יריעות אלגבריות - הרצאה שנייה

בהרצאה זו נדבר על רזולטנטות במימדים גבוהים.

אלגוריתם אוקלידס:

קלט: $(n, m, f(x), g(x))$ כאשר $\deg f \leq n,\ \deg f \leq m$
פלט: ה $\gcd$ של f ו g

1. אם $\deg f < n$:
   (א) נפעיל את האלגוריתם עם $(n-1, m, f, g)$
2. אם $\deg g < m$
   (א) נפעיל את האלגוריתם עם $(n, m-1, f, g)$
3. אם $n = -1$
   (א) נחזיר g
4. אם $m = -1$
   (א) נחזיר f
5. אם $n = 0$ או $m = 0$
   (א) נחזיר 1
6. אם $n \leq m$
   (א) נקרא ל $(n, m, f, a_n g - b_m x^{m-n} f)$
7. אם $n > m$
   (א) באופן דומה..

באופן דומה, ניתן לכתוב את האלגוריתם כ decision tree:

1. בכל שלב, המקדמים של הפולינומים שעובדים איתם הם פולינומים ב $a_0, \ldots, a_n, b_0, \ldots, b_m$

2. כל הסתעפות מייצגת האם פולינום כלשהו ב $a_0,\ldots,a_n,b_0,\ldots,b_m$ הוא אפס או לא.

3. הפולינומים במקדמים אלו הם עם מקדמים ב $\mathbb{Z}$.

הגדרה 0.1 צירוף בוליאני של קבוצות אלגבריות נקרא constructible set. אם כל אחד מהפולינומים הרלוונטים בעל מקדמים ב $\mathbb{Z}$ נאמר שהקבוצה מוגדרת מעל $\mathbb{Z}$.

מסקנה 0.2 הפונקציה

$$\mathrm{Poly}_{\leq n}\times \mathrm{Poly}_{\leq m}\to \mathrm{Poly}_{\leq n}$$

$$(f,g)\mapsto \gcd(f,g)$$

היא פולינומיאלית למקוטעין, וכל מקטע הוא constructible.

מסקנה 0.3 הקבוצה

$$\left\{(f,g)\in \mathrm{Poly}_{\leq n}\times \mathrm{Poly}_{\leq m}\mid \text{There is a common root of } f,g\right\}$$

היא constructible כתת קבוצה של $\mathrm{Poly}_{\leq n}\times \mathrm{Poly}_{\leq m}\subseteq \mathbb{C}^{n+m+2}$.

מסקנה 0.4 אם $f(x_1,\ldots,x_n,y)$ ו $g(x_1,\ldots,x_n,y)$ ב $\mathbb{C}[x_1,\ldots,x_n,y]$ ויהי

$$\pi:\mathbb{C}^{n+1}\to \mathbb{C}^n$$

$$(x_1,\ldots,x_n,y)\mapsto (x_1,\ldots,x_n)$$

אזי

$$\pi\left(Z\left(\{f,g\}\right)\right)$$

היא קונסטרוקטיבית.

באופן דומה נוכל לנסח את המסקנה הבאה:

משפט 0.5 (משפט Chevalley). אם $X\subseteq \mathbb{C}^{n+1}$ היא קבוצה אלגברית ו $\pi:\mathbb{C}^{n+1}\to \mathbb{C}^n$ היא ההטלה, אזי $\pi(X)$ קונסטרוקטיבית.

משפט זה נובע מהטענה הבאה:

טענה 0.6 $f_1,\dots,f_n,g_1,\dots,g_m \in \mathbb{C}[x]$, אזי

$$\{t \mid f_i(t)=0,\ g_j(t)\neq 0\}=\emptyset$$

אם ורק אם

$$\gcd(f_i) \mid \prod g_i \iff \gcd\left(f_i,\prod g_j\right)=\gcd(f_i)$$

הגדרה 0.7 (הגדרה גרועה): לוגיקה מסדר ראשון היא כל נוסחה שניתן לכתוב באמצעות משתנים, 0, 1, חיבור, כפל, סוגריים, $\exists,\forall$ ומקשרים לוגיים. לדוגמא,

$$(\forall a)(\forall b)(\forall c)\left(a\neq 0\rightarrow(\exists x)\left(ax^2+bx+c=0\right)\right)$$

היא נוסחה תקינה, אבל רק לכתוב $\forall a$ זה לא תקין. אם לנוסחא אין כמתים, היא נקראת "חופשייה מכמתים". אם לנוסחא אין משתנים חופשיים, היא נקראת "משפט".

הערה 0.8 נוסחא חופשייה מכמתים היא קמובינציה בוליאנית של נוסחאות מהצורה $f(x_1,\dots,x_n)=0$ כאשר $f\in\mathbb{Z}[x_1,\dots,x_n]$.

משפט 0.9 (ניסוח מחדש של Chevalley). אם $\phi(x_1,\dots,x_n,y)$ היא נוסחא חופשייה מכמתים, אזי יש נוסחא חופשייה מכמתים $\psi(x_1,\dots,x_n)$ כך שלכל שדה סגור אלגברית F, הנוסחאות $(\exists y)\,\phi(x_1,\dots,x_n,y)$ ו $\psi(x_1,\dots,x_n)$ שקולות.

מאינדוקציה ניתן להוכיח את המסקנה הבאה:

מסקנה 0.10 כל נוסחא שקולה לנוסחה חופשייה מכמתים.

מסקנה 0.11 כל משפט שקול למשפט ללא כמתים ומשתנים $(\wedge,\sim,1,0,+,\cdot,,)$. כל משפט כזה הוא קומיבנציה בוליאנית של מהצורה

$$1+1+\cdots+1=0$$

מסקנה 0.12 (עקרון Lefscholts). אם ϕ היא משפט מסדר ראשון שנכונה בשדה סגור אלגברית F, אזי היא נכונה בכל השדות הסגורים אלגברית מאותו מציין.

אם שאת ה Nullstelenzats לא ניתן לנסח כלוגיקה מסדר ראשון, אם נחסום את דרגות הפולינומים זה אפשרי, ולכן בפועל הוא נכון לכל שדה ממאפיין 0.

מסקנה 0.13 אם ϕ הוא משפט מסדר ראשון שנכון עבור $\overline{\mathbb{F}_p}$ לכל p ראשוני, אזי הוא נכון עבור $\mathbb{C}$.

הוכחה: כי אם $1+\cdots+1=0$ עבור מספר מסויים של אחדות, זה לא יהיה נכון עבור מאפיין שונה... ■

משפט 0.14 אם $f:\mathbb{C}^n\to\mathbb{C}^n$ היא העתקה פולינומיאלית חד חד ערכית, אזי היא גם על!

הוכחה: מספיק להוכיח את המשפט עבור פולינום

$$f:\overline{\mathbb{F}_p}^n\to\overline{\mathbb{F}_p}^n$$

יש $q=p^k$ כך שבפועל f מעל $\mathbb{F}_q$

$$f:\mathbb{F}_q^n\to\mathbb{F}_q^n$$

כעת עבור העתקה פולינומיאלית כזו, העובדה שהיא חח"ע גוררת שהיא על (כי השדה סופי). לכן ניתן להרחיב את זה ל $\mathbb{F}_{q^i}^n$ לכל i, ומכיוון ש

$$\overline{\mathbb{F}_q}^n=\bigcup_i\mathbb{F}_{q^i}^n\to\overline{\mathbb{F}_q}^n$$

כי אם יש איחוד של העתקות על, האיחוד הוא על. ■

הערה 0.15 ההפך לא נכון, יש העתקות על שאינן חח"ע. איפה זה נופל?