סמינר בנושא אנלוג להשערת קולץ בפולינומים

21 באוגוסט 2024

רקע מתמטי

סוג של נספח שאפשר לקרוא או לא או חלקית, לחשוב איפה לשים

- השדה $\mathbb{F}_2$ - הגדרה, טבלת כפל וחיבור, הגדרה של החוג $\mathbb{F}_2\left[x\right]$ (בלי לקרוא לו חוג)
- יחסים אסימפטוטיים

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$\mathbb{F}_2[x]$

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 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:

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

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

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

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

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

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

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

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

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

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

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 בf פרט ל1.

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.

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

ובכך הוכחנו את צעד האינדוקציה.
נקבל 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:

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

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

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

משפט 2.2. *יהי* $0 \neq f \in \mathbb{F}_2[x]$, *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

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

כנדרש. □

2.2 חסם משופר לזמן העצירה

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

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

סימנו בירוק צעדים מסוג $f\mapsto\frac{f}{x}$ ובסגול צעדים מסוג $f\mapsto(x+1)f+1$. 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:

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

כאשר r החזקה הגבוהה ביותר של x המחלקת את f.

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 $f\in\mathbb{F}_{2}[x]$ נגדיר את המיפויים הבאים:

- $T_{1}(f)=(x+1)f+1$
- $T_{2}(f)=\frac{f}{x^{r}}$ כאשר r החזקה המקסימלית של x המחלקת את f עבור $f\neq0$ ונגדיר גם $T_{2}(0)=0$
- $T_{3}(f)=(T_{2}\circ T_{1})(f)$

לכל $f\in\mathbb{F}_{2}[x]$ אי זוגי, הסדרה $(T_{3}^{n}(f))_{n\geq0}$ מהווה תת סדרה של $(T^{n}(f))_{n\geq0}$ שכן עבור f אי זוגי הפעלה יחידה של T_{3} שקולה להפעלה חוזרת של T עד להגעה לפולינום אי זוגי (שאינו f עצמו).

למה 2.4. *יהי $f\in\mathbb{F}_{2}[x]$ אי זוגי.* $t_{\min}(f,T)=2t_{\min}(f,T_{3})+\deg(f)$ *(בפרט $t_{\min}(f,T_{3})$ סופי)*

הוכחה. נוכיח את הטענה באינדוקציה שלמה על מעלת הפולינום f. אם $\deg f=0$ אז $f(x)=1$, $t_{\min}(f,T)=0$ וכן $t_{\min}(f,T_{3})=0$ ולכן השוויון נכון.

נניח שהטענה נכונה לפולינומים אי זוגיים ממעלה קטנה מn ונוכיח אותה לפולינומים אי זוגיים ממעלה n. ב2.1 הוכחנו כי עבור f אי זוגי, הנתון בצורה:

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

כאשר $1\leq r\leq d$ החזקה המקסימלית של x המחלקת את $f-1$, מתקיים כי לכל $1\leq j\leq r$:

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

בפרט עבור $j=r-1$:

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

נשים לב כי מההוכחה ב2.1 נובע כי $2(r-1)$ ההפעלות של T הן לסירוגין מסוג $f\mapsto (x+1)f+1$ ומסוג $f\mapsto \frac{f}{x}$ כלומר מתחלקות לזוגות של הפעלות שכל אחת מהן שקולה להפעלה אחת של T_3 ולכן:

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

נסמן $h(x)=(x+1)^{r-1}xg+1$.

$$T(h) = (x+1)^{r}xg+x$$

תהי כעת s החזקה המקסימלית של x המחלקת את $T(h)$, אז

$$T^{s}(T(h)) = T_2(T(h))$$

מצד שני מהגדרת T_3:

$$T_3(h) = T_2(T_1(h)) = T_2(T(h))$$

קיבלנו:

$$f \overbrace{\to}^{T^{2(r-1)}} h \overbrace{\to}^{T^{1+s}} T_2(T(h)) \qquad T^{2(r-1)+1+s}(f) = T_2(T(h)) \tag{1}$$

$$f \overbrace{\to}^{T_3^{r-1}} h \overbrace{\to}^{T_3} T_2(T(h)) \qquad T_3^{r}(f) = T_2(T(h)) \tag{2}$$

הפולינום $T_2(T(h))$ הוא אי זוגי. $T(h)$ ממעלה $n+1$ ולכן $T_2(T(h))$ ממעלה $n+1-s$. נזכיר כי מ2.1 נובע כי $T^2(h)=T^{2r}(f)$ זוגי כלומר $s\geq 2$ ולכן $n+1-s<n$ ואם כך מהנחת האינדוקציה:

$$t_{\min}(T_2(T(h)),T) = 2t_{\min}(T_2(T(h)),T_3)+(n+1-s)$$

ובשילוב עם 1 ו2 נקבל:

$$\begin{aligned} t_{\min}(f,T)-(2(r-1)+1+s) &= 2(t_{\min}(f,T_3)-r)+(n+1-s) \\ t_{\min}(f,T)-(2r-1+s) &= 2t_{\min}(f,T_3)-2r+(n+1-s) \\ t_{\min}(f,T) &= 2t_{\min}(f,T_3)+n \end{aligned}$$

והוכחנו את השוויון עבור פולינומים אי זוגיים ממעלה n. □

2.2.2 הפולינום ההדדי ומיפויים מקבילים

ברצוננו להמשיך ולחקור את הסדרה $(T_3^n(f))_{n\geq 0}$ 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 המיפוי $\hat{}:\mathbb{F}_2[x]\to\mathbb{F}_2[x]$ 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 $f(x)=\sum_{i=0}^{m}a_ix^i\in\mathbb{F}_2[x]$ כאשר $a_m\neq 0$ אז $\widehat{f}(x)=\sum_{i=0}^{m}a_ix^{m-i}$
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 $\widehat{x^kf}=\widehat{f}$
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:

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

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:

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

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

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

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

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:

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

ועל ידי החלפת אינדקס נוספת נקבל:

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

כעת ניעזר בחלק 3 ונקבל:

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

$\square$

2.3 סדרות משהו משהו

- אין לי שמץ עוד לא קראתי

3 שאלות פתוחות

4 ביבליוגרפיה

1. מאמר של לגריאן
2. מאמר ראשון
3. מאמר שני
4. עבודה של טרי טאו