סמינר בנושא אנלוג להשערת קולץ בפולינומים

24 בספטמבר 2024

רקע מתמטי

בכדי להבין את התוכן המוצג בסמינר זה, נדרשת היכרות עם סימונים אסימפטוטיים אותה ניתן לרכוש מעיון בפרק 3 של הספר **מבוא לאלגוריתמים** [6].

כמו כן נדרש ידע בסיסי בחוגים, ובפרט היכרות עם $\mathbb{F}_2\left[x\right]$, חוג הפולינומים מעל השדה הסופי $\mathbb{F}_2$. היכרות זו ניתן לרכוש מעיון בפרקים 14-18 של הספר **מבנים אלגבריים** [7].

1 מבוא

1.1 הצגת השערת קולץ

השערת קולץ, הידועה גם כבעיית "$3n+1$" היא בעיה פתוחה מפורסמת במתמטיקה המיוחסת באופן מסורתי ללותר קולץ, אשר נהגתה בשנות ה-30 של המאה ה-20. (ראו [1])

מגדירים מיפוי $\mathcal{C}:\mathbb{N}\to\mathbb{N}$ באופן הבא:

$$\mathcal{C}\left(n\right) = \begin{cases} \frac{n}{2} & n\equiv 0 \pmod 2 \\ 3n+1 & n\equiv 1 \pmod 2 \end{cases}$$

ההשערה היא שתהליך של הפעלה חוזרת של המיפוי $\mathcal{C}$, על כל מספר טבעי שנבחר, תביא לאחר מספר סופי של צעדים למספר 1. באופן פורמלי, לכל $n\geq 1$ קיים $k\geq 0$ כך ש-$\mathcal{C}^k\left(n\right)=1$.

נפעיל לדוגמה את התהליך על המספר $n=11$:

$$11\to 34\to 17\to 52\to 26\to 13\to 40\to 20\to 10\to 5\to 16\to 8\to 4\to 2\to 1$$

מצאנו כי $\mathcal{C}^{14}\left(11\right)=1$.

ההשערה הפכה למפורסמת בעיקר בשל פשטות הניסוח שלה, שהופכת אותה לנגישה גם למי שאינו מתמטיקאי.

למרות שההשערה עצמה טרם הוכחה או הופרכה, נעשו נסיונות רבים לפתור אותה ואף התקבלו תוצאות חלקיות מעניינות. (הבולטת בהן היא עבודתו של טרנס טאו, ראו [4])

1.2 בעיה אנלוגית ב-$\mathbb{F}_2\left[x\right]$

עבור בעיות אריתמטיות רבות, טבעי לבחון בעיה אנלוגית בחוגי פולינומים. בעיה אנלוגית כזו נחקרה בשנת 2008 על ידי Hicks, Mullen, Yucas וZavislak (ראו [2]).

מגדירים מיפוי $T:\mathbb{F}_2[x]\to\mathbb{F}_2[x]$ באופן הבא:

$$T(f) = \begin{cases} \frac{f}{x} & f\equiv 0 \pmod{x} \\ (x+1)f+1 & f\equiv 1 \pmod{x} \end{cases}$$

ושואלים - האם לכל $0\neq f\in\mathbb{F}_2[x]$ קיים $k\geq 0$ כך ש$T^k(f)=1$? לבעיה זו נקרא בהמשך "בעיית קולץ הפולינומיאלית".

נבצע לדוגמה הפעלה חוזרת של T על הפולינום x^2+1:

$$x^2+1\to x^3+x^2+x\to x^2+x+1\to x^3\to x^2\to x\to 1$$

כלומר $T^6\left(x^2+1\right)=1$.

מהשוואה בין T לבין $\mathcal{C}$ ניתן לראות כי האיבר הראשוני x בחוג $\mathbb{F}_2[x]$ ממלא את תפקידו של המספר הראשוני 2: ההתחלקות בו מורה לאיזה ענף של T לפנות כשם שההתחלקות ב2 מורה לאיזה ענף של $\mathcal{C}$ לפנות.

בהמשך להשוואה זו, לפולינום $f\in\mathbb{F}_2[x]$ המתחלק בx, כלומר מקיים $f\equiv 0 \pmod{x}$ אנו קוראים פולינום "זוגי" ולפולינום שאינו מתחלק בx אנו קוראים פולינום "אי-זוגי". נעיר כי $f\equiv f(0) \pmod{x}$ (הכוונה ב$f(0)$ היא לפולינום הקבוע שהמקדם החופשי שלו הוא תוצאת ההצבה של 0 בf) ולכן f הוא זוגי אם ורק אם $f(0)=0$.

1.3 "מבט על" של הסמינר

בסמינר זה נציג תשובה חיובית לבעיית קולץ הפולינומיאלית. לאחר קבלת תשובה חיובית זו טבעי לשאול - "כמה מהר" לוקח להגיע ל-1?

לכל מיפוי $M:\mathbb{F}_2[x]\to\mathbb{F}_2[x]$ ולכל $f\in\mathbb{F}_2[x]$ נגדיר:

$$t_{\min}(f,M) = \min\left\{k\geq 0 : M^k(f)=1\right\}$$

אם קיים k כזה, ואחרת נגדיר $t_{\min}(f,M)=\infty$.

למעשה, נוכיח שזמן העצירה סופי על ידי הוכחה כי לכל $0\neq f\in\mathbb{F}_2[x]$ מתקיים:

$$t_{\min}(f,T)\leq \deg(f)^2+2\deg(f)$$

ובסימונים אסימפטוטיים, $t_{\min}(f,T)=O\left(\deg(f)^2\right)$.

בשלב הבא, שמהווה את חלק הארי של הסמינר, נשפר את החסם הזה ונוכיח כי לכל $0\neq f\in\mathbb{F}_2[x]$ מתקיים:

$$t_{\min}(f,T)\leq (2\deg(f))^{1.5}+\deg(f)$$

משמע $t_{\min}(f,T)=O\left(\deg(f)^{1.5}\right)$.

לסיום, נוכיח תוצאה נוספת שמהווה אנלוג להשערה בנוגע לזמני העצירה של מספרים העונים לתבנית מסוימת, ביחס למיפוי $\mathcal{C}$.

הוכח (ראו [5]) כי סדרת זמני העצירה של המספרים 2^n+1 מכילה תתי סדרות חשבוניות עם הפרש משותף 1 שאורכן גדול כרצוננו. אותה תופעה זוהתה גם במספרים מתבניות אחרות דומות, מה שהוביל לניסוח ההשערה הבאה:

השערה 1.1. יהיו מספרים שלמים $a,b\geq 0$. סדרת זמני העצירה של המספרים $\left(2^a3^b\right)^n+1$ מכילה תתי סדרות חשבוניות שאורכן גדול כרצוננו, ובעלות הפרש משותף $a-b$.

נביא בהמשך הגדרה מדויקת למושג "מכילה תת סדרה חשבונית שאורכה גדול כרצוננו". התוצאה האנלוגית שנוכיח תהיה בנוגע לפולינומים מהצורה $\left(x^a\left(1+x\right)^b\right)^n+1$, והיא תיעשה על ידי חישוב נוסחה מדויקת לזמני העצירה של אותם הפולינומים.

2 תוצאות

2.1 הוכחה שזמן העצירה סופי

כדי להוכיח שזמן העצירה סופי, נתחיל בלהוכיח שלאחר מספר צעדים שחסום על ידי ביטוי התלוי במעלה של f, המעלה של f חייבת לקטון. עבור פולינום זוגי, נדרש צעד אחד להורדת המעלה. עבור פולינום אי זוגי, המצב מעט יותר מסובך. נתבונן למשל בפולינום x^7+x^5+1. על מנת להמחיש ויזואלית את הסדרה המתקבלת מהפעלות חוזרות של T, נאמץ את הסימון הבא של פולינום כוקטור בינארי:

x^7+x^5+1 ■□■□□□□■

ריבוע שחור מייצג את המקדמים שערכם 1 וריבוע לבן מייצג את המקדמים שערכם 0, וככל שמתקדמים שמאלה, החזקה של x עולה.

0	□■□■□□□□■
1	■■■■□□□■□
2	□■■■■□□□■
3	■□□□■□□■□
4	□■□□□■□□■
5	■■□□■■□■□
6	□■■□□■■□■
7	■□■□■□■■□
8	□■□■□■□■■
9	■■■■■■■□□
10	□■■■■■■■□
11	□□■■■■■■■

נתבונן בשורות $0,2,4,6,8$. ניתן לראות שבשורה 0 קיים מרווח של 4 מקומות בין החזקה הנמוכה ביותר לחזקה הבאה, לאחר מכן בשורה 2 המרווח הוא של 3 מקומות. זה ממשיך עד שהמרווח נעלם בשורה 8. לאחר מכן נדרשים עוד 3 צעדים כדי להגיע לפולינום ממעלה 6.

למה 2.1. יהי $f\in\mathbb{F}_2\left[x\right]$ כך ש$\deg\left(f\right)\geq 1$. קיים $1\leq m\leq 2\deg\left(f\right)+1$ כך שמתקיים:

$$\deg\left(T^m\left(f\right)\right) \quad = \quad \deg\left(f\right)-1$$

הוכחה. נסמן $d=\deg\left(f\right)$. אם f זוגי אז $T\left(f\right)=\frac{f}{x}$ ולכן,

$$\deg\left(T\left(f\right)\right)=d-1$$

במקרה זה $m=1$ מקיים את הטענה.

אם f אי זוגי, נרשום:

$$f \quad = \quad x^r g + 1$$

כאשר $1 \le r \le d$ החזקה המקסימלית של x המחלקת את $f-1$, כלומר $x \nmid g$. כמו כן $\deg g = d - r$. נעיר כי r הוא למעשה החזקה הנמוכה ביותר של x המופיעה בf פרט ל1.

נוכיח באינדוקציה כי לכל $1 \le j \le r$ מתקיים:

$$T^{2j}(f) \quad = \quad (x+1)^j x^{r-j} g + 1$$

עבור $j = 1$:

$$\begin{aligned} T(f) &= (x+1)(x^r g + 1) + 1 = (x+1) x^r g + x \\ T^2(f) &= (x+1) x^{r-1} g + 1 \end{aligned}$$

נניח כעת כי התוצאה נכונה עבור $1 \le j < r$ ונוכיח שהיא נכונה עבור $j+1$. מהנחת האינדוקציה:

$$T^{2j}(f) \quad = \quad (x+1)^j x^{r-j} g + 1$$

מכיוון ש$j < r$, הפולינום $(x+1)^j x^{r-j} g$ זוגי ולכן $T^{2j}(f)$ אי זוגי.

$$\begin{aligned} T^{2j+1}(f) &= (x+1)^{j+1} \left(x^{r-j} g + 1\right) + 1 = (x+1)^{j+1} x^{r-j} g + x \\ T^{2j+2}(f) &= (x+1)^{j+1} x^{r-(j+1)} g + 1 \end{aligned}$$

ובכך הוכחנו את צעד האינדוקציה.

נקבל בפרט עבור $j = r$:

$$T^{2r}(f) \quad = \quad (x+1)^r g + 1$$

נזכיר כי g אי זוגי ולכן $(x+1)^r g$ אי זוגי. זה גורר ש$T^{2r}(f)$ זוגי לכן:

$$T^{2r+1}(f) \quad = \quad \frac{(x+1)^r g + 1}{x}$$

ומתקיים:

$$\deg\left(T^{2r+1}(f)\right) \quad = \quad \deg\left(T^{2r}(f)\right) - 1 = d - 1$$

במקרה זה $m = 2r + 1 \le 2d + 1$ מקיים את הטענה. $\square$

כעת נקל להוכיח באינדוקציה על מעלת הפולינום את החסם שתיארנו בהקדמה.

משפט 2.2. יהי $0 \ne f \in \mathbb{F}_2[x]$, אז $t_{\min}(f,T) \le \deg(f)^2 + 2\deg(f)$.

הוכחה. נוכיח את הטענה באינדוקציה על מעלת f.

בסיס האינדוקציה: $\deg f = 0$. הפולינום היחיד ב$\mathbb{F}_2[x]$ שמעלתו 0 הוא 1 ולכן $t_{\min}(f,T) = 0$ והחסם מתקיים.

צעד האינדוקציה: יהי $f \in \mathbb{F}_2[x]$ כך ש$\deg f = d > 1$. על פי 2.1, קיים

$$1 \le m \le 2d + 1$$

כך ש $\deg\left(T^{m}\left(f\right)\right)=d-1$. מהנחת האינדוקציה,

$$t_{\min}\left(T^{m}\left(f\right),T\right) \leq \left(d-1\right)^{2}+2\left(d-1\right)$$

ומכאן

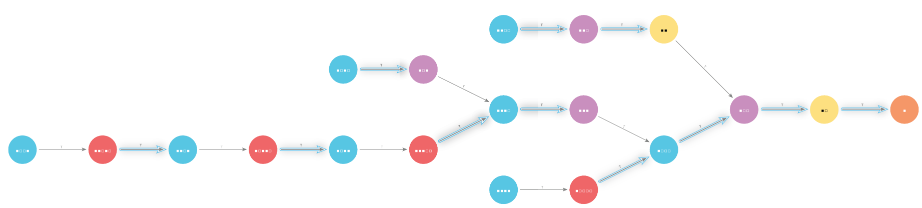
$$\begin{aligned}t_{\min}\left(f,T\right) &\leq t_{\min}\left(T^{m}\left(f\right),T\right)+m\\ &\leq \left(d-1\right)^{2}+2\left(d-1\right)+m\\ &\leq \left(d-1\right)^{2}+2\left(d-1\right)+2d+1=d^{2}+2d\end{aligned}$$

כנדרש. $\square$

2.2 חסם משופר לזמן העצירה

כפי שציינו במבוא, קיבלנו חסם אסימפטוטי ריבועי ל$t_{\min}\left(f,T\right)$ כתלות ב$\deg f$. בחלק זה נשפר את החסם ונוכיח $t_{\min}\left(f,T\right)=O\left(\left(\deg f\right)^{1.5}\right)$.

נתבונן במסלול שעושים פולינומים ממעלה עד 3 עד שהם מגיעים ל1:

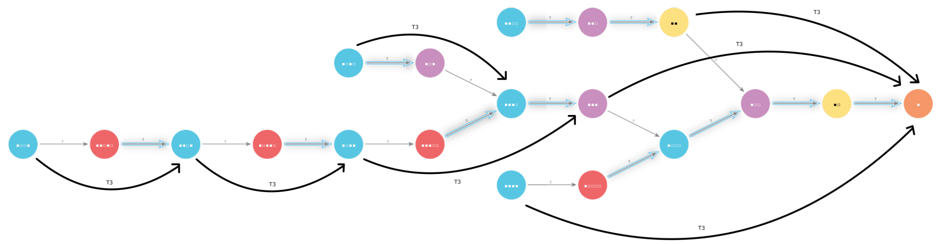


חץ מודגש מתאים לצעדים מסוג $f\mapsto\frac{f}{x}$ וחץ רגיל לצעדים מסוג $f\mapsto\left(x+1\right)f+1$. נשים לב שכל פולינום זוגי מגיע לפולינום אי זוגי לאחר רצף של חלוקות בx, ואם כך נוכל להוכיח חסם לפולינומים אי זוגיים בלבד ולאחר מכן להסיק ממנו חסם לכל פולינום שונה מ0 בעזרת הקשר הבא:

$$t_{\min}\left(f,T\right) = r+t_{\min}\left(\overbrace{\frac{f}{x^{r}}}^{\text{odd}},T\right)$$

כאשר r החזקה הגבוהה ביותר של x המחלקת את f.

פולינום אי זוגי עובר על ידי הצעד $f\mapsto\left(x+1\right)f+1$ לפולינום זוגי שבתורו עובר לפולינום אי זוגי לאחר רצף של צעדים מסוג $f\mapsto\frac{f}{x}$. נוכל לקבץ את רצף הפעולות האלו, למיפוי שבהמשך נקרא לו T_3. מהגדרתו, T_3 מעביר פולינום אי זוגי לפולינום האי זוגי הבא אחריו בסדרה $\left(T^{n}\left(f\right)\right)_{n\geq0}$. נתבונן בגרף הבא להמחשה (מומלץ להגדיל את המסמך בכדי לקרוא בבירור את התוויות):



מצאנו שמספיק לחקור את זמן העצירה של T_3 עבור פולינומים אי זוגיים, ומתברר שאם הופכים את סדר המקדמים של הפולינומים (האי זוגיים) בסדרה $\left(T_3^n\left(f\right)\right)_{n\geq 0}$ מקבלים סדרת פולינומים, אי זוגיים גם הם, שבה המעבר מפולינום לפולינום הבא מתואר על ידי מיפוי פשוט יותר מ-T_3 שנגדיר ונסמן בהמשך בתור S_3.

היתרון של המיפוי S_3 הוא שהפולינום $S_3^n\left(f\right)$ שווה לפולינום $\left(x+1\right)^n f$ ללא חלק מהמקדמים המובילים שלו (ראו 2.13)

נוכיח כי עבור פולינומים אי זוגיים $t_{\min}\left(f,S_3\right)=O\left(\left(\deg f\right)^{1.5}\right)$ ובעזרת הקשר בין T שאותה רצינו לחקור מלכתחילה לבין S_3 נוכל לגזור את החסם הרצוי לגבי T.

2.2.1 צמצום למקרה של פולינום אי זוגי

כפי שציינו במבוא ל2.2, ניתן לצמצם את הבעיה לפולינומים אי זוגיים בלבד. נתחיל בלהציג מספר מיפויי עזר.

הגדרה 2.3. לכל $f\in\mathbb{F}_2\left[x\right]$ נגדיר את המיפויים הבאים:

- $T_1\left(f\right)=\left(x+1\right)f+1$
- $T_2\left(f\right)=\frac{f}{x^r}$ כאשר r החזקה המקסימלית של x המחלקת את f עבור $f\neq 0$ ונגדיר גם $T_2\left(0\right)=0$
- $T_3\left(f\right)=\left(T_2\circ T_1\right)\left(f\right)$

לכל $f\in\mathbb{F}_2\left[x\right]$ אי זוגי, הסדרה $\left(T_3^n\left(f\right)\right)_{n\geq 0}$ מהווה תת סדרה של $\left(T^n\left(f\right)\right)_{n\geq 0}$ שכן עבור f אי זוגי הפעלה יחידה של T_3 שקולה להפעלה חוזרת של T עד להגעה לפולינום אי זוגי שוב בפעם הראשונה.

למה 2.4. יהי $f\in\mathbb{F}_2\left[x\right]$ אי זוגי. $t_{\min}\left(f,T\right)=2t_{\min}\left(f,T_3\right)+\deg\left(f\right)$ (כפרט $t_{\min}\left(f,T_3\right)$ סופי)

הוכחה. נוכיח את הטענה באינדוקציה שלמה על מעלת הפולינום f. אם $\deg f=0$ אז $f\left(x\right)=1$, $t_{\min}\left(f,T\right)=0$ וכן $t_{\min}\left(f,T_3\right)=0$ ולכן השוויון נכון.

יהי $d>1$. נניח שהטענה נכונה לפולינומים אי זוגיים ממעלה קטנה מ-d ונוכיח אותה לפולינומים אי זוגיים ממעלה d. יהי f אי זוגי, הנתון בצורה:

$$f\quad=\quad x^r g+1$$

כאשר $1 \leq r \leq d$ החזקה המקסימלית של x המחלקת את $f-1$. תהי s החזקה המקסימלית של x המחלקת את הפולינום $(x+1)^r xg + x$. נשים לב ש$s \geq 2$ כי:

$$(x+1)^r xg + x \quad = \quad x\left[(x+1)^r g + 1\right]$$

והפולינום $(x+1)^r g + 1$ זוגי כסכום של פולינומים אי זוגיים. נוכיח שמתקיים:

$$T^{2(r-1)+1+s}(f) \quad = T_3^{(r-1)+1}(f) = \quad \frac{(x+1)^r xg + x}{x^s} \tag{1}$$

ונוכל להשתמש בהנחת האינדוקציה על הפולינום $\frac{(x+1)^r xg+x}{x^s}$ שכן:

$$\begin{aligned}
\deg\left(\frac{(x+1)^r xg + x}{x^s}\right) &= \deg\left(\frac{(x+1)^r g + 1}{x^{s-1}}\right) \\
&= \deg\left((x+1)^r g + 1\right) - \deg\left(x^{s-1}\right) \\
&= \deg\left((x+1)^r g\right) - \deg\left(x^{s-1}\right) \\
&= r + \deg(g) - (s-1) = d - (s-1) \\
&= d - s + 1 \leq d - 1 < d
\end{aligned}$$

כדי להוכיח את 1 נוכיח שהתהליך שעובר f עד להגעה ל$\frac{(x+1)^r xg+x}{x^s}$ על ידי כל אחד מהמיפויים נראה כך:

$$\begin{array}{llll}
f \overbrace{\rightarrow}^{T^{2(r-1)}} (x+1)^{r-1} xg + 1 & \overbrace{\rightarrow}^{T} (x+1)^r xg + x & \overbrace{\rightarrow}^{T^s} & \dfrac{(x+1)^r xg + x}{x^s} \\
f \overbrace{\rightarrow}^{T_3^{r-1}} (x+1)^{r-1} xg + 1 & \overbrace{\rightarrow}^{T_3} & & \dfrac{(x+1)^r xg + x}{x^s}
\end{array} \tag{2}$$

ב2.1 הוכחנו כי מתקיים כי לכל $1 \leq j \leq r$:

$$T^{2j}(f) \quad = \quad (x+1)^j x^{r-j} g + 1$$

בפרט עבור $j = r-1$:

$$T^{2(r-1)}(f) \quad = \quad (x+1)^{r-1} xg + 1$$

כאשר מפעילים את T קורית אחת מהפעולות:

$$\begin{array}{ll}
(1) & f \mapsto (x+1) f + 1 \\
(2) & f \mapsto \dfrac{f}{x}
\end{array}$$

נשים לב כי מההוכחה ב2.1 נובע כי $2(r-1)$ ההפעלות של T הן לסירוגין מסוג (1) ו(2) כלומר מתחלקות ל$r-1$ זוגות של הפעלות כך שכל זוג הפעלות שקול להפעלה אחת של T_3 ולכן:

$$T_3^{r-1}(f) \quad = \quad (x+1)^{r-1} xg + 1$$

בכך הוכחנו את המעבר הראשון בכל שורה של 2. לגבי המעברים האחרים, הפולינום $(x+1)^{r-1}xg+1$ אי זוגי ולכן:

$$\begin{aligned} T\left((x+1)^{r-1}xg+1\right) &= (x+1)^{r}xg+x \\ T_1\left((x+1)^{r-1}xg+1\right) &= (x+1)^{r}xg+x \end{aligned}$$

נזכיר כי s החזקה הגבוהה ביותר של x המחלקת את $(x+1)^{r}xg+x$ ולכן מתקיים:

$$\begin{aligned} T^s\left((x+1)^{r}xg+x\right) &= \frac{(x+1)^{r}xg+x}{x^s} \\ T_2\left((x+1)^{r}xg+x\right) &= \frac{(x+1)^{r}xg+x}{x^s} \end{aligned}$$

כעת מ1 נובע:

$$\begin{aligned} t_{\min}(f,T) &= 2(r-1)+1+s+t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T\right) \\ t_{\min}(f,T_3) &= (r-1)+1+t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T_3\right) \end{aligned} \tag{3}$$

מצאנו כי $\deg\left(\frac{(x+1)^{r}xg+x}{x^s}\right)=d-s+1$ לכן מהנחת האינדוקציה:

$$t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T\right) = 2t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T_3\right)+d-s+1$$

נציב את זה ב3:

$$\begin{aligned} t_{\min}(f,T) &= 2(r-1)+1+s+2t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T_3\right)+d-s+1 \\ &= 2(r-1)+2+2t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T_3\right)+d \\ &= 2\left[(r-1)+1+t_{\min}\left(\frac{(x+1)^{r}xg+x}{x^s},T_3\right)\right]+d \\ &= 2t_{\min}(f,T_3)+d \end{aligned}$$

ובכך הושלם צעד האינדוקציה. $\square$

2.2.2 הפולינום ההדדי ומיפויים מקבילים

ברצוננו להמשיך ולחקור את הסדרה $\left(T_3^n(f)\right)_{n\geq 0}$ עבור f אי זוגי. מתברר כי אם נבצע היפוך של סדר המקדמים עבור כל הפולינומים שבסדרה נקבל שוב סדרה של פולינומים אי זוגיים. בסדרה זו נוכל לתאר את המעבר מפולינום נתון לפולינום הבא אחריו בעזרת מיפוי פשוט יותר מאשר T_3 שנגדיר ונסמן בS_3.

הפולינום המתקבל מפולינום נתון בעזרת היפוך סדר המקדמים נקרא הפולינום ההדדי. בחלק זה נציג תכונות בסיסיות של הפולינום ההדדי, נגדיר את המיפוי S_3 ונוכיח שעבור פולינומים אי זוגיים מתקיים $t_{\min}(f,S_3)=O\left((\deg f)^{1.5}\right)$.

הגדרה 2.5. יהי מיפוי היפוך סדר המקדמים $\hat{} : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ הפועל כך:

$$f \quad \mapsto \quad \widehat{f} = x^{\deg(f)} f\left(\frac{1}{x}\right)$$

נדבוק בקונבנציה ש$\deg(0) = -\infty$ ולכן מתקיים $\widehat{0} = 0$. לפולינום $\hat{f}$ נקרא הפולינום ההדדי של f.

למה 2.6. תכונות של המיפוי $f \mapsto \widehat{f}$:

1. אם $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_2[x]$ כאשר $a_m \neq 0$ אז $\widehat{f}(x) = \sum_{i=0}^{m} a_i x^{m-i}$
2. לכל $f, g \in \mathbb{F}_2[x]$ מתקיים $\widehat{fg} = \widehat{f}\widehat{g}$
3. לכל $f \in \mathbb{F}_2[x]$ ו$k \geq 0$ מתקיים $\widehat{x^k f} = \widehat{f}$
4. לכל $0 \neq f \in \mathbb{F}_2[x]$ מתקיים $\hat{\hat{f}} = \frac{f}{x^r}$ כאשר r החזקה המקסימלית של x המחלקת את f. בפרט אם f אי זוגי אז $\hat{\hat{f}} = f$.

הוכחה. נוכיח את התכונות:

1. $\deg f = m$ ולכן:

$$\widehat{f}(x) \quad = \quad x^m \sum_{i=0}^{m} a_i \left(\frac{1}{x}\right)^i = \sum_{i=0}^{m} a_i x^{m-i}$$

2. נוכיח על פי ההגדרה:

$$\begin{aligned} \left(\widehat{fg}\right)(x) &= x^{\deg(fg)} (fg)\left(\frac{1}{x}\right) = x^{\deg(f)+\deg(g)} f\left(\frac{1}{x}\right) g\left(\frac{1}{x}\right) \\ &= x^{\deg(f)} f\left(\frac{1}{x}\right) x^{\deg(g)} g\left(\frac{1}{x}\right) = \hat{f}(x)\,\hat{g}(x) = \left(\hat{f}\hat{g}\right)(x) \end{aligned}$$

3. על פי חלק 2:

$$\widehat{x^k f} \quad = \quad \widehat{x^k}\hat{f}$$

אבל $\widehat{x^k} = x^k \cdot \left(\frac{1}{x}\right)^k = 1$ ומכאן התוצאה הנדרשת.

4. נרשום $f = x^r g$. נסמן $g(x) = \sum_{i=0}^{m} a_i x^i$ כאשר $a_m \neq 0$ אז מחלק 1:

$$\widehat{g}(x) = \sum_{i=0}^{m} a_i x^{m-i}$$

על ידי החלפת אינדקס נקבל:

$$\widehat{g}\left(x\right)=\sum_{i=0}^{m}\overbrace{a_{m-i}}^{b_i}x^{i}$$

הפולינום g אי זוגי ולכן $a_0 \neq 0$ כלומר $b_m \neq 0$ לכן שוב נקבל מחלק 1 כי:

$$\hat{\hat{g}}\left(x\right)=\sum_{i=0}^{m}b_{i}x^{m-i}$$

ועל ידי החלפת אינדקס נוספת נקבל:

$$\hat{\hat{g}}\left(x\right)=\sum_{i=0}^{m}b_{m-i}x^{i}=\sum_{i=0}^{m}a_{m}x^{i}=g\left(x\right)$$

כעת ניעזר בחלק 3 ונקבל:

$$\hat{\hat{f}} \quad = \quad \widehat{\widehat{x^{r}g}}=\hat{\hat{g}}=g=\frac{f}{x^{r}}$$

□

הגדרה 2.7. עבור $f\in\mathbb{F}_2\left[x\right]$ יהיו:

- $S_1\left(f\right)=\left(x+1\right)f$
- $S_2\left(f\right)=f+x^{\deg(f)}$ (מאחר וf מעל השדה $\mathbb{F}_2$ הפעלה של S_2 מאפסת את המקדם העליון)
- $S_3\left(f\right)=\left(S_2\circ S_1\right)\left(f\right)$

למה 2.8. יהי f פולינום אי זוגי, אז מתקיים:

א. $\widehat{T_3\left(f\right)}=S_3\left(\hat{f}\right)$

ב. $t_{\min}\left(f,T_3\right)=t_{\min}\left(f,S_3\right)$

הוכחה. נוכיח:

1. $\widehat{T_3\left(f\right)}=T_2\left(\widehat{T_1\left(f\right)}\right)$. לפי סעיף 4 של 2.6 מתקיים $T_2\left(\widehat{T_1\left(f\right)}\right)=\widehat{T_1\left(f\right)}$. עבור g אי זוגי, הפעולה $g\mapsto\widehat{g+1}$ מאפסת את המקדם התחתון והופכת את סדר המקדמים ולכן שקולה לפעולה $g\mapsto S_2\left(\hat{g}\right)$ שהופכת את סדר המקדמים ואז מאפסת את המקדם העליון. נשתמש בתכונה זו עבור $g=\left(x+1\right)f$:

$$\widehat{T_1\left(f\right)} \quad = \quad \underbrace{\widehat{\left(x+1\right)f}}_{g}+1=S_2\left(\widehat{\left(x+1\right)f}\right)$$

לפי סעיף 2 של 2.6 מתקיים:

$$S_2\left(\widehat{(x+1)\,f}\right) = S_2\left(\widehat{(x+1)}\hat{f}\right) = S_2\left((x+1)\,\hat{f}\right)$$

נשים לב כי הביטוי האחרון שווה ל$S_2\left(S_1\left(\hat{f}\right)\right)$ כלומר ל$S_3\left(\hat{f}\right)$ ולכן הוכחנו $\widehat{T_3(f)} = S_3\left(\hat{f}\right)$.

2. מסעיף 1 מקבלים באינדוקציה מיידית כי לכל $n \geq 1$:

$$\widehat{T_3^n(f)} = S_3^n\left(\hat{f}\right)$$

נסמן $n = t_{\min}(f, T_3)$ ונתבונן בסדרה:

$$f, T_3(f), T_3^2(f) ..., T_3^n(f) = 1$$

אם נפעיל את המיפוי $f \mapsto \hat{f}$ על כל איברי הסדרה נקבל:

$$\widehat{f}, \widehat{T_3(f)}, \widehat{T_3^2(f)} ..., \widehat{1} = \widehat{f}, S_3\left(\widehat{f}\right), S_3^2\left(\widehat{f}\right), ..., 1$$

ובסדרה זו האיבר 1 מופיע רק במקום האחרון שכן עבור $m < n$, $T_3^m(f) \neq 1$ ומהיותו של $T_3^m(f)$ פולינום אי זוגי נקבל $\widehat{T_3^m(f)} \neq 1$ כי אילו היה מתקיים השוויון $\widehat{T_3^m(f)} = 1$ היינו יכולים להפעיל את מיפוי היפוך המקדמים שוב ולקבל $\widehat{\widehat{T_3^m(f)}} = \widehat{1}$ כלומר $T_3^m(f) = 1$ וזו סתירה. מצאנו אם כך שיש להפעיל n פעמים את S_3 על $\widehat{f}$ כדי להגיע ל1 בפעם הראשונה ולכן $t_{\min}\left(\hat{f}, S_3\right) = n$ כנדרש.

□

הלמה האחרונה מאפשרת לנו להתמקד בחסימה של זמן העצירה של S_3 בלבד, שהוא כאמור מיפוי פשוט יותר. נסכם זאת במסקנה.

מסקנה 2.9. יהי f אי זוגי. אז מתקיים:

$$t_{\min}(f, T) = 2t_{\min}\left(\hat{f}, S_3\right) + \deg(f)$$

הוכחה. נובע משילוב של סעיף 2 של 2.8 ו2.4. □

עבור פולינום $f(x) = \sum a_i x^i$ נשתמש בסימון $f|_{\leq n}$ עבור הפולינום $\sum_{i \leq n} a_i x^i$ כלומר משמיטים חזקות גבוהות מn.

למה 2.10. $f \equiv g \mod x^n$ אם ורק אם $f|_{\leq n-1} = g|_{\leq n-1}$

הוכחה. נסמן $f(x) = \sum a_i x^i$ וכן $g(x) = \sum b_i x^i$. $f \equiv g \mod x^n$ אם ורק אם $x^n | (f - g)$ וזה שקול לכך שלכל $0 \leq i < n$ מתקיים $a_i - b_i = 0$ כלומר מקדמי החזקות $0 \leq i \leq n-1$ של f, g מזדהים, וזה מתקיים אם ורק אם $f|_{\leq n-1} = g|_{\leq n-1}$. □

היתרון של המיפוי S_3 הוא שאנחנו יכולים לתאר בצורה יחסית פשוטה מה יהיה הפולינום שנקבל על ידי מספר הפעלות חוזרות שלו וזהו התוכן של שלוש הלמות הבאות.

למה 2.11. יהי $f(x)=x^n+g$ אי זוגי, כאשר $\deg(g)<n$. אז לכל $0\le i\le n-\deg(g)$ מתקיים $S_3^i(f)=x^n+(x+1)^i g=((x+1)f)|_{\le n}$.

הוכחה. יהי $r=n-\deg(f)$. נוכיח באינדוקציה על i כי לכל $0\le i\le r$ מתקיים השוויון הראשון. עבור $i=0$ השוויון ברור. יהי $i<r$ ונניח $S_3^i(f)=x^n+(x+1)^i g$. נשים לב כי $\deg\left((x+1)^i g\right)<n$ ולכן $\deg\left(S_3^i(f)\right)=n$. נחשב את $S_1\left(S_3^i(f)\right)$:

$$\begin{aligned}S_1\left(S_3^i(f)\right) &= (x+1)\left(x^n+(x+1)^i g\right)\\ &= x^{n+1}+x^n+(x+1)^{i+1}g\end{aligned}$$

כעת נחשב את $S_3\left(S_3^{i+1}(f)\right)$ כלומר נמצא את הפולינום המתקבל מהפעלה של S_3 על $S_3^i(f)$:

$$\begin{aligned}S_3^{i+1}(f) &= S_3\left(S_3^i(f)\right)=S_2\left(S_1\left(S_3^i(f)\right)\right)\\ &= S_2\left(x^{n+1}+x^n+(x+1)^{i+1}g\right)\\ &= x^n+(x+1)^{i+1}g\end{aligned}$$

נסביר את המעבר האחרון - $\deg\left((x+1)^{i+1}g\right)\le n$ ולכן $\deg\left(x^{n+1}+x^n+(x+1)^{i+1}g\right)=n+1$. בכך הוכחנו את צעד האינדוקציה.

נוכיח כעת את השוויון השני. לכל $0\le i\le r$ מתקיים $\deg\left((x+1)^i g\right)\le n$ ולכן:

$$S_3^i(f) = x^n+(x+1)^i g=\left(x^n+(x+1)^i g\right)|_{\le n}$$

מתקיים $x^n\equiv(x+1)^i x^n \mod x^n$ ולכן:

$$x^n+(x+1)^i g \quad \equiv_{x^n} \quad (x+1)^i x^n+(x+1)^i g=(x+1)^i(x^n+g)=(x+1)^i f$$

לכן אם כך לפי 2.10:

$$S_3^i(f) = \left(x^n+(x+1)^i g\right)|_{\le n-1}=\left((x+1)^i f\right)|_{\le n-1}$$

כמו כן x^n מופיע עם מקדם 1 בשני הביטויים לכן:

$$S_3^i(f) = \left(x^n+(x+1)^i g\right)|_{\le n}=\left((x+1)^i f\right)|_{\le n}$$

וקיבלנו את השוויון השני. $\square$

הלמה הבאה מקשרת בין זמן העצירה של f אי זוגי לזמן העצירה של פולינום אי זוגי ממעלה נמוכה יותר.

למה 2.12. יהי $f(x)=x^n+g(x)$ כאשר g אי זוגי ו־$n\ge 2$. נסמן $r=n-\deg(g)$ ונניח $r>0$. מתקיים $t_{\min}(f,S_3)=r-1+t_{\min}\left((x+1)^{r-1}g,S_3\right)$

הוכחה. לפי השוויון הראשון של 2.11:

$$S_3^r(f) = x^n + (x+1)^r g$$

מתקיים $\deg\left((x+1)^r g\right) = r + \deg(g) = n$ ולכן הוספה של x^n לפולינום הזה שקולה להפעלת S_2 ולכן:

$$S_3^r(f) = S_2\left((x+1)^r g\right) = S_2\left(S_1\left((x+1)^{r-1} g\right)\right) = S_3\left((x+1)^{r-1} g\right) \quad (4)$$

נשים לב כי מ2.11 נובע כי לכל $0 \le i \le r-1$ מתקיים $\deg\left(S_3^i(f)\right) = n$ ולכן בפרט $S_3^i(f) \neq 1$. אם כך:

$$t_{\min}(f, S_3) = r + t_{\min}\left(f, S_3^r(f)\right) \overbrace{=}^{(3)} r + t_{\min}\left(f, S_3\left((x+1)^{r-1} g\right)\right) \quad (5)$$

אם $(x+1)^{r-1} g \neq 1$ אז:

$$t_{\min}\left(f, S_3\left((x+1)^{r-1} g\right)\right) = t_{\min}\left(f, (x+1)^{r-1} g\right) - 1$$

והצבה של השוויון הנ"ל ב(4) נותנת את השוויון הדרוש. נניח בשלילה כי $(x+1)^{r-1} g = 1$ אז $g = 1$ וגם $(x+1)^{r-1} = 1$ כלומר $r = 1$. במקרה זה $n = r + \deg(g) = 1 + 0 = 1$ ולכן תנאי הטענה לא מתקיימים. □

למה 2.13. יהיו f, g פולינומים אי זוגיים.

1. $\deg\left(S_3(f)\right) \le \deg(f)$
2. לכל $k \ge 0$ מתקיים $S_3^k(f) = \left((x+1)^k f\right)|_{\le m}$ כאשר $m = \deg\left(S_3^k(f)\right)$
3. אם $g = f|_{\le n}$ אז $t_{\min}(g, S_3) \le t_{\min}(f, S_3)$

הוכחה. נוכיח את הסעיפים:

1. נשים לב שS_2 מקטין את המעלה של כל פולינום שונה מ0 ולכן:

$$\begin{aligned} \deg\left(S_3(f)\right) &= \deg\left(S_2\left(S_1(f)\right)\right) < \deg\left(S_1(f)\right) \\ &= \deg\left((x+1) f\right) = \deg(f) + 1 \end{aligned}$$

2. נוכיח את הטענה באינדוקציה על k. המקרה של $k = 0$ ברור, נניח כעת שהטענה נכונה עבור k ונוכיח עבור $k+1$. נסמן $h_1 = S_3^k(f)$ וכן $h_2 = S_3^{k+1}(f) = S_3(h_1)$. נסמן גם $d_1 = \deg(h_1)$ ו$d_2 = \deg(h_2)$ לפי 2.10:

$$h_1 \equiv (x+1)^k f \mod \left(x^{d_1+1}\right)$$

נכפול את שני האגפים ב$(x+1)$ ונקבל:

$$(x+1) h_1 \equiv (x+1)^{k+1} f \mod \left(x^{d_1+1}\right)$$

שוב לפי 2.10, $\left((x+1)^{k+1}f\right)|_{\le d_1} = ((x+1)h_1)|_{\le d_1}$. מחלק 1 של טענה זו $d_2 \le d_1$ ולכן מתקיים $\left((x+1)^{k+1}f\right)|_{\le d_2} = ((x+1)h_1)|_{\le d_2}$ אבל $((x+1)h_1)|_{\le d_2} = S_3(h_1)$ ולכן מתקיים $\left((x+1)^{k+1}f\right)|_{\le d_2} = S_3(h_1) = h_2$ כנדרש.

3. נסמן לכל $k \ge 0$, $f_k = S_3^k(f)$ וכן $g_k = S_3^k(g)$. נוכיח באינדוקציה שלכל $k \ge 0$ מתקיים כי $\deg(g_k) \le \deg(f_k)$ וכן $f_k \equiv g_k \mod x^{1+\deg(g_k)}$. המקרה $k=0$ ברור. נניח שהטענה נכונה עבור k ונכפול את שני אגפי השקילות ב$(x+1)$ כך שנקבל:

$$(x+1)f_k \equiv (x+1)g_k \mod x^{1+\deg(g_k)}$$

כמו כן מ$\deg(g_k) \le \deg(f_k)$ נקבל:

$$x^{1+\deg(g_k)} \equiv x^{1+\deg(f_k)} \mod x^{1+\deg(g_k)}$$

מכאן נקבל על ידי סכימה של השקילויות:

$$\begin{aligned} f_{k+1} &= (x+1)f_k + x^{\deg((x+1)f_k)} = (x+1)f_k + x^{1+\deg(f_k)} \\ &\equiv (x+1)g_k + x^{1+\deg(g_k)} = g_{k+1} \mod x^{1+\deg(g_k)} \end{aligned}$$

ומכיוון ש$\deg(g_k) \ge \deg(g_{k+1})$ מתקיים גם:

$$f_{k+1} \equiv g_{k+1} \mod x^{1+\deg(g_{k+1})}$$

וזה גורר לפי 2.10 כי $f_{k+1}|_{\le \deg(g_{k+1})} = g_{k+1}|_{\le \deg(g_{k+1})} = g_{k+1}$ ולכן $\deg(g_{k+1}) \le \deg(f_{k+1})$. בכך השלמנו את צעד האינדוקציה. כדי לקבל את טענת חלק 3 נסמן $k_0 = t_{\min}(f, S_3)$ אז $f_{k_0} = 1$ ומ$\deg(g_{k_0}) \le \deg(f_{k_0})$ מתחייב כי גם $g_{k_0} = 1$ ולכן $t_{\min}(g, S_3) \le k_0$.

□

למה 2.14. יהי $f = (x+1)^r g$ כאשר g אי זוגי (ולכן f גם אי זוגי) אז:

$$t_{\min}(f, S_3) \le 2\deg(f) - r + t_{\min}(g, S_3)$$

הוכחה. יהי s שלם כך שמתקיים $2^{s-1} \le \deg(f) < 2^s$. יהי $k = 2^s - r$ וכן $d = \deg\left(S_3^k(f)\right)$. לפי חלק 2 של 2.13:

$$\begin{aligned} S_3^k(f) &= \left((x+1)^k f\right)|_{\le d} = \left((x+1)^{2^s} g\right)|_{\le d} \\ &= \left(\left(x^{2^s}+1\right)g\right)|_{\le d} = \left(x^{2^s}g + g\right)|_{\le d} \end{aligned}$$

השתמשנו גם בשוויון $(x+1)^{2^s} = x^{2^s}+1$ שניתן לוודא את נכונותו בקלות באינדוקציה. לבסוף נבחין כי $\deg\left(x^{2^s}g\right) \ge 2^s > d$ ולכן $S_3^k(f) = g|_{\le d}$. כעת נשתמש בחלק 3 של 2.13 ונקבל:

$$\begin{aligned} t_{\min}(f, S_3) &\le k + t_{\min}(g|_{\le d}, S_3) \le k + t_{\min}(g, S_3) \\ &= 2^s - r + t_{\min}(g, S_3) \\ &\le 2\deg(f) - r + t_{\min}(g, S_3) \end{aligned}$$

□

משפט 2.15. יהי f פולינום אי זוגי, אז $t_{\min}(f,S_3) \le \sqrt{2}(\deg(f))^{1.5}$

הוכחה. נסמן $n=\deg(f)$ ונוכיח את הטענה באינדוקציה על n. אם $n=0$ אז $f=1$ ו$t_{\min}(1,S_3)=0$ לכן הטענה מתקיימת.

נניח שהטענה נכונה לפולינומים ממעלה קטנה מn ונוכיח שהיא נכונה לפולינומים ממעלה n. נרשום $f(x)=x^n+g(x)$ כאשר $\deg(g)=n-r$ עבור $r>0$. לפי 2.12 מתקיים:

$$t_{\min}(f,S_3) \quad = \quad r-1+t_{\min}\left((x+1)^{r-1}g,S_3\right)$$

נבחין בין שני מקרים אפשריים:

1. $r \le \sqrt{2n}$. נשתמש בהנחת האינדוקציה על הפולינום $(x+1)^{r-1}g$ שמעלתו $n-1$ ונקבל:

$$\begin{aligned}t_{\min}(f,S_3) &= r-1+\sqrt{2}(n-1)^{1.5} < \sqrt{2n}+(n-1)\sqrt{2n}\\ &= n\sqrt{2n}=\sqrt{2}n^{1.5}\end{aligned}$$

2. $r > \sqrt{2n}$. לפי 2.14:

$$\begin{aligned}t_{\min}(f,S_3) &= r-1+t_{\min}\left((x+1)^{r-1}g,S_3\right)\\ &\le r-1+2(n-1)-(r-1)+t_{\min}(g,S_3)\\ &< 2n+t_{\min}(g,S_3)\end{aligned}$$

$\deg(g)=n-r$ ולכן מהנחת האינדוקציה $t_{\min}(g,S_3) \le \sqrt{2}(n-r)^{1.5}$ נשתמש בחסם זה כדי להמשיך ולחסום את $t_{\min}(f,S_3)$:

$$\begin{aligned}t_{\min}(f,S_3) &< 2n+\sqrt{2}(n-r)^{1.5} \le 2n+(n-r)\sqrt{2n}\\ &< 2n+\left(n-\sqrt{2n}\right)\sqrt{2n}=n\sqrt{2n}=\sqrt{2}n^{1.5}\end{aligned}$$

בכך השלמנו את צעד האינדוקציה. □

כעת לא נותר אלא לשלב את התוצאות שקיבלנו על מנת להגיע לחסום המשופר על זמן העצירה של T.

משפט 2.16. יהי $0 \ne f \in \mathbb{F}_2[x]$ אז $t_{\min}(f,T) \le (2\deg(f))^{1.5}+\deg(f)$

הוכחה. נרשום $f=x^r g$ כאשר g אי זוגי. אז $t_{\min}(f,T)=r+t_{\min}(g,T)$. לפי 2.9 מתקיים:

$$t_{\min}(g,T) \quad = \quad 2t_{\min}(\hat{g},S_3)+\deg(g)$$

נשים לב $\deg(\hat{g})=\deg(g)=n-r$ ולכן לפי 2.15:

$$t_{\min}(g,T) \quad \le \quad 2\sqrt{2}(n-r)^{1.5}+(n-r)=(2(n-r))^{1.5}+n-r$$

לכן:

$$\begin{aligned}t_{\min}(f,T) &= r+t_{\min}(g,T) \le r+(2(n-r))^{1.5}+n-r\\ &= (2(n-r))^{1.5}+n < (2n)^{1.5}+n\end{aligned}$$

כנדרש. □

2.3 קיום סדרות חשבוניות בזמני העצירה של T

נגדיר כעת במדויק את מושג "קיום תתי סדרות חשבוניות שאורכן לא חסום" מה התוצאה שנרצה להוכיח.

הגדרה 2.17. תהי $(a_n)_{n\geq 0}$ סדרה ויהי $r \geq 0$. נאמר ש$(a_n)_{n\geq 0}$ מכילה סדרות חשבוניות באורך לא חסום ובעלות הפרש משותף r אם לכל $m \geq 1$ קיים $l \geq 0$ כך ש:

$$\begin{aligned} a_{l+1} &= a_l + r \\ a_{l+2} &= a_l + 2r \\ &\ldots \\ a_{l+(m-2)} &= a_l + (m-2)\,r \\ a_{l+(m-1)} &= a_l + (m-1)\,r \end{aligned}$$

כלומר התת סדרה $(a_{l+k})_{k=0}^{m-1}$ היא סדרה חשבונית עם הפרש r.

משפט 2.18. יהיו a, b מספרים שלמים אי שליליים כך ש$(a,b) \neq (0,0)$. נסמן

$$f_{a,b,n} = \left(x^a\,(1+x)^b\right)^n + 1$$

הסדרה $(t_{\min}\,(f_{a,b,n})\,, T)_{n\geq 1}$ מכילה סדרות חשבוניות באורך לא חסום ובעלות הפרש משותף $a - b$.

בחלק זה נוכיח את המשפט הנ"ל על ידי חישוב מפורש של $t_{\min}\,(f_{a,b,n}, T)$. גם כאן ניעזר במיפוי S_3 (הגדרה 2.7) ובמיפוי $f \mapsto \hat{f}$ של היפוך סדר המקדמים (הגדרה 2.5)

למה 2.19. לכל a, b שלמים אי שליליים כך ש$(a,b) \neq (0,0)$ ו$n \geq 1$. מתקיים פרט למקרה $(a,b,n) = (0,1,1)$:

$$t_{\min}\,(f_{a,b,n}, T) \quad = \quad 2t_{\min}\left((x+1)^{na+nb-1}, S_3\right) + 3na + nb - 2$$

הוכחה. לפי 2.9:

$$t_{\min}\,(f_{a,b,n}, T) \quad = \quad 2t_{\min}\left(\widehat{f_{a,b,n}}, S_3\right) + n\,(a+b) \tag{6}$$

נחשב את $\widehat{f_{a,b,n}}$ לפי הגדרה 2.5:

$$\begin{aligned} \widehat{f_{a,b,n}} &= x^{\deg(f_{a,b,n})} f_{a,b,n}\left(\frac{1}{x}\right) = x^{n(a+b)}\left(\left(\left(\frac{1}{x}\right)^a \left(1 - \frac{1}{x}\right)^b\right)^n + 1\right) \\ &= (x+1)^{nb} + x^{na+nb} \end{aligned}$$

נפריד מכאן למקרים $a = 0$ ו$a > 0$. אם $a = 0$ אז $\widehat{f_{a,b,n}}$ מתקבל מ$(x+1)^{nb-1}$ על ידי הפעלה של S_3. הנחנו $(a,b,n) \neq (0,1,1)$ ולכן $nb - 1 > 0$ ו$(x+1)^{nb-1} \neq 1$ ומכאן ש:

$$t_{\min}\left(\widehat{f_{a,b,n}}, S_3\right) \quad = \quad t_{\min}\left((x+1)^{nb-1}, S_3\right) - 1$$

הצבה של השוויון הנ"ל ב6 מניבה את השוויון הדרוש.
אם $a > 0$ אז תנאי 2.12 מתקיימים עבור $\widehat{f_{a,b,n}}$ שכן:

$$\deg\left(x^{na+nb} + (x+1)^{nb}\right) > \deg\left((x+1)^{nb}\right)$$

ולכן:

$$\begin{aligned} t_{\min}\left(\widehat{f_{a,b,n}}, S_3\right) &= (na + nb - nb) - 1 + t_{\min}\left((x+1)^{na+nb-1}, S_3\right) \\ &= na - 1 + t_{\min}\left((x+1)^{na+nb-1}, S_3\right) \end{aligned}$$

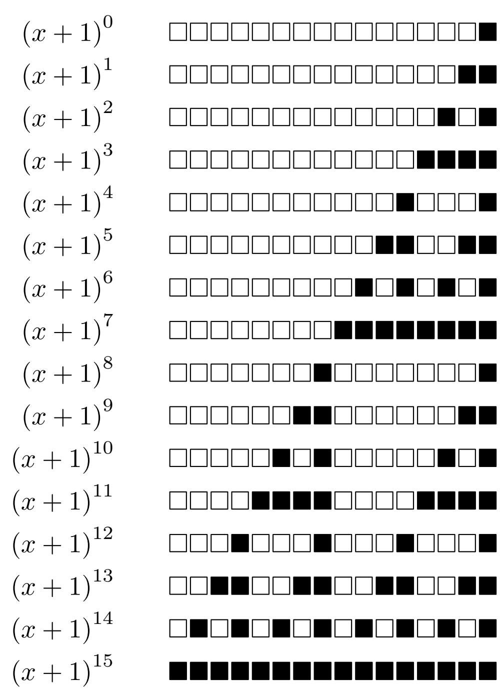
ושוב הצבה ב6 מניבה את השוויון הדרוש. $\square$

מהלמה האחרונה נובע שכדי לחשב את $t_{\min}\left(f_{a,b,n}, T\right)$ מספיק לחשב את $t_{\min}\left((x+1)^n, S_3\right)$ עבור $n \geq 1$.

למה 2.20. יהי $n \geq 1$ ונניח $2^{d-1} \leq n < 2^d$. אז:

$$t_{\min}\left((x+1)^n, S_3\right) = 2^d - n$$

בטרם נוכיח את הלמה, נתבונן בהמחשה של הפולינומים הללו:



קיבלנו את משולש שרפינסקי והסיבה לכך היא כזו - מצד אחד, את משולש שרפינסקי ניתן לבנות רקורסיבית בעזרת 3 עותקים של גרסה קטנה יותר שלו. מצד שני, את חישוב המקדמים

של הפולינומים $(x+1)^n$ עבור $n\in\left[0,2^{d+1}-1\right]$ ניתן גם לבצע רקורסיבית. נפריד לשני מקרים אפשריים של n והם: $n\in\left[0,2^d-1\right]$ ו-$n\in\left[2^d,2^{d+1}-1\right]$. הפולינומים בקבוצה השנייה מתקבלים מאלו בקבוצה הראשונה על ידי כפל ב $(x+1)^{2^d}$ בהתאמה כשהם מסודרים בסדר עולה של המעלות. מתקיים:

$$(x+1)^{2^d} = x^{2^d}+1$$

ולכן כפל של פולינום f בפולינום $(x+1)^{2^d}$ יוצר שני עותקים של f שאחד מהם מוזז ב2^d מקומות שמאלה. אם כך, הקבוצה $\left\{(x+1)^n : n\in\left[0,2^d-1\right]\right\}$ תורמת משולש אחד מסדר d, והקבוצה $\left\{(x+1)^n : n\in\left[2^d,2^{d+1}-1\right]\right\}$ תורמת שני משולשים מסדר d, זה לצד זה. נדגים: את הפולינומים $(x+1)^n$ עבור $n\in[0,7]$ ניתן לחלק לקבוצות $(x+1)^0,...,(x+1)^3$ ו$(x+1)^4,...,(x+1)^7$.

$$\begin{aligned}
(x+1)^4 &= (x+1)^4(x+1)^0=\left(x^4+1\right)(x+1)^0\\
(x+1)^5 &= (x+1)^4(x+1)^1=\left(x^4+1\right)(x+1)^1\\
(x+1)^6 &= (x+1)^4(x+1)^2=\left(x^4+1\right)(x+1)^2\\
(x+1)^7 &= (x+1)^4(x+1)^3=\left(x^4+1\right)(x+1)^3
\end{aligned}$$

ואז ניתן לקבל את המקדמים של ארבעת הפולינומים האחרונים על ידי שני עותקים של המקדמים של ארבעת הפולינומים הראשונים שאחד מהעותקים מוזז ארבע מקומות שמאלה.

להרחבה בנושא מומלץ מאוד לצפות בסרטון היוטיוב הזה [8] ובחלק השני שלו [9].

הוכחה. נוכיח ראשית כי $t_{\min}\left((x+1)^n,S_3\right)\le 2^d-n$. נסמן $m=\deg\left(S_3^{2^d-n}\left((x+1)^n\right)\right)$. לפי חלק 2 של 2.13:

$$S_3^{2^d-n}\left((x+1)^n\right) = \left((x+1)^{2^d}\right)|_{\le m}=\left(x^{2^d}+1\right)|_{\le m}$$

אבל לפי חלק 1 של אותה הלמה:

$$m\le\left(\deg(x+1)^n\right)=n<2^d$$

ולכן בהכרח $S_3^{2^d-n}\left((x+1)^n\right)=1$.

בשביל להוכיח את האי שוויון ההפוך, נשים לב לתכונה הבאה של S_3. אם פולינום f מכיל את החזקות x^{k_1},x^{k_2} כך ש $k_2-k_1>1$ ולא מכיל אף חזקה ביניהן, הפולינום $S_3(f)$ יכיל את החזקות x^{k_1+1},x^{k_2} ולא יכיל אף חזקה ביניהן. נוכיח:

$$S_3(f) = xf+f+x^{\deg(f)+1}$$

החזקות x^{k_1+1},x^{k_2} מופיעות בדיוק במחובר אחד מהשלושה.

x^{k_1+1}: מופיע בxf, לא מופיע בf ולא מופיע ב$x^{\deg(f)+1}$ כי $\deg(f)+1\ge k_2+1>k_1+1$.

x^{k_2}: מופיע בf, לא מופיע בxf (אילו היה מופיע, אז בf הייתה החזקה x^{k_2-1}) ולא מופיע ב$x^{\deg(f)+1}$ כי $\deg(f)+1>k_2$.

והחזקות x^i עבור $k_1+1<i<k_2$ לא מופיעות באף אחד מהמחוברים. אם כך הפולינומים $S_3^j(f)$ עבור $0\le j\le k_2-k_1-1$ לובשים את הצורה:

$$\begin{array}{rl} f & ...+x^{k_1}+x^{k_2}+... \\ S_3(f) & ...+x^{k_1+1}+x^{k_2}+... \\ & \vdots \\ S_3^{(k_2-k_1-2)}(f) & ...+x^{k_1+(k_2-k_1-2)}+x^{k_2}+... \\ S_3^{(k_2-k_1-1)}(f) & ...+x^{k_1+(k_2-k_1-1)}+x^{k_2}+... \end{array}$$

הם שונים כולם מ1 ולכן $t_{\min}(f,S_3)\ge k_2-k_1$. כדי לסיים נוכיח כי החזקות $x^{2^{d-1}},x^{n-2^{d-1}}$ מופיעות ב$(x+1)^n$, והחזקות שביניהן לא ונקבל:

$$t_{\min}\left((x+1)^n,S_3\right) \quad \ge \quad 2^{d-1}-\left(n-2^{d-1}\right)=2^d-n$$

נרשום:

$$\begin{aligned} (x+1)^n &= (x+1)^{2^{d-1}}(x+1)^{n-2^{d-1}}=\left(x^{2^{d-1}}+1\right)(x+1)^{n-2^{d-1}} \\ &= x^{2^{d-1}}(x+1)^{n-2^{d-1}}+(x+1)^{n-2^{d-1}} \\ &= x^{2^{d-1}}\left(x^{n-2^{d-1}}+...+1\right)+x^{n-2^{d-1}}+...+1 \\ &= x^n+...+x^{2^{d-1}}+x^{n-2^{d-1}}+...+1 \end{aligned}$$

ובכך נקבל את הנדרש. $\square$

נשים לב שהפולינום $(x+1)^n$ עבור $2^{d-1}\le n<2^d$ הוא ב2^{d-1} השורות התחתונות של משולש שרפינסקי שיוצרים הפולינומים $(x+1)^n$ עבור $n\in\left[0,2^d-1\right]$. אם כך הוא מורכב מהפולינום $(x+1)^{n-2^{d-1}}$ ומעותק שלו המוזז 2^{d-1} מקומות שמאלה.

החזקה $x^{n-2^{d-1}}$ היא הגבוהה ביותר בעותק הרגיל של $(x+1)^{n-2^{d-1}}$ והחזקה $x^{2^{d-1}}$ היא הנמוכה ביותר בעותק המוזז שמאלה של $(x+1)^{n-2^{d-1}}$ כלומר הן מהוות את ההפרדה בין שני העותקים של $(x+1)^{n-2^{d-1}}$.

מסקנה 2.21. לכל a,b שלמים אי שליליים כך ש$(a,b)\ne(0,0)$ ו$n\ge1$. מתקיים פרט למקרה $(a,b,n)=(0,1,1)$:

$$t_{\min}\left(f_{a,b,n},T\right) \quad = \quad 2^{d+1}+(a-b)\,n$$

כאשר d שלם המקיים $2^{d-1}<n\,(a+b)\le2^d$

הוכחה. האי שוויון של מספרים שלמים $2^{d-1}<n\,(a+b)\le2^d$ שקול ל:

$$2^{d-1}\le n\,(a+b)-1<2^d$$

לפי 2.20:

$$t_{\min}\left((x+1)^{na+nb-1},S_3\right) \quad = \quad 2^d-n\,(a+b)+1$$

נציב בשוויון שהוכחנו ב2.19 ונקבל:

$$\begin{aligned} t_{\min}\left(f_{a,b,n},T\right) &= 2t_{\min}\left(\left(x+1\right)^{na+nb-1},S_{3}\right)+3na+nb-2 \\ &= 2\left(2^{d}-n\left(a+b\right)+1\right)+3na+nb-2 \\ &= 2^{d+1}+na-nb \end{aligned}$$

□

כעת נשתמש בחישובים שערכנו כדי להוכיח את 2.18.

הוכחה. יהי $n\geq 2$, אז בהכרח $(a,b,n)\neq(0,1,1)$. נניח גם שn מקיים:

$$2^{d-1}<n\left(a+b\right)\leq 2^{d}$$

מצאנו ב2.21 שבתנאים אלו מתקיים:

$$t_{\min}\left(f_{a,b,n},T\right) = 2^{d+1}+\left(a-b\right)n$$

המספרים n המקיימים את התנאים האלו מהווים **רצף** של אינדקסים בסדרה $\left(t_{\min}\left(f_{a,b,n},T\right)\right)_{n\geq 1}$, ליתר דיוק:

$$n \in \left\{\left\lceil\frac{2^{d-1}}{a+b}\right\rceil,\left\lceil\frac{2^{d-1}}{a+b}\right\rceil+1,...,\left\lfloor\frac{2^{d}}{a+b}\right\rfloor\right\}\setminus\{1\}$$

נסמן את קבוצת האינדקסים הזו בA אז:

$$\left(t_{\min}\left(f_{a,b,n},T\right)\right)|_{n\in A} = 2^{d+1}+\left(a-b\right)n$$

כלומר זו תת סדרה חשבונית עם הפרש $(a-b)$. לסיום נשים לב שניתן לבחור את d גדול כרצוננו כדי שכמות האיברים בA שמהווה את אורך התת סדרה המבוקשת תהיה גדולה כרצוננו. □

3 שאלות פתוחות

מקורות

[1] Lagarias, J. C. (1985). The 3x + 1 Problem and Its Generalizations. The American Mathematical Monthly, 92(1), 3–23. https://doi.org/10.2307/2322189

[2] Hicks, K., Mullen, G. L., Yucas, J. L., & Zavislak, R. (2008). A Polynomial Analogue of the 3n + 1 Problem. The American Mathematical Monthly, 115(7), 615–622. http://www.jstor.org/stable/27642557

[3] Alon, G., Behajaina, A., & Paran, E. (2024). On the stopping time of the Collatz map in $\mathbb{F}_2\left[x\right]$. arXiv:2401.03210. https://doi.org/10.48550/arXiv.2401.03210

[4] Tao, T. (2022), Almost all orbits of the Collatz map attain almost bounded values. Forum of Mathematics Pi 10 (e12), 1-56.

[5] Yuzuriha Inori (https://mathoverflow.net/users/124627/yuzuriha-inori), Arithmetic progressions in stopping time of Collatz sequences, URL (version: 2019-12-20): https://mathoverflow.net/q/348733

[6] אורנשטיין, א'. (1995). **מבנים אלגבריים**. האוניברסיטה הפתוחה.

[7] קורמן, ת.ה., לייזרסון, צ.א., ריבסט ר.ל., ושטיין, ק'. (2008). **מבוא לאלגוריתמים** (סופר, ע', מתרגם). (מהדורה שנייה). האוניברסיטה הפתוחה. (פרסום ראשון במקור 2001)

[8] 3Blue1Brown. (2016, November 25). Binary, Hanoi, and Sierpinski, part 1 [Video]. Youtube. https://youtu.be/2SUvWfNJSsM?si=J9WZq9LZ1w7XW_Uy

[9] 3Blue1Brown. (2016, November 25). Binary, Hanoi, and Sierpinski, part 2 [Video]. Youtube. https://youtu.be/bdMfjfT0lKk?si=kbgMDUl3iEDpTNtS