עקומים אלגבריים - הרצאה 12

בהרצאה זו נמשיך לדבר על ספירת נקודות בעקומים. בפעם שעבר, לקחנו עקום פרוייקטיבי C לא סינגולרי מעל $\mathbb{F}_q$. הגדרנו מעין פונקציית זטא:

$$Z\left(t\right)=\sum_{0\leq D\in\mathrm{Div}\left(C\right)\left(\mathbb{F}_q\right)}t^{\deg D}$$

נגדיר את חבורת פיקארד

$$\mathrm{Pic}\left(C\right)\left(\mathbb{F}_q\right)={}^{\mathrm{Div}\left(C\right)\left(\mathbb{F}_q\right)}/_{\sim}$$

ואז נקבל ש

$$Z\left(t\right)=\sum_{D\in\mathrm{Pic}\left(C\right)\left(\mathbb{F}_q\right)}\frac{q^{\ell(D)}-1}{q-1}t^{\deg(D)}=$$

$$=\sum_{D\in\mathrm{Pic}\left(C\right)\left(\mathbb{F}_q\right),0\leq\deg D\leq 2g-2}\frac{q^{\ell(D)}-1}{q-1}t^{\deg D}+\sum_{\deg D>2g-2}\frac{q^{\deg D-g+1}-1}{q-1}t^{\deg D}$$

כעת אנו יודעים לחשב את המחובר הימני. נגדיר

$$\mathrm{Pic}^0\left(C\right)\left(\mathbb{F}_q\right)={}^{\mathrm{Div}^0\left(C\right)\left(\mathbb{F}_q\right)}/_{\sim}$$

ואז נקבל שהמחובר הימני הוא בדיוק

$$\left|\mathrm{Pic}^0\left(C\right)\left(\mathbb{F}_q\right)\right|\sum_{d>2g-2}\frac{q^d-1}{q-1}t^d=$$

$$=\frac{1}{q-1}\left|\mathrm{Pic}^0\left(C\right)\left(\mathbb{F}_q\right)\right|\cdot\frac{q^{2g-1}t^{2g-1}}{1-q+1}-\frac{t^d}{1-t}.$$

לכן סה"כ,

$$Z\left(t\right)=\frac{F\left(t\right)}{\left(1-t\right)\left(1-qt\right)}$$

כאשר $F\left(t\right)$ פולינום מדרגה $2g$.

דוגמא

אנו רוצים לחשב את גודל העקום

$$y^2 = x^3 - 2x$$

מעל $\mathbb{F}_{3^{100}}$. זה עקום אליפטי, ולכן מגנוס 1. לכן $F(t)$ יהיה מדרגה לכל היותר 2. נוכל לכתוב

$$Z(t) = \frac{a + bt + ct^2}{(1-t)(1-qt)}$$

סמן ב α, β את שורשי הפולינום. אזי מתקיים

$$|X(\mathbb{F}_{3^{100}})| = 3^{100} + 1 - \alpha^{100}\beta^{100}$$

למעשה, מספיק לדעת לחשב את $|X(\mathbb{F}_{26})|, |X(\mathbb{F}_9)|, |X(|\mathbb{F}_3)|$. מכיוון שקל לראות שאם נציב $t=0$ נקבל $Z(0)=1$ ולכן $a=1$, מספיק לדעת את $|X(\mathbb{F}_3)|$ ואת $|X(\mathbb{F}_q)|$. נחזור ל

$$Z(t) = \sum_{D \in \mathrm{Pic}(C)(\mathbb{F}_q), 0 \le \deg D \le 2g-2} \frac{q^{\ell(D)} - 1}{q-1} t^{\deg D} + \sum_{\deg D > 2g-2} \frac{q^{\deg D - g + 1} - 1}{q-1} t^{\deg D} =$$

$$= \frac{1}{q-1} \left(\sum_{D \in \mathrm{Pic}(C)(\mathbb{F}_q), 0 \le \deg D \le 2g-2} q^{\ell(D)} t^{\deg D} - \sum_{0 \le \deg D \le 2g-2} t^{\deg D} + \sum \cdots \right)$$

נסמן

$$S(t) = \sum_{D \in \mathrm{Pic}(C)(\mathbb{F}_q), 0 \le \deg D \le 2g-2} q^{\ell(D)} t^{\deg D}$$

ונקבל

$$S(t) = \sum_{D \in \mathrm{Pic}(C)(\mathbb{F}_q), 0 \le \deg D \le 2g-2} q^{\ell(D)} t^{\deg D} = \sum_{o \le \deg D \le 2g-2} q^{\ell(K-D)} t^{\deg(K-D)}$$

(החלפנו את D ב $K-D$). ומרימן רוך נקבל ש

$$= \sum q^{\ell(D) - \deg D + g - 1} t^{2g-2-\deg D} = q^{g-1} t^{2g-2} \sum q^{\ell(D)} \frac{1}{(qt)^{\deg D}} =$$

$$= q^{g-1} t^{2g-2} S\left(\frac{1}{q^t}\right)$$

מסתבר (ניתן להוכיח ע"י חישוב טורים גאומטריים) שגם שאר $Z(t)$ מקיימת אותה משוואה פונקציונלית, ולכן סה"כ $Z(t)$ מקיימת אותה. סה"כ נסכם:

1.

$$Z(t) = q^{g-1}t^{2g-2}Z\left(\frac{1}{q^t}\right)$$

2.

$$Z(t) = \frac{F(t)}{(1-t)(1-qt)}$$

3. משתי הנקודות הקודמות נובע ש

$$F(t) = q^g t^{2g} F\left(\frac{1}{q^t}\right)$$

וזה "מבטל לנו דרגת חופש נוספת". לכן בדוגמא הקודמת,

$$F(t) = 1 + bt + qt^2$$

ולכן מספיק לחשב את $|X(\mathbb{F}_3)|$.

4. מהנקודה הקודמת, קבוצת השורשים של $F(t)$ אינווריאנטית תחת ההעתקה

$$\alpha \mapsto \frac{q}{a}$$

כעת נציג משפט גדול וחשוב של Weil:

משפט 0.1 כל השורשים של $F(t)$ בעלי ערך מוחלט $q^{\frac{1}{2}}$. לכן,

$$||X(\mathbb{F}_q)| - q - 1| \leq 2g \cdot q^{\frac{1}{2}}$$

הוכחה: (הוכחה של Stepanov). הצעד הראשון יהיה להראות

$$\left|X\left(\mathbb{F}_{q^2}\right)\right| \leq q^2 + 1 + (2g+1) \cdot q$$

הרעיון הוא לבנות פולינום מדרגה נמוכה המתאפסים על $X\left(\mathbb{F}_{q^2}\right)$. נבחר נקודה $x \in X(\mathbb{F}_q)$. תהי

$$F : X \to X$$

העתקת פרוביניוס

$$[x:y:z]\mapsto[x^q:y^q:z^q]$$

יהי X_1 העקום

$$X_1=\{(x,F(x))\in X\times X\mid x\in X\}$$

$$X_2=\{(F(x),x)\in X\times X\mid x\in X\}$$

$$X_1,X_2\cong X,\ |X_1\cap X_2|=\left|X\left(\mathbb{F}_{q^2}\right)\right|$$

נבחר $*\in X(\mathbb{F}_q)$, ויהי

$$P_d=L(d[*])$$

וזוהי קבוצת הפונקציות הרציונליות על X שיש להן קוטב ב $*$ מדרגה קטנה/שווה ל d ורגולריות אחרת. משפט רימן-רוך אומר ש

$$\dim P_d=d-g+1$$

נתבונן ב

$$P_d\otimes P_\ell\longrightarrow\mathrm{Rat}(X\times X)\longrightarrow\mathrm{Rat}(X_1)\cong\mathrm{Rat}(X)$$

$$f\otimes g\longmapsto((x,y)\mapsto f(x)\,g(y))\longmapsto f(x)\cdot g(Fx)$$

התמונה של ההעתקה הזו היא בתוך $L((d+eq)[x])$. כעת נבחר d,e כך ש

1. ההעתקה

$$P_d\otimes P_\ell\longrightarrow\mathrm{Rat}(X_1)$$

חח"ע.

2. ההעתקה

$$P_d\otimes P_\ell\to\mathrm{Rat}(X_2)$$

היא לא חח"ע.

נניח כי אנו יכולים לעשות זאת. מ (2) נקבל שיש פונקציה רציונלית

$$h \in \mathrm{Rat}\,(X \times X)$$

שמתאפסת על X_2 (בפרט, מתאפסת על $X_1 \cap X_2$) אבל לא מתאפסת על X_1. אזי

$$h\mid_{X_1} \in L\left((d+eq)\,[*]\right)$$

$$|X_1 \cap X_2| \le |\text{zeros of } h\mid_{X_1} \le d + \ell q|$$

נראה שניתן לבחור d, e כאלו ע"י

$$d = q-1,\ \ e = 1+2g$$

במקרה זה,

$$|X_1 \cap X_2| \le d + eq = q - 1 + (1+2g)\,q = q^2 + (2g+1)\,q - 1$$

כעת צריך להוכיח את (1) ו (2). נתחיל מהוכחת (2): מכיוון ש

$$\dim\left(P_d \otimes P_\ell\right) = (d-q+1)\,(e-g+1) = q^2 - g^2 + q - g$$

ו

$$\dim\left(L\left(\ell + qd\right)\right) = q + qd - g + 1 = q + 2g + 1\,(q-1) - g + 1 =$$

$$= q^2 + g = 1$$

ואם q גדול מספיק, אזי

$$\dim\left(P_d \otimes P_\ell\right) > \dim\left(L\left(q + qd\,[*]\right)\right)$$

ואז ההעתקה לא יכולה להיות חח"ע. הוכחת (1) תשאר כתרגיל לבית.
אם $\mathrm{ord}_*\,(f) = \alpha$ ו $\mathrm{ord}_*\,(g) = \beta$ אזי

$$\mathrm{ord}_*\left(f \otimes g\mid_{X_1}\right) = \mathrm{ord}_*\left(f\,(x) \cdot g\,(F\,(x))\right)$$

$$\sum f_i \otimes g_i\mid_{X_1} = 0$$

$$\mathrm{ord}_*\left(f_i \otimes g_i\right) = \alpha_i + q\beta_i$$

נתבונן בזוגות $\{(\alpha_i,\beta_i)\}$ ונבחר (α,β) כך ש

$$\alpha+q\beta$$

מקסימלי. במקרה זה, נתבונן בביטויים עם $\alpha_i=\alpha$ ו $\beta_i=\beta$. במקרה זה, מכיוון ש

$$\alpha\le d<q$$

נקבל שכולם בעלי אותם α_i,β_i. יהי f^* בעל קוטב מסדר α ו g^* בעל קוטב מסדר β.

$$f_i=c_i\cdot f^*+\text{lower order terms}$$

$$g_i=d_i\cdot g^*+\cdots$$

$$\operatorname{ord}_*\left(\sum_{i\in I}f_i\otimes g_i\right)<\alpha+q\beta$$

ו

$$\operatorname{ord}_*\left(\sum_{i\in I}f_i\otimes g_i\right)=\operatorname{ord}_*\left(\sum\left(\sum c_id_i\right)f^*\otimes g^*\right)$$

ולכן

$$\sum c_id_i=0$$

ולכן סה"כ

$$\sum_{i=1}^{n}f_i\otimes g_i=\sum_{1}^{n}f_i\otimes g_i-\sum_{i\in I}c_id_i^*\otimes g^*=$$

$$=\sum_{i\in I}f_i\otimes g_i+\sum_{i\in I}f_i\otimes g_i-\sum_{i\in I}c_if^*\otimes d_ig^*=$$

$$=\sum_{i\in I^c}f_i\otimes g_i+\sum_{i\in I}(f_i-c_if^*)\otimes(g_i-d_ig^*)$$

כאשר למחוברים הימנים יש קטבים מסדר נמוך יותר. נמשיך באינדוקציה.
הוכחנו עד כה ש

$$q^2+1+\sum_{i=1}^{2g}\lambda_i^2=\left|X\left(\mathbb{F}_{q^2}\right)\right|\le q^2+1+(2g+1)\,q$$

אבל ניתן לחזור על התהליך לכל n ולקבל

$$q^{2n}+1+\sum_{i=1}^{2g}\lambda_i^{2n}=\left|X\left(\mathbb{F}_{q^2}\right)\right|\leq q^{2n}+1+\left(2g+1\right)q^n$$

כעת

$$\sum_{i=1}^{2g}\lambda_i^{2n}\leq\left(2g+1\right)q^n$$

נשאיף $n\to\infty$ ונקבל

$$|\lambda_i|\leq q^{\frac{1}{2}}$$

אבל מהמשוואה הפונקציונלית יש לנו סימטריה וקיבלנו ש $\frac{q}{\lambda_i}$ הוא גם שורש, ולכן

$$\left|\frac{q}{\lambda_i}\right|\leq q^{\frac{1}{2}}$$

ולכן

$$|\lambda_i|\geq q^{\frac{1}{2}}$$

ולכן סה"כ

$$|\lambda_i|=q^{\frac{1}{2}}$$

■