

סמינר בנושא אנלוג להשערת קולץ בפולינומים

28 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 $\mathbb{F}_2[x]$, 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 $\mathcal{C} : \mathbb{N} \rightarrow \mathbb{N}$ באופן הבא:

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

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 $\mathcal{C}^k(n) = 1$.

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

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

מצאנו כי $\mathcal{C}^{14}(11) = 1$.

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 $\mathbb{F}_2[x]$

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

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

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

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

$$T^6(x^2 + 1) = 1$$

מהשוואה בין T לבין 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 C לפנות.

בהמשך להשוואה זו, לפולינום $f \in \mathbb{F}_2[x]$ המתחלק ב- x , כלומר מקיים $f \equiv 0 \pmod{x}$ 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 ב- f) 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 $M: \mathbb{F}_2[x] \rightarrow \mathbb{F}_2[x]$ ולכל $f \in \mathbb{F}_2[x]$ נגדיר:

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

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

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

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

$$t_{\min}(f, T) = O(\deg(f)^2)$$

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

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

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

לסיום, נוכיח תוצאה נוספת שמהווה אנלוג להשערה בנוגע לזמני העצירה של מספרים העונים לתבנית מסוימת, ביחס למיפוי 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 $(2^a 3^b)^n + 1$ 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 $(x^a(1+x)^b)^n + 1$, 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 מהפעולות חוזרות של T , נאמץ את הסימון
 הבא של פולינום כקטור בינארי:

$$x^7 + x^5 + 1 \quad \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare$$

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

0	<table><tr><td>□</td><td>■</td><td>■</td><td>□</td><td>□</td><td>□</td><td>□</td><td>■</td></tr></table>	□	■	■	□	□	□	□	■
□	■	■	□	□	□	□	■		
1	<table><tr><td>■</td><td>■</td><td>■</td><td>■</td><td>□</td><td>□</td><td>□</td><td>□</td></tr></table>	■	■	■	■	□	□	□	□
■	■	■	■	□	□	□	□		
2	<table><tr><td>□</td><td>■</td><td>■</td><td>■</td><td>■</td><td>□</td><td>□</td><td>■</td></tr></table>	□	■	■	■	■	□	□	■
□	■	■	■	■	□	□	■		
3	<table><tr><td>■</td><td>□</td><td>□</td><td>□</td><td>■</td><td>□</td><td>□</td><td>□</td></tr></table>	■	□	□	□	■	□	□	□
■	□	□	□	■	□	□	□		
4	<table><tr><td>□</td><td>■</td><td>□</td><td>□</td><td>□</td><td>■</td><td>□</td><td>■</td></tr></table>	□	■	□	□	□	■	□	■
□	■	□	□	□	■	□	■		
5	<table><tr><td>■</td><td>■</td><td>□</td><td>□</td><td>■</td><td>■</td><td>□</td><td>□</td></tr></table>	■	■	□	□	■	■	□	□
■	■	□	□	■	■	□	□		
6	<table><tr><td>□</td><td>■</td><td>■</td><td>□</td><td>□</td><td>■</td><td>■</td><td>□</td></tr></table>	□	■	■	□	□	■	■	□
□	■	■	□	□	■	■	□		
7	<table><tr><td>■</td><td>□</td><td>■</td><td>□</td><td>■</td><td>□</td><td>■</td><td>□</td></tr></table>	■	□	■	□	■	□	■	□
■	□	■	□	■	□	■	□		
8	<table><tr><td>□</td><td>■</td><td>□</td><td>□</td><td>□</td><td>■</td><td>□</td><td>■</td></tr></table>	□	■	□	□	□	■	□	■
□	■	□	□	□	■	□	■		
9	<table><tr><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>□</td></tr></table>	■	■	■	■	■	■	■	□
■	■	■	■	■	■	■	□		
10	<table><tr><td>□</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>□</td></tr></table>	□	■	■	■	■	■	■	□
□	■	■	■	■	■	■	□		
11	<table><tr><td>□</td><td>□</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td><td>■</td></tr></table>	□	□	■	■	■	■	■	■
□	□	■	■	■	■	■	■		

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

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

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

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

במקרה זה $m = 1$ מקיים את הטענה.

אם f אי זוגי, נרשום:

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

כאשר $1 \leq r \leq d$ 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 ב f פרט ל 1. נוכיח באינדוקציה כי לכל $1 \leq j \leq r$ מתקיים:

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

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 $1 \leq j < r$ ונוכיח שהיא נכונה עבור $j+1$. מהנחת האינדוקציה:

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

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

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

ובכך הוכחנו את צעד האינדוקציה. נקבל בפרט עבור $j = r$:

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

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

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

ומתקיים:

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

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

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

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

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

$$1 \leq m \leq 2d + 1$$

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

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

ומכאן

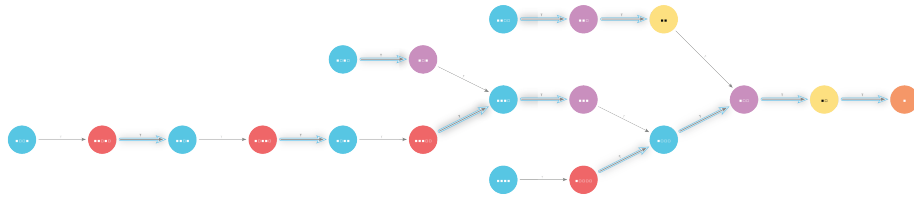
$$\begin{aligned} t_{\min}(f, T) &\leq t_{\min}(T^m(f), T) + m \\ &\leq (d-1)^2 + 2(d-1) + m \\ &\leq (d-1)^2 + 2(d-1) + 2d + 1 = d^2 + 2d \end{aligned}$$

□

כנדרש.

2.2 חסם משופר לזמן העצירה

כפי שצינו במבוא, קיבלנו חסם אסימפטוטי ריבועי ל- $t_{\min}(f, T)$ כתלות ב- $\deg f$. בחלק זה נשפר את החסם ונוכיח $t_{\min}(f, T) = O((\deg f)^{1.5})$. נתבונן במסלול שעושים פולינומים ממעלה עד 3 עד שהם מגיעים ל-1:



חץ מודגש מתאים לצעדים מסוג $f \mapsto \frac{f}{x}$ וחץ רגיל לצעדים מסוג $f \mapsto (x+1)f + 1$. נשים לב שכל פולינום זוגי מגיע לפולינום אי זוגי לאחר רצף של חלוקות ב- x , ואם כך נוכל להוכיח חסם לפולינומים אי זוגיים בלבד ולאחר מכן להסיק ממנו חסם לכל פולינום שונה מ-0 בעזרת הקשר הבא:

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

כאשר r החזקה הגבוהה ביותר של x המחלקת את f . פולינום אי זוגי עובר על ידי הצעד $f \mapsto (x+1)f + 1$ 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 $(T^n(f))_{n \geq 0}$. נתבונן בגרף הבא להמחשה (מומלץ להגדיל את המסמך בכדי לקרוא בבירור את התוויות):

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:

$$(x+1)^r xg + x = x[(x+1)^r g + 1]$$

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

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

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

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

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

$$\begin{aligned} f &\xrightarrow{T^{2(r-1)}} (x+1)^{r-1} xg + 1 \xrightarrow{T} (x+1)^r xg + x \xrightarrow{T^s} \frac{(x+1)^r xg + x}{x^s} \\ f &\xrightarrow{T_3^{r-1}} (x+1)^{r-1} xg + 1 \xrightarrow{T_3} \frac{(x+1)^r xg + x}{x^s} \end{aligned} \quad (2)$$

2.1ב הוכחנו כי מתקיים כי לכל $1 \leq j \leq r$:

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

בפרט עבור $j = r-1$:

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

כאשר מפעילים את T קורית אחת מהפעולות:

$$(1) \quad f \mapsto (x+1)f + 1$$

$$(2) \quad f \mapsto \frac{f}{x}$$

נשים לב כי מההוכחה 2.1ב 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:

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

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:

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

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.

2.2.2 הפולינום ההדדי ומיפויים מקבילים

ברצוננו להמשיך ולחקור את הסדרה $(T_3^n(f))_{n \geq 0}$ עבור f אי זוגי. בחלק זה נגדיר את המיפוי S_3 שאת תפקידו תיארנו במבוא 2.2.

הפולינום המתקבל מפולינום נתון בעזרת היפוך סדר המקדמים נקרא הפולינום ההדדי שלו. בחלק זה נציג תכונות בסיסיות של הפולינום ההדדי. לאחר מכן נוכיח סדרת למות שמהן ינבע כי עבור פולינומים אי זוגיים מתקיים $t_{\min}(f, S_3) = O((\deg f)^{1.5})$. לבסוף נשלב את התוצאות הקודמות כדי להוכיח שמתקיים $t_{\min}(f, T) = O((\deg f)^{1.5})$ עבור $f \neq 0$.

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

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

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

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

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

1. $\deg f = m$ ולכן:

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

2. נוכיח על פי ההגדרה:

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

3. על פי חלק 2:

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

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:

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

על ידי החלפת אינדקס נקבל:

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

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

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

ועל ידי החלפת אינדקס נוספת נקבל:

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

כעת ניעזר בחלק 3 ונקבל:

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

□

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

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

$$S_3(f) = (S_2 \circ S_1)(f)$$

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

$$1. \widehat{T_3(f)} = S_3(\widehat{f})$$

$$2. t_{\min}(f, T_3) = t_{\min}(\widehat{f}, S_3)$$

הוכחה.

1. $\widehat{T_3(f)} = T_2(\widehat{T_1(f)})$ תהי r החזקה המקסימלית של x המחלקת את $T_1(f)$. אז $T_1(f) = x^r T_2(T_1(f))$ לפי סעיף 3 של 2.6 מתקיים:

$$\widehat{T_1(f)} = x^r \widehat{T_2(T_1(f))} = T_2(\widehat{T_1(f)})$$

עבור g אי זוגי, הפעולה $g \mapsto \widehat{g+1}$ מאפסת את המקדם התחתון (שהוא 1) והופכת את סדר המקדמים ולכן שקולה לפעולה $g \mapsto S_2(\widehat{g})$ שהופכת את סדר המקדמים ואז מאפסת את המקדם העליון. נשתמש בתכונה זו עבור $g = (x+1)f$:

$$\widehat{T_1(f)} = \underbrace{(x+1)f}_g + 1 = S_2(\widehat{(x+1)f})$$

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:

$$f, T_3(f), T_3^2(f), \dots, T_3^n(f) = 1$$

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

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

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 $\widehat{T_3^m(f)} = \hat{1}$ היינו יכולים להפעיל את מיפוי היפוך המקדמים שוב ולקבל $T_3^m(f) = 1$ כלומר לפי סעיף 4 של 2.6 לקבל $T_3^m(f) = 1$ וזו סתירה. מצאנו אם כך שיש להפעיל n פעמים את S_3 על \hat{f} כדי להגיע ל 1 בפעם הראשונה ולכן $t_{\min}(\hat{f}, S_3) = n$ 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 פולינום שאינו 0. אז מתקיים:

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

הוכחה. נרשום:

$$f = x^r g$$

כאשר g אי זוגי. אז:

$$t_{\min}(f, T) = r + t_{\min}(g, T)$$

עבור g מתקיים לפי 2.4:

$$t_{\min}(g, T) = 2t_{\min}(g, T_3) + \deg(g)$$

ולפי סעיף 2 של 2.8:

$$t_{\min}(g, T_3) = t_{\min}(\hat{g}, S_3)$$

נשלב את השוויונות ונקבל:

$$\begin{aligned} t_{\min}(f, T) &= r + t_{\min}(g, T) = r + 2t_{\min}(g, T_3) + \deg(g) \\ &= r + 2t_{\min}(\hat{g}, S_3) + \deg g = 2t_{\min}(\hat{g}, S_3) + \deg(f) \end{aligned}$$

□ כדי לקבל את הנדרש נזכור כי לפי סעיף 3 של 2.6 מתקיים כי $\hat{f} = \hat{g}$.

בהינתן פולינום $f(x) = \sum a_i x^i$ נשתמש בסימון $f|_{\leq n}$ עבור הפולינום $\sum_{i \leq n} a_i x^i$. כלומר זהו הפולינום המתקבל מ- f על ידי השמטת חזקות גבוהות מ- n .

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

הוכחה. נסמן $f(x) = \sum a_i x^i$ וכן $g(x) = \sum b_i x^i$. $f \equiv g \pmod{x^n}$ אם ורק אם $x^n | (f - g)$ וזה שקול לכך שלכל $0 \leq i < n$ מתקיים $a_i - b_i = 0$ כלומר מקדמי החזקות $f|_{\leq n-1} = g|_{\leq n-1}$ 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 $0 \leq i \leq n - \deg(g)$ מתקיים $S_3^i(f) = x^n + (x+1)^i g = ((x+1)f)|_{\leq n}$

הוכחה. יהי $r = n - \deg(f)$. נוכיח באינדוקציה על i כי לכל $0 \leq i \leq r$ 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 $\deg((x+1)^i g) < n$ ולכן $\deg(S_3^i(f)) = n$. נחשב את $S_1(S_3^i(f))$:

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

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

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

נסביר את המעבר האחרון - $\deg((x+1)^{i+1} g) \leq n$ ולכן:

$$\deg(x^{n+1} + x^n + (x+1)^{i+1} g) = n+1$$

בכך הוכחנו את צעד האינדוקציה.

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

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

מתקיים $x^n \equiv (x+1)^i x^n \pmod{x^n}$ ולכן:

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

אם כך לפי 2.10:

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

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

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

□

וקיבלנו את השוויון השני.

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 $n \geq 2$. נסמן $r = n - \deg(g)$ ונניח $r > 0$. מתקיים $t_{\min}(f, S_3) = r - 1 + t_{\min}((x+1)^{r-1} g, S_3)$

הוכחה. לפי השוויון הראשון של 2.11:

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

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

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

נשים לב כי מהוכחת 2.11 נובע כי לכל $0 \leq i \leq r-1$ מתקיים $\deg(S_3^i(f)) = n$ ולכן בפרט $S_3^i(f) \neq 1$ אם כך:

$$t_{\min}(f, S_3) = r + t_{\min}(S_3^r(f), S_3) \stackrel{4}{=} r + t_{\min}\left(S_3\left((x+1)^{r-1} g\right), S_3\right) \quad (5)$$

אם $(x+1)^{r-1} g \neq 1$ אז:

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

העצה של השוויון הנ"ל 5 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.

$$1. \deg(S_3(f)) \leq \deg(f)$$

$$2. \text{ לכל } k \geq 0 \text{ מתקיים } S_3^k(f) = ((x+1)^k f) |_{\leq m} \text{ כאשר } m = \deg(S_3^k(f))$$

$$3. \text{ אם } g = f |_{\leq n} \text{ אז } t_{\min}(g, S_3) \leq t_{\min}(f, S_3)$$

הוכחה.

1. נשים לב ש- S_2 מקטין את המעלה של כל פולינום שונה מס ולכן:

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

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:

$$h_1 \equiv (x+1)^k f \pmod{x^{d_1+1}}$$

נכפול את שני האגפים ב- $(x+1)$ ונקבל:

$$(x+1)h_1 \equiv (x+1)^{k+1} f \pmod{x^{d_1+1}}$$

שוב לפי 2.10,

$$((x+1)h_1) |_{\leq d_1} = ((x+1)^{k+1} f) |_{\leq d_1}$$

מחלק 1 של טענה זו $d_2 \leq d_1$ ולכן מתקיים בפרט:

$$((x+1)h_1) |_{\leq d_2} = ((x+1)^{k+1} f) |_{\leq d_2}$$

אבל מהגדרת S_3 מתקיים $S_3(h_1) = ((x+1)h_1) |_{\leq d_2}$. נציב זאת בשוויון הקודם ונקבל:

$$h_2 = S_3(h_1) = ((x+1)^{k+1} f) |_{\leq d_2}$$

כנדרש.

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

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

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

$$x^{1+\deg(g_k)} \equiv x^{1+\deg(f_k)} \equiv 0 \pmod{x^{1+\deg(g_k)}}$$

מכאן נקבל על ידי סכימה של השקילויות:

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

לפי סעיף 1 של טענה זו $\deg(g_k) \geq \deg(g_{k+1})$ ולכן מתקיים ב-

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

וזה גורר לפי 2.10 כי:

$$f_{k+1}|_{\leq \deg(g_{k+1})} = g_{k+1}|_{\leq \deg(g_{k+1})} = g_{k+1}$$

ולכן מתקיים גם $\deg(g_{k+1}) \leq \deg(f_{k+1})$. 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 $\deg(g_{k_0}) \leq \deg(f_{k_0})$ מתחייב כי גם $g_{k_0} = 1$ ולכן $t_{\min}(g, S_3) \leq k_0$.

□

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

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

הוכחה. יהי s שלם כך שמתקיים $2^{s-1} \leq \deg(f) < 2^s$. נסמן:

$$\begin{aligned} k &= 2^s - r \\ d &= \deg(S_3^k(f)) \end{aligned}$$

לפי חלק 2 של 2.13:

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

השתמשנו גם בשוויון $(x+1)^{2^s} = x^{2^s} + 1$ שניתן לוודא את נכונותו בקלות באינדוקציה. לבסוף נבחין כי:

$$\deg(x^{2^s}g) \geq 2^s > \deg(f) \geq d$$

ולכן $S_3^k(f) = g|_{\leq d}$. כעת נשתמש בחלק 3 של 2.13 ונקבל:

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

□

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

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 מ- n 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:

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

נבחין בין שני מקרים אפשריים:

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

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

2. $r > \sqrt{2n}$. לפי 2.14:

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

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

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

□

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 $f \in \mathbb{F}_2[x]$ אז $0 \neq f$ אז $t_{\min}(f, T) \leq (2 \deg(f))^{1.5} + \deg(f)$ הוכחה. נרשום $f = x^r g$ כאשר g אי זוגי. אז $t_{\min}(f, T) = r + t_{\min}(g, T)$. לפי 2.9 מתקיים:

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

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

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

לכן:

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

□

כנדרש.

2.3 קיום סדרות חשבוניות בזמני העצירה של T

נגדיר כעת במדויק את מושג "קיום תתי סדרות חשבוניות שאורכן לא חסום" ואת 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:

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

כלומר תת הסדרה $(a_{l+k})_{k=0}^{m-1}$ 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 $\hat{f} \mapsto f$ 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 למקרים $(a, b, n) = (0, 1, 1)$, $(a, b, n) = (1, 0, 1)$:

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

הוכחה. לפי 2.9:

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

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 כעת למקרים $a=0$ ו $a>0$. נתחיל במקרה $a>0$. במקרה זה נסמן $g = (x+1)^{nb}$ ונקבל:

$$\begin{aligned} \widehat{f_{a,b,n}} &= x^{na+nb} + g \\ na+nb &> \deg(g) = nb \\ na+nb &\geq 2 \end{aligned}$$

האי שוויון האחרון נכון שכן אחרת $n(a+b) = 1$ ולכן $n = a+b = 1$ מה שגורר $(a,b,n) = (1,0,1)$ שזה מקרה שהוחרג בתנאי המשפט. אם כך תנאי 2.12 מתקיימים עבור $\widehat{f_{a,b,n}}$ ולכן:

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

והצבה ב6 מניבה את השוויון הדרוש.

אם $a=0$ אז:

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

הנחנו $(a,b,n) \neq (0,1,1)$ ולכן $nb-1 \geq b-1 > 0$ ו $(x+1)^{nb-1} \neq 1$ ומכאן ש:

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

□

ושוב הצבה של השוויון הנ"ל ב6 מניבה את השוויון הדרוש.

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

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

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

בטרם נוכיח את הלמה, נתבונן בהמחשה של הפולינומים הללו:

$(x+1)^0$	□□□□□□□□□□□□□□■
$(x+1)^1$	□□□□□□□□□□□□□■
$(x+1)^2$	□□□□□□□□□□□□■
$(x+1)^3$	□□□□□□□□□□□■
$(x+1)^4$	□□□□□□□□□□■
$(x+1)^5$	□□□□□□□□■
$(x+1)^6$	□□□□□□□■
$(x+1)^7$	□□□□□□■
$(x+1)^8$	□□□□□■
$(x+1)^9$	□□□□■
$(x+1)^{10}$	□□□■
$(x+1)^{11}$	□□■
$(x+1)^{12}$	□■
$(x+1)^{13}$	■
$(x+1)^{14}$	■
$(x+1)^{15}$	■

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 $n \in [0, 2^{d+1} - 1]$ ניתן גם לבצע רקורסיבית. נפריד לשני מקרים אפשריים של n והם: $n \in [0, 2^d - 1]$ ו- $n \in [2^d, 2^{d+1} - 1]$. 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 ב 2^d מקומות שמאלה. אם כך, הקבוצה $\{(x+1)^n : n \in [0, 2^d - 1]\}$ תורמת משולש אחד מסדר d , והקבוצה $\{(x+1)^n : n \in [2^d, 2^{d+1} - 1]\}$ תורמת שני משולשים מסדר d , זה לצד זה. נדגים: את הפולינומים $(x+1)^n$ עבור $n \in [0, 7]$ ניתן לחלק לקבוצות $(x+1)^0, \dots, (x+1)^7$ ו- $(x+1)^4, \dots, (x+1)^7$.

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

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 $t_{\min}((x+1)^n, S_3) \leq 2^d - n$. נסמן $m = \deg(S_3^{2^d-n}((x+1)^n))$. לפי חלק 2 של 2.13:

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

אבל לפי חלק 1 של אותה הלמה:

$$m \leq (\deg(x+1))^n = n < 2^d$$

ולכן בהכרח $S_3^{2^d-n}((x+1)^n) = 1$.
 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.
 מופיע ב xf , לא מופיע ב f ולא מופיע ב $x^{\deg(f)+1}$ כי $\deg(f) + 1 \geq k_2 + 1 > k_1 + 1$.
 מופיע ב f , לא מופיע ב xf (אילו היה מופיע, אז ב f 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 $0 \leq j \leq k_2 - k_1 - 1$ לובשים את הצורה:

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

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

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

נרשום:

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

□

ובכך נקבל את הנדרש.

נשים לב שהפולינום $(x+1)^n$ עבור $2^{d-1} \leq n < 2^d$ הוא ב- 2^{d-1} השורות התחתונות של משולש שרפינסקי שיוצרים הפולינומים $(x+1)^n$ עבור $n \in [0, 2^d - 1]$. 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- $(a, b) \neq (0, 0)$ ו- $n \geq 1$. מתקיים פרט למקרים $(a, b, n) = (0, 1, 1)$, $(a, b, n) = (1, 0, 1)$:

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

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

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

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

לפי 2.20:

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

נציב בשוויון שהוכחנו ב-2.19 ונקבל:

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

□

כעת נשתמש בחישובים שערכנו כדי להוכיח את 2.18.

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

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

מצאנו ב-2.21 שבתנאים אלו מתקיים:

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

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

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

נסמן את קבוצת האינדקסים הזו ב- A אז:

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

כלומר זו תת סדרה חשבונית עם הפרש $(a-b)$. לסיום נשים לב שניתן לבחור את d גדול כרצוננו כדי שכמות האיברים ב- A 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 $\mathbb{F}_2[x]$. 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/bdMfjT0IKk?si=kbGMDU13iEDpTNtS>