<u>מבנים אלגבריים – הרצאה 1</u>

<u>הקדמה</u>

<u>הסבר על הקורס</u>

המבנים האלגבריים עליהם נלמד בקורס זה הם:

- חבורה (עיקר הקורס)
- חוגים (טיפה)
- שדות (שתי טיפות)

כמו כן, נלמד בקורס על שני שימושים חשובים של המבנים הללו: **הצפנה וקידוד**.

המבחן: 4 שאלות, כל שאלה 28 נקודות.

- **שאלה 1**: $FreeStyle$.
- **שאלה 2:** תמורות ומשפט קיילי.
- **שאלה 3:** הצפנה.
- **שאלה 4:** קידוד.

<u>קידוד והצפנה</u>

מה זה **הצפנה**?:

- הסתרה.
- אמינות (לדוגמא, עדכון מייקרוסופט).
- שלימות.

מה זה **קידוד**?:

- מוסכמה לתבנית להעברת מידע.
- אנחנו ספציפית נתעניין בזיהוי ותיקון שגיאות.

לדוגמא, יום ההולדת של ארז הוא 2, כלומר 2.1. כמובן ששני הצדדים צריכים להסכים על הקידוד.

<u>המבנים האלגבריים</u>

<u>חבורה</u>

<u>הגדרה – חבורה</u>: חבורה היא קבוצה G יחד עם פעולה (בהעדר מידע נוסף, נשתמש בסימון הכפל) כך שמתקיימות התכונות הבאות:

1. <u>סגירות</u>: $\forall a,b \in G : a\cdot b \in G$.
2. <u>אסוציאטיביות</u>: $\forall a,b,c \in G : (ab)c = a(bc)$.
3. <u>ניטרלי (איבר יחידה)</u>: קיים $e_G \in G$ המקיים $\forall a \in G : a\cdot e_G = e_G \cdot a = a$.
4. <u>הופכיים</u>: $\forall a \in G\ \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e_G$.

<u>הערה</u>: אם הפעולה של החבורה מקיימת את חוק החילוף, כלומר $\forall a,b \in G : ab = ba$, החבורה נקראת **חילופית** או **קומוטטיבית** או **אבלית**.

<u>דוגמא</u>: האם $\mathbb{N}$ עם חיבור $(\mathbb{N},+)$ היא חבורה? אפילו אם 0 נמצא, והרי הוא איבר נייטרלי לחיבור, אין הופכיים.

$$2 + 2^{-1} = 0$$

אבל, $2^{-1} = -2$, והוא אינו שייך לקבוצה $\mathbb{N}$.

לעומת זאת, $(\mathbb{Z},+)$ היא חבורה. שימו לב ש-$0^{-1} = 0$ בחבורה זו. למעשה, זו תכונה כללית ש-$e_G^{-1} = e_G$ (תרגיל לבית).

<u>חוג</u>

<u>הגדרה – חוג</u>: חוג הוא קבוצה R עם שתי פעולות (שנקרא להן חיבור וכפל) כך שמתקיימות התכונות הבאות:

1. $(R,+)$ היא חבורה חילופית.
2. הכפל סגור, אסוציאטיבי ויש איבר יחידה.
3. <u>פילוג</u>: $\forall a,b,c \in R : [(a+b)c = ac + bc] \wedge [a(b+c) = ab + ac]$.

<u>מהו המופע המוכר ביותר לחוג שאינו שדה?</u>:

- המטריצות הריבועיות מגודל מסוים – החיבור בסדר, אך הכפל לא חילופי ולא כל המטריצות הפיכות.
- $\mathbb{Z}_n$ – חוג השאריות עם פעולות מודולו n.

<u>שדה</u>

<u>הגדרה – שדה</u>: שדה הוא קבוצה $\mathbb{F}$ עם שתי פעולות (שנקרא להן חיבור וכפל) כך שמתקיימות התכונות הבאות:

1. $(\mathbb{F},+)$ היא חבורה חילופית.
2. $(\mathbb{F}\setminus\{0\},\cdot)$ היא חבורה חילופית.
3. <u>פילוג</u>: $\forall a,b,c \in \mathbb{F} : a(b+c) = ab + ac$.

האם צריך לומר במפורש ש-$0 \neq 1$? לא, הרי $1 \in \mathbb{F}\setminus\{0\}$, ולכן ודאי $0 \neq 1$.

<u>חבורות</u>

<u>טענה (תכונת הצמצום)</u>: תהי חבורה G ויהיו $a,b,c \in G$ כך ש-$ab = ac$. אזי בהכרח $b = c$.

<u>הוכחה</u>:

$a \in G$ ולכן יש לו הופכי $a^{-1} \in G$. נכפול בו משמאל בשני צדי השוויון:

$$a^{-1}(ab) = a^{-1}(ac)$$

בזכות האסוציאטיביות נקבל:

$$(a^{-1}a)b = (a^{-1}a)c$$

$$eb = ec$$

$$b = c$$

■

באופן דומה, ניתן להוכיח צמצום מימין.

האם יתכן שבחבורה G יש שני איברי יחידה שונים? לא.

<u>הוכחה</u>:

יהיו $e,h \in G$ איברים ניטרליים.

$$h = \{\text{נייטרלי } e\} = eh = \{\text{נייטרלי } h\} = e$$

<u>הדוגמאות המרכזיות לחבורות</u>:

<u>הדוגמא הכי חשובה – חבורת התמורות</u>:

נגדיר את:

$$S_n = \{f : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \text{ הפונקציות ההפיכות}\}$$

עם פעולת ההרכבה.

נוכיח שאכן מדובר בחבורה:

1. <u>סגירות</u>: תהיינה $f,g \in S_n$. צ"ל $fg = f \circ g \in S_n$.
אכן הרכבת הפיכות היא הפיכה.
2. <u>אסוציאטיביות</u>: אכן הרכבה היא פעולה אסוציאטיבית (מבדידה).
3. <u>ניטרלי</u>: פונקציית הזהות הפיכה ולכן שייכת ל-S_n, וכמובן שהיא ניטרלית להרכבה (מבדידה).
4. <u>הופכיים</u>: לכל $f \in S_n$ קיימת פונקציה הופכית f^{-1} וגם היא שייכת ל-S_n כי ההופכית הפיכה.

<u>הערה</u>: באופן כללי, אוסף כל הפונקציות ההפיכות מקבוצה לעצמה היא חבורה. עבור הקבוצה A נסמן חבורה זו ב-S_A.

<u>**דוגמא**</u>:

נביט בקבוצת כל המטריצות ההפיכות:

$$GL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} : |A| \neq 0\}$$

האם $(GL_n(\mathbb{F}), +)$ **חבורה?** לא, אין ניטרלי וסגירות, ואין דברים נוספים.

האם $(GL_n(\mathbb{F}),\cdot)$ **חבורה?** כן. בקצרה: כפל הפיכות הפיכה, כפל מטריצות אסוציאטיבי, מטריצת היחידה הפיכה וניטרלית ולכל מטריצה הפיכה יש הופכית שגם היא הפיכה.

מבנים אלגבריים – הרצאה 2 (קבוצת הרצאה 01)

נושא ההרצאה: תתי-חבורות ותתי-חבורות ציקליות

תזכורת

הגדרה – חבורה: חבורה היא קבוצה עם פעולה כך שמתקיימות 4 תכונות – סגירות, קיבוץ, קיום איבר נייטרלי, קיום איברים הופכיים.

דוגמאות:

- $GL_n(\mathbb{F})$ – מטריצות הפיכות עם כפל.
- $\mathbb{Z}$ עם חיבור.
- S_n עם הרכבה.

תתי-חבורות

הגדרה – תת-חבורה: תהי חבורה G. תת-קבוצה $H \subseteq G$ נקראת תת-חבורה של G אם H היא חבורה ביחס לאותה פעולה.

דוגמאות טריוויאליות לתתי-חבורות: $G, \{e_G\}$.

קריטריון מקוצר לתת-חבורה: תהי חבורה G ותהי תת-קבוצה H. אזי H תת-חבורה של G אם ורק אם מתקיימים שני התנאים הבאים:

1. $e_G \in H$.
2. לכל $a, b \in H$ מתקיים כי $ab^{-1} \in H$.

הוכחה:

בכיוון ראשון, נניח ש-H תת-חבורה, ונוכיח ששני התנאים מתקיימים.

מכיוון ש-H תת-חבורה, יש בה איבר ניטרלי לפעולה. האיבר הזה צריך להיות ניטרלי רק לאיברים מתוך H. האם ייתכן שמדובר באיבר אחר פרט לניטרלי של G?

נביט בניטרלי של H - $e_H \in H$.

$$e_H e_H = e_H$$

כלפי e_H הוא ניטרלי כי מדובר באיבר מ-H. כלפי e_G לא ברור בכלל ש-e_H נייטרלי, ולכן אנחנו הולכים בכיוון הזה.

$$e_H e_G = e_H$$

כי e_G ניטרלי בכל החבורה.

ביחד נסיק:

$$e_H e_H = e_H e_G$$

ולפי תכונת הצמצום נובע כי $e_H = e_G$.

הרווחנו גם את מה שרצינו להוכיח (תנאי 1), אבל על הדרך הוכחנו שהניטרלי של תת-חבורה חייב להיות הניטרלי של החבורה המקורית.

כעת לתנאי 2 – יהיו $a, b \in H$. צ״ל $ab^{-1} \in H$.

מכיוון ש-H תת-חבורה, ולכן חבורה, יש בה הופכי ל-b. נקרא לו c. האם הוא חייב להיות ההופכי של b ב-G? לא. לכן, נוכיח את זה.

$$bc = e_H$$

$$bb^{-1} = e_G$$

אבל ראינו ש-$e_H = e_G$, ולכן:

$$bc = bb^{-1}$$

ולפי צמצום, אכן:

$$b^{-1} = c \in H$$

ולכן, מכיוון ש-$a, b^{-1} \in H$, ומכיוון ש-H תת-חבורה, לפי סגירות גם:

$$ab^{-1} \in H$$

בכיוון השני:

נתון כי מתקיימים שני התנאים, צ״ל כי H תת-חבורה של G.

1. צ״ל סגירות:
   יהיו $a, b \in H$. צ״ל $ab \in H$, אבל נתון לנו בלבד כי $ab^{-1} \in H$.
   ידוע כי $e_G, b \in H$ (לפי תנאי 1). יחד עם תנאי 2 ניתן להסיק כי $e_G b^{-1} \in H$.
   כלומר, כמובן:
   $$b^{-1} \in H$$
   כעת, $a, b^{-1} \in H$, ולכן לפי תנאי 2:
   $$a(b^{-1})^{-1} \in H$$
   אבל:
   $$(b^{-1})^{-1} = b$$
   וקיבלנו אכן ש-
   $$ab \in H$$
2. אסוציאטיביות – מקרה פרטי של אסוציאטיביות הפעולה על כל G.
3. ניטרלי – נתון ש-$e_G \in H$, ומכיוון שהוא ניטרלי בכל החבורה, בפרט הוא ניטרלי ב-H.
4. הופכיים – הוכחנו כבר לכל כי לכל $b \in H$ גם $b^{-1} \in H$.

■

דוגמאות לתתי חבורות:

- $SL_n(\mathbb{F}) = \{M \in \mathbb{F}^{n\times n} : |M| = 1\}$

האם זו תת-חבורה של $GL_n(\mathbb{F})$ (ברור שזו תת-קבוצה, הרי מטריצות עם דטרמיננטה 1 הן הפיכות).

1. אכן $|I| = 1$, ולכן $I \in SL_n$
2. תהיינה $A, B \in SL_n$. צ״ל ש-$AB^{-1} \in SL_n$.
כלומר, צ״ל $|AB^{-1}| = 1$.

$$|AB^{-1}| = |A||B^{-1}| = \frac{|A|}{|B|} = \frac{1}{1} = 1$$

- האם מעגל היחידה הוא תת-חבורה של $\mathbb{C}$?

המרוכבים הם חבורה עם חיבור, ומעגל היחידה אינו תת-חבורה, למשל $1 + 1 = 2$ לא שייך למעגל היחידה.

- $A = \{z \in \mathbb{C} : |z| = 1\}$

האם זו תת-חבורה של $\mathbb{C} \setminus \{0\}$ (הפעולה היא כמובן כפל)?
כן, וההוכחה כמעט זהה ל-SL_n

- $\{1, -1, i, -i\}$

האם זו תת חבורה של $\mathbb{C} \setminus \{0\}$?
האמת שכן, אבל נראה זאת באמצעות הנושא של תתי-חבורות ציקליות בהמשך.
בעצם, נראה בהמשך כי $\langle i\rangle = \{1, -1, i, -i\}$.

- $\left\{\pm\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \pm\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}, \pm\begin{pmatrix}0 & i\\i & 0\end{pmatrix}, \pm\begin{pmatrix}i & 0\\0 & -i\end{pmatrix}\right\} \subseteq GL_2(\mathbb{C})$ - קווטרניונים.

- $\mathbb{C} \setminus \{0\} = \left\{\begin{pmatrix}a & b\\-b & a\end{pmatrix} \in \mathbb{R}^{2\times 2} \middle| a^2 + b^2 \neq 0\right\}$

האם זו תת חבורה של $GL_2(\mathbb{R})$?
שימו לב לא לשכוח להוכיח שזה בכלל מוכל!
בשיעורי בית הוכחתם שזו אכן תת-חבורה.

$$\begin{pmatrix}a & b\\-b & a\end{pmatrix} \cdot \begin{pmatrix}c & d\\-d & c\end{pmatrix} = \begin{pmatrix}ac - bd & ad + bc\\-(ad + bc) & ac - bd\end{pmatrix}$$

זה בדיוק כפל מרוכבים!
למעשה, זו אחת הדרכים להגדיר את המרוכבים:

$$a + bi = \begin{pmatrix}a & b\\-b & a\end{pmatrix}$$

תתי-חבורות ציקליות

("ציקליות" מלשון $cycle$)

סימונים:

איך קוראים לזה כשמבצעים פעולה בין איבר לעצמו מספר פעמים?

$$1+1+1+1=4\cdot 1$$

$$2\cdot 2\cdot 2=2^3$$

בהתאם לכך, בחבורה שהפעולה שלה מסומנת בכתיב כפלי, נגדיר:

$$a^n=aa\cdots a$$

n פעמים.

אבל, אם הפעולה של החבורה היא בכתיב חיבורי, אזי נסמן:

$$na=a+a+\cdots+a$$

n פעמים.

דוגמא: נביט בחבורה $\mathbb{Z}_7$ (עם חיבור מודולו 7).

$$5\cdot 2=2+2+2+2+2=3$$

הגדרה:

כמו כן, נגדיר:

$$a^0=e_G$$

וכן:

$$a^{-n}=(a^{-1})^n$$

תרגיל לבית שקל להוכיח: $(a^{-1})^n=(a^n)^{-1}$

הגדרה – תת-חבורה ציקלית: תהי G חבורה ויהי $a\in G$. נגדיר את תת-החבורה הציקלית להיות:

$$\langle a\rangle=\{a^n|n\in\mathbb{Z}\}$$

למעשה, צריך להוכיח שהקבוצה הזו היא אכן תת-חבורה.

הוכחה:

מתוך סגירות ברור ש-$\langle a\rangle\subseteq G$.

כעת נראה את הקריטריון המקוצר:

1. אכן $e_G=a^0\in\langle a\rangle$.
2. יהיו $a^n,a^k\in\langle a\rangle$. צ"ל: $a^n(a^k)^{-1}\in\langle a\rangle$

אכן:

$$a^n(a^k)^{-1}=a^n(a^{-1})^k=\{\text{תרגיל}\}=a^{n-k}\in\langle a\rangle$$

דגש: זה לא נובע מחוקי חזקות, הרי לא מדובר בחזקות של ממשיים.

<u>דוגמא</u>:

$$G = \mathbb{Z}_{12}$$

$$\langle 3\rangle = \{\cancel{3^0, 3^1, 3^{-1}, 3^2, 3^{-2}}\} = \{0,3,3+3,3+3+3\} = \{0,3,6,9\}$$

<u>דוגמא</u>:

$$G = \mathbb{C}\ \{0\}$$

$$\langle i\rangle = \{1, i, -1, -i\}$$

עוד לא הוכחנו שזה מכסה את כל החזקות, נוכיח בהמשך.

<u>הגדרה – סדר של איבר</u>: תהי חבורה G, ויהי $a \in G$. נגדיר את ה<u>סדר</u> של האיבר $o(a)$ להיות החזקה החיובית (גדולה מאפס) הקטנה ביותר עבורה $a^{o(a)} = e_G$.

<u>שאלה</u>: האם לכל איבר מוגדר סדר?

תשובה: לא. למשל $1 \in \mathbb{Z}$, חזקותיו הן: $1,2,3,4, \dots$, ולעולם הן לא תהיינה שוות לאיבר הניטרלי 0.

$$\langle 1\rangle = \{0,1,-1,2,-2,\dots\} = \mathbb{Z}$$

למעשה, השלמים היא חבורה ציקלית – כלומר, היא שווה לתת-החבורה הציקלית של אחד מאיבריה.

<u>שאלה</u>: האם בחבורה אינסופית יתכן שלאיבר יהיה סדר סופי?

תשובה: לכל חבורה G מתקיים כי $o(e_G) = 1$. למעשה, איבר היחידה הוא היחיד שהסדר שלו הוא 1 (קל לראות).

<u>שאלה</u>: האם פרט לאיבר היחידה, ייתכן שבחבורה אינסופית יהיה איבר עם סדר סופי?

תשובה: כן. בחבורה $G = \mathbb{C} \setminus \{0\}$ מתקיים כי: $o(i) = 4$.

<u>שאלה</u>: האם ייתכן שבחבורה סופית יהיה איבר מסדר אינסופי?

תשובה: לא. נוכיח בהמשך שבחבורה סופית לכל איבר יש סדר סופי.

מבנים אלגבריים – הרצאה 3 (קבוצת הרצאה 01)

נושא ההרצאה: תתי-חבורות ציקליות ותמורות

תזכורת

הגדרה – תת-חבורה ציקלית: תהי G חבורה כלשהי, ויהי $a \in G$. אזי תת-החבורה הציקלית של a הינה:

$$\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$$

הגדרה – סדר של איבר: סדר של איבר $o(a)$ הוא החזקה החיובית הקטנה ביותר כך ש-$a^{o(a)} = e_G$.

דוגמא: $o(e_g) = 1$. כמו כן, אם $o(a) = 1$, אזי $a = a^1 = e_G$.

תתי-חבורות ציקליות

משפט: תהי חבורה G, ויהי $a \in G$. אזי:

$$o(a) = |\langle a\rangle|$$

כלומר, הסדר של האיבר הוא בדיוק הגודל של תת-החבורה הציקלית.

מסקנה: אם G סופית, כל תת-חבורה שלה מוכלת בה ולכן סופית, ולכן בפרט תתי-החבורות הציקליות, ולכן לכל איבר בחבורה יש סדר סופי.

הוכחת המשפט: ישנם שני מקרים בעולם: איברים מסדר סופי, ואיברים מסדר אינסופי.

(תזכורת: הסדר הוא אינסופי אם באף חזקה חיובית לא מקבלים את איבר היחידה)

מקרה 1: יהי $a \in G$ בעל סדר סופי, כלומר:

$$o(a) = n$$

נוכיח ש-$|\langle a\rangle| = n$.

נוכיח למעשה יותר מזה, ש:

$$\langle a\rangle = \{e_G, a, a^2, \dots, a^{n-1}\}$$

נראה שהחזקות הללו מכסות את כל החזקות, כולל השליליות.

כמו-כן, נראה שכלל האיברים הללו שונים זה מזה, ולכן אכן:

$$|\langle a\rangle| = |\{e_G, a, a^2, \dots, a^{n-1}\}| = n$$

נב"ש שקיימות שתי חזקות $0 \le r_1 < r_2 \le n-1$ כך ש-$a^{r_1} = a^{r_2}$.

נכפיל את שני הצדדים ב-a^{-r_1}, ונקבל:

$$e_G = a^{r_2 - r_1}$$

כעת קיבלנו:

$$0 \le r_2 - r_1 \le n-1$$

בסתירה לכך שהסדר הוא n, כי מצאנו חזקה נמוכה יותר שנותנת את איבר היחידה.

כעת, נתפנה להוכיח ש:

$$\langle a\rangle = \{e_G, a, a^2, \dots, a^{n-1}\}$$

נוכיח הכלה דו-כיוונית:

כיוון 1: טריוויאלי. ברור ש:

$$\{e_G, a, a^2, \dots, a^{n-1}\} \subseteq \langle a\rangle$$

הרי בצד שמאל יש חזקות מסוימות של a וצד ימין הוא קבוצת **כל** החזקות של a.

כיוון 2: יהי $a^k \in \langle a\rangle$. צ״ל

$$a^k \in \{e_G, a, a^2, \dots, a^{n-1}\}$$

ניעזר בחילוק עם שארית (נוכיח בהמשך במדויק שזה תמיד אפשרי):

$$k = p \cdot n + r$$

כאשר $0 \le r \le n-1$.

זה נכון גם אם $k < 0$.

כעת,

$$a^k = a^{pn+r} = (a^n)^p a^r = (e_G)^p a^r = a^r \in \{e_G, a, a^2, \dots, a^{n-1}\}$$

<u>מקרה 2</u>: יהי $a \in G$ בעל סדר אינסופי.

צ״ל שגם $\langle a\rangle$ אינסופית.

נב״ש ש-$\langle a\rangle$ סופית.

מכיוון שיש אינסוף מספרים שלמים, שתי חזקות שונות חייבות מתישהו לחזור לאותו המספר. כלומר, קיימות $0 \le r_1 < r_2$ כך ש-$a^{r_1} = a^{r_2}$.

לכן, כמו קודם:

$$e_G = a^{r_1 - r_2}$$

מכיוון שמצאנו חזקה חיובית $r_2 - r_1 > 0$ של a שנותנת את איבר היחידה, זו סתירה לכך שסדר האיבר אינסופי.

■

תמורות

הגדרה – תמורה: תמורה היא סידור של המספרים מ-1 עד n.

תזכורת: S_n היא קבוצת התמורות (פונקציות הפיכות) מקבוצה בגודל n לעצמה (סופית). באופן כללי, לקבוצה כלשהי (לאו דווקא סופית) מגדירים S_A אך לא מגדירי סימן.

הערה: $|S_n| = n!$.

הערה: $|S_\emptyset| = 0! = 1$.

הגדרה – סימן של תמורה: תהי $f \in S_n$. הסימן של התמורה f הוא:

$$sign(f) = \prod_{i<j} \frac{f(j) - f(i)}{j - i}$$

הערה: $\forall f \ : sign(f) \in \{\pm 1\}$.

מינוח: אם סימן התמורה הוא -1 – אומרים שהיא אי-זוגית או שלילית, ואם הסימן הוא 1 אומרים שהיא זוגית או חיובית.

דוגמא:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S$$

אזי:

$$sign(f) = \frac{1-3}{2-1} \cdot \frac{2-3}{3-1} \cdot \frac{4-3}{4-1} \cdot \frac{2-1}{3-2} \cdot \frac{4-1}{4-2} \cdot \frac{4-2}{4-3} = - \cdot - \cdot + \cdot + \cdot + \cdot +$$

דוגמא: תהי $I \in S_n$.

אזי:

$$sign(I) = \prod_{i<j} \frac{j-i}{j-i} = 1$$

כלומר, הסימן של תמורת הזהות הוא תמיד 1, לכל n. תמורת הזהות היא תמורה חיובית או זוגות.

טענה – כפליות הסימן: תהיינה $f, g \in S_n$. אזי:

$$sign(f \circ g) = sign(f) \cdot sign(g)$$

הוכחה:

לפי הגדרת הסימן:

$$sign(f \circ g) = \prod_{i<j} \frac{f(g(j)) - f(g(i))}{j - i} =$$

$$= \prod_{i<j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \prod_{i<j} \frac{g(j) - g(i)}{j - i}$$

$= sign(g)$

שווה ל-$sign(f)$ מכיוון ש-g חח"ע ועל ואוסף הזוגות $i \neq j$ שווה לאוסף הזוגות $(g(i), g(j))$

ולכן $sign(f \circ g) = sign(f) \cdot sign(g)$, כנדרש. ■

<u>דוגמא</u>:

$$A = \{1,2,3\}$$

$$g(1) = 2, \qquad g(2) = 3, \qquad g(3) = 1$$

$$(1,2), (1,3), (2,3)$$

$$\big(g(1), g(2)\big) = (2,3)$$

$$\big(g(1), g(3)\big) = (2,1)$$

$$\big(g(2), g(3)\big) = (3,1)$$

$$sign(g) = \frac{g(1) - g(2)}{1-2} \cdot \frac{g(1) - g(3)}{1-3} \cdot \frac{g(2) - g(3)}{2-3} = 1 \cdot \frac{1}{-2} \cdot \frac{2}{-1} = +1$$

<u>הגדרה – חילוף</u>: יהיו $1 \le p_1 \ne p_2 \le n$. נגדיר את <u>החילוף</u> $f = (p_1 p_2) \in S_n$.

על-ידי:

$$f(x) = \begin{cases} p_2 & x = p_1 \\ p_1 & x = p_2 \\ x & \text{אחרת} \end{cases}$$

<u>הערה</u>: זוהי פונקציה חח״ע ועל, ולכן היא תמורה.

<u>חישוב סימן תמורת החילוף</u>: נסמן את שאר האיברים בתמורה מ-3 עד n ב-$p_3, \dots, p_n$.

$$sign\big((p_1p_2)\big) = \frac{p_1 - p_2}{p_2 - p_1} \cdot \frac{p_3 - p_2}{p_3 - p_1} \cdot \dots \cdot \frac{p_n - p_2}{p_n - p_1} \cdot \frac{p_3 - p_1}{p_3 - p_2} \cdot \dots \cdot \frac{p_n - p_1}{p_n - p_2} \cdot \dots \cdot \frac{p_4 - p_3}{p_4 - p_3} \cdot \dots \cdot \frac{p_n - p_{n-1}}{p_n - p_{n-1}} = -1$$

כלומר, חילוף הוא תמורה <u>אי-זוגית</u>.

<u>הגדרה – מחזור</u>: יהיו $1 \le p_1, \dots, p_k \le n$ שונים. נגדיר את <u>המחזור</u>:

$$(p_1 \dots p_k) = (p_1p_2) \circ (p_2p_3) \circ \dots \circ (p_{k-1}p_k)$$

סימן מחזור באורך k הוא $(-1)^{k-1}$.

<u>הערה</u>: נשים לב שאם ישנו מספר זוגי של איברים במחזור, אז הסימן הוא אי-זוגי, ואם ישנו מספר אי-זוגי של איברים במחזור, אז הסימן הוא זוגי.

<u>דוגמא</u>:

$$(4\ 2\ 6\ 3) \in S_6$$

$$(4\ 2\ 6\ 3) = (4\ 2)(2\ 6)(6\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{pmatrix}$$

<u>טענה</u>: המחזור $f = (p_1 \dots p_k)$ הוא התמורה:

$$f(x) = \begin{cases} p_1 & x = p_k \\ p_i & x = p_{i-1} \\ x & \text{אחרת} \end{cases}$$

<u>הוכחת הטענה</u>:

$$f = (p_1 p_2) \dots (p_{i-1} p_i) \dots (p_{k-1} p_k)$$

יהי $x \neq p_1, \dots, p_k$

ונקבל:

$$f(x) = x$$

יהי $2 \leq i \leq k$, ועבורו:

$$f(p_{i-1}) = p_i$$

ועבור k:

$$f(p_k) = p_1$$

כנדרש. ■

<u>דוגמא</u>:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$$

נפרק את התמורה להרכבה של מחזורים:

$$f = (1\ 3\ 4)(2\ 7\ 5\ 6) = + \cdot - = -$$

<u>דוגמא</u>:

$$g = (1\ 2\ 3)$$

מחזור באורך אי-זוגי הוא (באופן אירוני) תמורה זוגית והסימן שלו חיובי.

<u>דוגמא</u>:

$$g(1) = 2, \quad g(2) = 4, \quad g(3) = 1, \quad g(4) = 5, \quad g(5) = 3$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = (1\ 2\ 4\ 5\ 3)$$

$$sign(g) = +$$

<u>דוגמא</u>:

$$sign \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = sign(1\ 2\ 4)(3\ 5) = + \cdot - = -$$

מבנים אלגבריים – הרצאה 4 (קבוצת הרצאה 01)

נושא ההרצאה: הומומורפיזם ואיזומורפיזם בין חבורות, משפט קיילי

תזכורת

למדנו על סימן של תמורה.

הבטחנו שכל חבורה היא במובן מסוים תת-חבורה של חבורת תמורות, והיום נוכל להתחיל להוכיח את זה.

הקדמה

דוגמה:

{שילת, גיתית, אביעד, תומר}

הפעולה: אדם א' ניגש לאדם ב' ומשדל אותו להטריל את אדם ג'.

מי הוא האיבר הנייטרלי? אם הנייטרלי ניגש למישהו, אז מטרילים את המישהו. אם הנייטרלי מדבר עם עצמו, הוא מטריל את עצמו.

נגיד שתומר הוא האיבר הנייטרלי. מתקיים:

ש = ג · א

ג = ש · א

א = ש · ג

{אריאל, הודיה, יניר, ***אוסקר***}

כעת, לא נספר מה הפעולה. ***אוסקר*** נייטרלי. יניר · הודיה נותן אריאל, יניר · אריאל נותן הודיה, והודיה · אריאל נותן יניר.

בעצם, שמנו לב שמדובר ב**אותה גברת בשינוי אדרת**! זו בעצם אותה החבורה, רק ששינינו את השמות של האיברים!

נמשיך עוד קצת עם הדוגמה:

{בנות, בנים}

בנות = בנות · בנים

בנים = בנים · בנים

בנים = בנות · בנות

הנייטרלי הוא האיבר "בנים" (זה הגיוני כי תומר הוא בן).

אז ראינו את "אותה הגברת בשינוי אדרת" (איזומורפיזם). ראינו אפשרות לקבץ את האיברים לקבוצות שונות שפועלות כמו האיברים (ממש כמו יחסי שקילות ומחלקות שקילות (הומומורפיזם).

הרעיון בהכללה – זיהוי מבנה של חבורה אחת בתוך חבורה אחרת.

בלינארית העתקות ליניאריות שמרו על המבנה של מרחב וקטורי.

<u>דוגמא</u>:

למשל, חיבור בין שלמים, אפשר לקבץ כזוגיים ואי-זוגיים.

<u>הומומורפיזם ואיזומורפיזם</u>

<u>הגדרה – הומומורפיזם</u>: תהיינה שתי חבורות G, H (לאו דווקא עם אותה הפעולה). נגדיר שפונקציה $f : G \to H$ נקראת <u>הומומורפיזם</u> אם לכל $g_1, g_2 \in G$ מתקיים:

$$f(g_1 \cdot_G g_2) = f(g_1) \cdot_H f(g_2)$$

<u>כך, למשל</u>:

$$f(\text{שילת}) = f(\text{גיתית} \cdot \text{אביעד}) = \text{הודיה} \cdot \text{יניר} = \text{אריאל}$$

$$g(\text{שילת}) = g(\text{גיתית} \cdot \text{אביעד}) = \text{בנות} \cdot \text{בנים} = \text{בנות}$$

<u>הגדרה – איזומורפיזם</u>: אם f הומומורפיזם הפיך (חח"ע ועל) הוא נקרא <u>איזומורפיזם</u>.

<u>הגדרה – חבורות איזומורפיות</u>: אם קיים איזומורפיזם בין שתי חבורות הן נקראות איזומורפיות (אותה גברת בשינוי אדרת).

האם "אותה גברת בשינוי אדרת" הוא ביטוי מתמטי? האם ניתן לתרגם אותו לטיעון מתמטי? כלומר, האם שמירה על מבנה החבורה זה טיעון מתמטי?

קשה להגדיר "שומר על המבנה" באופן מדויק (מעבר ל"איזומורפיזם"), אך אפשר להראות שתכונות מסוימות נשמרות.

<u>תכונה</u>: יהי $f : G \to H$. אם f הומומורפיזם, אזי $f(e_G) = e_H$.

הוכחה:

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G)$$

ולפי תכונת הצמצום נקבל:

$$e_H = f(e_G)$$

כנדרש. ■

<u>שאלה</u>: האם $o(g) = o\big(f(g)\big)$? לא באופן כללי בהומומורפיזמים, כן באיזומורפיזמים.

<u>דוגמא:</u>

$$f : \mathbb{Z} \to \{0\}$$

האם מדובר בהומומורפיזם?

$$f(a+b) = 0, \qquad f(a) + f(b) = 0 + 0 = 0$$

אכן קיבלנו:

$f(a+b) = f(a) + f(b)$ לכל $a, b \in \mathbb{Z}$.

לכן, אכן מדובר בהומומורפיזם. אמנם:

$$o(1) = \infty, \qquad o\big(f(1)\big) = o(0) = 1$$

וקיבלנו כי $o(g) \neq o\big(f(g)\big)$.

<u>תכונה</u>: יהי $f\,:\,G\to H$ הומומורפיזם. אזי לכל $g\in G$ מתקיים: $o\big(f(g)\big)\le o(g)$.

הוכחה: תרגיל בית. ■

<u>תכונה</u>: יהי $f\,:\,G\to H$ איזומורפיזם, אזי לכל $g\in G$ מתקיים: $o\big(f(g)\big)=o(g)$

<u>תכונה</u>: $f(g^{-1})\neq f^{-1}(g)$

<u>שימו לב</u>: אם ההומומורפיזם אינו הפיך (כלומר זה לא איזומורפיזם). לא בהכרח מוגדר בכלל f^{-1}.

<u>תכונה</u>: יהי $f\,:\,G\to H$ הומומורפיזם. אזי לכל $g\in G$ מתקיים: $f(g^{-1})=\big(f(g)\big)^{-1}$.

ההבדל הוא בין הפונקציה ההופכית (שלא בהכרח קיימת) שפועלת על g (וזה בכלל לא הגיוני שהיא תפעל על G), לבין ההופכי ב-H של התמונה של g.

כלומר, במילים פשוטות, איבר וההופכי שלו תמיד נשלחים לזוג איברים שהם ההופכיים זה של זה.

הוכחה:

ראשית, נסח שוב במדויק: יהי $f\,:\,G\to H$ הומומורפיזם בין חבורות. אזי לכל $g\in G$ מתקיים:

$$f(g^{-1})=\big(f(g)\big)^{-1}$$

כלומר, צריך להוכיח בעצם:

על-מנת להוכיח ש-$f(g^{-1})$ הוא ההופכי של $f(g)$ כפי שטענו, צריך להראות שמכפלתם היא האיבר הנייטרלי של H.

אכן:

$$f(g)f(g^{-1})=f(gg^{-1})=f(e_G)=e_H$$

כנדרש. ■

כמו בהעתקות לינאריות, נרצה לדבר על גרעין ותמונה של הומומורפיזם.

מה השגנו מגרעין ותמונה בהעתקות? הגרעין אמר כמה ההעתקה חח"ע, והתמונה אמרה כמה ההעתקה על.

אותו דבר יקרה כאן.

<u>הגדרה – תמונה וגרעין של הומומורפיזם</u>: יהי $f\,:\,G\to H$ הומומורפיזם. נגדיר את <u>התמונה</u>:

$$Im\,f=\{f(g)|g\in G\}$$

ונגדיר את <u>הגרעין</u>:

$$Ker\,f=\{g\in G|f(g)=e_H\}$$

<u>טענה</u>: התמונה היא תת-חבורה של הטווח, והגרעין הוא תת-חבורה של התחום.

הוכחה: לפי הקריטריון המקוצר. תרגיל בית. ■

<u>טענה</u>: f חח"ע אם ורק אם $Ker\,f=\{e_G\}$, וכן f על אם ורק אם $Im\,f=H$.

הוכחה: תרגיל בית. ■

<u>סימון</u>: איזומורפיזם מסמנים כך: $\cong$.

<u>תכונה</u>: יהי $f\,:\,G\to H$ הומומורפיזם חח"ע. אזי $G\cong Im\,f$ (במילים, G איזומורפית לתמונה של f, שהיא תת-חבורה של H).

הוכחה: נצמצם את הפונקציה f כדי לקבל פונקציה חח"ע ועל מ-G לתמונה של f.

$$f\,:\,G\to Im(f)$$

■

תהי חבורה G, ונביט בחבורת התמורות S_G. S_G היא חבורה כל הפונקציות ההפיכות מ-G לעצמה (עם פעולת ההרכבה).

<u>דוגמא</u>:

$$G=\{1,-1,i,-i\}=\langle i\rangle$$

$$|S_G|=4!=24$$

ניתן לדוגמא חלק מהתמורות כאן:

$$S_G=\{I,(1\ \ -1),(1\ \ -i\ \ \ i)$$

$$(1\ \ -i\ \ \ i)=\begin{pmatrix}1 & -1 & i & -i\\ -i & -1 & 1 & i\end{pmatrix}$$

הפעולה בחבורה המקורית G בדוגמא היא כפל. בחבורת התמורות, כלומר חבורת הפונקציות S_G הפעולה היא הרכבה.

גודל החבורה המקורית הוא 4, וגודל חבורת התמורות הוא 24.

אנחנו נבנה פונקציה חח"ע:

$$\phi\,:\,G\to S_G$$

ששולחת כל איבר מ-G לתמורה כלשהי (כלומר, לפונקציה).

<u>הערה</u>: הומומורפיזם חח"ע ייקרא <u>שיכון</u>, כי הוא משכן את G בתוך הטווח, כך ש"כל איבר מקבל סוויטה פרטית").

ואז נסיק את משפט קיילי.

<u>משפט קיילי</u>: כל חבורה איזומורפית לתת-חבורה של חבורת התמורות.

$$G\cong Im\,f$$

במילים פשוטות, כל חבורה בעולם היא תת-חבורה של חבורת התמורות (מקסימום בשינוי אדרת), וכל פעולה היא בעצם הרכבה.

נדגים ראשית על הדוגמא:

$$\phi(1)=\begin{pmatrix}1 & -1 & i & -i\\ 1 & -1 & i & -i\end{pmatrix}$$

$$\phi(-1)=\begin{pmatrix}1 & -1 & i & -i\\ -1 & 1 & -i & i\end{pmatrix}$$

<u>שימו לב</u>: הפונקציה שהיא התמורה לא צריכה להיות הומומורפיזם, אלא סתם פונקציה הפיכה.

$$\phi(i) = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & -1 \end{pmatrix}$$

$$\phi(-1) = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$$

<u>הערה</u>: באופן כללי, $\phi(g) = f_g$, כאשר $f_g(a) = ga$.

מבנים אלגבריים – הרצאה 5 (קבוצת הרצאה 01)

נושא ההרצאה: משפט קיילי ומשפט לגראנז'

תזכורת

תהי G חבורה, אז S_G היא חבורת כל הפונקציות ההפיכות מ-G לעצמה.

אנחנו רוצים לבנות פונקציה:

$$\varphi : G \to S_G$$

ששולחת כל איבר מ-G לפונקציה בחבורת התמורות, ושהיא תהיה:

1. מוגדרת היטב.
2. הומומורפיזם
3. חח"ע.

אם נבנה כזו (קוראים לה שיכון קיילי, אגב), נקבל את **משפט קיילי**:

$$G \cong im(\varphi)$$

כלומר, החבורה (שהיא חבורה כלשהי) איזומורפית לתת-חבורה של חבורת התמורות.

ראשית, לכל איבר $a \in G$ נתאים פונקציה f_a המוגדרת על-ידי:

$$f_a(g) = ag$$

במילים, הפונקציה מפעילה את a על כל איבר שהיא מקבלת.

ברור ש:

$$f_a : G \to G$$

נגדיר את **שיכון קיילי** על-ידי:

$$\varphi(a) = f_a$$

כלומר, שולחים כל איבר לפונקציה ש"כופלת" באותו האיבר.

מה צריך להראות על-מנת להוכיח ששיכון קיילי מוגדר היטב? צריך להראות שהפונקציות הללו ב-S_G.

הוכחת משפט קיילי

הוכחה ש-f_a חח"ע ועל:

חח"ע: יהיו $g_1, g_2 \in G$ כך ש-$f_a(g_1) = f_a(g_2)$. לכן:

$$ag_1 = ag_2$$

לפי צמצום:

$$g_1 = g_2$$

ולכן חח"ע.

על: יהי $g \in G$. צריך למצוא $x \in G$ כך ש-$f_a(x) = g$.

כלומר:

$$ax = g$$

קל לראות ש-$x = a^{-1}g$ מקיים את הדרוש.

כלומר, עד כה הגדרנו (היטב) פונקציה

$$\varphi : G \to S_G$$

על-ידי:

$$\varphi(a) = f_a \in S_G$$

<u>השלב הבא – להוכיח שמדובר בהומומורפיזם</u>:

יהיו $a_1, a_2 \in G$. צ"ל:

$$\varphi(a_1 \cdot_G a_2) = \varphi(a_1) \circ \varphi(a_2)$$

כלומר, צ"ל:

$$f_{a_1a_2} = f_{a_1} \circ f_{a_2}$$

התחום והטווח הם G ושווים, צ"ל להוכיח שכל איבר נשלח לאותו מקום.

יהי $x \in G$.

$$f_{a_1a_2}(x) = (a_1a_2)x$$

$$f_{a_1} \circ f_{a_2}(x) = f_{a_1}\left(f_{a_2}(x)\right) = f_{a_1}(a_2x) = a_1(a_2x)$$

שני הביטויים שווים כי חבורה מקיימת אסוציאטיביות.

<u>נותר שלב אחרון – להוכיח ששיכון קיילי φ הוא חח"ע</u>:

יהיו $a_1, a_2 \in G$ כך ש:

$$\varphi(a_1) = \varphi(a_2)$$

לכן:

$$f_{a_1} = f_{a_2}$$

צ"ל $a_1 = a_2$.

נציב בתמורות את איבר היחידה:

$$f_{a_1}(e) = f_{a_2}(e)$$

$$a_1e = a_2e$$

$$a_1 = a_2$$

מעתם, אם מבקשים למצוא תת-חבורה של תמורות שאיזומורפית ל-G, מותר ישירות לקחת את התמונה משיכון קיילי.

משפט לגראנז'

הקדמה:

תהי חבורה G ותהי תת-חבורה $H \subseteq G$.

הגדרה: לכל איבר $a \in G$ נגדיר את המחלקה:

$$aH = \{ah | h \in H\}$$

דוגמא:

$$G = S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

נביט בתת-החבורה:

$$H = \langle(1\ 3)\rangle = \{I, (1\ 3)\}$$

נביט בכל המחלקות של H:

$$IH = \{I, (1\ 3)\} = H$$

$$(1\ 2)H = \{(1\ 2), (1\ 3\ 2)\}$$

שיטה מהירה לחישוב:

$$(1\ 2)(1\ 3) = (2\ 1)(1\ 3) = (2\ 1\ 3) = (1\ 3\ 2)$$

$$(1\ 3)H = \{(1\ 3), I\} = H$$

$$IH = (1\ 3)H = H$$

$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$$

$$(2\ 3)(1\ 3) = (2\ 3)(3\ 1) = (2\ 3\ 1)$$

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (2\ 3)\} = (2\ 3)H$$

$$(1\ 2\ 3)(1\ 3) = (2\ 3)$$

$$(1\ 3\ 2)H = \{(1\ 3\ 2), (1\ 2)\}$$

סה"כ קיבלנו 3 מחלקות שכל אחת הכילה שני איברים.

גודל כל המחלקות שווה, ושווה לגודל של H.

המסקנה (שתקרא משפט לגראנז', בערך) היא שהגודל של תת-החבורה חייב לחלק את גודל החבורה.

מה אנחנו רוצים לעשות?

ראשית, אנחנו רוצים להגדיר יחס שקילות שייצר לנו את המחלקות הללו בדיוק, כי אז זה מבטיח שהחבורה מתחלקת למחלקות שאין ביניהן חיתוך אך הן מכסות את הכל (חלוקה).

לפני הגדרת יחס השקילות, נדגים. נרצה לחלק את השלמים למחלקות הבאות:

$$\{0, \pm 3, \pm 6, \dots\}, \qquad \{1, -2, 4, -5, 7, -8\}, \qquad \{2, -1, 5, -4, 8, -7\}$$

(זה בעצם $3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$)

מה היחס שמגדיר ששני איברים באותה המחלקה?

נבדוק שההפרש בין כל שני איברים מתחלק ב-3.

נגדיר את הרעיון הזה ליחס שקילות כללי:

תהי חבורה G ותת-חבורה H. נגדיר יחס שקילות R על-ידי:

לכל $g_1, g_2 \in G$:

$$g_1 R g_2$$

אם ורק אם:

$$g_1^{-1} g_2 \in H$$

נוכיח שני דברים:

1. מדובר ביחס שקילות.
2. לכל $a \in G$ מתקיים $[a]_R = aH$.
3. לכל $a \in G$ מתקיים $|aH| = |H|$.

ואז אם G סופית נקבל את **<u>משפט לגראנז'</u>**:

$$|H| \cdot |[G : H]| = |G|$$

כאשר $[G : H]$ הוא ה**<u>אינדקס</u>** של תת-החבורה, שמוגדר להיות כמות המחלקות השונות.

המסקנה היא שהגודל של כל תת-חבורה של חבורה סופית חייב לחלק את גודל החבורה.

<u>הוכחת יחס שקילות</u>:

רפלקסיביות: יהי $g \in G$. צ"ל ש-gRg. צ"ל:

$$g^{-1} g \in H$$

ברור כי $g^{-1} g = e$ ו-H היא תת-חבורה ולכן מכילה את האיבר הניטרלי של החבורה.

סימטריות: יהיו $g_1, g_2 \in G$ כך ש-$g_1 R g_2$. צ"ל $g_2 R g_1$.

נתון:

$$g_1^{-1} g_2 \in H$$

לכן גם ההופכי ב-H (כי זו תת-חבורה):

$$(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \in H$$

כפי שרצינו.

טרנזיטיביות: יהיו $g_1, g_2, g_3 \in G$ כך ש-$g_1Rg_2,\ \ g_2Rg_3$. צ"ל g_1Rg_3.

נתון כי:

$$g_1^{-1}g_2 \in H$$

$$g_2^{-1}g_3 \in H$$

מכיוון ש-H תת-חבורה, המכפלה גם ב-H:

$$g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3 \in H$$

הוכחנו שמדובר ביחס שקילות.

נעצור לדוגמא רגע:

בדוגמא של התמורות:

$$(1\ 3\ 2), (1\ 2) \in (1\ 3\ 2)H$$

לכן אנו מצפים כי:

$$(1\ 3\ 2)^{-1}(1\ 2) \in H$$

נחשב:

$$(2\ 3\ 1)(1\ 2) = (1\ 3)$$

<u>כעת יהי $a \in G$. צ"ל:</u>

$$\underline{[a]_R = aH}$$

נבצע הכלה דו-כיוונית בין שתי הקבוצות:

כיוון ראשון: יהי $x \in [a]_R$. צ"ל כי $x \in aH$.

נתון כי:

$$a^{-1}x \in H$$

קיים $h \in H$ כך ש:

$$a^{-1}x = h$$

לכן:

$$x = ah \in aH$$

כיוון שני: יהי $ah \in aH$. צ"ל כי $ah \in [a]_R$.

צ"ל $aRah$, כלומר:

$$a^{-1}(ah) \in H$$

אבל אכן:

$$a^{-1}ah = h \in H$$

<u>דבר אחרון, יהי $a \in G$, צ״ל ש-$|H| = |aH|$.</u>

נבנה פונקציה חח״ע ועל בין שתי הקבוצות. נגדיר:

$$f : H \to aH$$

על-ידי:

$$f(h) = ah$$

ברור שהיא מוגדרת היטב, מתכונת הצמצום קל להראות שהיא חח״ע, וקל להראות גם שהיא על בעזרת ההופכי של a.

סה״כ הוכחנו את משפט לגראנז׳. ■

מבנים אלגבריים – הרצאה 6 (קבוצת הרצאה 01)

נושא ההרצאה: המחלק המשותף הגדול ביותר (gcd)

המטרה: להבין את חבורת אוילר בשביל להגיע ל-RSA.

הגדרה – יחס שקילות 'מודולו n': יהי $n \in \mathbb{N}$. נגדיר יחס שקילות 'מודולו n' באופן הבא:

$$a \equiv_n b \Leftrightarrow \exists k \in \mathbb{Z} : a = b + kn$$

קל להוכיח שמדובר ביחס שקילות.

הערה: באתר מסומן $a \equiv b \bmod n$.

משפט החלוקה עם שארית (חוגים): יהי $a \in \mathbb{Z}$ ויהי $n \in \mathbb{N}$ (רוצים לחלק את a ב-n עם שארית). אזי קיימים q, r יחידים כך ש:

1. $a = qn + r$ (q נקרא המנה, r נקרא השארית).
2. $0 \leq r < n$ (בתכונת לעתים פעולת המודולו תחזיר דווקא שארית שלילית).

דוגמא:

$$10 = 2 \cdot 4 + 2$$

נחלק את 10 ב-4. המנה תהא 2, והשארית גם 2.

$$-18 = (-3) \cdot 7 + 3$$

נחלק את מינוס 18 ב-7. המנה תהא מינוס 3, והשארית תהא 3.

הוכחת משפט החלוקה:

נוכיח ראשית קיום:

נתחיל בלהוכיח קיום עבור $a \geq 0$. נעשה זאת באינדוקציה על a עבור n כלשהו.

בדיקה: עבור $a = 0$:

$$0 = 0 \cdot n + 0$$

יהי a עבורו הטענה נכונה. נוכיח עבור $a + 1$:

$$a + 1 = (qn + r) + 1 = qn + (r + 1)$$

אם $0 \leq r + 1 < n$, סיימנו – מצאנו את המנה והשארית.

אחרת, מכיוון ש-$0 \leq r < n$, המצב היחיד שנותן הוא $r + 1 = n$. במצב זה:

$$a + 1 = qn + (r + 1) = qn + n = (q + 1)n + 0$$

ושוב מצאנו מנה ושארית.

שנייה לפני שנעבור הלאה, המחשה:

$$10 = 2 \cdot 4 + 2$$

$$11 = 2 \cdot 4 + 3$$

$$12 = 2 \cdot 4 + 4 = 3 \cdot 4 + 0$$

כעת נעבור ל-$a < 0$:

אם $a < 0$, אזי $-a > 0$.

לפי מה שהוכחנו, קיימים מנה ושארית כך ש:

$$-a = qn + r$$

$$a = (-q)n - r$$

אם $r = 0$, סיימנו.

אחרת, $0 < r < n$. נוסיף ונחסיר n:

$$a = (-q)n - n + n - r$$

במקרה זה $0 < (n - r) < n$, ולכן:

$$a = (-q - 1)n + (n - r)$$

ושוב קיבלנו מה ושארית כך שתנאים 1 ו-2 מתקיימים.

נוכיח יחידות:

נניח ש-q_1, q_2 מנות ו-r_1, r_2 שאריות מתאימות המקיימות את תנאים 1 ו-2. צ"ל שהמנות שוות והשאריות שוות.

במדויק, נתון לנו:

$$a = q_1 n + r_1 = q_2 n + r_2$$

$$0 \leq r_1, r_2 < n$$

כעת:

$$q_1 n - q_2 n = r_2 - r_1$$

$$(q_1 - q_2)n = r_2 - r_1$$

כעת:

$$-n < r_2 - r_1 < n$$

מי הכפולה השלמה היחידה של n בטווח זה (הרי $(q_1 - q_2)n = r_2 - r_1$)? אפס!

ולכן:

$$r_2 - r_1 = 0$$

ולכן:

$$q_1 - q_2 = 0$$

יהי $n \in \mathbb{N}$, ויהיו $a, b \in \mathbb{Z}$, ונסמן את השאריות שלהם בחלוקה ב-n על-ידי r_a, r_b. האם השארית של ab היא $r_a r_b$? לא! כי ייתכן שמכפלת השאריות גדולה מ-n.

אבל נכון לומר:

טענה: $ab \equiv_n r_a r_b$.

מסקנה: לכל חזקה k: $a^k \equiv_n = (r_a)^k$.

הוכחה:

$$a = q_a n + r_a$$

$$b = q_b n + r_b$$

$$ab = (q_a n + r_a)(q_b n + r_b) = n(n q_a q_b + r_a q_b + r_b q_a) + r_a r_b$$

■

דוגמא:

$$n = 7, \qquad a = 11, \qquad b = 10$$

$$r_a = 4, \qquad r_b = 3$$

$$110 = 15 \cdot 7 + 5 \neq r_a r_b$$

הגדרה – המחלק המשותף הגדול ביותר (gcd): יהיו $n, k \in \mathbb{N}$. נגדיר את $\underline{\gcd(n,k)}$ להיות המספר הטבעי הגדול ביותר שמחלק גם את n וגם את k.

1 מחלק את שניהם, ומספר שגדול משניהם לא יכול לחלק אף אחד מהם. אז יש לנו קבוצה סופית לא ריקה של מחלקים משותפים, מתוכם יש אחד שהוא הגדול ביותר.

דוגמא: $\gcd(6,15) = 3$

הערה: הסיבוכיות של חישוב כוח-ישיר ("כוח בלי מוח") היא גודל המספר הקטן מהשניים. בפועל ניתן למצוא את ה-gcd בסיבוכיות לוגריתמית.

למה זה ממש ממש חשוב לנו? כל העניין של הצפנה הוא ביעילות האלגוריתמים. זה לא שאנחנו לא יודעים איך לשבור הצבנה – אפשר לנסות הכל.

טענה: יהיו $n > k \in \mathbb{N}$. אזי $\gcd(n,k) = \gcd(n-k,k)$.

כיצד זה עוזר לחישוב ה-gcd? בכל שלב, עושים חלוקה עם שארית של הגדול עם הקטן.

$$\gcd(15,6) = \gcd(15-6,6) = \gcd(3,6) = \gcd(3,3) = 3$$

<u>הוכחת הטענה</u>: צ"ל:

$$\gcd(n,k)=\gcd(n-k,k)$$

נוכיח טענה אפילו יותר קשה! נוכיח שהמחלקים המשותפים של n,k הם בדיוק המחלקים המשותפים של $n-k,k$ ואז בפרט הגדול ביותר הוא אותו אחד.

נוכיח באמצעות הכלה דו כיוונית:

אם $x|n,k$, אזי $x|(n-k)$ כפי שרצינו.

נרחיב:

$$n=q_1x$$

$$k=q_2x$$

לכן:

$$n-k=(q_1-q_2)x$$

בכיוון ההפוך, אם $x|(n-k),k$, אזי $x|\big((n-k)+k\big)$, כלומר $x|n$.

$$n-k=q_1x$$

$$k=q_2x$$

$$n=(n-k)+k=(q_1+q_2)x$$

<u>הערה</u>: $\mathbb{Z}_n$ שדה אם ורק אם הוא ראשוני.

<u>הוכחה ההערה</u>: כיוון אחד – אם n אינו ראשוני, יש מחלקי אפס וזה לא שדה. מה לגבי הכיוון השני?

<u>שאלה</u>: נביט בשדה $\mathbb{Z}_{11}$. מצאו את ההופכי של $7\in\mathbb{Z}_{11}$.

$$-7=4$$

$$7^{-1}=?$$

הדרך הגרועה ("כוח בלי מוח") היא לרוץ על כל האפשרויות.

אנחנו נמצא דרך מהירה יותר (לגוריתמית) ובנוסף על הדרך נוכיח שזה שדה אם המספר של המודולו ראשוני.

<u>טענה</u>: יהיו $n,k\in\mathbb{N}$. אזי קיימים $a,b\in\mathbb{Z}$ כך ש-$\gcd(n,k)=an+bk$.

<u>דוגמא</u>:

$$\gcd(7,11)=1$$

$$(-3)\cdot 7+2\cdot 11=1$$

<u>מסקנה</u>: $-3=\equiv_{11} 8$ הוא ההופכי של 7.

הסבר: $1\equiv_{11}7\cdot(-3)$. מכיוון ש-8 הוא השארית של מינוס 3 נובע כי גם $1\equiv_{11}7\cdot 8$.

<u>הוכחת הטענה</u>: נוכיח זאת באינדוקציה על $n+k$.

<u>בדיקה</u>: הסכום המינימלי הוא 2, כאשר שני המספרים שווים ל 1:

$$\gcd(1,1) = 1 = 1 \cdot 1 + 0 \cdot 1$$

יהי m עד אליו הטענה נכונה, נוכיח עבור $n+k=m$.

צ"ל a,b כך ש:

$$\gcd(n,k) = an + bk$$

אם $n=k$:

$$\gcd(n,k) = \gcd(n,n) = n = 1 \cdot n + 0 \cdot k$$

אחרת, $n>k$ (או ההפך), ולכן:

$$\gcd(n,k) = \gcd(n-k,k)$$

כעת:

$$(n-k)+k = n < n+k = m$$

לכן לפי הנחת האינדוקצייה כי קיימים a,b כך ש:

$$\gcd(n,k) = \gcd(n-k,k) = a(n-k) + bk = an + (b-a)^{k}$$

שיטת ההוכחה הזו גם נותנת אלגוריתם למציאת ה-a,b שכאמור נחוצים לנו בהמשך.

האלגוריתם לחשוב ה- gcd ומציאת ה-a,b נקרא <u>אלגוריתם אוקלידס</u>. אתם צריכים לשלוט במימוש של זה, כי במבחן אתם נדרשים לכך.

<u>דוגמא</u>:

$$\gcd(49,14) = \gcd(7,14) = \gcd(7,7) = 1 \cdot 7 + 0 \cdot 7$$

$$49 - 3 \cdot 14 = 7$$

$$14 - 7 = 7$$

הולכים לשוויון האחרון, כלומר $1 \cdot 7 + 0 \cdot 7$, וכל פעם מחליפים את המספר החדש באיך שהגענו אליו. אז מסדרים את הביטוי כצירוף של שני המספרים הקודמים וכן הלאה.

$$\gcd(49,14) = 1 \cdot 7 + 0 \cdot 7 = 1 \cdot 7 + 0 \cdot (14 - 7) = 1 \cdot 7 + 0 \cdot 14 =$$
$$= 1 \cdot (49 - 3 \cdot 14) + 0 \cdot 14 = 1 \cdot 49 + (-3) \cdot 14$$

<u>דוגמא</u>:

$$\gcd(9,4) = \gcd(1,4) = \gcd(1,1) = 1 \cdot 1 + 0 \cdot 1$$

$$1 = 9 - 2 \cdot 4$$
$$1 = 4 - 3 \cdot 1$$

$$\gcd(9,4) = 1 \cdot 1 + 0 \cdot 1 = 1(4 - 3 \cdot 1) = 1 \cdot 4 + (-3) \cdot 1$$
$$= 1 \cdot 4 + (-3)(9 - 2 \cdot 4) = (-3) \cdot 9 + 7 \cdot 4$$

<u>הערה להמשך</u>: $4^{-1} mod\ 9 = 7$

29/11/20

מבנים אלגבריים – הרצאה 7 (קבוצת הרצאה 01)

נושא ההרצאה: חבורת אוילר, משפטי אוילר ופרמה, מבוא להצפנה

תזכורת:

$\gcd(n,k)$ הוא המספר הטבעי הגדול ביותר שמחלק את זוג המספרים n,k.

לכל $n,k\in\mathbb{N}$ קיימים שלמים $a,b\in\mathbb{Z}$ כך ש-$an+bk=\gcd(n,k)$.

הגדרה: זוג מספרים טבעיים נקראים **זרים** אם $\gcd(n,k)=1$.

נביט בחוג השאריות $\mathbb{Z}_n$ (חיבור וכפל מודולו n).

מה חסר לחוג על-מנת להיות שדה? (חוג – חבורה חילופית ביחס לחיבור, הכפל אסוציאטיבי, יש איבר יחידה וחוק הפילוג)

חסרים חילופיות הכפל, ואיברים הופכיים (לכל איבר ששונה מאפס).

בחוג השאריות יש חילופיות לכפל, השאלה היא לגבי הופכיים.

משפט: חוג השאריות $\mathbb{Z}_n$ הוא שדה אם ורק אם n ראשוני.

תזכורת: 1 אינו ראשוני.

הערה: יש שדות שכמות האיבריים בהם היא חזקה של מספר ראשוני, אבל הפעולות הן לא מודולו n.

$$\mathbb{Z}_4=\{0,1,2,3\}$$

$$2\cdot 2=0$$

2 אינו הפיך, ולכן $\mathbb{Z}_4$ לא שדה למרות ש-$4=2^2$.

טענה: בחוג השאריות $\mathbb{Z}_n$, כל $1\le k\in\mathbb{Z}_n$ הפיך אם ורק אם k,n זרים.

מסקנה: המשפט שאמרנו. כי עבור ראשוניים, כל מי שקטן מהר זר להם, כי הם מתחלקים רק בעצמם וב-1.

אם p ראשוני ו-$1\le k<p$, ברור ש-$\gcd(k,p)$ מחלק את p, וכמו-כן $\gcd(k,p)\le k$, ולכן בהכרח $\gcd(k,p)=1$.

עבור מספרים שאינם ראשוניים, המחלקים שלהם אינם זרים להם. הרי אם $a|n$ אזי $\gcd(a,n)=a$.

הוכחת הטענה:

נניח ש-$1\le k\in\mathbb{Z}_n$ הפיך, ונוכיח ש-$\gcd(n,k)=1$.

נסמן $\gcd(n,k)=m$.

m כמובן מחלק את n,k:

$$n=tm,\qquad k=qm$$

$$qn=tqm=tk\equiv_n 0$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד״ר ארז שיינר)

קיבלנו $tk \equiv_n 0$.

נכפול בהופכי של k, ונקבל $t \equiv_n 0$.

אבל זה אומר ש-$n|t$ (או ש-t הוא בכלל אפס).

ברור ש-$t \neq 0$, מכיוון ש-$n = tm$.

מכיוון ש-$0 < t \leq n$, נובע ש-$t = n$.

ולכן $m = 1$.

בכיוון ההפוך, נניח n, k זרים, וצ"ל k הפיך.

נתון $\gcd(n,k) = 1$. לכן, קיימים $a, b \in \mathbb{Z}$ כך ש-$an + bk = 1$.

כלומר $bk \equiv_n 1$.

דגש קטן: b יכול להיות שלילי או גדול מ-n.

נסמן ב-r_b את שארית החלוקה של b ב-n, ונקבל $r_b \cdot k \equiv_n 1$.

כלומר $k^{-1} = r_b$.

■

על הדרך למדנו אלגוריתם למציאת ההופכי! (שהוא יעיל – סיבוכיות זמן לוגריתמית):

1. נחשב $an + bk = \gcd(n,k) = 1$.
2. ההופכי הוא r_b.

הגדרה: יהי $n \in \mathbb{N}$. נגדיר את חבורת אוילר U_n להיות קבוצת כל הטבעיים שזרים ל-n וקטנים או שווים לו.

אזי U_n אכן חבורה עם כפל מודולו n.

הוכחה:

הרי לקחנו את כל האיברים ההפיכים מודולו n.

1. סגירות – מכפלת הפיכים היא הפיכה.
2. אסוציאטיביות – כפל הוא אסוציאטיבי.
3. איבר יחידה – 1 זר לכל המספרים ושייך לחבורה.
4. הופכיים – ההופכי של הפיך הוא הפיך.

■

דוגמא:

$$U_{12} = \{1, 5, 7, 11\}$$

מכיוון שכל המספרים בריבוע שווים 1, מדובר בחבורה שאינה ציקלית.

תזכורת: חבורה ציקלית אם ורק אם יש לה איבר שהסדר שלו שווה לגודל החבורה.

הגדרה: יהי $n \in \mathbb{N}$. נגדיר את פונקציית אוילר:

$$\phi(n) = |U_n|$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

תזכורת: למדנו שגודל תת-חבורה של חבורה סופית מחלק את גודל החבורה (לגראנז').

בפרט, גודל תת-חבורה ציקלית מחלק את גודל החבורה.

אבל גודל תת-החבורה הציקלית שווה לסדר של היוצר.

ביחד: תהי G חבורה סופית ויהי $a \in G$, אזי $o(a)$ מחלק את $|G|$.

<u>**מסקנה**</u>: יהי $a \in U_n$. מתקיים $o(a)$ מחלק את $|U_n| = \phi(n)$.

כלומר:

$$t \cdot o(a) = \phi(n)$$

לכן:

$$a^{\phi(n)} \equiv_n 1$$

<u>הסבר</u>:

$$a^{\phi(n)} = a^{t \cdot o(a)} = \left(a^{o(a)}\right)^t \equiv_n 1^t = 1$$

בעצם הוכחנו את משפט אוילר.

<u>**משפט אוילר**</u>: יהי $n \in \mathbb{N}$ ויהי $1 \le a < n$ כך ש-a זר ל-n. אזי:

$$a^{\phi(n)} \equiv_n 1$$

(מכיוון ש-a זר ל-n מתקיים כי $a \in U_n$)

<u>**הערה**</u>: אם a מכפלה של n נקבל 0 ולא 1.

<u>**המשפט הקטן של פרמה**</u>: יהי $p \in \mathbb{N}$ ראשוני, ויהי $1 \le a < p$. אזי:

$$a^{p-1} \equiv_p 1$$

<u>הוכחת המשפט הקטן של פרמה</u>:

$$\phi(p) = p - 1$$

$$U_p = \{1, 2, 3, \dots, p-1\}$$

כלומר, לפי אוילר, סיימנו.

■

איך פרמה קיבל משפט על שמו כשהוא סה"כ הציב באוילר לכאורה (אמנם זה המשפט הקטן). כי הסיפור הפוך – פרמה גילה את התוצאה הזו לגבי ראשוניים, ואוילר גילה שאפשר להכליל אותה כך למספרים כלשהם.

<u>**נוסח נוסף של המשפט הקטן של פרמה (מתאים לכל המספרים)**</u>: יהי p ראשוני, לכל מספר a מתקיים: או ש-a זר ל-p או ש-a כפולה שלמה של p.

ולכן לכל המספרים:

$$a^p \equiv_p a$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

הצפנה

מטרות הצפנה:

1. להסתיר מידע.
2. אמינות ושלמות המידע (זה בדיוק המידע ששלחו לי, לא הוסיפו ולא גרעו).
3. זהות השולח (אני יודע מי שלח את המידע).

למשל, עבור עדכון תוכנה – אני רוצה להיות בטוח שמייקרוסופט יצרו אותו, וכך הם בדיוק שלחו אותו, אבל אלא אם אני מתבייש מחבריי משתמשי המק, אין סיבה להסתיר.

אל תממשו את זה בבית! יש מיליון קאצ׳ים קטנים שאתם עשויים לפספס.

עכשיו, אז למה בכלל ללמוד את זה, אם מחייבים אותנו להשתמש בספריות קיימות?

מי שמשתמש בהצפנה בלי להבין את הרעיונות מאחורה יכול להיות מאוד פגיע גם אם הספרייה מושלמת.

דוגמא:

מטא-דאטא – המידע על המידע.

נניח ששלחתי מידע בווטסאפ:

המידע = ההודעה

דוגמאות למידע על המידע = מי שלח למי ומתי, אורך המידע, כמה פעמים המידע חוזר על עצמו – משכיחות אותיות ניתן בקלות למצוא את הטקסט המקורי, למשל.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד״ר ארז שיינר)

מבנים אלגבריים – הרצאה 8 (קבוצת הרצאה 01)

נושא ההרצאה: RSA

אנחנו התחלנו לדבר על הצפנה.

הבסיס – ההנחה היא שכל דבר שאני אומר, מישהו יכול לשמוע.

זה קצת דומה לדואר. נניח שבזמן הקורונה אנחנו רוצים לשלוח את מחברת הבחינה עם הציון בדואר. איך ניתן לעשות זאת ולהבטיח שאף אחד פרט לסטודנט לא יראה את הציון?

קופסא עם מנעול. לסטודנט יש מפתח, האוניברסיטה נועלת.

איך המפתח הגיע לסטודנט אם המנעול באוניברסיטה? איך שלחנו את המפתח בלי שאף אחד העתיק אותו?

דרך אחת היא להיפגש פיזית באופן מאובטח פיזי (ברינקס).

נניח שזה לא אפשרי, כי זה ציון של המכינה והסטודנט מעולם לא היה בקמפוס.

האוניברסיטה יכולה לנעול ולשלוח לסטודנט. אמנם אף אחד לא יוכל לקרוא את הציון, אך זה כולל את התלמיד עצמו.

התלמיד יכול לנעול בעצמו ולשלוח לאוניברסיטה. מי כעת יכול לפתוח את התיבה? אף אחד. האוניברסיטה תפתח את המנעול שלה ותחזיר לסטודנט. בדרך רק הסטודנט יכול לפתוח. כעת הסטודנט פותח את התיבה - ואז מתחרט שהוא עשה את זה.

המנגנון של RSA אינו כזה כל כך, אבל זה כן דומה לדיפי הלמן.

מנעול עם קפיץ – הוא מנעול שניתן לפתוח רק עם מפתח, אבל לנעול אותו אפשר בקליק.

ב-RSA הסטודנט ישלח לאוניברסיטה מנעול שלו עם קפיץ פתוח, האוניברסיטה תנעל באמצעותו את הציון ותחזיר לו.

מה האנשים בדרך שראו את המנעול יכלו לעשות? לנעול משהו בלי לפתוח.

הם יכולים להרוס את התקשורת, אנחנו לא נלחמים בזה.

המנגנון הזה הוא כבד. בפועל מעבירים בשיטה זו (הצפנה פומבית) מפתח סודי, ואז עוברים להצפנה סימטרית (בה לשני הצדדים יש סוד משותף).

השיטות להעביר את המפתח הסודי = הצפנה פומבית - RSA, DH.

<u>RSA</u>:

ראשית נתאר ממש את האלגוריתם, ואחר כך נסביר איך ולמה הוא עובד.

אריק ובנץ רוצים להעביר מידע אחד לשני בלי שאף אחד יוכל לקרוא אותו, ונניח שהם לא גרים יחד ויכולים לתאם מפתח.

אריק רוצה לשלוח לבנץ מידע, אז בנץ צריך להכין מנעול קפיץ.

בנץ בוחר שני מספרים ראשוניים גדולים (נניח בסביבות 2^{1024}), נסמן אותם p, q.

בנץ מחשב את המספרים $n = pq$ וכן $m = (p-1)(q-1)$.

בנץ בוחר מספר e זר ל-m.

המנעול קפיץ (מפתח פומבי) של בנץ הוא הזוג (n, e). בנץ מפרסם את זה באופן חופשי.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

אריק נועל את המידע שלו, שהוא מספר $1 \le x < n$, באופן הבא:

$$x^e \mod n$$

כלומר, המידע הנעול הוא שארית החלוקה ב-n של x^e.

מה המפתח של בנץ?

בנץ מחשב את ההופכי של e מודולו m. יש כזה כי הם זרים. נסמן את ההופכי הזה ב-d.

בנץ לוקח את המידע המוצפן $y = x^e \mod n$.

בנץ מחשב את:

$$x = y^d \mod n$$

<u>עניינים טכניים בדרך</u>:

1. איך מוצאים ראשוניים כאלה גדולים? נלמד בהמשך.
2. איך מכפילים מספרים גדולים? לוגריתמי, הרי סיבוכיות הכפל היא לינארית בכמות הספרות.
3. מה הבעיה פשוט לפרק את n ולקבל את כל המידע של בנץ? הסיבוכיות היא $\sqrt{n}$ (יש אולי שיפורים). במקרה שלנו בערך 2^{1024} – לא ישים בעליל.
4. איך מחשבים את ההופכי מודולו? אוקלידס המורחב (לוגריתמי).
5. העלאה בחזקת מספר גדול? הסיבוכיות היא גם לוגריתמית – כמות הספרות.

בעצם יש לכולם את x^e (בחבורה $\mathbb{Z}_n$), והם רוצים למצוא את x. זו בעיית השורש הדיסקרטי.

<u>הערה</u>: אם $a \equiv_n 1$, האם $2^a \equiv_n 2$?

ממש לא, $n = 3, a = 4$:

$$4 \equiv_3 1$$

$$2^4 = 16 \equiv_3 1$$

$$2^4 \not\equiv_3 2$$

איך זה קשור? מה אתה רוצה מחיינו?

$$y \equiv_n x^2$$

לכאורה:

$$y^d \equiv_n x^{ed} \equiv_n x$$

אבל:

$$ed \not\equiv_n 1$$

אלא:

$$ed \equiv_m 1$$

מה שנראה מוזר, הוא בעצם הדבר הנכון שעובד, נראה זאת עוד מעט.

רגע, אז עכשיו בכלל לא נשמע הגיוני ש:

$$x = y^d \mod n$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

ראשית,

יהיו שני ראשוניים p, q. נוכיח כי $\varphi(pq) = (p-1)(q-1)$.

הוכחה:

נסמן $n = pq$

תזכורת:

$$\varphi(n) = |U_n|$$

כמות המספרים בין 1 ל-n שזרים ל-n.

כמות המספרים בין 1 ל-n היא סה"כ n. נוריד ממנה את כל המספרים שאינם זרים ל-pq.

המחלקים של n הם $\{1, p, q, n\}$. נשים לב שמספר אינו זר ל-pq אם ורק אם יש להם מחלק משותף, כלומר אם ורק אם הוא מתחלק ב-p או ב-q.

נמצא את כל המספרים שמתחלקים ב-q ואת כל המספרים שמתחלקים ב-p.

$$p, 2p, 3p, \dots, qp = n$$

באופן דומה המספרים שמתחלקים ב-q הם:

$$q, 2q, 3q, \dots, pq = n$$

בינתיים זה $q + p$ מספרים. אבל אולי חלק חוזרים זה על זה. מי יכול לחזור על עצמו? מספר שמתחלק גם ב-p וגם ב-q, ולכן הוא לפחות n, ולכן n הוא היחיד.

סה"כ:

$$\varphi(pq) = \varphi(n) = n - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$$

■

<u>משפט RSA</u>: יהיו p, q ראשוניים, נסמן $n = pq$ וכן $m = (p-1)(q-1)$. יהי e זר ל-m ויהי d ההופכי של e ב-U_m (חייב להיות כזה כי $\gcd(e, m) = 1$). יהי $1 \leq x < n$, ונסמן $y = x^e \in \mathbb{Z}_n$. אזי: $$x = y^d \bmod n$$

הוכחה:

נחלק לשני מקרים:

מקרה 1 הוא $\gcd(x, n)$:

לכן $x \in U_n$. ידוע ש-$d = e^{-1} \in U_m$, כלומר:

$$de \equiv_m 1$$

כלומר קיים שלם k כך ש:

$$de = 1 + km$$

כעת,

$$y^d \equiv_n (x^e)^d \equiv_n x^{ed} = x^{1+km} = x \cdot x^{km} = x \cdot x^{k\varphi(n)} = x \cdot \left(x^{\varphi(n)}\right)^k \equiv_n x \cdot 1^k = x$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

לפי משפט אוילר.

מקרה שני – כעת נניח $\gcd(x,n) \neq 1$:

מכיוון ש-$x < n$, אזי $\gcd(x,n) = p$ או $\gcd(x,n) = q$.

נניח ש-$x = tp$. המקרה השני דומה.

מכיוון ש-$x < n$, ברור ש-$\gcd(x,q) = 1$. אחרת x מתחלק גם ב-q, ולכן x מתחלק ב-n, בסתירה.

לפי המשפט הקטן של פרמה:

$$x^{q-1} \equiv_q 1$$

שוב נסמן:

$$ed = 1 + km$$

לכן, גם:

$$x^{km} = x^{k(p-1)(q-1)} = (x^{q-1})^{k(p-1)} \equiv_q 1$$

מה הבעיה? זה מודולו q אבל אנחנו צריכים מודולו n.

בעצם הראינו:

$$x^{km} = 1 + hq$$

כעת:

$$x^{ed} = x^{1+km} = x(x^{km}) = x(1+hq) = x + xhq = x + tphq = x + thn \equiv_n x$$

■

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

20/12/20

מבנים אלגבריים – הרצאה 9 (קבוצת הרצאה 01)

נושא ההרצאה: הצפנה – המשך: אלגוריתם מילר-רבין וחתימה

אלגוריתם מילר-רבין

למדנו על RSA, ואחד החסרונות המרכזיים עד כה הוא הצורך במספרים ראשוניים גדולים.

האם יש חברות שמחזיקות טבלאות של מספרים ראשוניים ומוכרות לכל קונה? אם כן, החברה הזו יכולה לפרוץ לכולם!

זה ממש לא עובד ככה, אלא אנחנו מגרילים מספרים ראשוניים.

אם נגריל מספר, כיצד נבדוק האם הוא ראשוני? ומה הסיכוי שהוא ראשוני?

הסיכוי – ידוע שמתוך n הטבעיים הראשונים, בערך $\frac{n}{\log(n)}$ הם ראשוניים.

אם כך, אם נגריל מתוך n המספרים הטבעיים הראשונים מספר, מה הסיכוי שהוא ראשוני?

הסיכוי הוא:

$$\frac{\frac{n}{\log(n)}}{n}=\frac{1}{\log(n)}$$

אם המספרים בסדר גודל של 2^{1024}, הסיכוי שנגריל מספר ראשוני הוא בערך אחד ל-1000.

שוב, איך נדע אם מצאנו ראשוני?

נחלק בכל המספרים עד השורש 2^{512}, נוריד את הזוגיים 2^{511} – לא יעיל.

רעיון:

למדנו את המשפט הקטן של פרמה, שאמר שלכל ראשוני p ולכל $1\le a<p$ מתקיים כי:

$$a^{p-1}\equiv_p 1$$

נגריל a ונבדוק האם זה מתקיים. אם לא, אזי p אינו ראשוני!

מה הסיכוי ש-a ישקר לי?

יש מספרים שעבורם יש הרבה מאוד שקרנים כאלה, כלומר המספר אינו ראשוני אך כמעט כל ה-a מקיימים את פרמה הקטן.

למשל:

$$302^{2464}\equiv_{2465} 1$$

נשים לב כי:

$$302^{2464}=(302^{1232})^2\equiv_{2465} 1$$

יהי p ראשוני, ונניח כי $x^2\equiv_p 1$ עבור $1\le x<p$. אזי בהכרח:

$$x=1 \quad \text{או} \quad x=p-1$$

תכף נוכיח שזה אכן נכון. אבל בואו נבחן את הדוגמא לעיל תחת ההיגיון הזה.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

<u>הגדרה</u>: יהי n מספר, ונציג את $n-1=2^s r$ עבור r אי-זוגי.

מספר $1\le a<n$ נקרא <u>עד חזק</u> לראשוניות של n אם מתקיים אחד משני הדברים הבאים:

1. $a^r \equiv_n 1$
2. אחד מבין $a^r, a^{2r}, a^{2^2 r}, a^{2^{s-1} r}$ שקול ל-$n-1$ מוד n.

<u>שימו לב</u>: אם מתישהו:

$$a^{2^k r} \equiv_n n-1 \equiv_n -1$$

אזי:

$$\left(a^{2^k r}\right)^2 = a^{2^{k+1} r} \equiv_n (-1)^2 = 1$$

בהנחה שהמשפט שאנחנו עוד צריכים להוכיח נכון, אם p ראשוני, כל המספרים $1\le a<p$ הם עדים חזקים לראשוניות שלו.

לדוגמא: 302 הוא עד חזק לראשוניות של 2465 כי $302^{154} \equiv_{2465} 2464$

$$2465 = 2^5 \cdot 77$$

גילו שאם n אינו ראשוני, לכל היותר **רבע** מהמספרים עד אליו יכולים להיות עדים חזקים לראשוניותו.

כלומר, אם נגריל k מספרים, בהנחה ש-n אינו ראשוני, הסיכוי שכולם ישקרו:

$$\left(\frac{1}{4}\right)^k$$

אם ניקח $k \approx 512$ אז הסיכוי שנחשוב שהמספר ראשוני בהינתן שהוא לא, שקול לסיכוי לנחש את הסיסמא (זניח).

זהו אלגוריתם מילר-רבין, והוא לא מסתיים בביטחון מוחלט שמדובר בראשוני, אלא בסיכוי גבוה (מאוד) שמדובר בראשוני.

מספיק שמצאנו a אחד שאינו עד חזק, ואנחנו בטוחים שלא מדובר במספר ראשוני.

נרשום את הדוגמא עם 302 כאלגוריתם מסודר (מילר-רבין).

האם 2465 ראשוני?

בואו נבדוק האם למשל 302 הוא עד חזק לראשוניות. אם לא – המספר אינו ראשוני בוודאות. אם כן – אולי.

ראשית, נשים לב כי:

$$2465 - 1 = 2^5 \cdot 77$$

$$302^{77} \equiv_{2465} 302 \neq 1, 2464$$

נמשיך הלאה – נעלה בריבוע!

$$302^{154} \equiv_{2465} 302^2 \equiv_{2465} 2464$$

ולכן מדובר בעד חזק לראשוניות של 2465. שקרן!

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

נוכיח את הטענה:

טענה: אם p ראשוני, ויהי $1 \le x < p$ כך ש-$x^2 \equiv_p 1$, אזי $x = 1$ או $x = p - 1$.

הוכחה:

$\mathbb{Z}_p$ הוא שדה מכיוון ש-p ראשוני.

נתון לנו שבתוך השדה הזה:

$$x^2 = 1$$

$$x^2 - 1 = 0$$

$$(x-1)(x+1) = 0$$

מכיוון שמדובר בשדה, אין מחלקי אפס ולכן בהכרח:

$$x = -1 = p - 1 \quad \text{או} \quad x = 1$$

■

הערה:

למשל:

$$3^2 \equiv_8 1$$

למרות ש:

$$3 \neq 1, 7$$

זה לא סותר את הטענה כי 8 אינו ראשוני!

דוגמא:

$$p = 1171$$

$$p - 1 = 2 \cdot 585$$

נגריל את העד 32:

$$32^{585} \equiv_{1171} 1170$$

ולכן הוא עד חזק לראשוניות של 1171.

דוגמא:

$$301^{1232} \equiv_{2465} 1$$

אבל:

$$301^{616} \equiv_{2465} 1886$$

ולכן "גילינו" כי 2465 אינו ראשוני.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

חתימה

נחזור קצת להבין כיצד האינטרנט עובד.

במלון, אני רוצה לגלוש לדף של מדור עתודה.

אנחנו מבקשים משרת ה-DNS (הראוטר של בית המלון) את כתובת ה-IP של מדור עתודה.

מה הראוטר יענה לי? את הכתובת של עצמו אולי, ואולי את הכתובת הנכונה, אבל אחרי שניגש אליה הוא ייתן לי את הדף שלו.

למה זה ממש חמור? המלון יכול להציג לי דף שנראה כמו גוגל, ולבקש שם וסיסמא, ולי אין לכאורה דרך לדעת מזה.

לאחר שהייתי מקיש שם וסיסמא, האם המלון יכול היה להמשיך בהתחזות? או שהייתי עולה עליו? כן, כי הוא יכול להיכנס בשמי לגוגל, ולהעביר לי את כל מה שהוא רואה. והכל מוצפן!

(היום ג'ימייל מגנים על-ידי הודעה על כניסה ממחשב אחר)

כלומר, אני רוצה הבטחה שהיישות מולי היא מי שאני רוצה לפנות אליה.

נניח שיש דרך לחתום על המידע, איך אני אוודא שהחתימה מקורית? נניח שלבנק יש איזה מספר גלוי שרק הוא יכול לאשש ששייך לו, איך אני יודע מה המספר של הבנק?

בפועל, צרובים על המכשיר שאנחנו קונים מפתחות מסוימים לאתרים שמנהלים מפתחות של אתרים אחרים. אנחנו פונים לאתרים הבטוחים, ושואלים אותם מה המפתחות של האתרים שאנחנו רוצים לגלוש בהם.

אם מישהו נוגע לי במכשיר לפני שקיבלתי אותו, אני פרוץ לחלוטין.

התהליך נקרא מתקפת האדם הנדחף (Man in the Middle Attack) – אנחנו מצפינים מולו מושלם, הוא מצפין מול הבנק/גוגל מושלם ועדיין הוא קרא הכל בדרך.

אז נניח שבשיטה הפיזית אנחנו יכולים להיות בטוחים במפתחות ציבוריים של מי שחשוב לנו לדבר איתו. איך אפשר להיות בטוח שזה הוא? (נניח באמצעות RSA).

נניח המפתח של בנק מזרחי הוא (e,n). נשלח לו סיסמא שמוצפנת למפתח הזה, רק הוא יכול לפתוח אותה, רק שנינו יודעים אותה, ואפשר לדבר חופשי.

מה לגבי חתימה?

נניח שמיקרוסופט יצרו עדכון גרסא ולי יש את הקובץ בידיים, אני רוצה לוודא שהוא אותנטי. אני לא רוצה להוריד את הקובץ מחדש ממיקרוסופט בתהליך מוצפן.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר)

27/12/20

מבנים אלגבריים – הרצאה 10

נושא ההרצאה: הצפנה – המשך: חתימה – המשך, דיפי-הלמן; תתי-חבורות נורמליות

<u>תזכורת</u>:

אמרנו שאנחנו רוצים להיות בטוחים עם מי אנחנו מדברים, וההנחה היא שהשגנו בדרכים בטוחות את המפתחות הפומביים (e, n) של מי שאנחנו מדברים איתו.

<u>חתימה – המשך</u>

נניח שמיקרוסופט משחררים עדכון גרסא. אני רוצה להיות בטוח שזה שלהם ושלא התעסקו עם זה בדרך.

היופי הוא שניתן לעשות זאת בקלות באמצעות RSA.

<u>פונקציות גיבוב</u>: <u>הרעיון על רגל אחת</u>: זו פונקציה ששולחת כל קובץ מידע שהיא מקבלת למספר קטן של בתים כך שהסיכוי ששני קבצים יישלחו לאותו המקום מאוד נמוך. ברור שהתנגשויות תאורטיות קיימות, אבל הקטע הוא לדאוג לכך שהסיכוי שזה יקרה אפסי.

לעדכון התוכנה של מיקרוסופט יש ערך מגובב x ובלתי אפשרי (קשה מאוד) לייצר תוכנה אחרת שגם הערך המגובב שלה הוא x. פונקציית הגיבוב אינה סודית אלא ההפך, כולם יודעים להפעיל את אלגוריתם הגיבוב.

<u>מהו תהליך החתימה - כלומר, התהליך בו מיקרוסופט חותמים על המידע באופן שאף אחד לא יכול לזייף?</u>

1. מיקרוסופט מבצעים גיבוב. נקרא לקובץ h ולגיבוב x.
2. מיקרוסופט מחשבים את $y = x^d \in \mathbb{Z}_n$.
3. מיקרוסופט שולחת את h, y.

<u>איך נבדוק שהמידע אותנטי?</u>

נגבב את h ונוודא שאנחנו מקבלים את $y^e \in \mathbb{Z}_n$, הרי לפי ההוכחה של RSA: $x \equiv_n x^{de} \equiv_n y^e$.
רק מיקרוסופט יודעים את d, ויכולים לייצר את הגיבוב הזה.

<u>שאלה</u>: האם מיקרוסופט לא חשפו את ה-d בתהליך הזה? הרי כולם קיבלו את x^d...

זו **בעיית הלוג הדיסקרטי**, אנחנו יודעים את הבסיס ורוצים למצוא את המעריך. גם בעיה זו קשה.

<u>בסיכום קצר</u>: המשתמש מקבל קובץ h וגיבוב מוצפן y. המשתמש מוודא ש-y^e שווה מוד n לגיבוב של h. רק מיקרוסופט יכלו לחשב את $x^d = y$.

<u>מטרת הגיבוב</u>: להגיע למספר שקטן מ-n, עליו אפשר להפעיל כלים של RSA.

<u>שימו לב</u>: בשיטה זו גם הבטחנו את זהות הכותב וגם את שלמות ואמינות המידע, כי אי אפשר לזייף את הגיבוב.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

דיפי-הלמן

נזכיר שבעזרת RSA אנחנו לא נוהגים להעביר מידע בדיוק, אלא סיסמא שבעזרתה נעבור להצפנה סימטרית.

דיפי-הלמן היא שיטה לתאם ישירות סיסמא, ואי אפשר להעביר באמצעותה מידע כלל. בניגוד ל-RSA איתו אפשר להעביר מידע אחר, אבל זה לא נהוג.

נדגיש מתמטית – סיסמא היא מספר גדול כלשהו, שרק שני הצדדים יודעים.

האלגוריתם:

- נבחר מספר גדול p, הוא יהיה ידוע לכולם.
- אריק בוחר מספר אקראי $1 < a < p$ – סוד.
- בנץ בוחר מספר אקראי $1 < b < p$ – סוד.
- בוחרים ביחד מספר $1 < g < p$ שגם יהיה מפורסם לכולם.

- אריק שולח לבנץ את $g^a \bmod p$.
- בנץ שולח לאריק את $g^b \bmod p$.

האם מתוך המידע הזה ניתן לחלץ את a, b? לא, זו בעיית הלוג הדיסקרטי.

- אריק מעלה את מה שקיבל בחזקת a, בנץ מעלה את מה שקיבל בחזקת b, ושניהם יודעים את g^{ab} – זו תהיה הסיסמה המשותפת.

מה הדרישות לגבי g, p?

רוצים g שכאשר מעלים אותו בחזקות, לא חוזרים על אותו ביטוי מהר, אחרת יהיה קל לרוץ על כל החזקות, ולזייף את a.

פרקטית –

נבחר זוג ראשוניים p, q כך ש-$p = 2q + 1$.

איך עושים זאת בפועל? מגרילים ראשוני q עד ש-$2q + 1$ גם ראשוני.

אנחנו נביט בחבורה U_p. כמה איברים יש בה?

$$|U_p| = p - 1$$

מה הסדרים האפשריים של איברים בחבורה זו?

$$1, 2, q, 2q$$

1 הוא הסדר של איבר היחידה בלבד, 2 הוא הסדר של $p - 1$ בלבד. כל איבר אחר הוא לפחות מסדר q, כלומר סדר גדול מאוד. לא ניתן לרוץ על כל החזקות.

נגריל $g \neq 1, p - 1$ והוא די בטוח.

איך נדע אם הסדר של איבר כזה הוא q או $2q$? נעלה בחזקת q, ונראה אם יוצא איבר היחידה.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

27/12/20

העלאה בחזקה גבוהה

$$13 = 2^3 + 2^2 + 2^0$$

$$x^{13} = x^{2^3} \cdot x^{2^2} \cdot x$$

כאשר נעלה את איקס בריבוע שוב ושוב נקבל בקלות חזקות "גבוהות" של 2.

1024 אינו מספר גדול, אבל 2^{1024} ענק.

$$x, x^2, x^4, x^8$$

תתי-חבורות נורמליות

נחזור לקצת מבנים אלגבריים, ולאחר מכן נגיע לקידוד.

תזכורת: אם G חבורה ו-H תת-חבורה שלה, ראינו שאפשר לחלק את G למחלקות לפי H:

$$aH$$

השתמשנו בזה על-מנת להוכיח את לגראנז': הכמות של האיברים ב-G מתחלקת בכמות האיברים ב-H.

כעת, אנחנו רוצים לבצע פעולה בין המחלקות.

כלומר, בהינתן חבורה G ותת-חבורה H אנחנו רוצים להביט בחבורה חדשה שאיבריה הן המחלקות, והפעולה היא... שאלה טובה. למה? גם שאלה טובה.

ראינו כבר את הרעיון בהומומורפיזמים באופן כללי, כשקיבצנו לפי בנים או בנות. כעת אנחנו רוצים לנסח את זה פורמלית ולהוכיח.

דוגמא:

$$\mathbb{Z} = G, \qquad 3\mathbb{Z} = H$$

יש לנו 3 מחלקות:

$$0 + 3\mathbb{Z}, \qquad 1 + 3\mathbb{Z}, \qquad 2 + 3\mathbb{Z}$$

איך נבצע פעולה בין שתי המחלקות?

לפני שנאמר במדויק, ניחוש מושכל:

$$(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}$$

כיצד נגדיר את זה?

רעיון, מכיוון ש:

$$1 + 2 = 0$$

פשוט נחבר בין הנציגים.

הבעיה – מי אמר שזה מוגדר היטב?

$$(2 + 3\mathbb{Z}) = (5 + 3\mathbb{Z})$$

$$(1 + 3\mathbb{Z}) + (5 + 3\mathbb{Z}) = 6 + 3\mathbb{Z}$$

האם תמיד נגיע לאותה תוצאה?

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

27/12/20

השאלה שקולה לשאלה הבאה: אם נבחר מספרים ונעשה מודולו אחרי כל חיבור, או קודם נחבר ובסוף מעלה מודולו, האם נגיע לאותו דבר?

תשובה: כן, ואפשר להוכיח את זה ישירות על מודולו, אנחנו נוכיח באופן הרבה יותר כללי.

נחזור לנסות להגדיר באופן כללי פעולה בין מחלקות.

רעיון:

$$\{1,2\}+\{3,4\}=\{4,5,6\}$$

<u>הגדרה</u>:

תהי חבורה G, ותהיינה שתי תתי-קבוצות $A,B\subseteq G$.

נגדיר:

$$AB=\{a\cdot b|a\in A,b\in B\}$$

האם זה יעזור לנו עם המחלקות?

נזכור שכל המחלקות באותו גודל.

$$|aH|=|bH|=|H|$$

$$|aHbH|\leq|H|^2$$

אנחנו רצינו לעשות פעולה בין מחלקות, אנחנו רוצים מתוך סגירות לקבל מחלקה. המינימום הוא שזה יהיה בגודל של מחלקה. אחרי זה גם צריך לוודא שזו אכן מחלקה.

מסתבר שאם H תת-חבורה נורמלית, הכל עובד (אחרת לא).

נגדיר מה זה בכלל תת-חבורה נורמלית ונוכיח שזה מסתדר.

<u>הגדרה</u>: תהי חבורה G ותהי תת-חבורה H. אזי H נקראת <u>תת-חבורה נורמלית</u> של G אם לכל $a\in G$ מתקיים כי:

$$aH=Ha$$

כלומר, במילים פשוטות, אם כופלים את כל איברי H משמאל באיבר כלשהו, נקבל בדיוק את אותם איברים כמו אם נכפול את כל איברי H באיבר הזה מימין.

<u>דוגמא</u>:

$$G=S_3,\qquad H=\{I,(1\ 3)\}$$

$$(1\ 2)H=\{(1\ 2),(1\ 3\ 2)\}$$

$$H(1\ 2)=\{(1\ 2),(1\ 2\ 3)\}\neq(1\ 2)H$$

לכן, H אינה תת-חבורה נורמלית.

כעת, נבחר את תת-החבורה:

$$H=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$$

כעת, $H(1\ 2)$ היא קבוצה של 3 תמורות שליליות.

מכיוון שיש בדיוק 3 תמורות כאלה בחבורה, בהכרח נקבל את כולן, ואותו טיעון יעבוד מכל צד ולכל תמורה אי-זוגית. מכאן שזו תת-חבורה נורמלית.

© Roee Oscar – King of Sikumim

<u>טענה</u>: אם H תת-חבורה נורמלית, אזי לכל $a,b\in G$:

$$aHbH=(ab)H$$

כלומר, הפעולה האינטואיטיבית שחשבנו עליה היא אכן הפעולה שקיבלנו. נוכיח זאת.

הוכחה:

נבצע הכלה דו-כיוונית.

יהי

$$ah_1bh_1\in aHbH$$

צריך להוכיח שאיבר זה בקבוצה הימנית.

כעת, אמנם ייתכן ש:

$$h_1b\neq bh_1$$

אבל:

$$h_1b\in Hb=bH$$

כלומר:

$$h_1b\in bH$$

כלומר:

$$h_1b=bk_1$$

ולכן:

$$ah_1bh_2=abk_1h_2\in(ab)H$$

בכיוון ההפוך:

$$abh\in(abH)$$

אבל:

$$abh=aebh\in aHbH$$

<u>הגדרה</u>: תהי חבורה G ותהי תת-חבורה נורמלית H. נגדיר את <u>חבורת המנה</u> להיות אוסף המחלקות עם הפעולה הזו.

$$G\ /\ H\in\{aH|a\in G\}$$

<u>האם זו חבורה יחד עם פעולה זו?</u>

הוכחנו סגירות. קל לוודא שאיבר היחידה הוא $eH=H$. אסוציאטיביות נובעת בקלות מאסוציאטיביות הפעולה של G, וכמו-כן המחלקה ההופכית של aH היא $a^{-1}H$.

<u>הערה</u>: הכל נכון בזכות השוויון:

$$aHbH=(ab)H$$

שהוכחנו.

המטרה – משפט האיזומורפיזם הראשון.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

27/12/20

<u>משפט האיזומורפיזם הראשון</u> : יהי הומומורפיזם $f : G_1 \to G_2$.

נסמן ב- $K = \ker f$ (נוכיח שהוא בהכרח נורמלי).

$$G_1 / K \cong Im(f)$$

<u>דוגמא</u> :

$$f : \mathbb{Z} \to \mathbb{Z}_3$$

$$K = 3\mathbb{Z}$$

$$\mathbb{Z} / 3\mathbb{Z} \cong \mathbb{Z}_3$$

הוכחת המשפט – בהרצאה הבאה.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

מבנים אלגבריים – הרצאה 11

נושא ההרצאה: תתי-חבורות נורמליות – המשך ; קידוד : מבוא, קוד לינארי

תתי-חבורות נורמליות – המשך

הצגנו את מספר האיזומורפיזם הראשון :

יהי $f : G \to H$ הומומורפיזם בין חבורות. אזי :

$$G / \ker f \cong im\, f$$

נוכיח שבהכרח $\ker f$ תת-חבורה נורמלית.

למעשה, נראה בדיוק מי הן המחלקות לפי הגרעין.

נסמן $K = \ker f$.

יהי $a \in G$. נוכיח כי :

$$aK = \{b \in G | f(b) = f(a)\} = Ka$$

ולכן K תת-חבורה נורמלית.

נוכיח את השוויון משמאל, והשוויון מימין מאוד דומה.

כלומר, במילים פשוטות, המחלקות לפי הגרעין הן קבוצות המקורות של כל איבר בתמונה.

המחשה :

$$\{\text{רועי, אוסקר, גיתית, שילת}\} \to \{\text{בנים, בנות}\}$$

הגרעין :

$$K = \{\text{רועי, אוסקר}\}$$

$$\text{גיתית}K = \{\text{גיתית, שילת}\}$$

בין היתר, נובע שכמות המקורות של כל תמונה זהה.

נוכיח :

$$aK = \{b \in G | f(b) = f(a)\}$$

בכיוון 1, יהי $ak \in aK$. צריך להוכיח כי $f(ak) = f(a)$.

אבל :

$$f(ak) = f(a) \cdot f(k) = f(a) \cdot e_H = f(a)$$

בכיוון 2, יהי $b \in G$ כך ש-$f(b) = f(a)$. צריך להוכיח כי $b \in aK$.

לפי הנתון :

$$\left(f(a)\right)^{-1} \cdot f(b) = e_H$$

$$e_H = f(a^{-1}) \cdot f(b) = f(a^{-1}b)$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

לכן:

$$a^{-1}b = k \in K$$

ולכן:

$$b = ak \in aK$$

בדיוק כמו רצינו. ההוכחה של השוויון השני דומה.

■

תזכורת – משפט האיזומורפיזם הראשון:

יהי $f : G \to H$ הומומורפיזם בין חבורות. אזי:

$$G \,/\, \ker f \cong im\, f$$

הראינו שהגרעין נורמלית, ולכן הביטוי בכלל מוגדר

על-מנת להוכיח את משפט האיזומורפיזם הראשון, צריך לבנות הומומורפיזם הפיך:

$$\varphi : G \,/\, K \to im\, f$$

נגדיר את הפונקציה:

$$\varphi(aK) = f(a)$$

צריך להראות:

1. מוגדר היטב, כלומר, אם $aK = bK$ אזי $\varphi(aK) = \varphi(bK)$ (פחות או יותר עשינו את זה).
2. הומומורפיזם, כלומר, $\varphi\big((aK)(bK)\big) = \varphi(aK)\varphi(bK)$
3. חח״ע, כלומר, אם $\varphi(aK) = \varphi(bK)$ אזי $aK = bK$
4. על.

הוכחה מלאה כתרגיל.

■

קידוד - מבוא

קידוד שונה מהצפנה – הצפנה מטרתה הייתה להסתיר, ולהבטיח את זהות הכותב ושלמות ואמינות המידע.

קידוד מדבר באופן עקרוני על הפרוטוקול, כלומר, איך להעביר את המידע, אבל פרקטית, כשאנחנו אומרים קידוד אנחנו מתכוונים לחלק מאוד ספציפי של הפרוטוקול שנסביר תכף.

נחזור אחורה – נניח שאני רוצה לשלוח למישהו יום בחודש וחודש בשנה בהם ניפגש.

בפועל אני שולח בתים של מידע (מספרים):

$$3 \;\; 1 \ldots$$

צריך לתאם בין שני הצדדים מה כל ביט אומר (פרוטוקול). זה לא מוסתר – כולם מכירים את הפרוטוקול.

נניח שאני שלחתי מידע מסוים. האם לצד השני יש דרך לדעת אם נפלה שגיאה בדרך?

מדי פעם ביטים מתחלפים בשליחה בגלל רעשים והפרעות למיניהם.

בגדול לא. המטרה של קידוד (במשמעות של מבנים אלגבריים) היא זיהוי ותיקון שגיאות.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד״ר ארז שיינר – קבוצת הרצאה 01)

בואו נמציא ביחד שיטה בה נדע אם התרחשה טעות, בהנחה שלא התרחשה יותר מטעות אחת.

דרך אחת – נשלח פעמיים:

$$11010\ 11010$$

אם נפלה טעות אחת, שתי פיסות המידע לא תהיינה זהות ונדע שקרתה תקלה.

אם נפלו שתי טעויות, יש סיכוי שלא נעלה על זה.

האם נוכל לדעת היכן הייתה הטעות בהנחה שהייתה רק טעות אחת? לא.

תנו רעיון לכך שגם נוכל לדעת איפה הייתה השגיאה:

$$11010\ 11010\ 11010$$

כאן, אם נפלה טעות אחת, נוכל לתקן אותה.

הרוב קובע.

כעת, על-מנת לזהות שגיאה אחת הכפלנו את המידע, ועל-מנת לתקן שגיאה אחת שילשנו את המידע. זה נורא.

בפועל, על-מנת לזהות שגיאה מספיק להוסיף ביט אחד. על-מנת להיות מסוגל לתקן שגיאה אחת, מספיק להוסיף לוג ביטים של המידע.

<u>דוגמא ראשונה - Parity Bit</u>:

נניח שהמידע שלי בביטים הוא:

$$a_1, \ldots, a_k$$

נחשב ביט שהוא סכום ביטי המידע, ונוסיף אותו בסוף:

$$b = a_1 + \cdots + a_k$$

(בשדה הבינארי)

ונשלח:

$$a_1, \ldots, a_k, b$$

אם לא הייתה טעות, מה אמור לקרות?

נסכום את כל הביטים כולל האחרון:

$$a_1 + \cdots + a_k + b = b + b = 0$$

כצד ניתן לתאר טעות באופן אלגברי? מוסיפים 1 לביט.

כלומר, אם נפלה שגיאה בשידור, בין אם בביט מידע או בביט היתירות, מה יהיה הסכום החדש של כל הביטים ששודרו?

$$a_1 + \cdots + a_k + b + 1 = 1 \neq 0$$

ואז נדע בוודאות שהייתה שגיאה.

קל לראות שמספר זוגי של שגיאות יעבור מתחת לראדאר (כלומר, לא נדע שהיו שגיאות), וכל מספר אי-זוגי נדע בוודאות שהיו שגיאות.

אני לא יכול לתקן, כי אני לא יודע מאיפה הגיע ה-1 הנוסף.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

<u>דוגמא שנייה - Checksum</u> :

Checksum שראינו ב-IP, TCP, UDP הוא אותו דבר בדיוק, רק ברמת שני בתים.

$$\underbrace{1\,1\,0\,0\,1\,1}_{\text{מידע}}\ \underbrace{1\,0\,1}_{\text{יתירות}}$$

$$(1,1,0)+(0,1,1)=(1,0,1)$$

אם אין שגיאה, סכום כל החבילות (במקרה זה בגודל 3 ביטים) צריך להיות אפס. שגיאה אחת בטוח תזוהה.

<u>הגדרה – יתירות</u> : יתירות זה החלק שאנחנו מוסיפים למידע לצורך זיהוי ותיקון שגיאות.

דוגמת חישוב ספרת ביקורת בתעודת זהות (האלגוריתם וההסבר המלאים ב-math-wiki) :

$$156$$

$$6\cdot 2=12\to 3$$

$$5$$

$$1\to 2$$

$$3+5+2=10$$

$$10-10=0$$

ולכן תעודת הזהות תהיה :

$$1560$$

<u>קוד לינארי</u>

(הכל בשדה הבינארי אלא אם נגיד אחרת)

כל מטריצה בינארית $A^{m\times k}$ מגדירה קידוד לינארי, כפי שנסביר כעת.

נביט במטריצה :

$$G=\begin{pmatrix} I_k \\ A \end{pmatrix}\in(\mathbb{Z}_2)^{(k+m)\times k}$$

דוגמא :

$$A=\begin{pmatrix}1&0&1\\0&1&1\end{pmatrix}$$

$$G=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\0&1&1\end{pmatrix}$$

אנחנו יכולים לקודד מידע באורך k על-ידי כפל במטריצה המקודדת G.

נקבל מילה מקודדת באורך $n=k+m$, כאשר הוספנו m ביטים של יתירות.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\0&1&1\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}=\begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}$$

נשים לב שהמילה המקודדת הכילה את המידע ולאחריו ביטי היתירות.

נראה שזה המצב תמיד:

בהינתן מידע v:

$$Gv=\begin{pmatrix}I\\A\end{pmatrix}v=\begin{pmatrix}Iv\\Av\end{pmatrix}=\begin{pmatrix}v\\Av\end{pmatrix}$$

כלומר היתירות היא Av.

שימו לב: אורך המידע הוא כמות העמודות של A ואורך היתירות הוא כמות השורות של A.

מה עושים בצד השני על-מנת לבדוק אם היו טעויות? מה מצפים שיקרה?

לכאורה, הצד השני יכול לקודד את המידע בעצמו, ולוודא שמקבלים אותו דבר. בפועל של התאוריה, עושים משהו קצת אחר.

נביט במטריצה המפענחת הבאה:

$$H=\begin{pmatrix}A & I_m\end{pmatrix}$$

$$HGv=\begin{pmatrix}A & I\end{pmatrix}\begin{pmatrix}v\\Av\end{pmatrix}=Av+Av=0$$

כלומר, אם לא היו שגיאות, אנחנו מצפים לקבל אפס, כאשר מכפילים את המילה המקודדת ב-H. אם לא קיבלנו אפס, אז בטוח היו טעויות. אם קיבלנו אפס, כרגע זה לא אומר יותר מדי.

<u>**סיכום ביניים**</u>:

שני הצדדים מסכימים על A מקודדת מראש.

אריק רוצה לשלוח v – המידע.

אריק מקודד את המילה למילה המקודדת Gv ושולח לבנץ.

אולי מתרחשות טעויות בדרך.

בנץ מקבל מילה מקודדת u.

בנץ כופל את u ב-H, אם לא היו טעויות הוא יקבל אפס:

$$Hu=H(Gv)=0$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

נביט במקרה הספציפי ש-A היא שורת אחדות:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_1 + \cdots + a_2 \end{pmatrix}$$

מקבלים בדיוק את ה-Parity Bit ורואים שהוא סוג של קוד לינארי.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד״ר ארז שיינר – קבוצת הרצאה 01)

10/01/21

מבנים אלגבריים – הרצאה 12

נושא ההרצאה: קידוד: קוד לינארי – המשך, קידוד פולינומי

תזכורת:

כל מטריצה בינארית $A \in \mathbb{Z}_2^{m\times k}$ מגדירה לנו קוד לינארי.

המידע = מילה באורך k.

כופלים את המידע במטריצה המקודדת $G = \begin{pmatrix} I \\ A \end{pmatrix}$.

מקבלים מילה מקודדת $Gv = \begin{pmatrix} v \\ Av \end{pmatrix}$ – המידע + יתירות.

הצד השני כופל במטריצה המפענחת $H = \begin{pmatrix} A & I \end{pmatrix}$. הוא רואה אפס אם ורק אם המילה חוקית – זה לא אומר שלא היו שגיאות שהפכו ממילה חוקית אחת לאחרת. אם הוא רואה ש-$Hu \neq 0$ הוא בטוח שהייתה שגיאה.

קוד לינארי – המשך

אנחנו רוצים לחקור מה הקשר בין בחירת המטריצה לזיהוי הטעויות ואולי אף תיקון הטעויות.

ראשית, אנחנו רוצים להציג טעות באופן אלגברי.

נניח $u \in \mathbb{Z}_2^{m+k}$ הוא מילה מקודדת כלשהי. איך נציג את הווקטור שמתקבל מהווקטור הזה יחד עם טעות?

הווקטור u שהשתנה בו הביט ה-i הוא:

$$u + e_i$$

נניח מצב כזה:

אריק רצה לשלוח לבנץ את המידע v, אז הוא חישב את $u = Gv$ ושלח לבנץ. בדרך היו רעשים, ובנץ קיבל $u + e_i$.

$$H(u + e_i) = Hu + He_i = C_i(H)$$

האם בנץ היה עולה על זה שקרתה טעות בדרך?

כן, אם העמודה ה-i ב-H שונה מאפס.

מסקנה: אפשר לזהות שגיאה אחת בוודאות אם ורק אם ב-H אין עמודת אפסים.

האם ניתן לתקן את השגיאה? כלומר, לדעת באיזה ביט הייתה השגיאה?

כן, אם אין שתי עמודות זהות ב-H.

מסקנה: אפשר לתקן שגיאה יחידה אם ורק אם אין עמודת אפסים ב-H וגם אין שתי עמודות זהות.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

דוגמא:

$$A=\begin{pmatrix}1&1&1&0\\1&0&1&1\\0&1&1&1\end{pmatrix}$$

$$G=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&1&0\\1&0&1&1\\0&1&1&1\end{pmatrix}$$

$$H=A=\begin{pmatrix}1&1&1&0&1&0&0\\1&0&1&1&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}$$

$$v=(1,0,0,1)$$

$$Gv=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&1&0\\1&0&1&1\\0&1&1&1\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\0\\1\\1\\0\\1\end{pmatrix}$$

אריק ישלח לבנץ את:

$$u=(1,0,0,1,1,0,1)$$

נניח שבנץ קיבל את:

$$u'=(1,0,1,1,1,0,1)$$

בנץ כופל ב-H:

$$Hu'=(1,1,1)$$

ראשית, בנץ יודע שזה לא מה שאריק שלח לו.

בהנחה שהייתה שגיאה יחידה, בנץ יודע שהיא בביט השלישי מכיוון ש-Hu' היא העמודה השלישית של H.

כעת, נניח שהתרחשו שתי טעויות:

$$u''=(1,0,1,0,1,0,1)$$

$$Hu''=(1,0,1)$$

בנץ עשוי להסיק שהייתה טעות בביט החמישי, אבל בפועל היו שתי טעויות בביטים 3 ו-4 וסכום העמודות השלישית והרביעית הוא העמודה החמישית.

$$H\left(u+e_i+e_j\right)=C_i(H)+C_j(H)$$

אם סכום שתי עמודות שווה לעמודה אחרת ב-H, אי אפשר לתקן שתי טעויות (כי לא ניתן לדעת אם זו טעות אחת או שתיים).

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד״ר ארז שיינר – קבוצת הרצאה 01)

אז אם אני רוצה להיות מסוגל לתקן שגיאה אחת, אמרנו שאני רוצה H בלי עמודת אפסים, ובלי שתי עמודות זהות.

מה הקשר בין גודל המידע לגודל היתירות?

נניח שיש m ביטי יתירות. לכן, ב-A יש m שורות.

כמה עמודות אפשריות בכלל יש עם m שורות? 2^m.

אסור לחזור על עמודות ממטריצת היחידה, ואסור לשים עמודת אפסים, לכן מעבר לכך נותרו $2^m - m - 1$ עמודות שאפשר לשים ב-A ועדיין להיות מסוגלים לתקן שגיאה יחידה.

יוצא שהיתירות היא בערך לוג המידע.

עם 32 ביטים ניתן להגן (עד כדי שגיאה יחידה) על 4 גיגה של מידע.

היום, עם קצב המידע המטורף, למה צריך בכלל לתקן שגיאות? לכאורה, עדיף לבקש לשלוח שוב.

1. אם אני בשיחת וידאו, לא מעניין אותי פריים מלפני כמה שניות.
2. אם המידע לא עובר בתקשורת, אלא צרוב על מדיה (דיסק, הארדדיסק, דיסקאונקי).

ככל שנמצא, ב-ethernet אמנם ניתן לתקן, אך לא מתקנים.

__**הגדרה**__: יהי קוד לינארי. נגדיר את $d_{\min}$ להיות המרחק הכי קטן בין שתי מילים מקודדות בקוד (במובן של מרחק המינג – מספר ביטים שונה).

איך ניתן לקשר בין ה-$d_{\min}$ לדברים שאמרנו קודם?

האם ייתכן שיש שתי מילים חוקיות שהמרחק ביניהן הוא 1?

$$u_2 = u_1 + e_i$$

אם שתיהן חוקיות, אז:

$$Hu_2 = H(u_1 + e_i) = 0$$

וכמו כן:

$$Hu_1 = 0$$

לכן נובע:

$$He_i = C_i(H) = 0$$

כלומר, ה-$d_{\min} = 1$ אם ורק אם יש עמודת אפסים ב-H.

זה בדיוק המצב שאי אפשר לזהות אפילו שגיאה אחת.

נניח ש-$d_{\min} = 2$. אזי, אם u_1 מילה חוקית:

$$H(u_1 + e_i) \neq 0$$

אבל יש מילים חוקיות במרחק 2:

$$u_2 = u_1 + e_i + e_j$$

מה זה אומר על המטריצה? סכום שתי עמודות הוא אפס. זה נכון אם ורק אם הן זהות.

כלומר, כן נזהה שגיאה אחת, אבל לא נזהה שתיים.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

האם ניתן לתקן שגיאה אחת?

נניח שקיבלתי:

$$u + e_i$$

זיהיתי שהייתה שגיאה, האם אוכל לתקנה?

כמובן ש-u היא מילה חוקית במרחק 1, אך גם:

$$u + e_i + e_j$$

כעת, אם $d_{\min} = 3$:

$$H\left(u + e_i + e_j\right) \neq 0$$

זה שקול לכך שאין שתי עמודות זהות.

פה אפשר לתקן שגיאה אחת, מדוע?

אחרת, יש מילה אחת שבמרחק 1 ממנה שתי מילים חוקיות.

$$u' + e_i$$

$$u' + e_j$$

המרחק ביניהן הוא 2, ומצאנו שתי מילים חוקיות במרחק שקטן מה-$d_{\min}$, בסתירה.

קידוד פולינומי

נביט בחוג הפולינומים עם מקדמים בינאריים:

$$R = \{a_n x^n + \cdots + a_0 | a_i \in \mathbb{Z}_2\}$$

עם חיבור וכפל אינטואיטיביים.

דוגמאות:

$$(1 + x)(1 + x^2) = 1 + x^2 + x + x^3$$

$$(1 + x)(1 + x + x^2) = 1 + x + x^2 + x + x^2 + x^3 = 1 + x^3$$

בחוג השלמים למדנו על חלוקה עם שארית. גם בחוג הפולינומים יש תכונה דומה:

לכל זוג פולינומים f, g קיימים פולינומים q, r כך ש:

$$f = qg + r$$

כאשר הדרגה של r (החזקה הגדולה ביותר שהמקדם שלה אינו אפס) היא קטנה מהדרגה של g.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

דוגמא:

$$x^2 + x + 1$$

$$\boldsymbol{x^3 + 1 | x + 1}$$

$$+x^3 + x^2$$

$$x^2 + 1$$

$$+x^2 + x$$

$$x + 1$$

$$+x + 1$$

$$0$$

במקרה זה $q = (x^2 + x + 1)$ ו-$r = 0$.

איך כל זה קשור לקידוד?

כל פולינום מדרגה m מתאים לוקטור בינארי עם $m + 1$ רכיבים (המקדמים).

דוגמא:

$$(1, 0, 1, 1) \leftrightarrow x^3 + x + 1$$

מה הקידוד הפולינומי? (נוכיח שזה מקרה פרטי של קוד לינארי)

הפעם כל פולינום יגדיר קוד לינארי, ואורך המידע לא חייב להיות קבוע.

הפולינום המקודד ייקרא g, ונניח שהוא מדרגה m.

המידע יהיה הפולינום f.

נחלק את $x^m f$ בפולינום g. השארית היא היתירות, ואנחנו נשלח לצד השני את $x^m f + r$.

היתירות היא m ביטים.

למה חיברנו את היתירות ל-$x^m f$?

כי בעצם כפל ב-x^m עושה שיפט:

$$(1, 0, 1) \leftrightarrow x^2 + 1$$

$$x^3(x^2 + 1\ ) = x^5 + x^3 \leftrightarrow (1, 0, 1, 0, 0, 0)$$

מכיוון ש-r מדרגה קטנה או שווה ל-$m - 1$ הוא לעולם לא ישפיע על יותר מ-m הביטים האחרונים.

.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

מבנים אלגבריים – הרצאה 13

נושא ההרצאה: קידוד: קידוד פולינומי – המשך

תזכורת:

$$x^4 + x^2 + 1 \leftrightarrow (1,0,1,0,1)$$

יהי פולינום $g(x)$ מדרגה m. הוא מגדיר לנו קוד פולינומי באופן הבא:

יהי מידע $f(x)$. נחלק את $x^m f(x)$ ב-$g(x)$ (חלוקה עם שארית):

$$x^m f(x) = q(x)g(x) + r(x)$$

כאשר $\deg(r) < m$.

הקידוד (מה שנשלח) יהיה:

$$x^m f(x) + r(x)$$

קידוד פולינומי – המשך

הסברים:

מה הכפל ב-x^m עושה למידע? שיפט של m ביטים שמאלה:

$$f(x) = x^2 + 1 \leftrightarrow (1,0,1)$$

$$x^3 f(x) = x^5 + x^3 \leftrightarrow (1,0,1,0,0,0)$$

מכיוון ש-$\deg(r) < m$ הוא מיוצג על-ידי m ביטים. כלומר, $x^m f(x)$ שחרר m ביטים פנויים מימין, אליהם נכנסת השארית שהיא היתירות.

דוגמא:

$$g(x) = x^2 + 1$$

המידע הוא:

$$(1,1,1,0)$$

$$f(x) = x^3 + x^2 + x$$

נקודד:

$$x^2 f(x) = x^5 + x^4 + x^3$$

נחלק את זה בפולינום המקודד g:

$x^3 + x^2 + 1$
$\boldsymbol{x^5 + x^4 + x^3 | x^2 + 1}$
$x^5 + x^3$
x^4
$x^4 + x^2$
x^2
$x^2 + 1$
1

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

סה"כ הפולינום המקודד הוא:

$$x^2f(x) + r = x^5 + x^4 + x^3 + 1 \leftrightarrow \left(\underbrace{1,1,1,0}_{\text{מידע}}, \underbrace{0,1}_{\text{יתירות}}\right)$$

איך הצד השני יודע שהוא קיבל מילה חוקית? (עזבו שגיאות, אלא מילה מקודדת כלשהי).

$$x^m f(x) = q(x)g(x) + r(x)$$

נוסיף לשני האגפים $r(x)$:

$$x^m f(x) + r(x) = q(x)g(x)$$

כלומר מילה היא חוקית אם ורק אם היא מתחלקת ב-g ללא שארית (לא קשה להראות גם את הכיוון השני).

מה טוב בזה? כמה שגיאות מזהים? וכדומה.

נעבור ל**קידוד ציקלי**, שעונה על השאלות הללו.

כעת, נתחום את גודל המידע.

k – כמות ביטי המידע, m – כמות ביטי היתירות (כלומר $\deg(g) = m$) וגודל המילה המקודדת הוא $n + k + m$.

נגדיר **<u>הזזה ציקלית</u>** של וקטור מילה באורך n:

$$(a_{n-1}, \dots, a_1, a_0) \to (a_{n-2}, \dots, a_0, a_{n-1})$$

קוד נקרא **<u>ציקלי</u>** אם לכל מילה חוקית (מתחלקת ב-g) גם ההזזה הציקלית שלה היא מילה חוקית (מתחלקת ב-g).

1. למה שזה אי פעם יקרה?
2. למה לעזאזל שנרצה שזה יקרה?

למה אנחנו רוצים את זה:

<u>טענה</u>: אם g מייצר קוד פולינומי ציקלי, ונניח $\deg(g) = m$, אזי כל השגיאות שיקרו בטווח של m ביטים במקום כלשהו במילה, יהפכו את המילה ללא חוקית.

במילים אחרות, נזהה כל שגיאות כאלה.

כלומר, אם ניקח את כל הביטים מהשגיאה הראשונה ועד האחרונה כולל, נקבל לא יותר מ-m ביטים.

<u>דוגמא</u>:

נניח שהמילה המקודדת היא:

$$(1,0,1,0,1,1,1,0)$$

נניח $\deg(g) = 3$.

$$\left(1,0, \underbrace{0,0,0}_{\text{טווח}}, 1,1,0\right)$$

נזהה טעות כזו אם אכן מדובר בקוד ציקלי.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

$$(1,0,1,1,1,1,1,1)$$

טעות כזו לא בטוח נזהה.

למשל אם $k \approx 4G$ ביטים, ונוסיף $m = 32$ ביטי יתירות, נזהה כל שגיאה בטווח של 32 ביטים.

למה זה מתאים לעולם הבעיה של התקשורת? כי הפרעות בתקשורת באות בפרץ, וייפגעו בסיכוי סביר כמה ביטים ולאו דווקא אחד. אנחנו מניחים שלא יהיה יותר מפרץ שגיאה אחד בפקטה, אבל רוצים לטפל במקרה שהיו כמה שגיאות באזור קרוב.

מדוע זה נכון?

ראשית, מכיוון שהיתירות עבור מידע נתון היא יחידה (הרי השארית היא יחידה).

כל שגיאה ב-m הביטים של היתירות תהפוך את המילה ללא חוקית.

זה היה נכון מאז ומעולם בקידוד.

כעת, מכיוון שהקוד ציקלי, ניתן להזיז אותו עד שטווח נתון של m ביטים יהיה בדיוק באזור היתירות.

<u>דוגמא</u>:

$$\left(1,0,\underbrace{0,0,0}_{\text{טווח}},1,1,0\right) \rightarrow \left(1,1,0,1,0,\underbrace{0,0,0}_{\text{טווח}}\right)$$

כעת, ללא השגיאה המילה היא חוקית, מכיוון שהקוד ציקלי והזזות ציקליות הן חוקיות.

אז עם השגיאה זה בוודאות לא חוקי! ולכן גם לפי ההזזות זה לא חוקי (כי הזזות זה תהליך הפיך).

הוכחנו באופן עקרוני שאם היו שגיאות בטווח של m ביטים אז המילה אינה חוקית, כלומר אינה מתחלקת ב-g.

אז כעת, משנוכחנו לראות שאכן קודים ציקליים הם שימושיים ומגניבים, איך נדע אם קוד הוא ציקלי והאם בכלל יש כאלה?

ראשית, כמו תמיד, אנחנו רוצים להציג את פעולת ההזזה הציקלית כפעולה אלגברית כלשהי.

<u>דוגמא</u>:

$$(1,0,1,1,0,1) \leftrightarrow x^5 + x^3 + x^2 + 1$$

ההזזה הינה:

$$(0,1,1,0,1,1) \leftrightarrow x^4 + x^3 + x + 1$$

$$x(x^5 + x^3 + x^2 + 1) + x^6 + 1 = x^4 + x^3 + x + 1$$

כלומר, אם $a_{n-1} = 1$, ההזזה הציקלית של $f(x)$ היא:

$$x \cdot f(x) + x^n + 1$$

ואם $a_{n-1} = 0$ ההזזה הציקלית היא:

$$x \cdot f(x)$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

דוגמא:

$$(0,1,1,0,1,1) \leftrightarrow x^4 + x^3 + x + 1$$

ההזזה תהיה:

$$(1,1,0,1,1,0) \leftrightarrow x^5 + x^4 + x^2 + x$$

הערה: בעצם לוקחים את $x \cdot f(x)$ מודולו $x^n + 1$.

אם $\deg(f) < n - 1$, כלומר $a_{n-1} = 0$, ומדובר במילה חוקית $f = q(x)g(x)$, אז בכל קידוד:

$$x \cdot f(x) = x \cdot q(x)g(x)$$

אכן מילה חוקית.

אבל, אם $\deg(f) = n - 1$, כלומר $a_{n-1} = 1$, המילה המקודדת הינה:

$$x \cdot f(x) + x^n + 1$$

מתי זה יתחלק ב—g לדעתכם? אם ורק אם g מחלק את $x^n + 1$.

משפט: g מדרגה m יוצר קוד פולינומי ציקלי עבור מידע מאורך k אם ורק אם g מחלק את $x^n + 1$ ללא שארית.

כלומר, g מחלק את:

$$x^{m+k} + 1$$

ללא שארית.

דוגמא:

פרוטוקול Ethernet משתמש בתיקון שגיאות ציקלי הנקרא $CRC32$, ובפרט בפולינום:

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

הפולינום $g(x)$ מחלק את $x^{2^{32}-1} - 1$, כלומר הוא מתאים לקידוד של עד למעלה מ-4 מיליארד ביטים של מידע.

דוגמא:

ידוע ש-(וקל לוודא) $x^3 + x + 1$ מחלק את $x^7 + 1$ ללא שארית.

לכן, הפולינום $g(x) = x^3 + x + 1$ מייצר קידוד ציקלי עבור 4 ביטי מידע.

הרי:

$$7 = m + k$$

$$m = \deg(g)$$

$$k = \text{כמות ביטי המידע}$$

ננסה, נקודד את $(1,1,0,0)$.

$$f(x) = x^3 + x^2$$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

כעת, נכפול ב-x^3:

$$x^3 f = x^6 + x^5$$

נחלק:

$x^3 + x^2 + x$
$\mathbf{x^6 + x^5 | x^3 + x + 1}$
$x^6 + x^4 + x^3$
$x^5 + x^4 + x^3$
$x^5 + x^3 + x^2$
$x^4 + x^2$
$x^4 + x^2 + x$
x

הפולינום המקודד הוא:

$$x^3 f(x) + x \leftrightarrow (1, 1, 0, 0, 0, 1, 0)$$

נבצע הזזה ציקלית, ונראה אם המילה נשארת חוקית.

$$x^6 + x^2 + 1 \leftrightarrow (1, 0, 0, 0, 1, 0, 1)$$

נחלק:

$x^3 + x + 1$
$\mathbf{x^6 + x^2 + 1 | x^3 + x + 1}$
$x^6 + x^4 + x^3$
$x^4 + x^3 + x^2 + 1$
$x^4 + x^2 + x$
$x^3 + x + 1$
$x^3 + x + 1$
0

<u>דוגמא לקוד שאינו ציקלי</u>:

די בטוח ש-$x^3 + 1$ אינו מחלק את $x^7 + 1$ ללא שארית.

נקודד את המידע $(1, 1, 0, 0)$:

$$f(x) = x^3 + x^2$$

$$x^3 f(x) = x^6 + x^5$$

נחלק:

$x^3 + x^2 + 1$
$\mathbf{x^6 + x^5 | x^3 + 1}$
$x^6 + x^3$
$x^5 + x^3$
$x^5 + x^2$
$x^3 + x^2$
$x^3 + 1$
$x^2 + 1$

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)

סה"כ, הפולינום המקודד הינו:

$$x^6 + x^5 + x^2 + 1 \leftrightarrow (1,1,0,0,1,0,1)$$

כעת נבצע הזזה ציקלית:

$$(1,0,0,1,0,1,1) \leftrightarrow x^6 + x^3 + x + 1$$

האם זה מתחלק ב-$x^3 + 1$?

$$x^3$$
$$\boldsymbol{x^6 + x^3 + x + 1 | x^3 + 1}$$
$$x^6 + x^3$$
$$x + 1$$

השארית אינה איפס, הקוד אינו ציקלי, ונגמר הקורס.

© Roee Oscar – King of Sikumim
(מבוסס על ההרצאה של ד"ר ארז שיינר – קבוצת הרצאה 01)