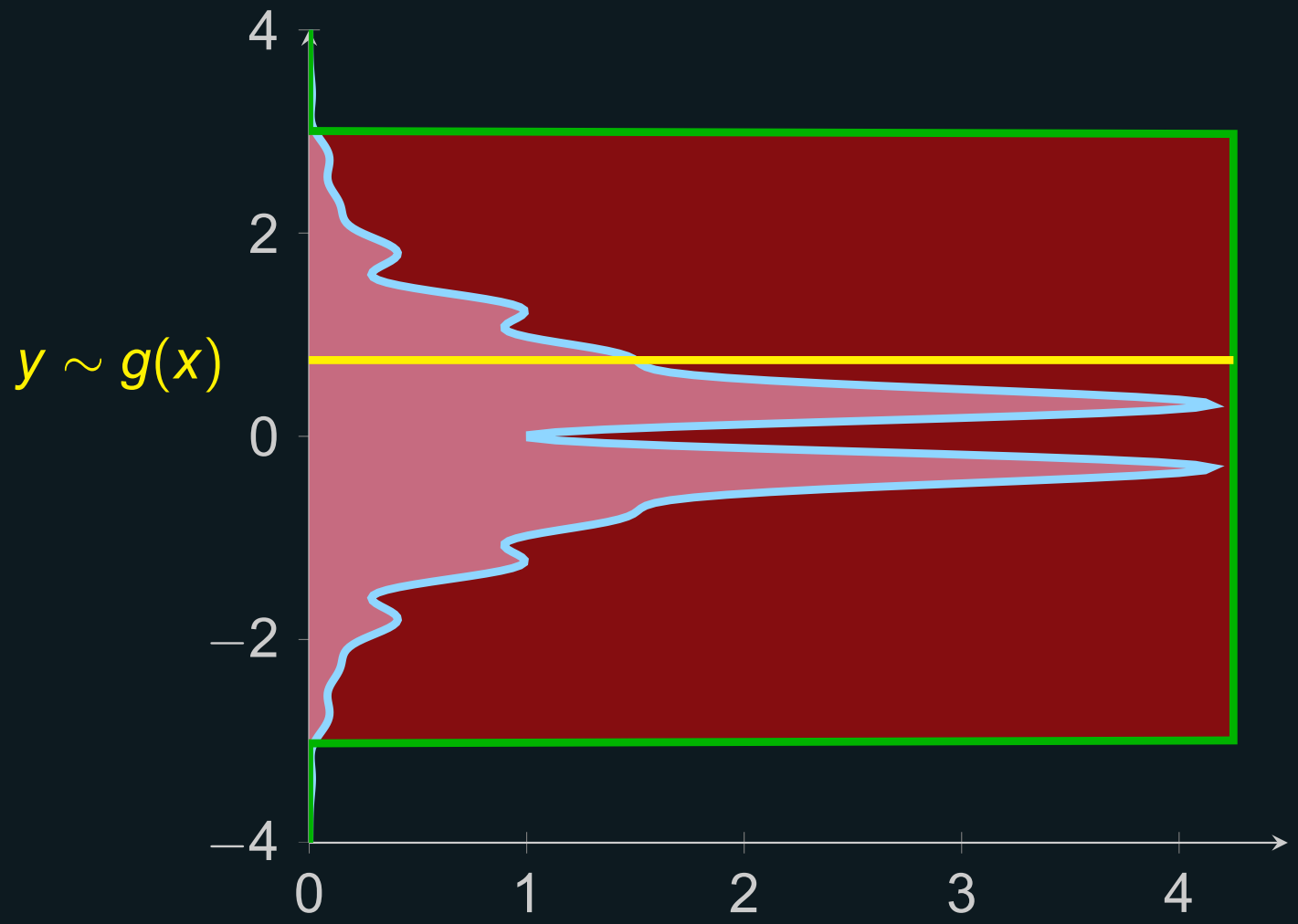
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



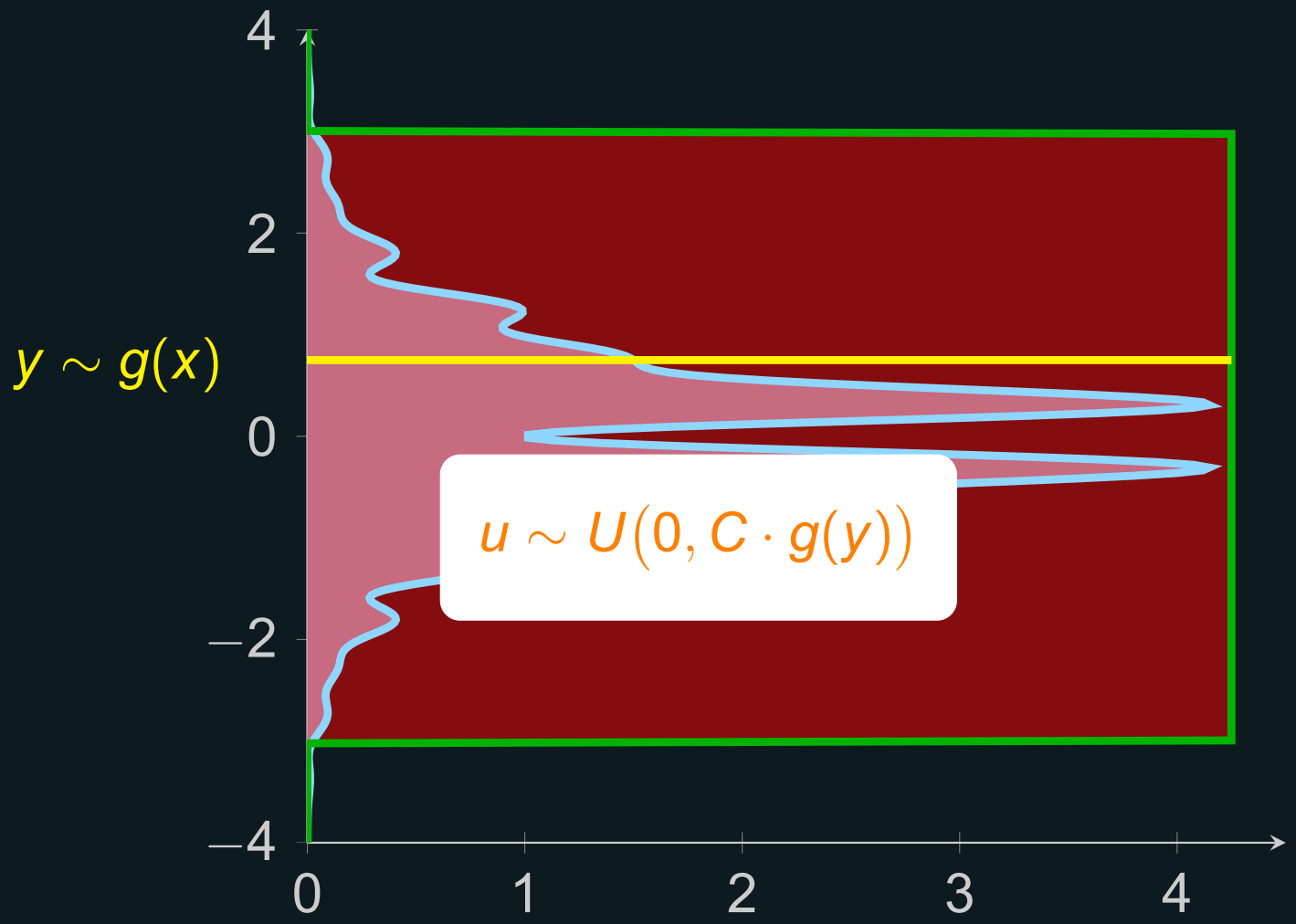
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



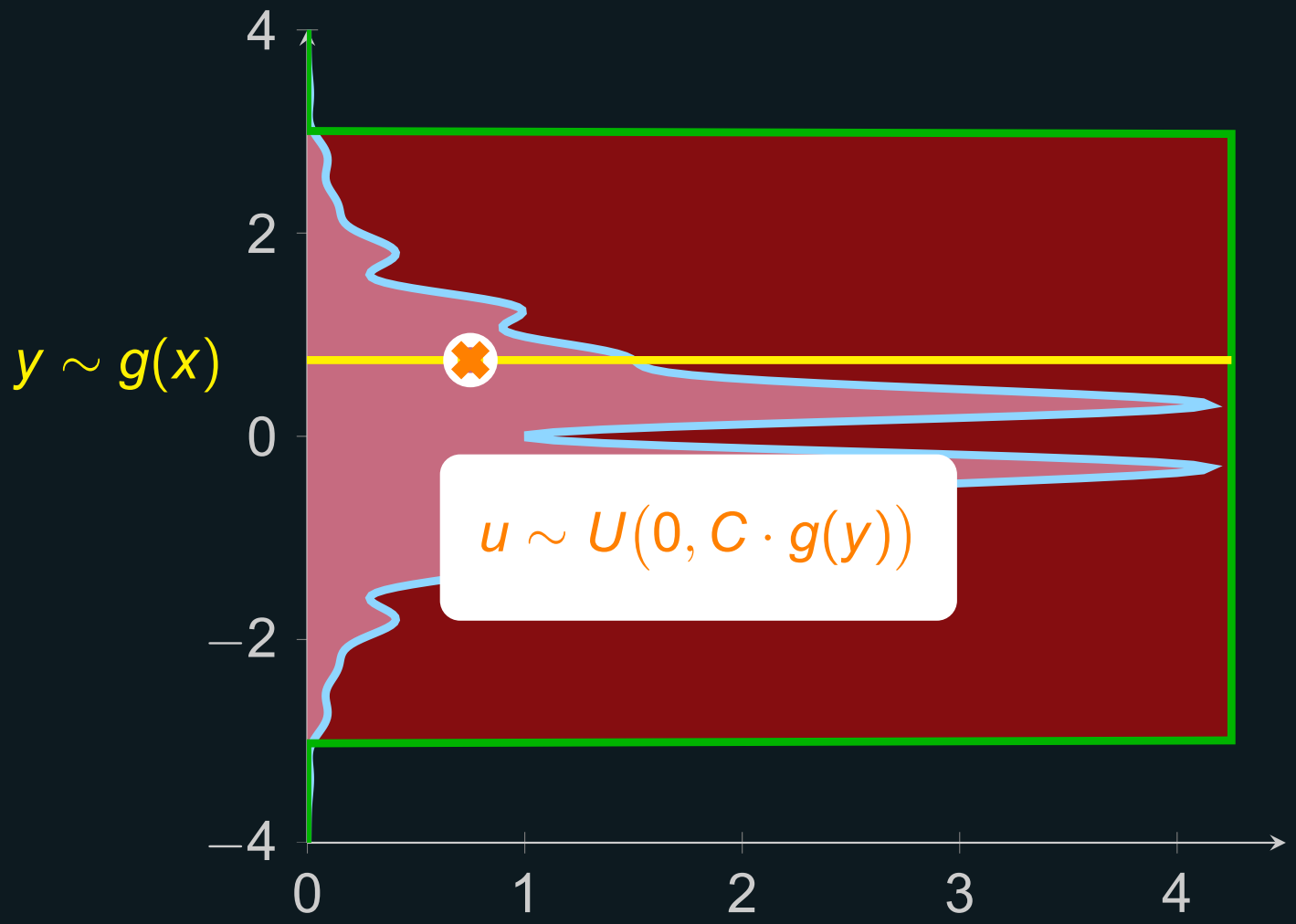
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



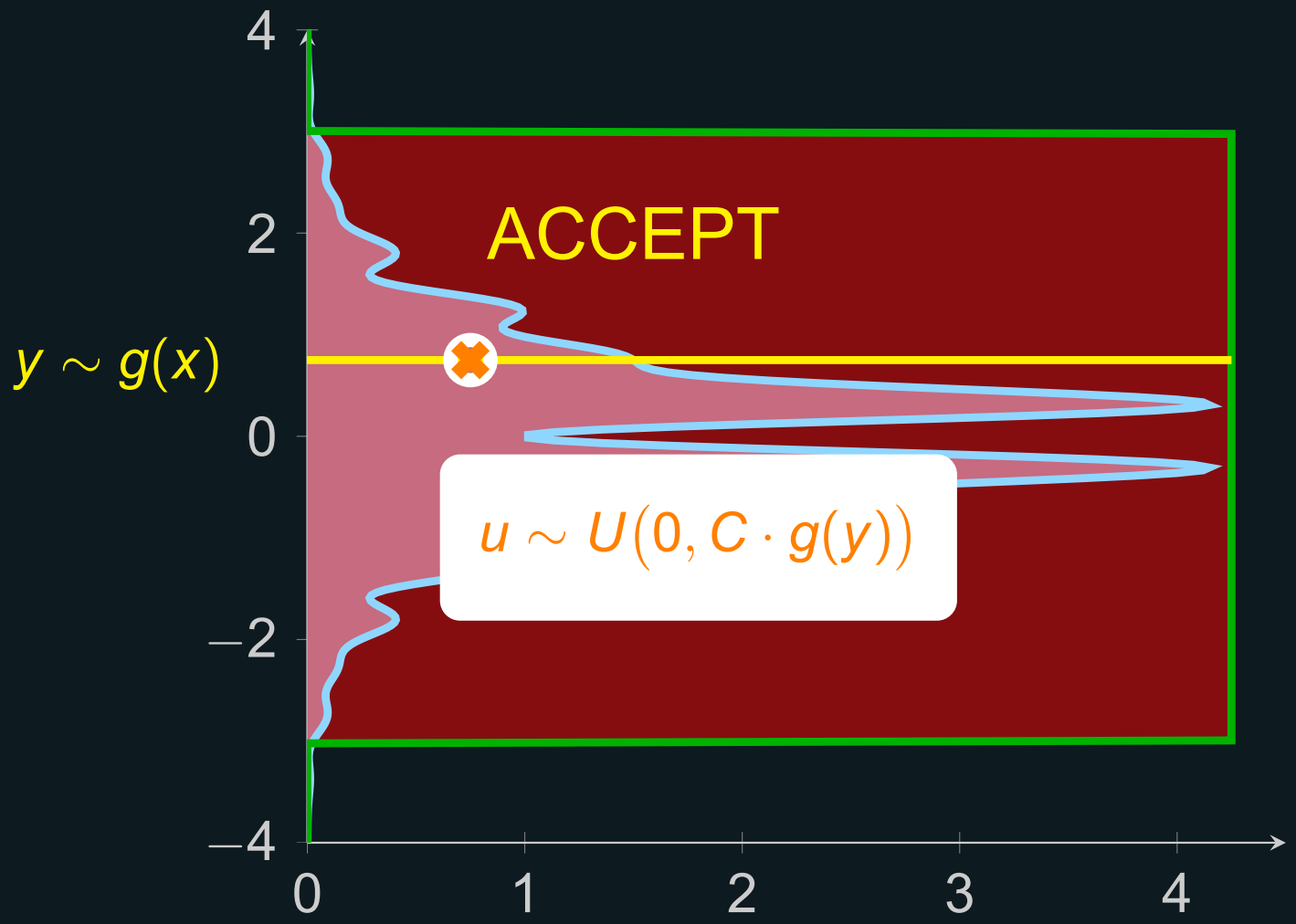
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



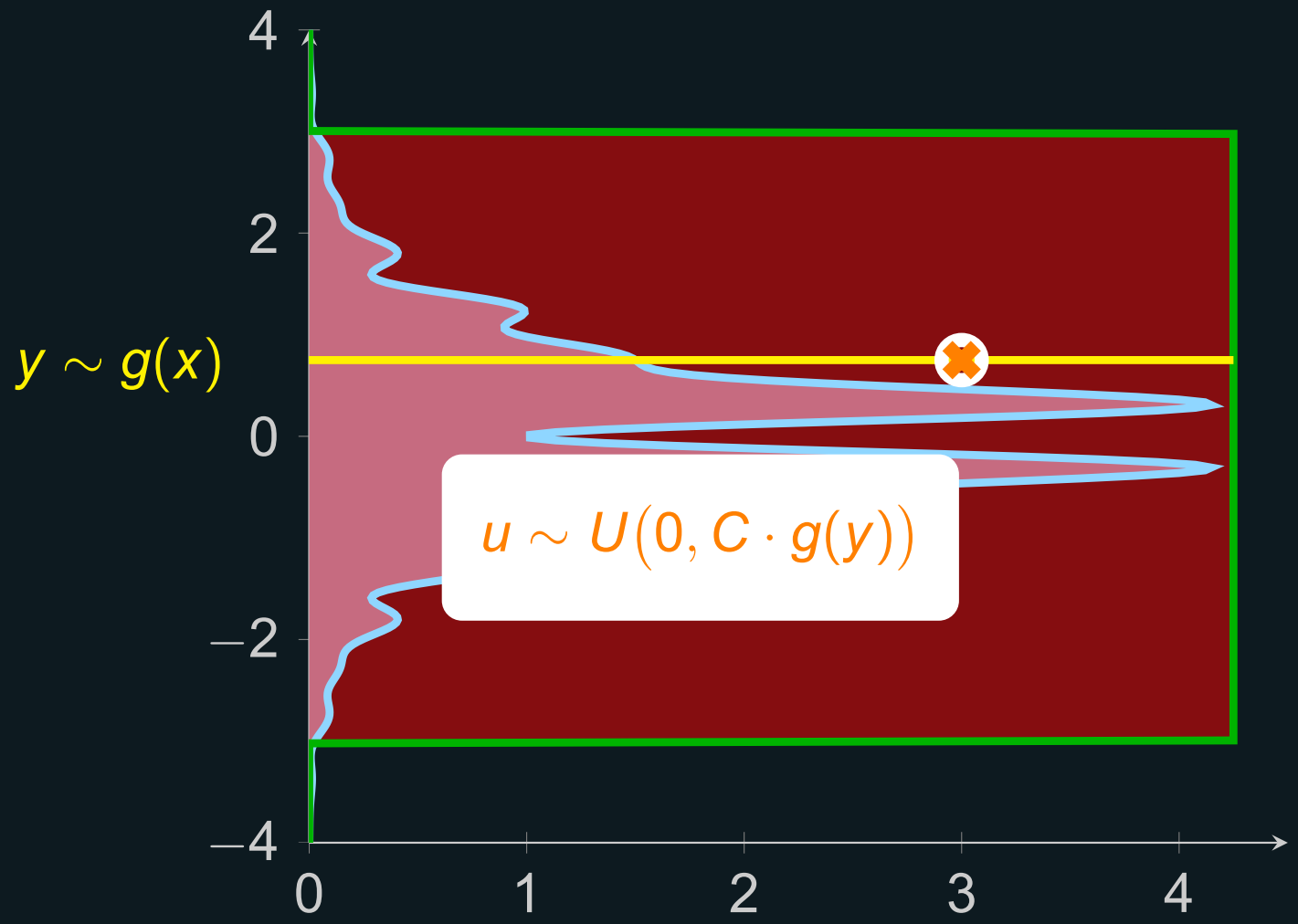
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



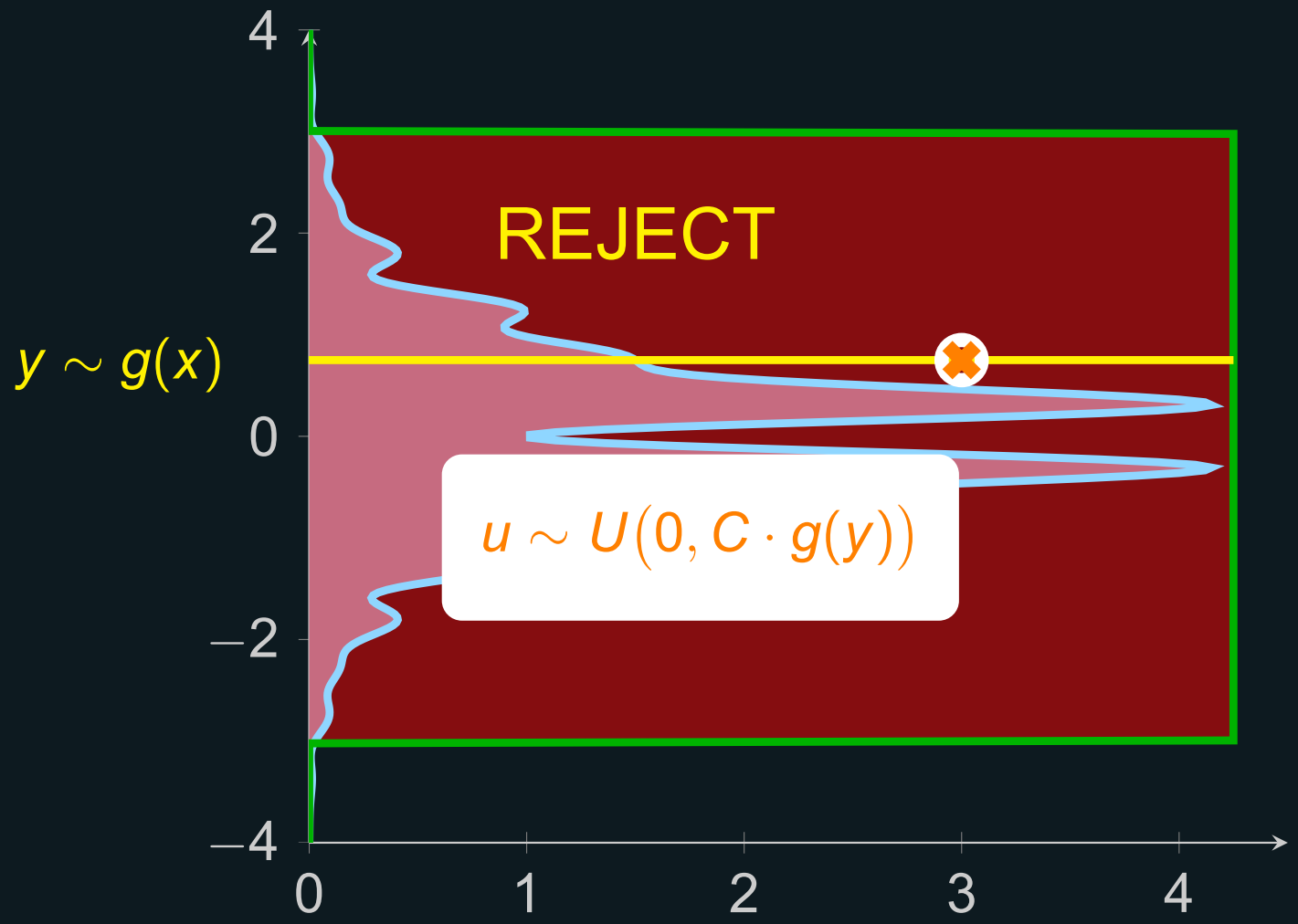
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



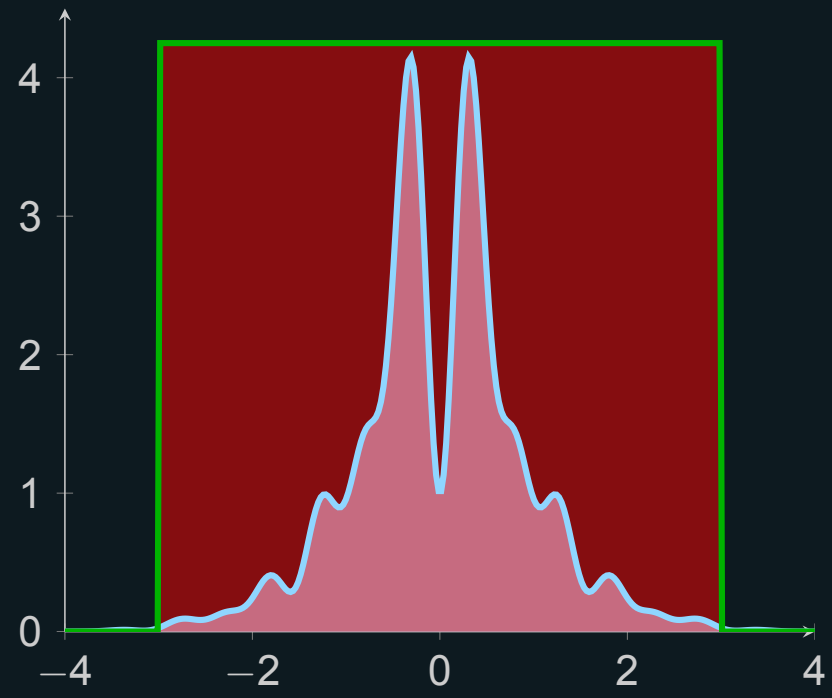
קבלה-דחייה

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$

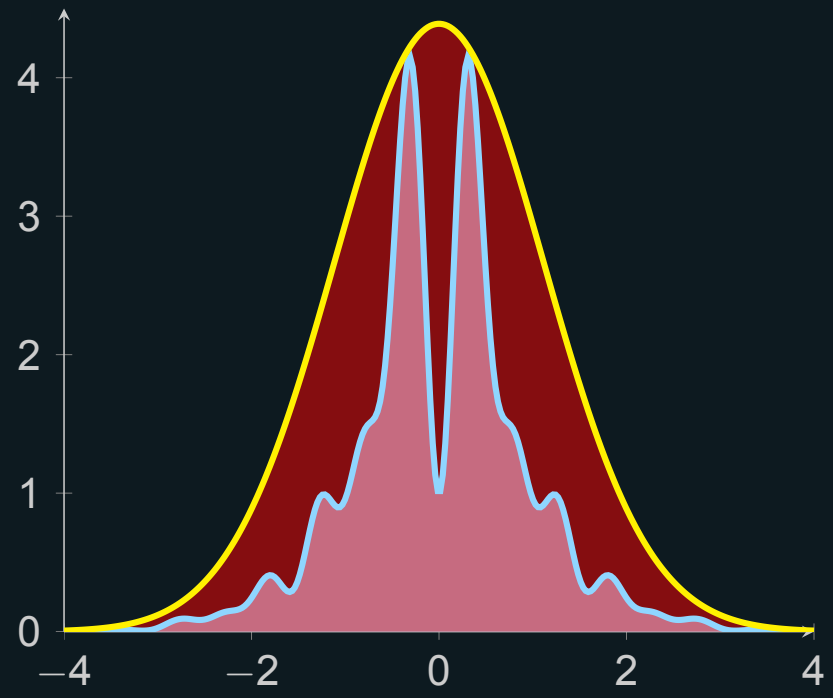


קבלה-דחייה יעילות

$$f(x) = e^{-x^2/2}\left(\sin^2(6x) + 3\cos^2(x)\sin^2(4x) + 1\right)$$



Acceptance Rate: 23.5%



Acceptance Rate: 53.63 %

קבלה-דחייה

1. מצא פונקציה חוסמת $t(x) \geq f(x)$
2. $c = \int t(x)\,dx$
3. נרמול: $r(x) = \frac{t(x)}{c}$

אלגוריתם דגימה:

1. דגום $y \sim r(x)$
2. דגום $u \sim U(0,1)$
3. אם $u \leq \frac{f(y)}{t(y)}$ החזר y
4. אחרת חזור ל-1

תרגיל

בחוג לריקוד טנגו יש 60% רקדנים מבוגרים ו־40% רקדנים צעירים.
התפלגות שעת הריקוד של כל אחת מהקבוצות נתונות ע"פ הפונקציות הבאות:

צעיר:

$$f(x)=\begin{cases}\frac{3x}{8} & 0\le x\le 2\\ \frac{1}{4} & 2\le x\le 3\\ 0 & \text{otherwise}\end{cases}$$

מבוגר:

$$f(x)=\begin{cases}\frac{1}{2} & 0\le x\le 2\\ 0 & \text{otherwise}\end{cases}$$

א. פתחו אלגוריתם דגימה לזמן הריקוד של רקדן, ללא שימוש בקבלה־דחייה.

ב. פתחו אלגוריתם דגימה לזמן הריקוד של רקדן, באמצעות קבלה־דחייה.

פתרון - קומפוזיציה - מבוגרים

$$f(x) = \begin{cases} \frac{1}{2} & 0 \le x \le 2 \\ 0 & \text{otherwise} \end{cases}$$

$$F(x) = \begin{cases} 0 & x \le 0 \\ \frac{x}{2} & 0 \le x \le 2 \\ 1 & x \ge 2 \end{cases}$$

$$F(x) = \frac{x}{2} = u \qquad \Rightarrow \qquad x = 2u$$

בדיקה:

$$u = 0 \Rightarrow x = 0, \qquad u = 1 \Rightarrow x = 2$$

פתרון - קומפוזיציה - צעירים

$$f(x)=\begin{cases}\frac{3x}{8} & 0\le x\le 2\\ \frac{1}{4} & 2\le x\le 3\\ 0 & \text{otherwise}\end{cases}$$

$$F(x)=\begin{cases}0 & x\le 0\\ \frac{3x^2}{16} & 0\le x\le 2\\ \frac{1}{4}+\frac{x}{4} & 2\le x\le 3\\ 1 & x\ge 3\end{cases}$$

$0\le x\le 2$:

$$F(x=2)=\frac{3x^2}{16}=\frac{3}{4}$$

$$\frac{3x^2}{16}=u\Rightarrow x=\sqrt{\frac{16u}{3}}$$

בדיקה:

$$u=0\Rightarrow x=0,\ u=\frac{3}{4}\Rightarrow x=2$$

$2\le x\le 3$:

$$F(x)=\frac{1}{4}+\frac{x}{4}=u\Rightarrow x=4u-1$$

בדיקה:

$$u=\frac{3}{4}\Rightarrow x=2$$

$$u=1\Rightarrow x=3$$

פתרון - קומפוזיציה

אלגוריתם:

1. דגום $u_1, u_2 \sim U(0,1)$
2. אם $0 < u_1 < 0.4$
   i. אם $u_2 \leq 0.75$ החזר $\sqrt{\frac{16u_2}{3}}$
   ii. אחרת החזר $4u_2 - 1$
3. אחרת החזר $2u_2$

פתרון - קבלה דחייה

ראשית, נייצר פונקציית צפיפות משותפת:

$$f(x) = \begin{cases} 0.4 \cdot \frac{3x}{8} + 0.6 \cdot \frac{1}{2} & 0 \le x \le 2 \\ 0.4 \cdot \frac{1}{4} & 2 \le x \le 3 \\ 0 & \text{otherwise} \end{cases}$$

נבחר פונקציה חוסמת:

$$t(x) = \begin{cases} \frac{6}{10} & 0 \le x \le 3 \\ 0 & \text{otherwise} \end{cases} \qquad c = \int_0^3 t(x)\,dx = \frac{18}{10}$$

ולכן פונקציית ההצעה המנורמלת היא:

$$r(x) = \begin{cases} \frac{1}{3} & 0 \le x \le 3 \\ 0 & \text{otherwise} \end{cases}$$

פתרון קבלה־דחייה

אלגוריתם דגימה ל־$r(x)$:

1. דגום $u \sim U(0,1)$
2. החזר $3u$

אלגוריתם דגימה ל־$f(x)$:

1. דגום $y \sim r(x)$
2. דגום $u \sim U(0,1)$
3. אם $u \leq \frac{f(y)}{t(y)}$ החזר $x = y$, אחרת חזור לשלב 1.

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

קבלה-דחייה מימוש ב -Python

https://colab.research.google.com/drive/1Y2yQwhYakcy7H-VgB5xieje1afpfSI7v

דגימה 2 - מוטיבציה

עד עכשיו הנחנו שיש לנו מקור שמחזיר מספרים מהתפלגות $U(0,1)$.

כעת נשאל שאלה בסיסית יותר:

איך מייצרים את המספרים האלה במחשב?

דגימה 2 - מוטיבציה

עד עכשיו הנחנו שיש לנו מקור שמחזיר מספרים מהתפלגות $U(0,1)$.

כעת נשאל שאלה בסיסית יותר:

איך מייצרים את המספרים האלה במחשב?

התשובה: בדרך כלל לא מייצרים אקראיות אמיתית, אלא רצף דטרמיניסטי שנראה אקראי.

דגימה 2 - מוטיבציה

עד עכשיו הנחנו שיש לנו מקור שמחזיר מספרים מהתפלגות $U(0,1)$.

כעת נשאל שאלה בסיסית יותר:

איך מייצרים את המספרים האלה במחשב?

התשובה: בדרך כלל לא מייצרים אקראיות אמיתית, אלא רצף דטרמיניסטי שנראה אקראי.

רצף כזה נקרא **פסאודו-אקראי**.

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

מחולל מספרים פסאודו-אקראיים

דגימה בסימוצלציה משמעה פסודו-אקראיות. נרצה שיטות לחולל מספרים אקראיים בין 0 ל- 1 בהם נשתמש עבור אלגוריתמי דגימה.

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

מחולל מספרים פסאודו-אקראיים

דגימה בסימוצלציה משמעה פסודו-אקראיות. נרצה שיטות לחולל מספרים אקראיים בין 0 ל- 1 בהם נשתמש עבור אלגוריתמי דגימה.

"אין דבר נקרא מקרי אלא ביחס לליקוי ידיעתנו."

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

מחולל מספרים פסאודו-אקראיים

דגימה בסימוצלציה משמעה פסודו-אקראיות. נרצה שיטות לחולל מספרים אקראיים בין 0 ל- 1 בהם נשתמש עבור אלגוריתמי דגימה.

"אין דבר נקרא מקרי אלא ביחס לליקוי ידיעתנו."

— ברוך שפינוזה, תורת המידות 1677

LCG - Linear Congruential Generator

פונקציית $LCG(a, c, m, z_0)$ מקבלת ארבעה פרמטרים:

- z_0 - Seed
- m - Modulus
- a - Multiplier
- c - Increment

הרצה:

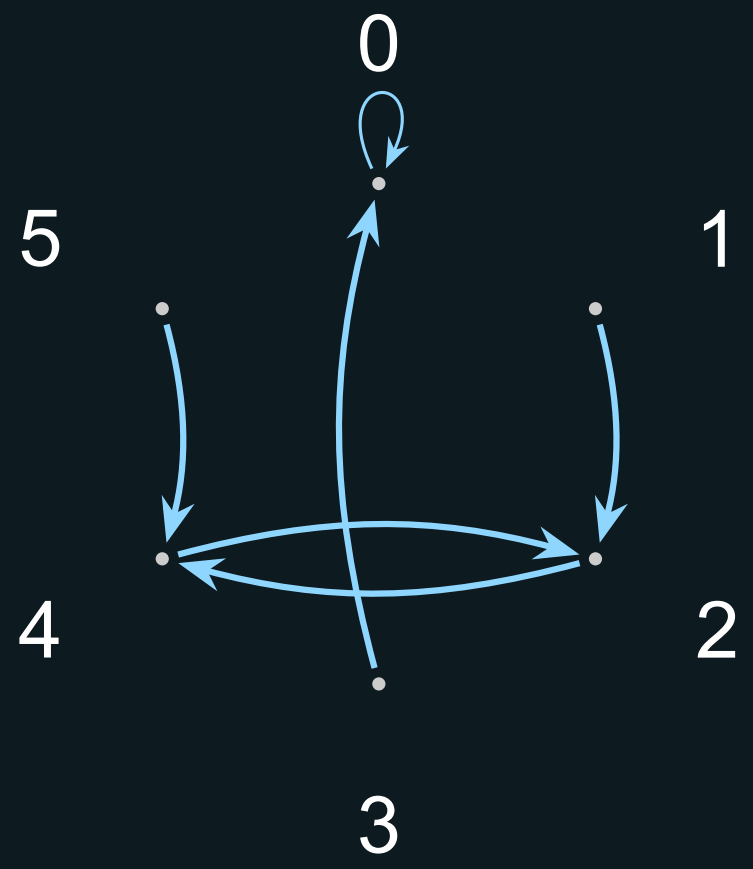
$$Z_i = (aZ_{i-1} + c) \bmod m \qquad 0 \leq Z_i < m$$

$$U_i = \frac{Z_i}{m}, \qquad 0 \leq U_i < 1$$

LCG - חשבון מודולרי המחשה

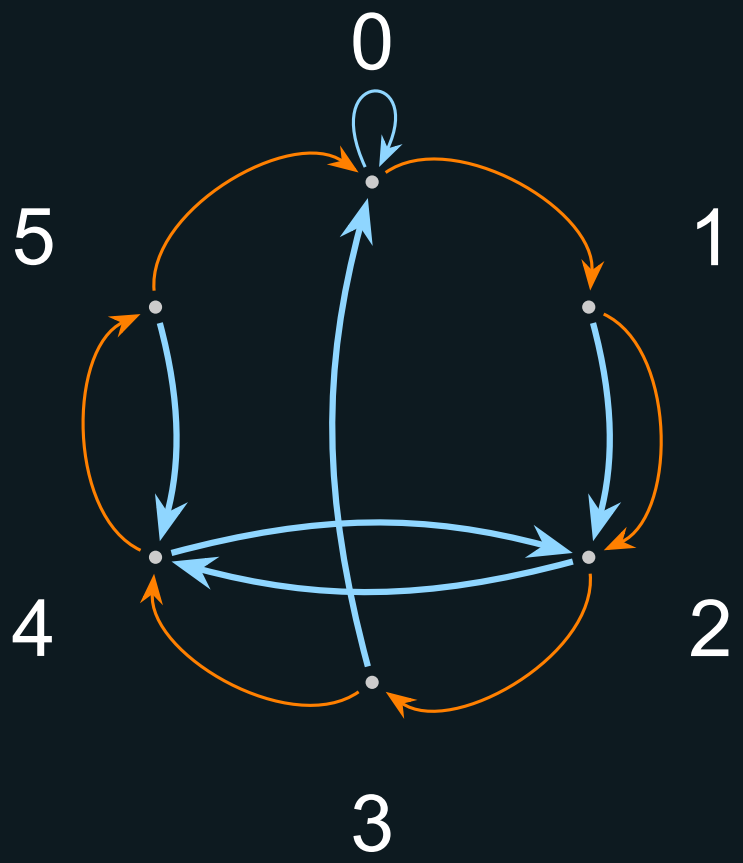
אפשר להבין את פעולת המחולל כהליכה פסודו-רנדומלית על גרף האריתמטיקה מעל חוג בגודל m.

$m = 6,\ a = 2$



LCG - חשבון מודולרי המחשה

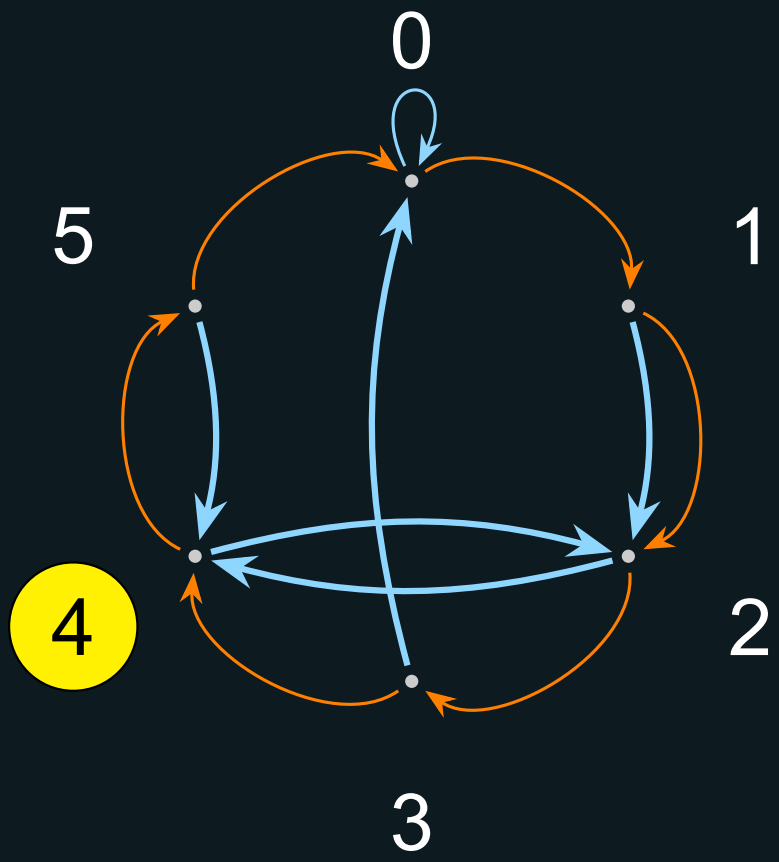
$m = 6,\ a = 2\ ,c = 1$



LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$

$Z_0 = 4$

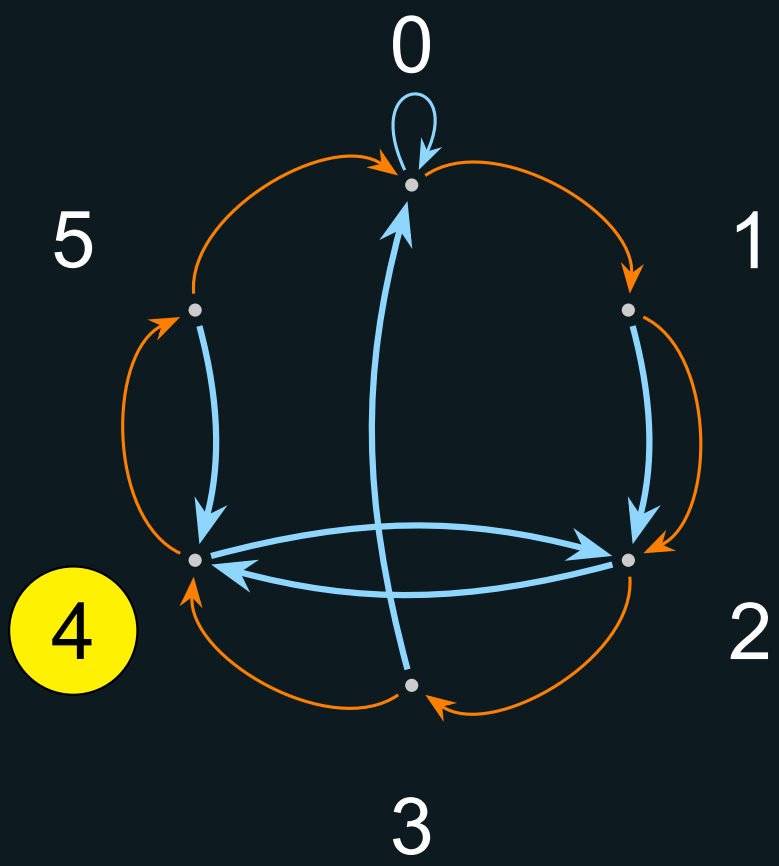


LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$

$Z_0 = 4$

$Z_1 = (2Z_{i-1} + 1) \bmod 6$

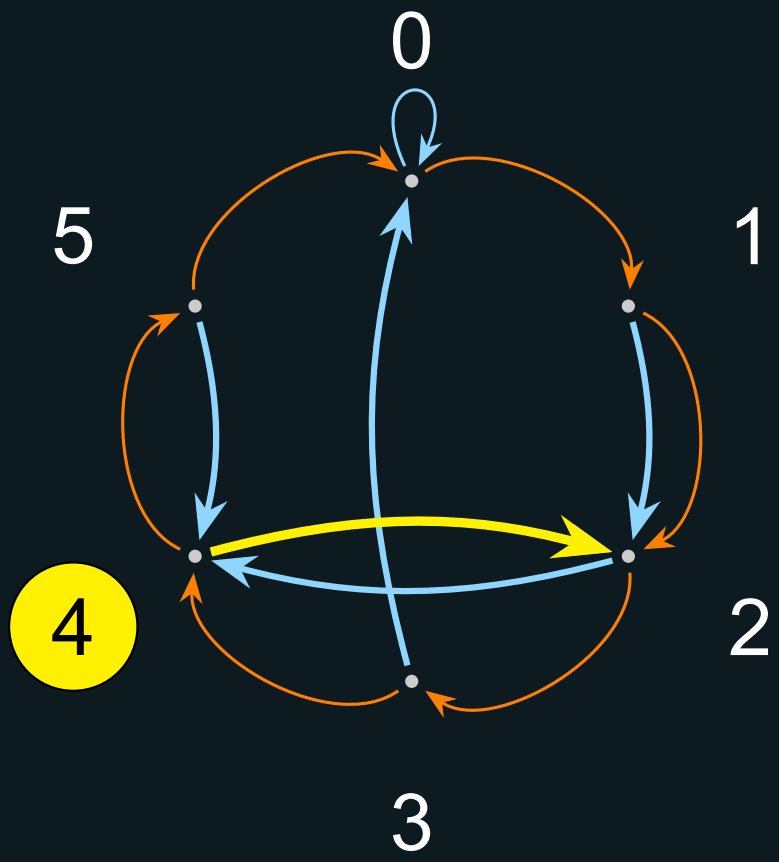


LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$

$Z_0 = 4$

$Z_1 = (2Z_0 + 1) \bmod 6$

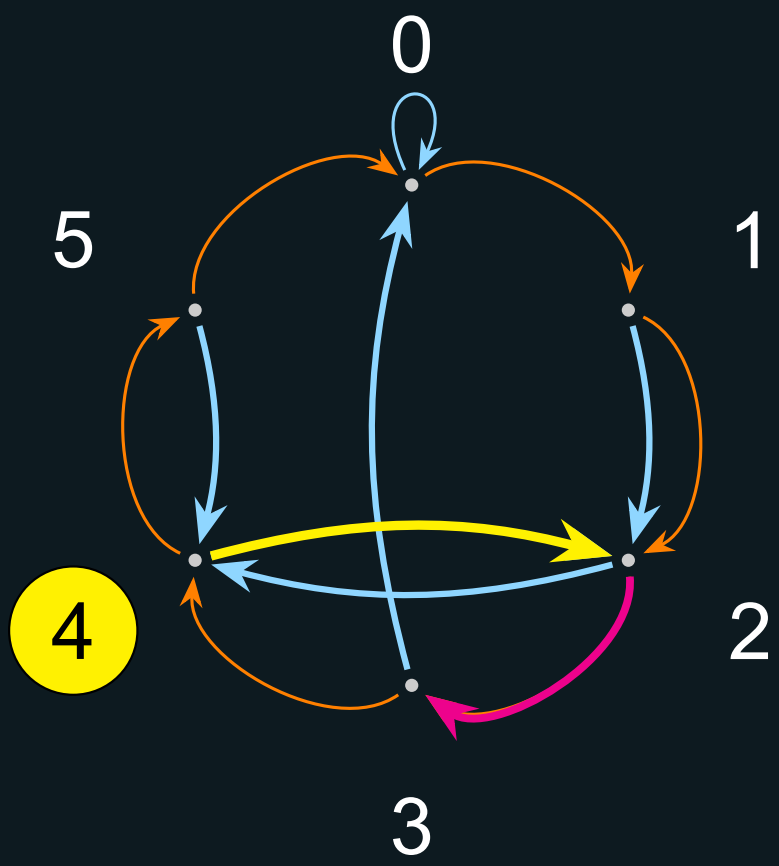


LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$

$Z_0 = 4$

$Z_1 = (2 \cdot 4 + 1) \bmod 6$

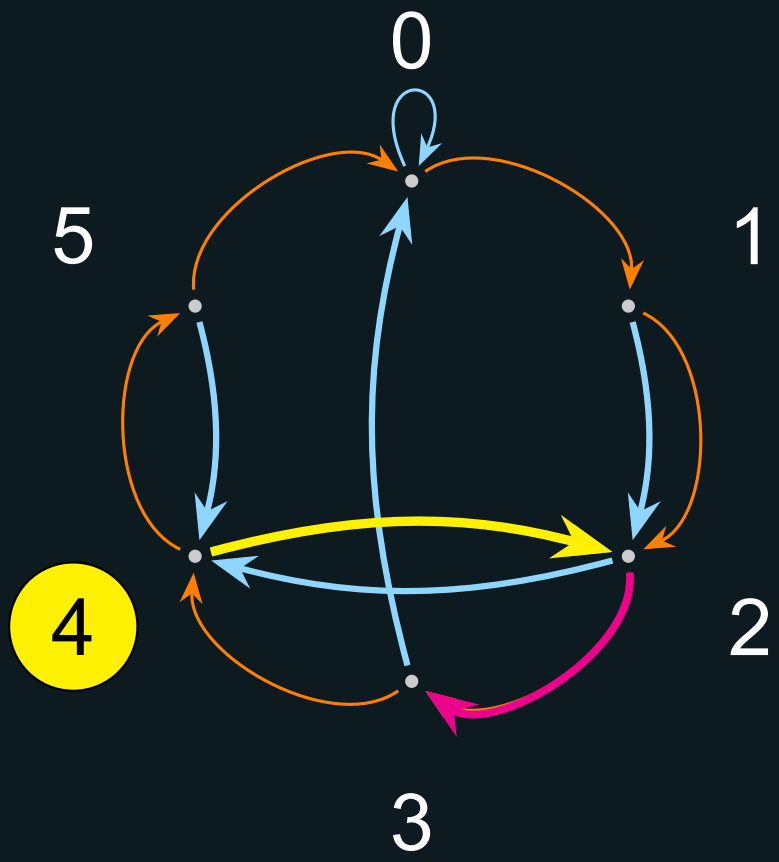


LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$

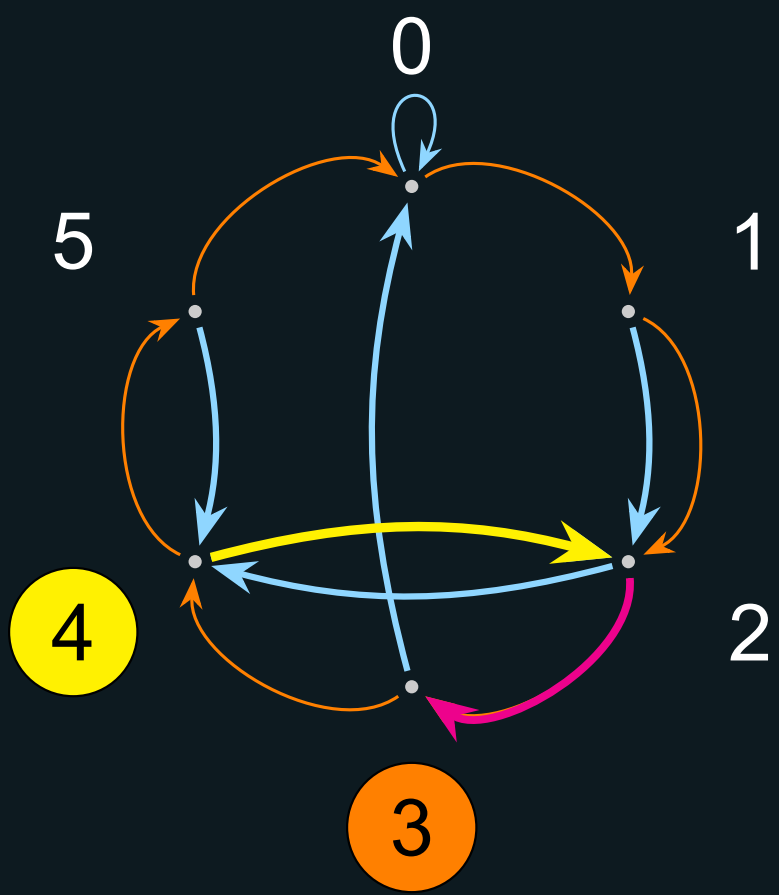
$Z_0 = 4$

$Z_1 = 3$



LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



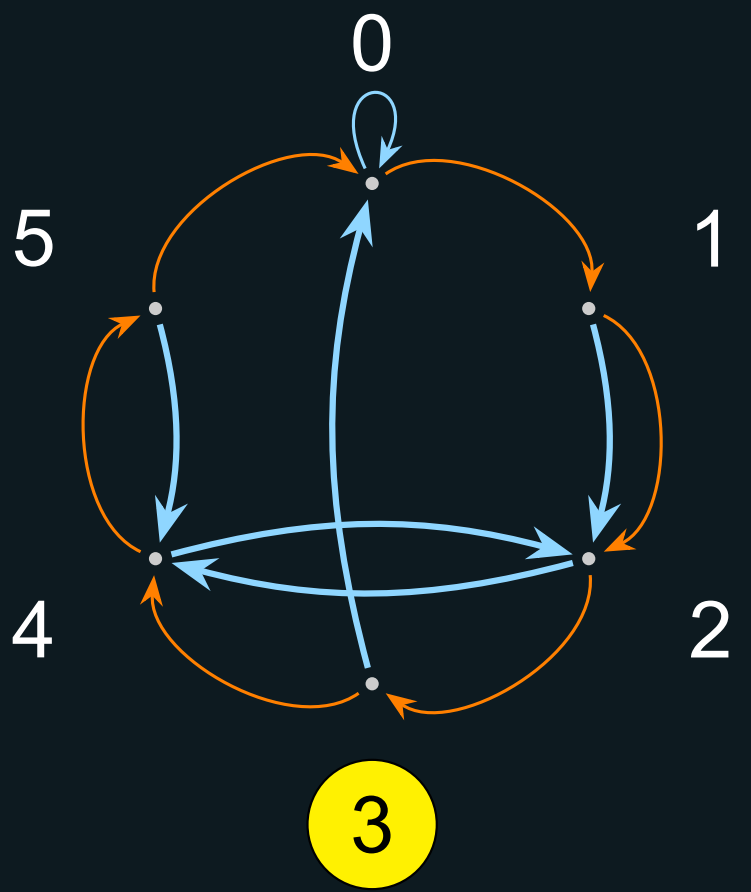
$Z_0 = 4$

$Z_1 = 3$

$Z_2 = (2Z_1 + 1) \bmod 6$

LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



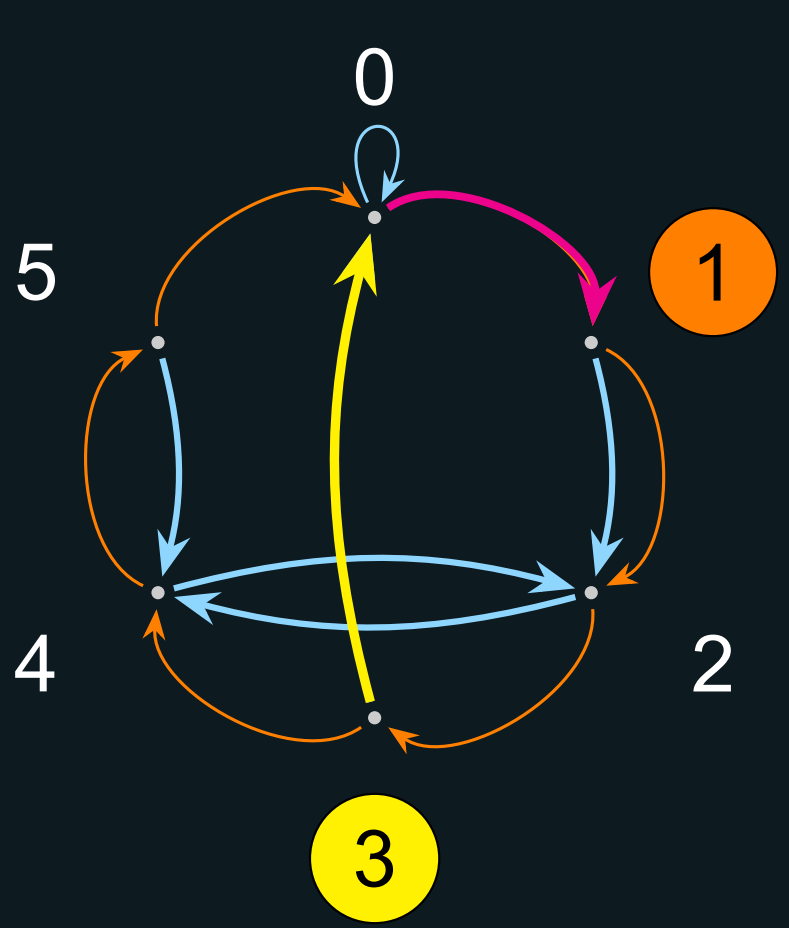
$Z_0 = 4$

$Z_1 = 3$

$Z_2 = (2 \cdot 3 + 1) \bmod 6$

LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



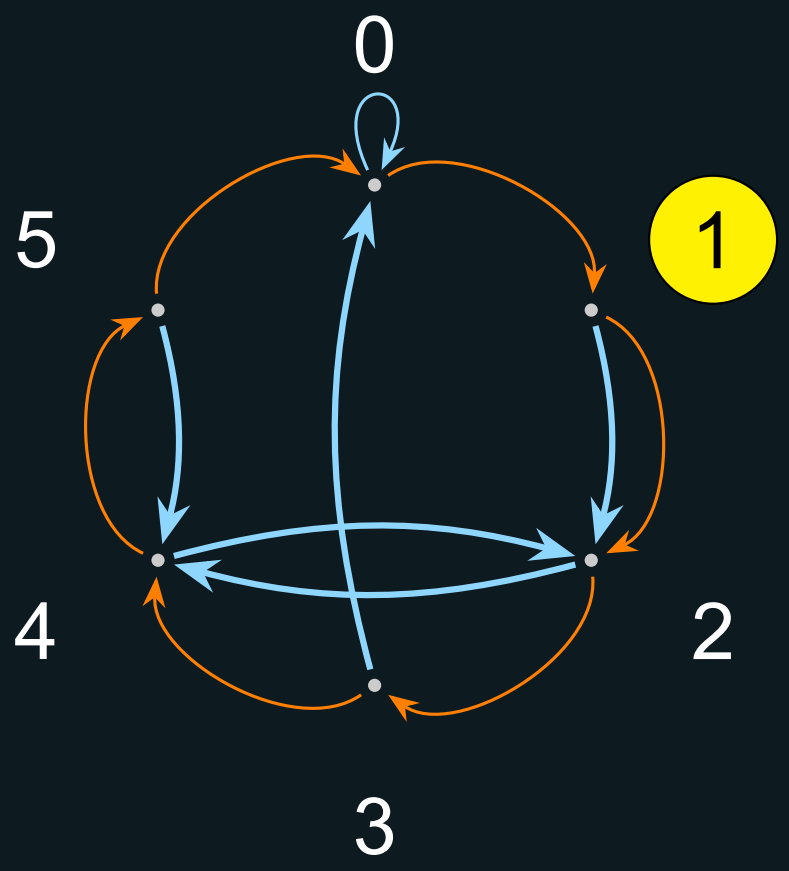
$Z_0 = 4$

$Z_1 = 3$

$Z_2 = 1$

LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



$Z_0 = 4$

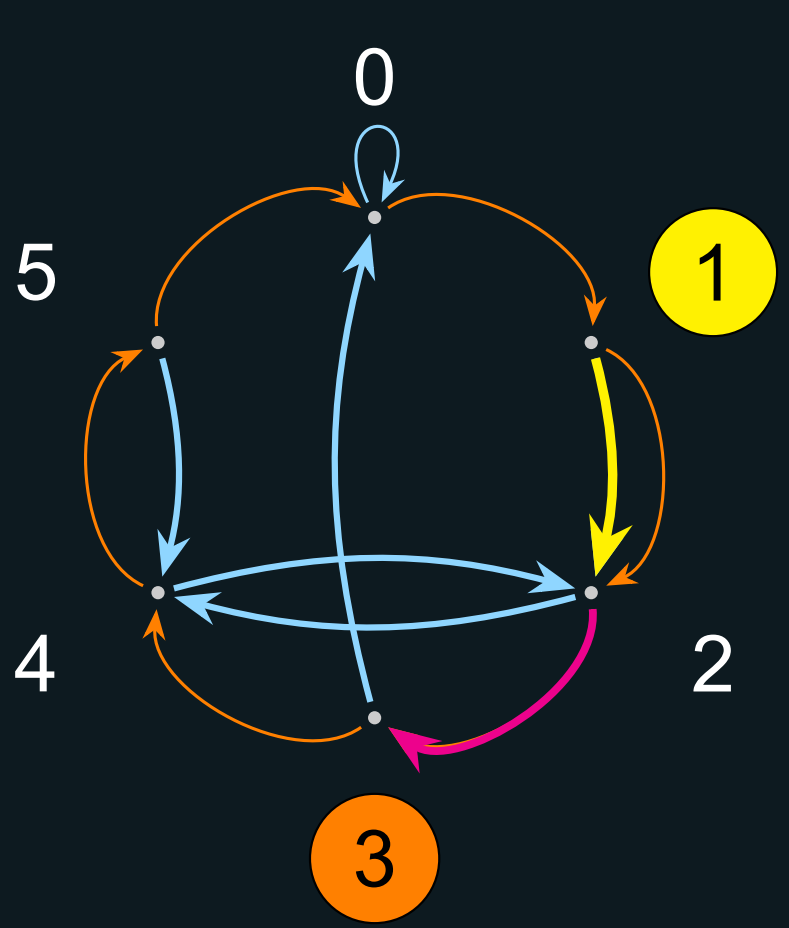
$Z_1 = 3$

$Z_2 = 1$

$Z_3 = (2Z_2 + 1) \bmod 6$

LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



$Z_0 = 4$

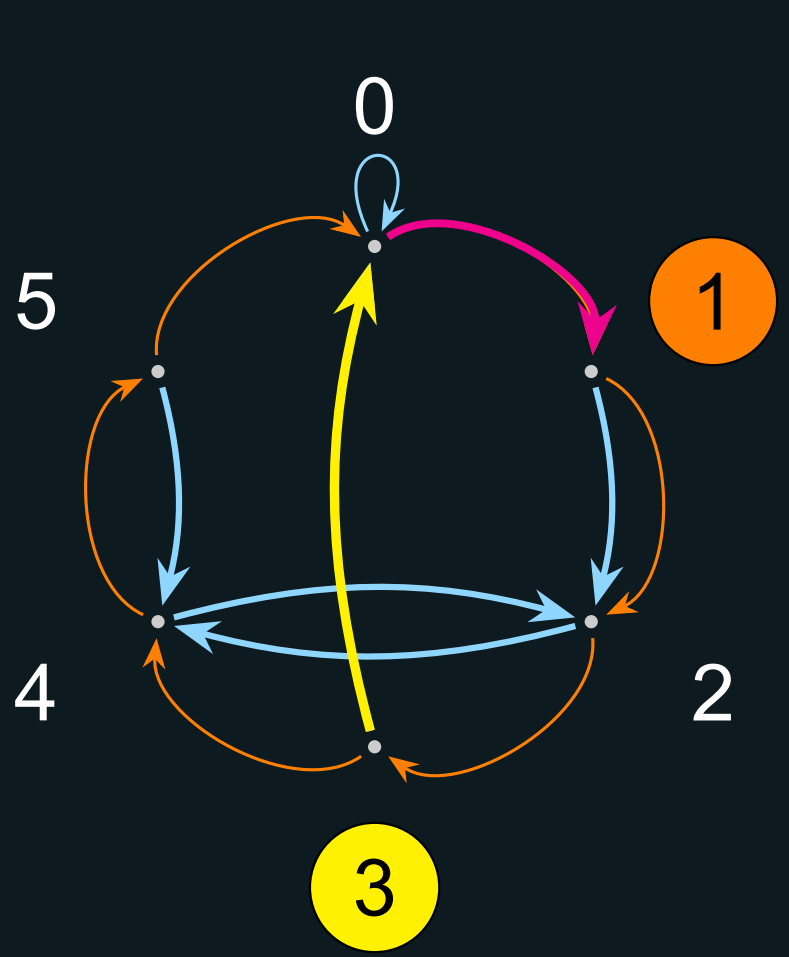
$Z_1 = 3$

$Z_2 = 1$

$Z_3 = 3$

LCG - חשבון מודולרי המחשה

$m = 6,\ a = 2\ ,c = 1$



$Z_0 = 4$

$Z_1 = 3$

$Z_2 = 1$

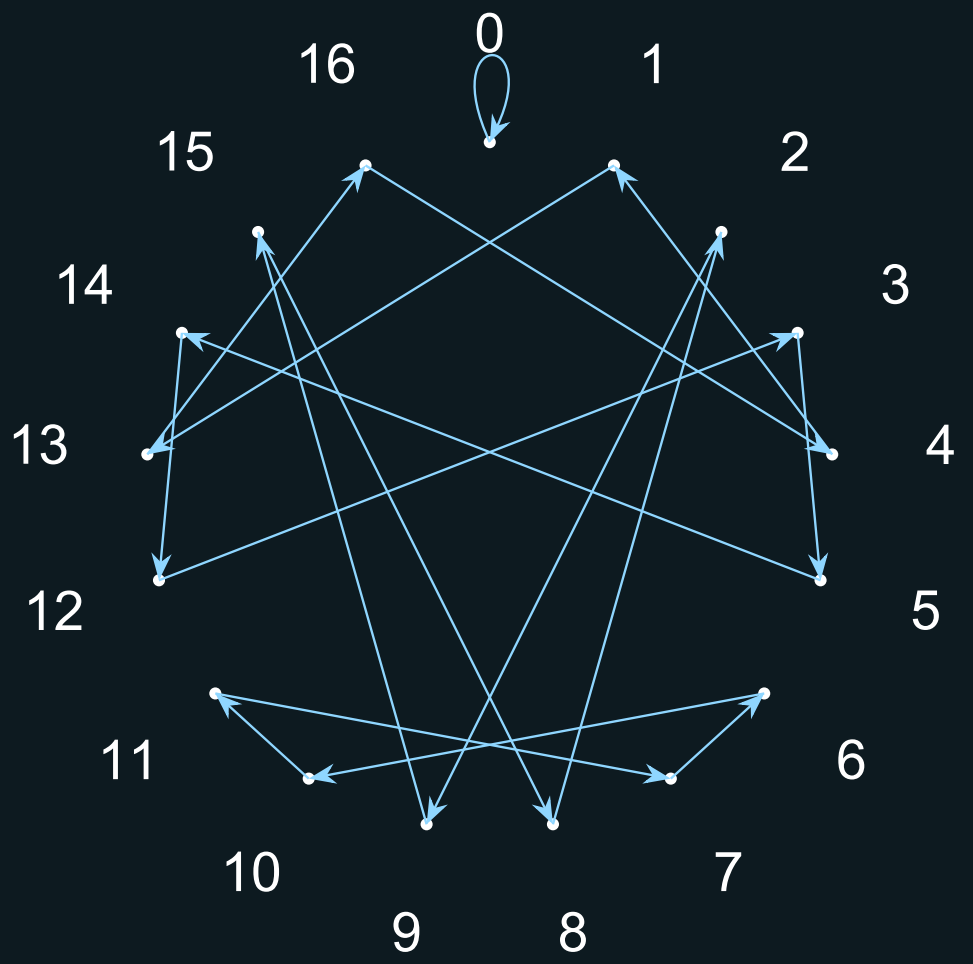
$Z_3 = 3$

$Z_4 = 1$

$\vdots$

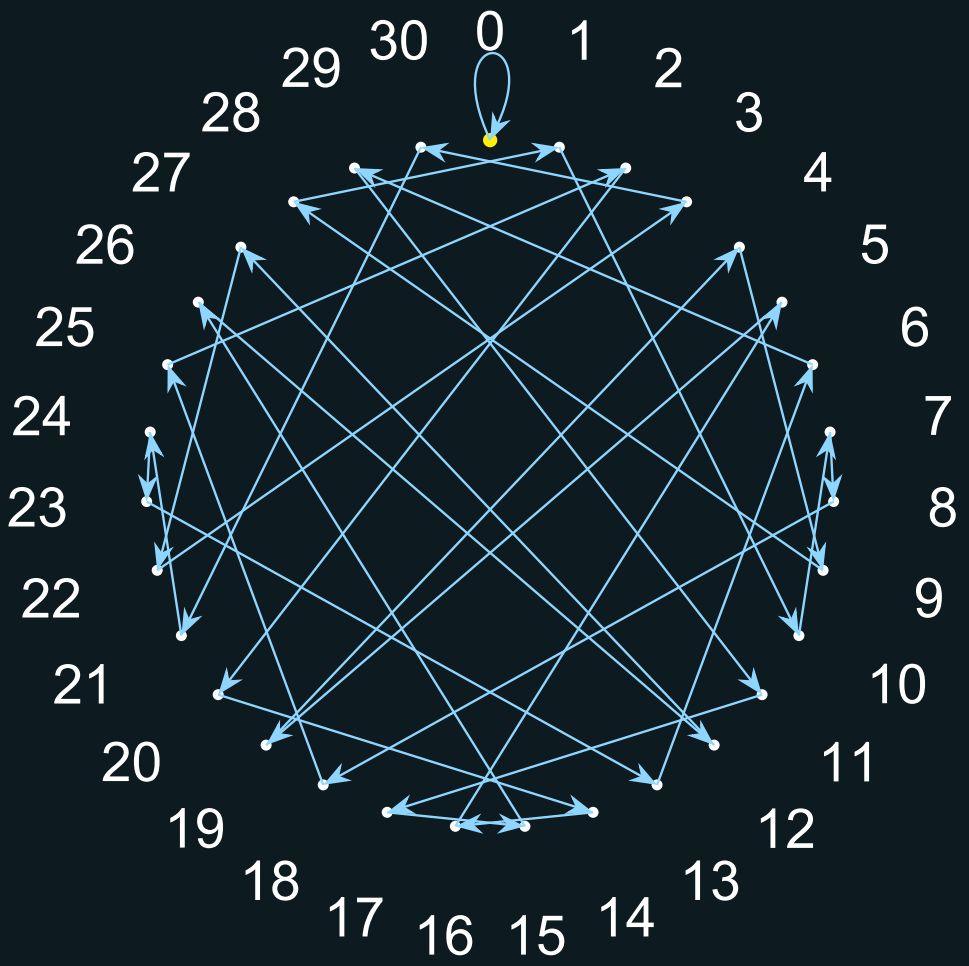
LCG - חשבון מודולרי המחשה

$m = 17, a = 13$



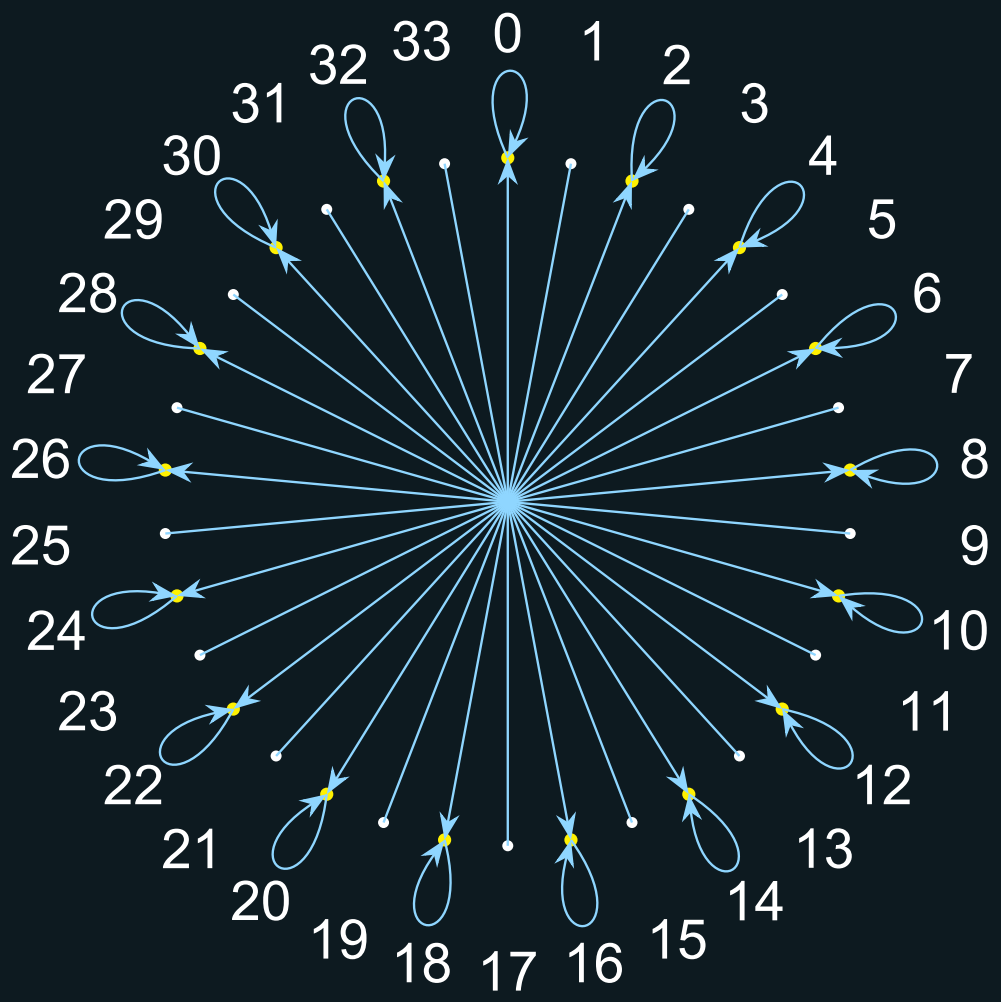
LCG - חשבון מודולרי המחשה

$m = 31, a = 10$



LCG - חשבון מודולרי המחשה

$m = 34,\ a = 18$



LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים.

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

ע"פ משפט האל-דובל (עבור $c \neq 0$ ועבור כל SEED):

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

ע"פ משפט האל-דובל (עבור $c \neq 0$ ועבור כל SEED):

- m ו a הם ***מספרים זרים***. הגורם המשותף הגדול ביותר שלהם הוא 1.

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

ע"פ משפט האל-דובל (עבור $c \neq 0$ ועבור כל SEED):

- m ו a הם ***מספרים זרים***. הגורם המשותף הגדול ביותר שלהם הוא 1.
- כל גורם ראשוני של m הוא גורם של $a - 1$.

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

ע"פ משפט האל-דובל (עבור $c \neq 0$ ועבור כל SEED):

- m ו a הם ***מספרים זרים***. הגורם המשותף הגדול ביותר שלהם הוא 1.
- כל גורם ראשוני של m הוא גורם של $a - 1$.
- אם 4 הוא גורם של m אז הוא גם גורם של $a - 1$.

LCG - סיכום

אם נתכנן את מחולל הLCG שלנו היטב נוכל לקבל m מספרים פסודו-אקראיים. איך נבחר את הפרמטרים?

ע"פ משפט האל-דובל (עבור $c \neq 0$ ועבור כל SEED):

- m ו a הם ***מספרים זרים***. הגורם המשותף הגדול ביותר שלהם הוא 1.
- כל גורם ראשוני של m הוא גורם של $a - 1$.
- אם 4 הוא גורם של m אז הוא גם גורם של $a - 1$.

סיכום:

- זמן ריצה מהיר - סיבוכיות $O(1)$
- מימוש פשוט מאוד
- רגיש מאוד לבחירת הפרמטרים. פרמטרים גרועים עלולים לגרום למחזור קצר, נקודות קבועות ואובדן אקראיות.
- ניתן לחיזוי מלא - אינו מתאים לקריפטוגרפיה.

קידוד בינארי

נזכור כיצד מספרים מיוצגים בבינארי:

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

1	1	0	1
2^3	2^2	2^1	2^0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

LFSR - Linear Feedback Shift Register

פונקציית $LFSR(n, T, s_0)$ מקבלת שלושה פרמטרים:

- n - מספר הביטים באוגר (register)
- n-bit Seed - s_0
- $T \subseteq \{1, \ldots, n\}$ - קבוצת ה־Taps

הרצה:

1. מחשבים ביט חדש באמצעות XOR על ה־Taps
2. מזיזים את כל הביטים ימינה
3. מכניסים את הביט החדש משמאל

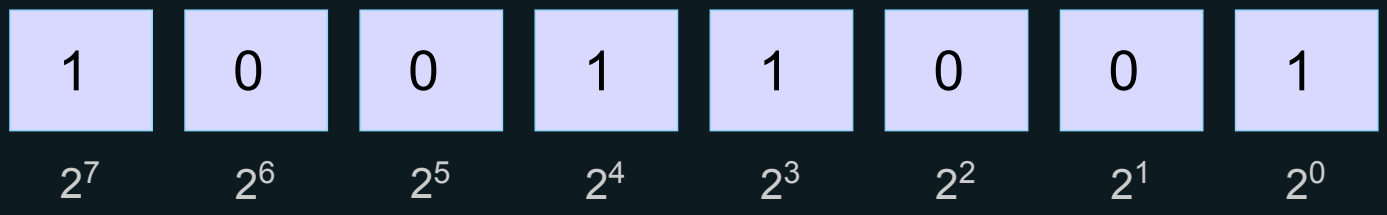
הפלט הוא רצף ביטים פסאודו־אקראי

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

LFSR - Linear Feedback Shift Register

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

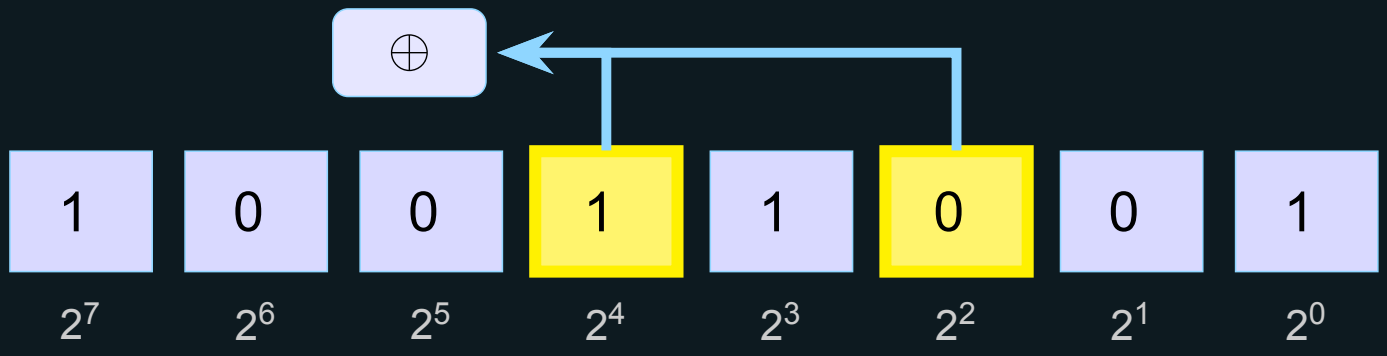
LFSR - Linear Feedback Shift Register



אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

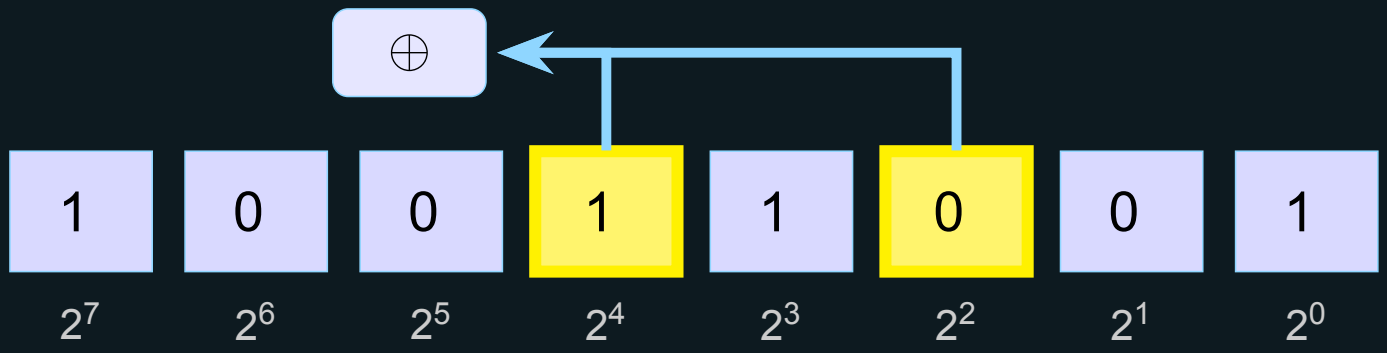
LFSR - Linear Feedback Shift Register

LFSR - Linear Feedback Shift Register



אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

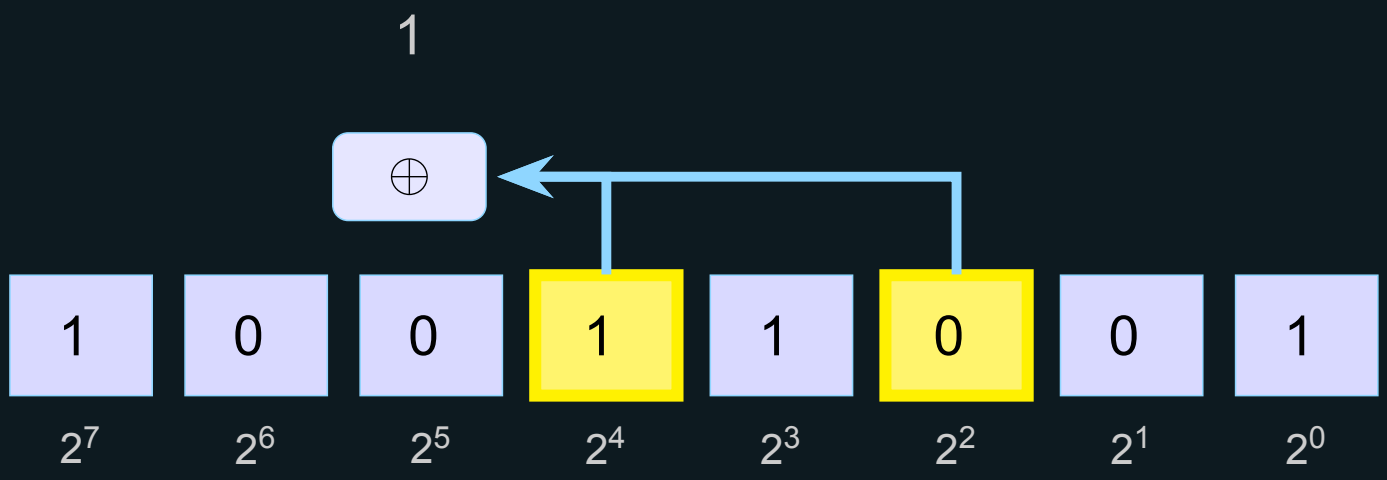
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

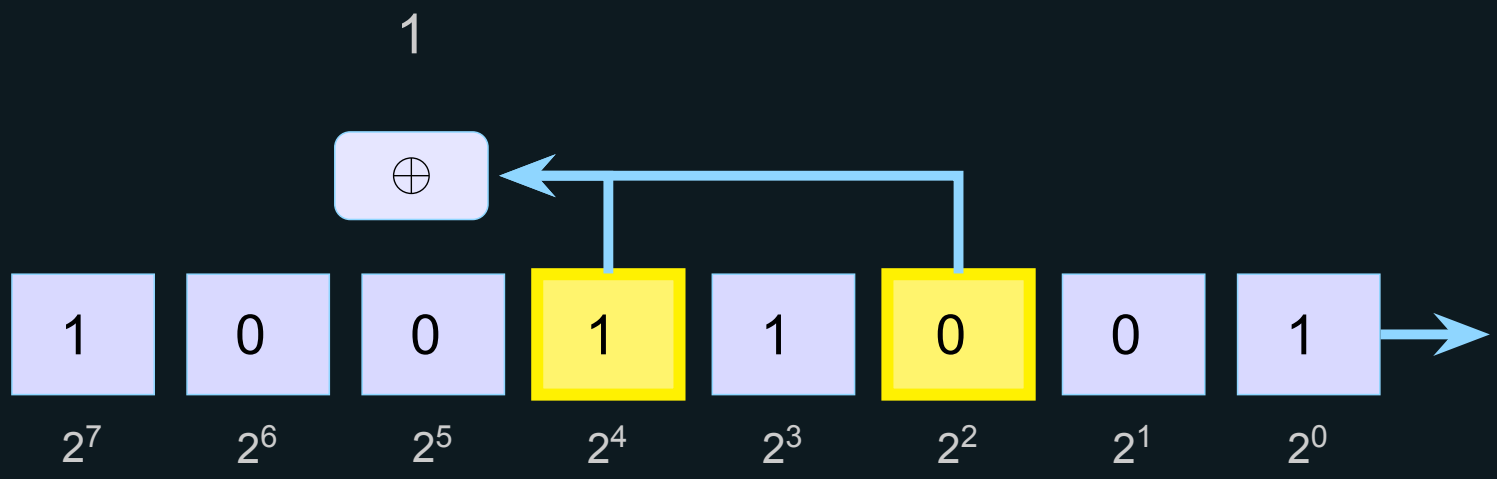
אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

LFSR - Linear Feedback Shift Register



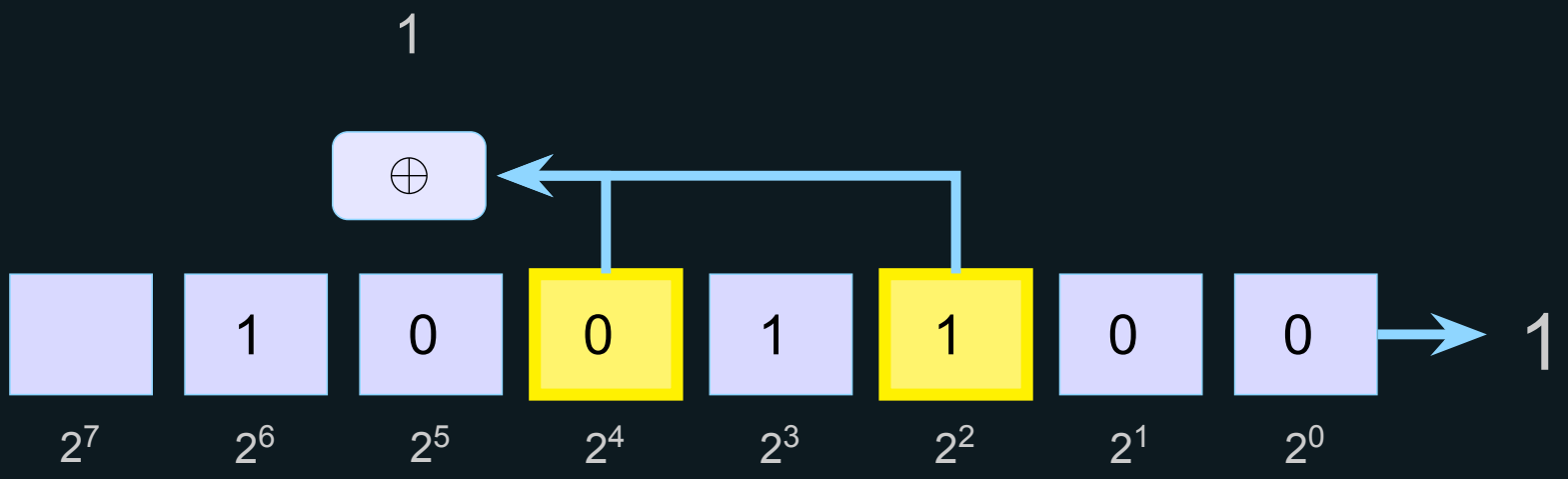
x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

LFSR - Linear Feedback Shift Register



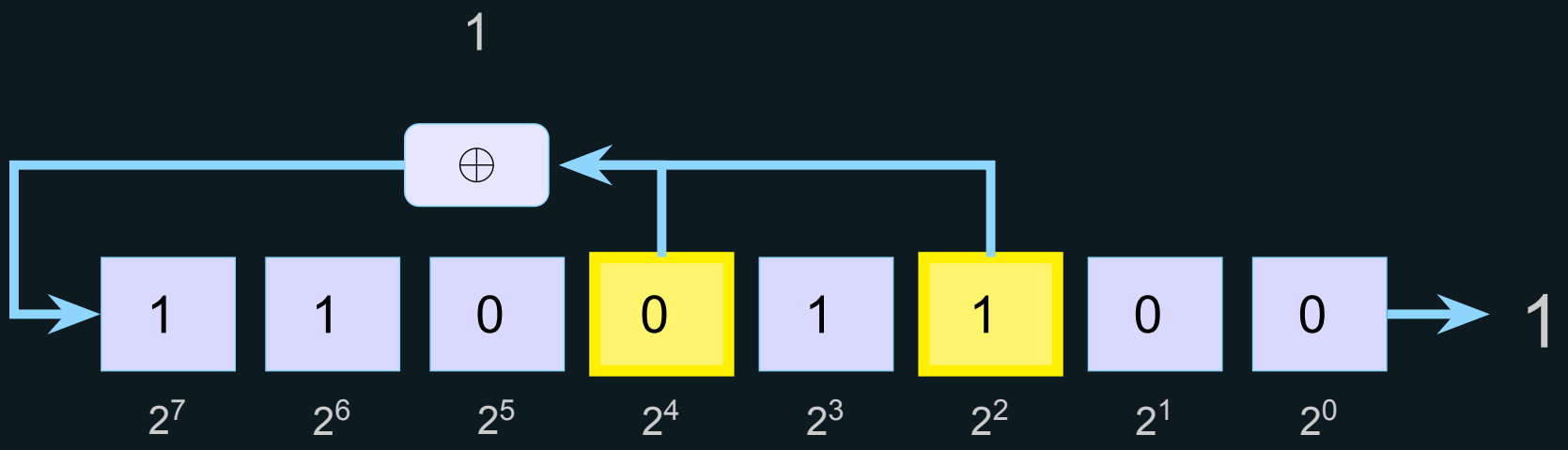
x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

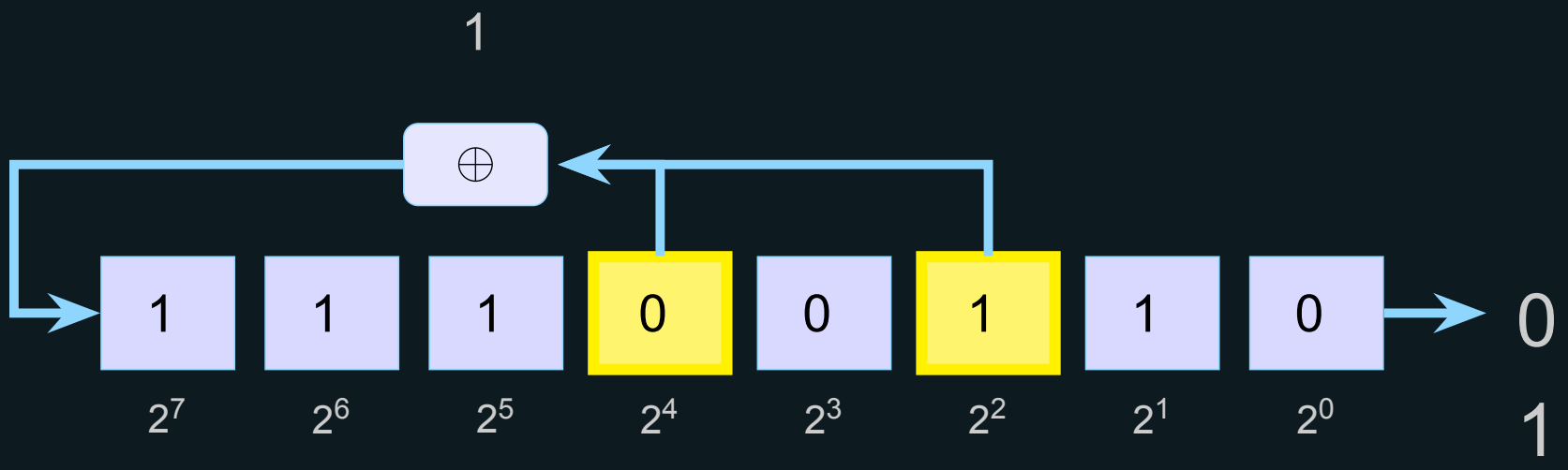
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

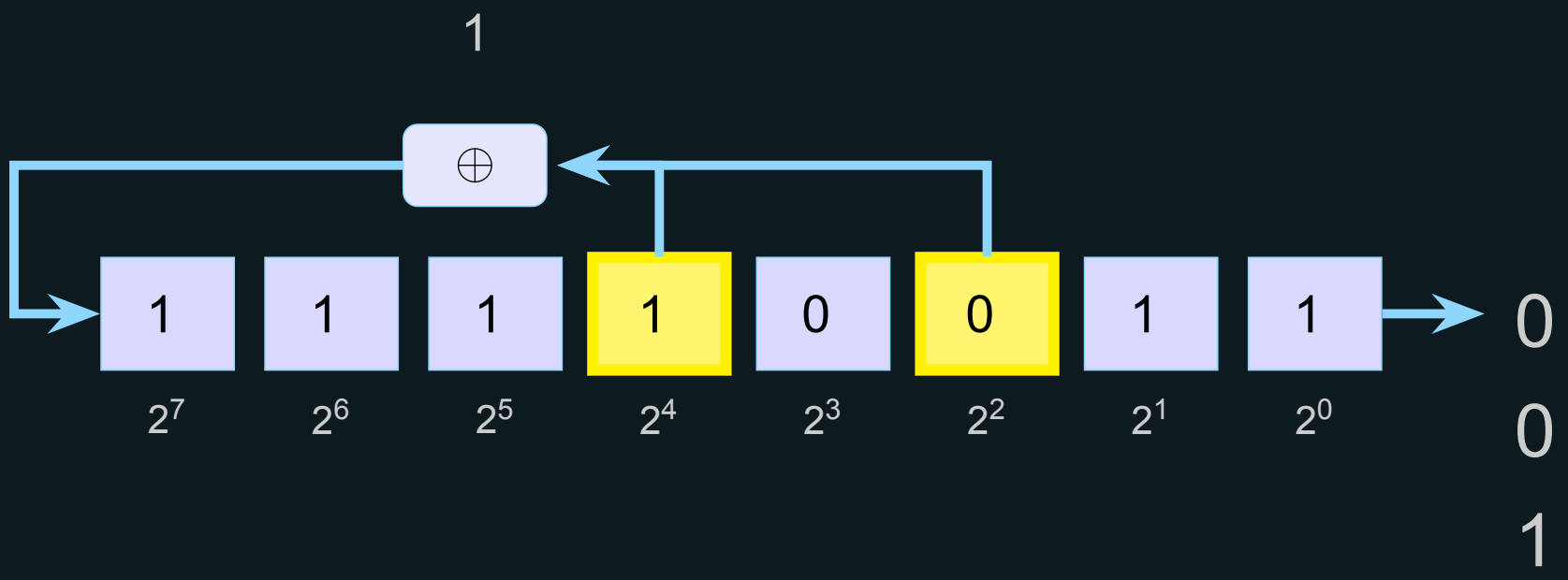
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

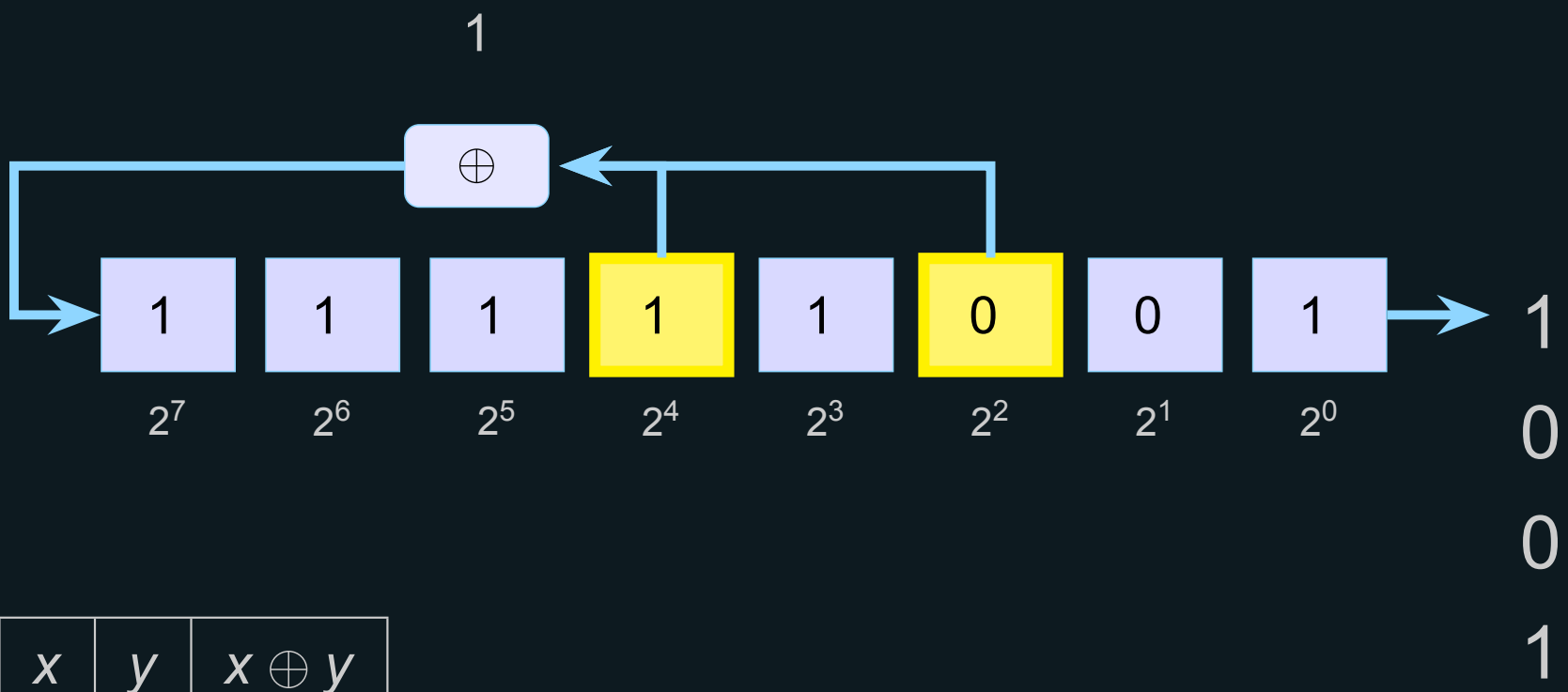
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

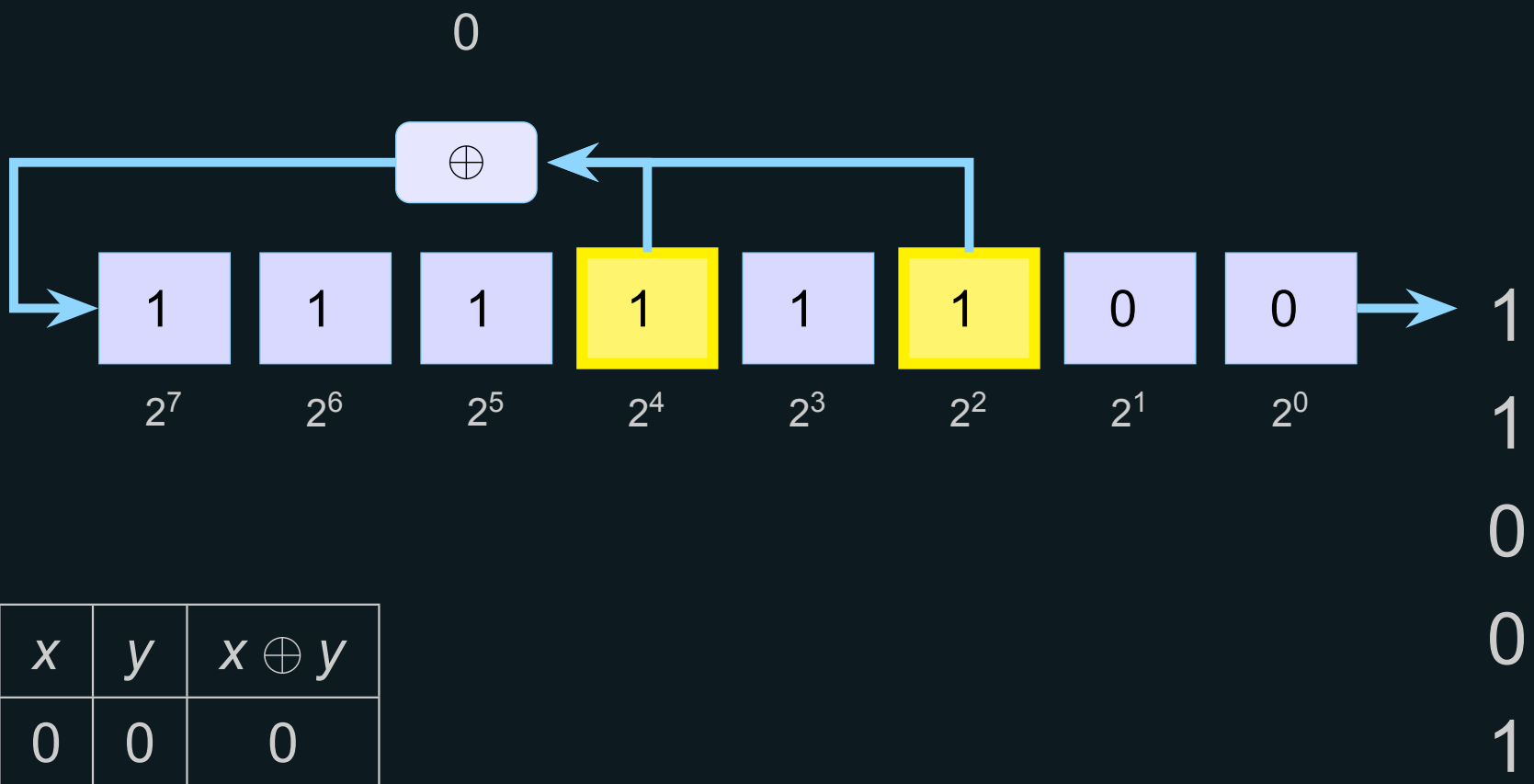
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

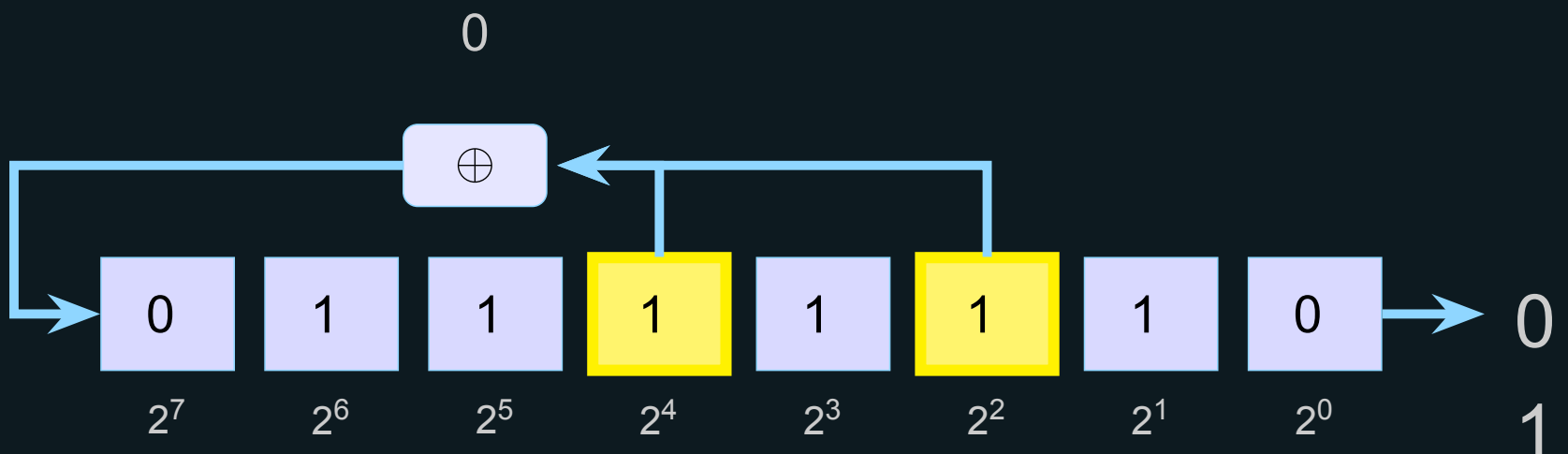
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

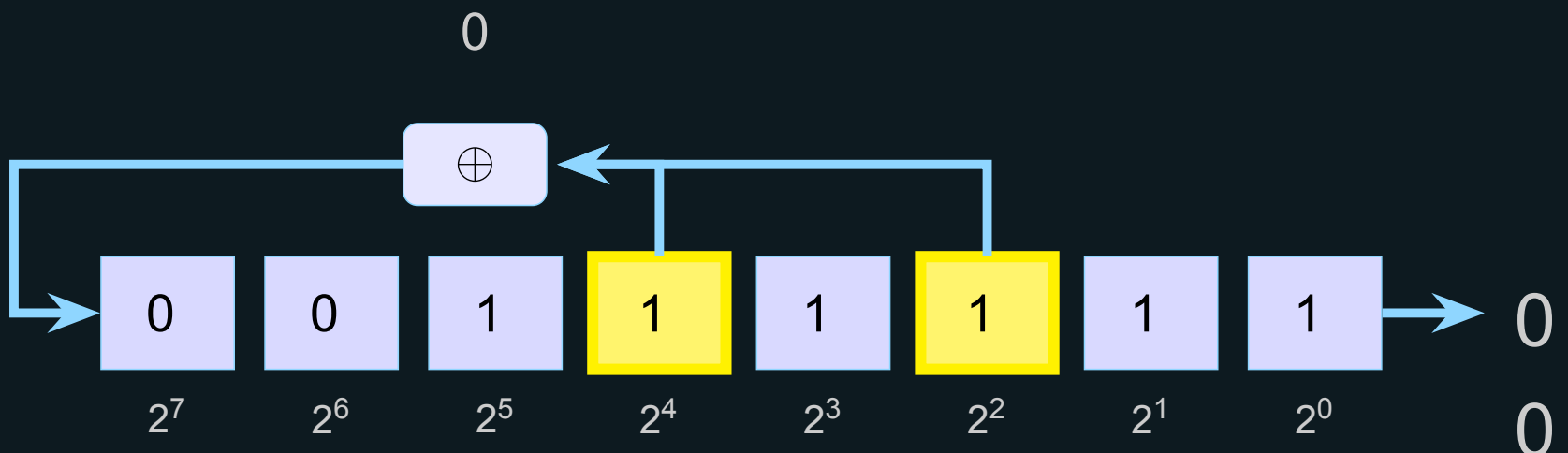
LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

LFSR - Linear Feedback Shift Register



x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

LFSR - סיכום

- LFSR מתוכנן היטב עם n ביטים יכול לייצר $2^n - 1$ ביטים פסודו-אקראיים לפני חזרה על הרצף.
- חשוב לזכור:
  - ה־Seed לא יכול להיות כולו אפסים.
  - יש לבחור Taps המתאימים לפולינום פרימיטיבי (לרוב משתמשים בטבלאות מוכנות).
  - בדרך כלל מספר זוגי של Taps נותן תוצאות טובות.

LFSR - סיכום

- LFSR מתוכנן היטב עם n ביטים יכול לייצר $2^n - 1$ ביטים פסודו-אקראיים לפני חזרה על הרצף.
- חשוב לזכור:
  - ה־Seed לא יכול להיות כולו אפסים.
  - יש לבחור Taps המתאימים לפולינום פרימיטיבי (לרוב משתמשים בטבלאות מוכנות).
  - בדרך כלל מספר זוגי של Taps נותן תוצאות טובות.

סיכום:

- זמן ריצה מהיר - סיבוכיות $O(1)$
- מימוש פשוט מאד אפילו יותר מLCG.
- רגישות לבחירת הTaps וה SEED.
- ניתן לחיזוי מלא - אינו מתאים לקריפטוגרפיה.

אוניברסיטת בן-גוריון בנגב
جامعة بن غوريون في النقب
Ben-Gurion University of the Negev

LCS ו LFSR מימוש ב-Python

https://colab.research.google.com/drive/1ci24R2rMBxdVcLuSkLioieiLSktrb6f6