

שיעור 3

15.11.16

15 בנובמבר 2016

1 תורת החבורות

משפט 1.1 תהי G חבורה, אזי $H \subseteq G$ נקראת תת חבורה אם H חבורה בעצמה (תת אותה פעולה של G) (ספציפית $a \cdot b \in H \iff a, b \in H$, וקיים הופכי ב- H לכל $a, b \in H$, איבר היחידה של G נמצא ב- H)

דוגמא: ב- $\mathbb{Z}_{6,+}$ הקבוצה $\{0, 2, 4\}$ היא תת חבורה וגם $\{0, 3\}$ תת חבורה, אך למשל $\{0, 4\}$ אינה תת חבורה כי $4 +_6 4 = 2 \notin \{0, 4\}$

משפט 1.2 משפט Lagrange

תהי G חבורה סופית ו- $H \subseteq G$ תת חבורה שלה. אזי $|H| \mid |G|$

הגדרה 1.3 קוסט שמאלי: $aH = \{a \cdot h \mid h \in H\}$ (בדרך כלל זאת קבוצה ולא חבורה)

הנחה: נראה תחילה כי לכל $a, b \in G$ או שמתקיים $aH = bH$ או $aH \cap bH = \emptyset$.
נניח ש- $aH \cap bH \neq \emptyset$ ונראה $aH = bH$.

מההנחה קיימים $h_1, h_2 \in H$ כך $ah_1 = bh_2$.
ניקח $h \in H$ כלשהו. $ah = (b \cdot h_2 \cdot h_1^{-1})h = b(h_2 h_1^{-1} h)$ כאשר $h_2 h_1^{-1} h \in H$.
כלומר מתקיים $ah \in bH$ משום שזה נכון לכל $h \in H$ מתקיים $aH \subseteq bH$.
מטעמי סימטריה מתקיים גם $bH \subseteq aH$ ולכן קיבלנו

$$aH \cap bH = \emptyset \Rightarrow aH = bH$$

קעת נראה כי לכל $a \in G$ מתקיים $|aH| = |H|$ (הקוסטים), מגדירים יחס שקילות על G , נגדיר $a \sim b$ אם מתקיים $aH = bH$ (בדוק בעצמך - טרנוטיבי, רפלקסיבי, סימטרי) (יחס שקילות מפרק את הקבוצה למחלקות שקילות זרות. נרצה להראות כי הן שוות גודל) לסיים, נראה כי כל aH שוי גודל:

זה נובע מכך שההעתקה (ב- G) $x \rightarrow ax$ היא ח.ח.ע.
 $(ax_1 = ax_2 \Rightarrow x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2)$

$|aH| \leq |H|$ ולו היה קטן יותר היינו מקבלים עבור $h_1 \neq h_2$ שמתקיים $ah_1 = ah_2$ וזאת סתירה לח.ח.ע.
ולכן לכל a מתקיים $|aH| = |H|$ ולכן aH השונים הם שוי גודל וזרים ולכן $|H| \mid |G|$

הגדרה 1.4 סדר של איבר בחבורה *order*

תהי G חבורה סופית ו- $g \in G$ נתבונן ב- g, g^2, g^3, \dots נשים לב כי קיים $m \geq 1$ כך שמתקיים $g^m = 1_e$ וכן m מינימלי לתכונה זאת.
זה m יקרא הסדר של g .

לדוגמא:

\mathbb{Z}_5^* ללא 0, חבורת ההפיכים מודולו 5
למשל מהו הסדר של 3 בחבורה זאת?

$ord(3) = 4$ משום שהאיבר הקטן ביותר שמקיים $3^m = 1_e \pmod{5}$ הינו 4.
 $ord(4) = 2$ משום שמתקיים שהאיבר הקטן ביותר שמקיים $4^m = 1_e \pmod{5}$ הינו 2.

הגדרה 1.5 ת"ח ציקלית

החזקות השונות של g $\{g^0 = 1_e, g, g^2, \dots, g^{m-1}\}$ מגדירות תת-חבורה של G
תת חבורה זו נקראת תת החבורה הציקלית הנוצרת על ידי g , ומסומנת $\langle g \rangle = \{g^0 = 1_e, g, g^2, \dots, g^{m-1}\}$
נאמר כי G היא ציקלית אם קיים איבר $g \in G$ שחזקות שלו יוצרות את כל G במקרה זה g יקרא יוצר של G ונסמן $\langle g \rangle = G$

משפט 1.6 המשפט הקטן של פרמה

אם p ראשוני וקיים a $1 \leq a \leq p-1$ אזי $a^{p-1} = 1 \pmod{p}$

הנחה: נתבונן ב- \mathbb{Z}_p^* לכל $1 \leq a \leq p-1$ יש סדר m $a^m = 1 \pmod{p}$ וסדר זה מחלק את $p-1$ (ממשפט לגראנג'). ולכן $p-1 = m \cdot h$ ומתקיים $(a^m)^h = a^{p-1} = 1 \pmod{p}$

Synchronous Stream Ciphers ("imitating" one time pad) •

LSFR-Linear Feedback Shift Registers •

The shrinking Generator Stream Cipher •

RC4 •

(pseudo random generator, one way function) PRGs and OW Function •

Bit commitment •

בעולם הפיזי A מכניסה למעטפה $b = 0$ או $b = 1$, ההתחייבות אינה ניתנת לשינוי, B אינו יודע מה יש במעטפה עד שנפתח.

• נשתמש ב PRG ביישיל לפתור את בעיית ה Bit commitment

B בוחר $r \in \{0, 1\}^{3n}$ באקראי ושולח ל A

A בוחרת $s \in \{0, 1\}^n$ ושולחת, אם $b = 0$ את $G(s)$ אם $b = 1$ את $G(s) \oplus r$

כאשר ה"מעטפה" נפתחת A שולחת ל B את s וכך B יודע אם בחרה $b = 0$ או $b = 1$.

האם A יכולה לשלוח s' שמקיים $G(s') = G(s) \oplus r$ וכך לשנות את ההתחייבות שלה?

נסתכל על שיקולי ספירה, כמה זוגות (s, s') יש? 2^{2n} , כמה r יש? 2^{3n} .

אם $G(s') = G(s) \oplus r$ אז $G(s) \oplus G(s') = r$ עבור צד שמאל יש לכל היותר 2^{2n} אפשרויות ועבור צד ימין 2^{3n} אז שימצא s' הינו זניח.

• פונקציות רנדומאליות

• פונקציות פסאודו רנדומאליות (PRF)