מבוא לקירובים דיופנטיים

סמסטר: 2013 ב׳
מרצה: פרופ׳ ברק וייס
נכתב ע״י: יוני רוזנשיין (yoni.vl@gmail.com)

תוכן עניינים

מבוא

הבעיה הבסיסית בקירובים דיופנטיים

נתון מספר ממשי $x \in \mathbb{R}$ ופרמטר Q.

צריך למצוא מספר רציונלי $\frac{p}{q} \in \mathbb{Q}$ כך ש- $0 < q \le Q$, ו- $\left|x - \frac{p}{q}\right|$ קטן ככל האפשר.

דוגמה: $\frac{355}{113} = 3.14159292\ldots$ הוא קירוב ל- π (6 ספרות אחרי הנקודה מזדהות). הוא פותר את הבעיה עבור $x = \pi$ ו- $Q = 114$ (ולמעשה גם ל- Q-ים גדולים יותר).

משפט (דיריכלה).

לכל x ממשי ולכל $Q > 1$ שלם קיים רציונלי $\frac{p}{q}$ כך ש- $0 < q \le Q$ ו- $\left|x - \frac{p}{q}\right| \le \frac{1}{qQ}$ (או, באופן שקול, $\left|qx - p\right| \le \frac{1}{Q}$).

להחליף אי שוויון חלש בחזק ולהיפך

הוכחה.

נחלק את $[0,1]$ ל- Q תתי הקטעים $\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left[1 - \frac{1}{Q}, 1\right]$.

נסתכל על $Q+1$ המספרים $0, 1, \{x\}, \{2x\}, \ldots, \{(Q-1)x\}$ שנמצאים בקטע $[0,1]$.

Q

($\{z\} := z - \lfloor z \rfloor$ החלק השברי של המספר.)

לפי עקרון שובך היונים, שניים מהם נופלים באותו תת-קטע. כלומר, $(k < \ell)$ p_1, p_2, k, ℓ, r כך ש-

$$\frac{r}{Q} \le kx - p_1, \ell x - p_2 \le \frac{r+1}{Q}$$

(כל המספרים ניתנים להצגה כ- $ax - b$ כאשר a, b שלמים.)

לכן: $\frac{1}{Q} \ge \left|\ell x - p_2 - kx + p_1\right| = \left|(\ell - k)x - (p_2 - p_1)\right| =: \left|qx - p\right|$

מש"ל.

מסקנה. לכל $x \in \mathbb{R} \setminus \mathbb{Q}$ יש אינסוף פתרונות לאי-שוויון $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$ $(*)$.

הוכחה. אם $q < Q$ אז $\left|x - \frac{p}{q}\right| \le \frac{1}{qQ} < \frac{1}{q^2}$. לכן כל פתרון עם Q כלשהו יקיים את אי-השוויון.

לכן, לפי משפט דיריכלה, יש לפחות פתרון אחד.

כעת, אם $x \notin \mathbb{Q}$ ו- $p_1, q_1, \ldots, p_n, q_n$ פתרונות ל- $(*)$, נבחר Q כך ש- $\frac{1}{Q} < \min_{i=1,\ldots,n} \left|q_i x - p_i\right|$.

לפי משפט דיריכלה יש פתרון והוא חייב להיות פתרון חדש, ומכאן יש אינסוף פתרונות.

מש"ל.

הערה. יש אנשים המכנים את המסקנה "משפט דיריכלה" אך נדגיש שהמסקנה היא יותר חלשה. לדוגמה, נחשוב על Q כעל מגבלה על הזכרון שמשתמשים בו כדי לייצג מספר רציונלי במחשב. במקרה זה, משפט דיריכלה הוא אפליקטיבי, ואומר שיש ייצוג קרוב ומכמת את הקירוב; לעומתו, המסקנה לא נותנת מידע כמותי על הקירוב.

הערה. ההנחה ש- $x \notin \mathbb{Q}$ במסקנה היא חיונית.

כי אם $x = \frac{r}{s}$ ו- $\frac{p}{q}$ מקיים את $(*)$, אז $\frac{1}{q^2} > \left|\frac{r}{s} - \frac{p}{q}\right| = \frac{|rq-ps|}{sq}$.

אם המונה טבעי ואינו אפס אז הוא לפחות 1, ולכן $\frac{1}{sq} < \frac{1}{q^2}$, כלומר $q < s$, ויש מספר סופי של פתרונות.

שאלה. האם אפשר לשפר את התוצאה במסקנה? האם אפשר להחליף את הביטוי $\frac{1}{q^2}$ למשל ב- $\frac{1}{q^3}$ או $\frac{1}{q^{2+\varepsilon}}$ או $\frac{1}{q^2 \log q}$?

הגדרה.

- x נקרא <u>מקורב רע</u> (<u>badly approximable</u>) אם קיים $0 < C = C(x)$ כך שיש רק מספר סופי של פתרונות לאי-שוויון $\left|x - \frac{p}{q}\right| < \frac{C}{q^2}$.
- מסמנים ב- BA את קבוצת המספרים המקורבים רע.

טענה. המספר $\phi = \frac{1+\sqrt{5}}{2}$ מקורב רע, ואפשר לבחור בתור $C(\phi)$ כל מספר קטן מ- $\frac{1}{\sqrt{5}}$.

הוכחה. נסמן $P(x) = x^2 - x - 1$ (הפולינום המינימלי של ϕ מעל $\mathbb{Q}$). נגדיר $\phi' = \frac{1-\sqrt{5}}{2}$, ואז $P(x) = (x-\phi)(x-\phi')$, ונבחר $C < \frac{1}{\sqrt{5}}$.

נניח בשלילה שקיים פתרון p,q למשוואה. מכיוון שהפולינום P הוא מדרגה 2 ואין לו שורשים רציונליים, מתקיים $\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^2}$ (הסבר: כמו קודם, עושים מכנה משותף q^2 ומשתמשים בכך שהמונה הוא טבעי שונה מאפס).

$$\frac{1}{q^2} \leq \left|P\left(\frac{p}{q}\right)\right| = \left|\frac{p}{q} - \phi\right|\left|\frac{p}{q} - \phi'\right| \overset{\text{Assumption}}{<} \frac{C}{q^2}\left(\left|\frac{p}{q} - \phi'\right|\right) \overset{\text{Triangle}}{\leq} \frac{C}{q^2}\left(\left|\frac{p}{q} - \phi\right| + |\phi - \phi'|\right) <$$
$$< \frac{C}{q^2}\left(\frac{C}{q^2} + \sqrt{5}\right) = \frac{\sqrt{5}C}{q^2} + \frac{C^2}{q^4}$$

לכן $1<\sqrt{5}C+\frac{C^2}{q^2}$. אם נניח בשלילה שיש <u>אינסוף</u> פתרונות, אז ניתן להשאיף את q לאינסוף ולקבל $1\le\sqrt{5}C$, בסתירה לבחירה $C<\frac{1}{\sqrt{5}}$. לכן יש רק מספר סופי של פתרונות.

מש"ל.

תרגיל. x מקורב רע $\Leftrightarrow$ קיים C כך שאין פתרונות <u>כלל</u> ל- $\left|x-\frac{p}{q}\right|<\frac{C}{q^2}$.

שאלות קלאסיות.

- האם π מקורב רע?
- האם $\sqrt[3]{2}$ מקורב רע?
- שאלות דומות עבור מספרים ספציפיים.

(שאלות פתוחות, מאוד קשות.)
שאלות דיופנטיות על מספרים ספציפיים נוטות להיות קשות. לדוגמה, לא יודעים להוכיח שספרה כלשהי מופיעה אינסוף פעמים בפיתוח העשרוני של π.

הערה.

- כל מספר אלגברי מדרגה 2 מקורב רע. ההוכחה לכך זהה להוכחה עבור ϕ לעיל.
- **משפט (Roth, 1956).** לכל מספר אלגברי x ולכל $\varepsilon>0$ יש לכל היותר מספר סופי של פתרונות למשוואה $\left|x-\frac{p}{q}\right|<\frac{1}{q^{2+\varepsilon}}$.
- השאלה למשל לגבי $\frac{1}{q^2\log q}$, או שיפורים אחרים שבין $\frac{1}{q^2}$ לבין $\frac{1}{q^{2+\varepsilon}}$, פתוחה.

התורה המידתית של קירובים דיופנטיים

(Metric theory of Diophantine approximation)

הגדרה. נניח ש- $\psi(q)\searrow 0$.

- x נקרא ψ-מקורב אם יש אינסוף פתרונות לאי-שוויון $\left|x-\frac{p}{q}\right|<\psi(q)$.
- את קבוצת המספרים ה- ψ מקורבים נסמן $\psi\text{-approx}$.

שואלים מה הגודל (במובנים שונים: מידה, קטגוריה, מימד האוסדורף...) של הקבוצה הזו כתלות ב- ψ.

משפט (Khintchine, ~1930).

א. אם $\sum_q q\psi(q)<\infty$, אז מידת לבג של $\psi\text{-approx}$ היא אפס.

ב. אם $\sum_q q\psi(q)=\infty$, אז מידת לבג של <u>המשלים</u> של $\psi\text{-approx}$ (כלומר, של קבוצת המספרים המקורבים <u>רע</u> לפי ψ) היא אפס.

מסקנה. BA היא קבוצה ממידה אפס.

שאלה פתוחה. האם אפשר להחליף במשפט את מידת לבג במידת קנטור?

מדוע לא שואלים שאלות דומות לזו של משפט Khintchine, עם קטגוריית Baire במקום מידה? בגלל שהתשובה טריוויאלית:

טענה. <u>לכל</u> ψ, הקבוצה ψ-approx היא G_δ וצפופה (ובפרט, מקטגוריית Baire גדולה).

הוכחה.

יש שקילות $x \in \left(\frac{p}{q}-\psi(q), \frac{p}{q}+\psi(q)\right) \iff \left|x-\frac{p}{q}\right|<\psi(q)$.

נסמן $\mathcal{A}_{p,q} := \left(\frac{p}{q}-\psi(q), \frac{p}{q}+\psi(q)\right)$.

$x \in \psi\text{-approx} \iff$ יש אינסוף ערכים של p,q כך ש- $x \in \mathcal{A}_{p,q}$.

למעשה, גם אינסוף ערכים של q. כי עבור q קבוע, יש רק מספר סופי של p-ים שיכולים להתאים לו. (ואפשר להניח ש- $q \to \infty$ כי $\psi(q) \searrow 0$). לכן:

$$\psi\text{-approx} = \bigcap_{Q=1}^{\infty} \bigcup_{\substack{p,q \\ q \geq Q}} \mathcal{A}_{p,q}$$

לכל Q, הקבוצה $\bigcup_{\substack{p,q \\ q \geq Q}} \mathcal{A}_{p,q}$ היא קבוצה פתוחה המכילה את כל הרציונליים עם מכנה גדול מ- Q, ואלה (לכל Q קבוע) צפופים ב- $\mathbb{R}$, ולכן זוהי קבוצה פתוחה צפופה.

לכן ψ-approx היא חיתוך בן מניה של קבוצות פתוחות צפופות, ולכן היא G_δ וצפופה (לפי משפט Baire).

מש"ל.

הכללות למימדים גבוהים

מהמסקנה ממשפט דיריכלה קיבלנו שיש אינסוף פתרונות ל- $\left|x-\frac{p}{q}\right|<\frac{1}{q^2} \iff |qx-p|<\frac{1}{q}$.

הכללות רב-מימדיות: מתייחסים ל- x,p,q כוקטורים או מטריצות במימדים יותר גבוהים.

למשל: $\vec{X} \in \mathbb{R}^d$, $\vec{P} \in \mathbb{Z}^d$, $q \in \mathbb{N}$, ו- $\psi(q) \searrow 0$.

<u>שאלת הקירוב הסימולטני.</u> בהינתן $\vec{X} \in \mathbb{R}^d$, נורמה $\|\ \|$, ו- ψ, האם קיימים אינסוף פתרונות לאי-שוויון

$$\left\|\vec{X}-\frac{1}{q}\vec{p}\right\|<\psi(q)$$

במשתנים $\vec{p} \in \mathbb{Z}^d$ ו- $q \in \mathbb{N}$?

משפט (דיריכלה). לכל $\vec{X} \in \mathbb{R}^d$ יש אינסוף פתרונות במשתנים $\vec{p} \in \mathbb{Z}^d$ ו- $q \in \mathbb{N}$ לאי-שוויון

$$\left\|\vec{X}-\frac{1}{q}\vec{p}\right\|_\infty<\frac{1}{q^{1+1/d}}$$

בעיה נוספת: $\vec{X} \in \mathbb{R}^d$ והפעם $\vec{q} \in \mathbb{Z}^d$, ו- $p \in \mathbb{Z}$.

בהינתן $\vec{X} \in \mathbb{R}^d$, נורמה $\|\ \|$, ו- ψ, האם קיימים אינסוף פתרונות ב- $\vec{q} \in \mathbb{Z}^d$, ו- $p \in \mathbb{Z}$ לאי-שוויון

$$\left\|\vec{X}\cdot\vec{q}-p\right\|<\psi\left(\|\vec{q}\|\right)$$

דוגמה המכלילה את שתי הבעיות הנ"ל:
בהינתן $X \in M_{m,n}(\mathbb{R})$, נורמה $\|\ \|$ ו- ψ, האם יש אינסוף פתרונות ב- $\vec{p} \in \mathbb{Z}^m$ ו- $\vec{q} \in \mathbb{Z}^n$ לאי-שוויון

$$\|X\vec{q} - \vec{p}\| < \psi(\|\vec{q}\|)$$

לכל הבעיות הללו קיימות גרסאות של משפט דיריכלה (שמוכחות גם הן עם עקרון שובך היונים), וגרסאות של משפט חינצ'ין (עם מידת לבג על $\mathbb{R}^d$ או על $M_{m,n}(\mathbb{R}) \cong \mathbb{R}^{mn}$). אפשר לשאול גם על מידות אחרות:

משפט (משפט Sprindzhuk / השערת Mahler).
לכל $\varepsilon > 0$, כמעט לכל $x \in \mathbb{R}$ יש רק מספר סופי של פתרונות לאי-השוויון הבא:

$$\left\| \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^d \end{pmatrix} - \frac{1}{q}\vec{p} \right\| < \frac{1}{q^{1+1/d+\varepsilon}}$$

בפרמטרים $q \in \mathbb{N}$ ו- $\vec{p} \in \mathbb{Z}^d$.

כאן, מדובר על מידת לבג על העקום $x \mapsto (x, x^2, \dots, x^d)$. השאלה של הקירוב של נקודות על העקום הזה עולה באופן טבעי בשאלות של קירוב עם מספרים אלגבריים.
יש שאלות דומות לגבי קירוב עם מידות פרקטליות.

תבניות ריבועיות

שאלה יותר כללית, עדיין ב-2 מימדים:
ראינו שעבור x-ים מסויימים (מקורבים רע) ו- C-ים מסויימים, לכל $p,q \in \mathbb{Z}$ $(q \neq 0)$, מתקיים
$\left|x - \frac{p}{q}\right| \geq \frac{C}{q^2}$, או באופן שקול, $|q^2x - pq| \geq C$.
נתמקד בביטוי האחרון ונמצא שהוא תבנית בילינארית ב- p,q.

שאלה. בהינתן $f(p,q) = \alpha p^2 + \beta pq + \gamma q^2$ (תבנית בילינארית), כאשר $\alpha, \beta, \gamma \in \mathbb{R}$, האם

$$\inf_{(p,q)\in\mathbb{Z}^2\setminus\{0\}} |f(p,q)| > 0$$

זה מכליל שאלות בנוגע למספרים מקורבים רע:
במקרה של $\beta = -1$ ו- $\alpha = 0$ השאלה שקולה לשאלה האם γ מקורב רע.

דוגמה אחרת: $p^2 + q^2$ היא תבנית חיובית לחלוטין: תמיד $p^2 + q^2 \geq 1$ (ב- $\mathbb{Z}^2 \setminus \{0\}$).

לכן הבעיה מעניינת רק אם הסיגנטורה של f היא $(1,-1)$, כלומר

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \alpha(x - \mu y)(x - \nu y) \quad (\mu, \nu \in \mathbb{R})$$

כלומר, הדיסקרימיננטה חיובית: $\beta^2 - 4\alpha\gamma > 0$.

בעיות לא הומוגניות

$X \in M_{m,n}(\mathbb{R})$, $\vec{p} \in \mathbb{Z}^m$, $\vec{q} \in \mathbb{Z}^n$, $\vec{Y} \in \mathbb{R}^m$ ($\vec{Y}$ יהיה ההזזה – הגורם הלא הומוגני בהעתקה אפינית).

האם יש אינסוף פתרונות בהינתן $X, \vec{Y}$ לאי-שוויון

$$\left\| X\vec{q} + \vec{Y} - \vec{p} \right\| < \psi\left(\|\vec{q}\| \right)$$

כלומר, כאן מדובר בקירוב דיופנטי להעתקה הלינארית $\vec{v} \mapsto X\vec{v} + \vec{Y}$.

מקרה פרטי: $m = n = 1$; $|xq + y - p| < \psi(q)$?

פירוש גיאומטרי

פירושים גיאומטריים לחלק מהשאלות שראינו:

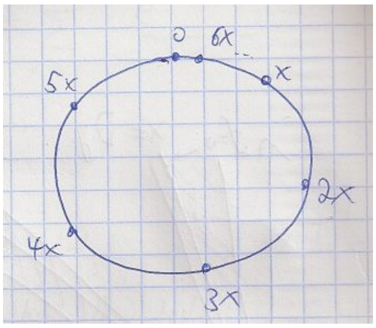
- כאשר $m = n = 1$: $\left| x - \frac{p}{q} \right| < \psi(q)$ - רוצים "למצוא רציונלי ליד x".

  זה שקול ל- $|qx - p| < q\psi(q) = \tilde{\psi}(q)$.

  פירוש גיאומטרי לבעיה: נתבונן ב- $x \in \mathbb{R}/\mathbb{Z} = [0,1]/_{1 \sim 0} = \mathbb{T}^1 = \mathcal{S}^1$ (נקודה ממשית במעגל).

  אנו שואלים באיזה קצב (לאורך תת-סדרה) המסלול $x, 2x, 3x, \ldots \pmod 1$ מתקרב ל- 0.

  הבעיה הלא-הומוגנית $|qx + y - p| < \psi(q)$ דנה בשאלה, בהינתן (x, y), באיזה קצב (לאורך תת-סדרה) המסלול $x, 2x, 3x, \ldots \pmod 1$ מתקרב ל- y ב- $\mathcal{S}^1$.



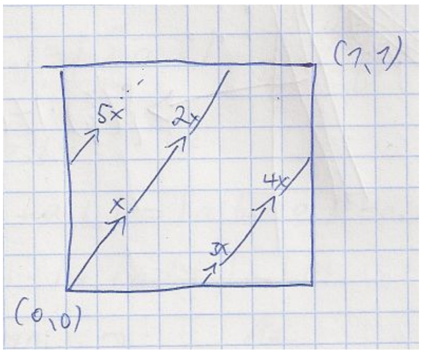
- כאשר $n = 1, m = 2$:

  $\left\| \vec{X} - \frac{1}{q}\vec{p} \right\| < \psi(q)$; מנסים לקרב את $\vec{X}$ ע"י וקטורים רציונליים עם מכנה משותף q.

  $\left\| q\vec{X} - \vec{p} \right\| < \tilde{\psi}(q)$. מסתכלים על הוקטורים $\vec{X}, 2\vec{X}, 3\vec{X}, \ldots$, שתי הקואורדינטות מודולו 1, ושואלים על קצב ההתקרבות לראשית הצירים לאורך תת-סדרה.

  כלומר, כאן אנו מסתכלים על $\vec{X}$ בתור וקטור בטורוס הדו-מימדי:

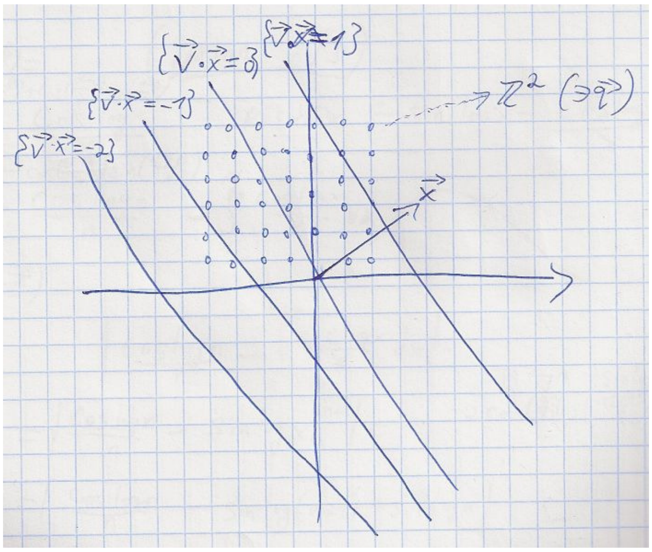
$$\vec{X} \in \mathbb{R}^2/\mathbb{Z}^2 = \mathbb{T}^2 = [0,1]^2 \Big/ \begin{matrix} (0,y) \sim (1,y) \\ (x,0) \sim (x,1) \end{matrix}$$



- כאשר $n=2, m=1$:

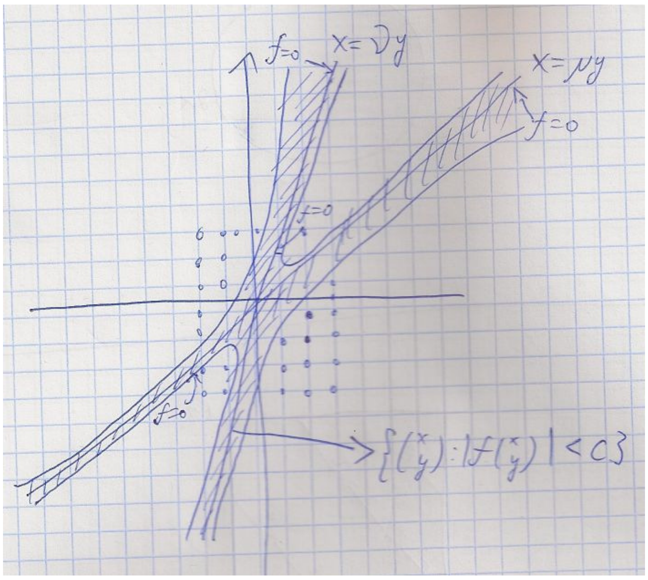
$$\left|\vec{q}\cdot\vec{X}-p\right|<\psi\left(\|\vec{q}\|\right).$$

$\vec{X}$ נתון, שואלים האם יש וקטורים שלמים $\vec{q}$ שקרובים לקבוצה $\left\{\vec{v}\in\mathbb{R}^2 : \vec{v}\cdot\vec{X}\in\mathbb{Z}\right\}$.



- השאלה על התבניות הריבועיות:

$f(x,y)=\alpha x^2+\beta xy+\gamma y^2=a(x-\mu y)(x-\nu y)$. האם $\inf_{(p,q)\in\mathbb{Z}^2\setminus\{0\}}\left|f(p,q)\right|>0$?



השאלה הגיאומטרית היא האם הקבוצה המאויירת (השטח החסום המוגדר ע"י $|f| < C$) מכילה נקודות שריג פרט ל-$(0,0)$?

במקרה של תבנית ב-2 משתנים עם סיגנטורה $(1,1)$, בדרך-כלל ("למרבית" הבחירות של המקדמים (α,β,γ)) לכל $C>0$ תהיה נקודה ב-$\mathbb{Z}^2\setminus\{0\}$ בתוך הקבוצה $\left\{\vec{X} : \left|f\left(\vec{X}\right)\right| < C\right\}$.

משפט (השערת אופנהיים, משפט מרגוליס).
נניח ש-Q תבנית בילינארית ב-$n\geq 3$ משתנים, עם סיגנטורה (p,q), $p,q>0$.
נניח ש-Q לא כפולה של פולינום עם מקדמים שלמים.
אז לכל C יש $\vec{q}\in\mathbb{Z}^n\setminus\{0\}$ כך ש-$\left|Q(\vec{q})\right| < C$.

2013-03-06

סימון: $\langle\alpha\rangle := \operatorname{dist}(\alpha,\mathbb{Z}) = \min_{p\in\mathbb{Z}}|\alpha-p|$.

מסקנה ממשפט דיריכלה: $x\notin\mathbb{Q}$ $\Leftarrow$ יש אינסוף פתרונות p,q למשוואות (השקולות)

$$q\langle qx\rangle < 1 \iff \langle qx\rangle < \frac{1}{q} \iff \left|x-\frac{p}{q}\right| < \frac{1}{q^2}$$

כמו-כן, ראינו שאם $x=\phi=\frac{1+\sqrt{5}}{2}$ אז עבור $C<\frac{1}{\sqrt{5}}$ יש רק מספר סופי של פתרונות לאי-השוויון $q\langle qx\rangle < C$.

תזכורת. x נקרא <u>מקורב רע</u> ($x\in \mathrm{BA}$) אם קיים C כך שלכל p,q, $\left|x-\frac{p}{q}\right|\geq\frac{C}{q^2}$ $\iff$ $q\langle qx\rangle\geq C$.

מימד האוסדורף.

אם $X \subset \mathbb{R}^n$ אז יש ל- X מימד האוסדורף, המסומן $\dim(X)$, בעל התכונות הבאות:

א. X בת-מניה או סופית $\Leftarrow \dim(X)=0$.

ב. $X \subset Y \Leftarrow \dim(X) \le \dim(Y)$.

ג. אם X עקום חלק או בעל אורך אז $\dim(X)=1$.

ד. אם X יריעה חלקה ממימד k אז $\dim(X)=k$.

ה. אם X קבוצת קנטור אז $\dim(X)=\frac{\log 2}{\log 3}$.

אנו נראה ש- $\dim(\mathrm{BA})=1$, כלומר המימד המקסימלי שיכול להיות לתת-קבוצה של $\mathbb{R}$. כלומר, למרות ש- BA זניחה מבחינת מידה, היא גדולה מבחינת מימד האוסדורף.

תזכורת – תבניות ריבועיות.

$$f(x,y)=\alpha x^2+\beta xy+\gamma y^2$$

נניח ש- f בעלת סיגנטורה $(1,1)$, כלומר $f(x,y)=a(x-\mu_1 y)(x-\mu_2 y)$ עם $\mu_1,\mu_2 \in \mathbb{R}$.

שאלה: האם $\inf_{(p,q)\in\mathbb{Z}^2\setminus\{0\}} |f(p,q)|>0$?

כמו שיש הרבה מספרים מקורבים רע, כך יש הרבה תבניות שבהן האינפימום הנ"ל הוא חיובי. (ניתן להגדיר מימד האוסדורף על תבניות.)

<u>הערה.</u> האי-שוויון שמשפט דיריכלה פותר עבור $\theta \in \mathbb{R}$ הוא $q\langle q\theta\rangle<1$, או $q|q\theta-p|<1$, וזוהי תבנית ריבועית ב- p,q.

משפט (השערת אופנהיים, משפט מרגוליס, 1986).

נניח ש- f תבנית ב- $n\ge 3$ משתנים, עם סיגנטורה (p,q), $p,q>0$.

נניח ש- f לא כפולה של פולינום עם מקדמים שלמים. אזי $\inf_{\vec{x}\in\mathbb{Z}^n\setminus\{0\}} |f(\vec{x})|=0$.

<u>הערה.</u> ההוכחה משתמשת בכלים של תורה ארגודית ופעולות של חבורות אלגבריות.

השערת Littlewood (בעיה פתוחה, מאז שנות ה-30).

לכל $\alpha,\beta\in\mathbb{R}$, $\liminf_{q\to\infty} q\langle q\alpha\rangle\langle q\beta\rangle=0$.

הערה. אם $\alpha \notin \mathrm{BA}$ ההשערה מתקיימת (כי $\lim_{q\to\infty} q\langle q\alpha\rangle=0$), ולכן היא מתקיימת כמעט לכל זוג α,β.

משפט (איינזידלר-קאטוק-לינדנשטראוס).

$\dim\left(\left\{(\alpha,\beta): \text{Littlewood's conjecture is incorrect for } (\alpha,\beta)\right\}\right)=0$. (מימד האוסדורף.)

ניתן לחשוב על $q\langle q\alpha\rangle\langle q\beta\rangle$ בתור $q|q\alpha-p_1||q\beta-p_2|$ - מכפלה של 3 תבניות לינאריות.

שברים משולבים וקירובים טובים ביותר

נסמן ב- $\mathcal{S}$ את כל הסדרות הסופיות או האינסופיות של הטבעיים.
את תת-הקבוצה של סדרות סופיות נסמן ב- $\mathcal{S}_0$.

אנו נראה שקיימת העתקה $\mathrm{cf}:\mathcal{S}\to[0,1]$ (מלשון continued fraction) בעלת התכונות הבאות:

- מעתיקה את $\mathcal{S}_0$ ל- $[0,1]\cap\mathbb{Q}$ באופן $2\leftarrow 1$-ערכי ועל (כלומר לכל ערך יש בדיוק 2 מקורות)
- מעתיקה את $\mathcal{S}\setminus\mathcal{S}_0$ ל- $[0,1]\setminus\mathbb{Q}$ באופן חח"ע ועל

הגדרה של cf על סדרות סופיות:

$$\mathrm{cf}(a_1,\dots,a_N)=\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots_{\;a_N}}}$$

היתירות: קל לראות שאם $a_N\ge 2$ אז $a_N=a_N-1+\frac{1}{1}$, ואז

$$\mathrm{cf}(a_1,\dots,a_N)=\mathrm{cf}(a_1,\dots,a_N-1,1)$$

כלומר, כל סדרה סופית שבה האיבר האחרון הוא 1 שוות-ערך תחת cf לסדרה סופית כלשהי שבה האיבר האחרון אינו 1, ולהיפך.

הגדרה של cf על סדרות אינסופיות:

$$\mathrm{cf}(a_1,a_2,\dots):=\lim_{n\to\infty}\mathrm{cf}(a_1,a_2,\dots,a_n)$$

הגדרה.

יהי $\theta\in\mathbb{R}$. נאמר ש- $\frac{p}{q}$ הוא <u>קירוב טוב ביותר (best approximant)</u> עבור θ אם:

- $q>0$
- $\langle q\theta\rangle=|q\theta-p|$
- לכל $0<q'<q$, $\langle q'\theta\rangle>\langle q\theta\rangle$

פירוש גיאומטרי.

נתבונן במעגל $\mathbb{T}=\mathbb{R}/\mathbb{Z}$ ובאיבר θ (מודולו 1) על המעגל. נסובב את θ על המעגל, כלומר נתבונן על הסדרה $\theta,2\theta,3\theta,\dots$ ב- $\mathbb{T}$. בכל פעם שאיבר בסדרה יותר קרוב ל- 0 מכל קודמיו, זהו $q\theta$ עבור קירוב טוב ביותר כלשהו $\frac{p}{q}$.

<u>אם θ רציונלי אז יש קירוב טוב ביותר יחיד (כי יש q שעבורו $q\theta\equiv 0 \mod 1$).</u> יש מספר סופי

נניח ש- $\theta\notin\mathbb{Q}$. יש אינסוף קירובים טובים ביותר (ממשפט דיריכלה). נסדר את ה- q-ים לפי סדר:

$$0<1=q_1<q_2<\dots$$

לפי ההגדרה של קירוב טוב ביותר, נובע:

- $\langle q_n\theta\rangle = |q_n\theta - p_n|$.
- לכל $q < q_{n+1}$, $\langle q\theta\rangle \geq \langle q_n\theta\rangle$ $(*)$.

כמו-כן, מתקיים: $1 \overset{\text{Dirichlet}}{\leq} q_n\langle q_n\theta\rangle < q_{n+1}\langle q_n\theta\rangle$ $(**)$. (<u>הסבר:</u> ממשפט דיריכלה נובע שקיים $q < q_{n+1}$ כך ש-$q_{n+1}\langle q\theta\rangle \leq 1$, והרי כל $q < q_{n+1}$ מקיים $\langle q\theta\rangle \geq \langle q_n\theta\rangle$.)

טענה.

א. המספרים $\frac{p_n}{q_n}$ הם כל הקירובים הטובים ביותר ל-θ, q_n בסדר עולה.

ב. אם θ רציונלי אז יש N כך ש-$\theta = \frac{p_N}{q_N}$.

ג. אם $\theta \notin \mathbb{Q}$ אז $\frac{p_n}{q_n} \xrightarrow{n\to\infty} \theta$.

הוכחה.

א. מיידי מהבניה ומההגדרות.

ב. מיידי מהבניה ומההגדרות.

ג. נובע מ-$(**)$:

$$\langle q_n\theta\rangle = |q_n\theta - p_n| \overset{(**)}{<} \frac{1}{q_{n+1}}$$

ולכן

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \xrightarrow{n\to\infty} 0$$

מש"ל.

טענה. ל-$q_{n+1}\theta - p_{n+1}$ ול-$q_n\theta - p_n$ יש סימנים הפוכים.

הוכחה. נניח בשלילה שהם שווי-סימן. נשתמש במקרה השוויון של אי-שוויון המשולש:

$$|x+y| = \begin{cases} |x|+|y| & x, y \text{ have the same sign} \\ \big||x|-|y|\big| & x, y \text{ have different signs} \end{cases}$$

נסמן $p' = p_{n+1} - p_n$ ו-$q' = q_{n+1} - q_n$. נשים לב ש-$q' < q_{n+1}$, אבל

$$\langle q'\theta\rangle \leq |q'\theta - p'| = \left|(q_{n+1}\theta - p_{n+1}) - (q_n\theta - p_n)\right| \overset{\text{Triangle}}{=}$$
$$= \big||q_{n+1}\theta - p_{n+1}| - |q_n\theta - p_n|\big| = \langle q_n\theta\rangle - \langle q_{n+1}\theta\rangle < \langle q_n\theta\rangle$$

בסתירה ל-$(*)$. **מש"ל.**

טענה. $\det\begin{pmatrix} p_n & q_n \\ p_{n+1} & q_{n+1}\end{pmatrix} = q_{n+1}p_n - q_n p_{n+1} = \pm 1$; ובפרט, $\gcd(p_n, q_n) = 1$.

הוכחה.

מהטענה הקודמת, ל-$q_n\theta - p_n$ ו-$q_{n+1}\theta - p_{n+1}$ סימנים הפוכים.

לכן $\frac{p_n}{q_n}$ ו- $\frac{p_{n+1}}{q_{n+1}}$ בצדדים שונים של θ, ובפרט הם שונים זה מזה. לכן

$$0 \neq \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{q_{n+1}p_n - q_n p_{n+1}}{q_n q_{n+1}}$$

מכאן, $\left|q_{n+1}p_n - q_n p_{n+1}\right| > 0$. מצד שני,

$$\left|q_{n+1}p_n - q_n p_{n+1}\right| = \left|q_n\left(q_{n+1}\theta - p_{n+1}\right) - q_{n+1}\left(q_n\theta - p_n\right)\right| \overset{\text{Triangle (Same signs...)}}{=}$$

$$= q_n\left\langle q_{n+1}\theta\right\rangle + q_{n+1}\left\langle q_n\theta\right\rangle < 2q_{n+1}\left\langle q_n\theta\right\rangle \overset{\text{Dirichlet}}{\leq} 2$$

המעבר הלפני אחרון: במחובר הראשון ($q_n\left\langle q_{n+1}\theta\right\rangle$) אם נחליף את הכופל q_n ב- q_{n+1} רק נגדיל (ממש) את הערך, וגם אם נחליף את $\left\langle q_{n+1}\theta\right\rangle$ ב- $\left\langle q_n\theta\right\rangle$ רק נגדיל (ממש) את הערך.

בסה"כ, קיבלנו:

$$0 < \left|q_{n+1}p_n - q_n p_{n+1}\right| < 2$$

אבל $\left|q_{n+1}p_n - q_n p_{n+1}\right|$ שלם, ולכן $\left|q_{n+1}p_n - q_n p_{n+1}\right| = 1$.

מש"ל.

מסקנות.

1. הסימן של $q_{n+1}p_n - q_n p_{n+1}$ הפוך לסימן של $q_n\theta - p_n$.
2. $q_{n+1}p_n - q_n p_{n+1} = -\left(q_n p_{n-1} - q_{n-1}p_n\right)$.
3. $q_n\left\langle q_{n+1}\theta\right\rangle + q_{n+1}\left\langle q_n\theta\right\rangle = 1$.

הוכחה.

1. הסימן של $q_{n+1}p_n - q_n p_{n+1}$ שווה לסימן של $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}$. ראינו שהשברים $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ נמצאים בצדדים שונים של θ. אזי, $q_{n+1}p_n - q_n p_{n+1} > 0 \iff \frac{p_n}{q_n} > \theta \iff q_n\theta - p_n < 0$.
2. נובע מ-1, כי ראינו שהסימן של $q_n\theta - p_n$ הפוך לסימן של $q_{n+1}\theta - p_{n+1}$.
3. חישבנו במהלך ההוכחה הקודמת וראינו שביטוי זה שווה ל- $\left|q_{n+1}p_n - q_n p_{n+1}\right|$.

מש"ל.

טענה.

לכל $n \geq 2$ יש a_n טבעי כך ש-

$$\begin{cases} q_{n+1} = a_n q_n + q_{n-1} \\ p_{n+1} = a_n p_n + p_{n-1} \\ \left|q_{n-1}\theta - p_{n-1}\right| = a_n\left|q_n\theta - p_n\right| + \left|q_{n+1}\theta - p_{n+1}\right| \qquad (***) \end{cases}$$

הוכחה.

לפי מסקנה 2 לעיל,

$$p_n\left(q_{n+1} - q_{n-1}\right) = q_n\left(p_{n+1} - p_{n-1}\right)$$

מכאן p_n מחלק את אגף ימין, אבל ראינו קודם ש- $\gcd\left(p_n, q_n\right) = 1$ ולכן $p_n \mid p_{n+1} - p_{n-1}$.

אם כך, נסמן: $a_n = \frac{p_{n+1}-p_{n-1}}{p_n}$; זהו מספר חיובי שלם, ואכן מתקיים $p_{n+1}=a_n p_n + p_{n-1}$.

כמו-כן, ע"י הצבה במשוואה שקיבלנו לעיל ממסקנה 2, נקבל: $q_{n+1}-q_{n-1}=a_n q_n$.

כך קיבלנו את 2 הזהויות הראשונות. הזהות $(***)$ נובעת משתי הזהויות שלפניה:

$$a_n\left|q_n\theta-p_n\right|+\left|q_{n+1}\theta-p_{n+1}\right| \overset{\text{Triangle (different signs...)}}{=} \left|a_n\left(q_n\theta-p_n\right)-\left(q_{n+1}\theta-p_{n+1}\right)\right|=$$
$$=\left|a_n\left(q_n\theta-p_n\right)-a_nq_n\theta-q_{n-1}\theta+a_np_n+p_{n-1}\right|=\left|q_{n-1}\theta-p_{n-1}\right|$$

מש"ל.

ע"י בדיקה זהירה של תנאי ההתחלה, מקבלים את התוצאה הבאה:

משפט. יהי $0<\theta<1$ ונגדיר a_n, p_n, q_n לפי נוסחת הנסיגה הבאה:

$$\begin{cases} p_0=1; \quad q_0=0; \quad p_1=0; \quad q_1=1 \\ q_{n+1}=a_nq_n+q_{n-1} \\ p_{n+1}=a_np_n+p_{n-1} \\ a_n=\left\lfloor \frac{\left|q_{n-1}\theta-p_{n-1}\right|}{\left|q_n\theta-p_n\right|}\right\rfloor \end{cases}$$

אזי $\frac{p_n}{q_n}$ הם הקירובים הטובים ביותר ל-θ עבור $n\geq 1$ אם $a_1=1$ ועבור $n\geq 2$ אם $a_1\geq 2$.

<u>הערה.</u> הנוסחה ל-a_n מתקבלת מזהות $(***)$, ע"י חלוקה והעברת אגפים.

סימונים.

- אם $0<\theta<1$ אי-רציונלי, מסמנים $\theta=\left[a_1,a_2,\ldots\right]$.
- אם $0<\theta<1$ רציונלי, הנוסחאות שבמשפט יתנו $\theta=\left[a_1,\ldots,a_N\right]$ כאשר $a_N\geq 2$.
  מוסכמה: נאמר גם ש-$\theta=\left[a_1,\ldots,a_N-1,1\right]$.
- אם $\theta=0$ אז $\theta=\left[\ \right]$.
- אם $\theta\in\mathbb{R}$ כלשהו, רושמים $\theta=a_0+\theta'$, כאשר $a_0\in\mathbb{Z}$ ו-$0\leq\theta'<1$, ואז מסמנים $\theta=\left[a_0;a_1,a_2,\ldots\right]$ כאשר $\theta'=\left[a_1,a_2,\ldots\right]$.

(כלומר, כל המספרים המופיעים ב-$[\ ]$ טבעיים פרט למספר שלפני ה-; שמותר לו להיות שלילי.)

- המספרים a_n נקראים <u>partial quotients</u> של θ, או <u>מקדמי הפיתוח של השבר המשולב (continued fraction coefficients)</u> של θ.
- המספרים $\frac{p_n}{q_n}$ נקראים <u>convergents</u> של θ. אנו נקרא להם <u>הקירובים הנובעים מפיתוח השבר המשולב</u> של θ.

את הנוסחה $(***)$ אפשר לרשום כנוסחת נסיגה כך:

$$\theta_n=\frac{\left|q_n\theta-p_n\right|}{\left|q_{n-1}\theta-p_{n-1}\right|} \qquad \theta_0=1$$

ואז מתקיים:

$$\begin{cases} \theta_1 = \theta \\ \dfrac{1}{\theta_n} = a_n + \theta_{n+1} \\ \theta_{n+1} = \left\{ \dfrac{1}{\theta_n} \right\} \\ a_n = \left\lfloor \dfrac{1}{\theta_n} \right\rfloor \end{cases}$$

הגדרה. <u>העתקת גאוס</u> היא הפונקציה $\mathcal{G}:(0,1)\to[0,1);\ x\mapsto\left\{\frac{1}{x}\right\}$.

באמצעות הסימונים האחרונים, מקבלים שהסדרה θ_n היא המסלול של העתקת גאוס החל מ- $\theta_1=\theta$. אם בשלב כלשהו מקבלים $\mathcal{G}(\theta_n)=0$ אז לא ניתן להפעיל יותר את העתקת גאוס; זה קורה עבור θ רציונלי.

את ההעתקה cf שתיארנו בתחילת השיעור אפשר להגדיר באופן הבא: משתמשים ב- $[a_1,\ldots,a_N,\ldots]$ ובנוסחאות הנסיגה כדי לקבל את $\frac{p_n}{q_n}$. נוכיח מיד שקיים $\lim_{n\to\infty}\frac{p_n}{q_n}$. גבול זה הוא $\mathrm{cf}([a_1,a_2,\ldots])$.

הראינו שאם $0<\theta<1$, אז אפשר לבנות $[a_1,a_2,\ldots]$ באמצעות נוסחאות הנסיגה של θ:

$\theta_1=\theta,\ \frac{1}{\theta_n}=a_n+\theta_{n+1}$, ומתקיים $\lim_{n\to\infty}\frac{p_n}{q_n}=\theta$.

נותר להראות <u>שלכל</u> סדרה $(a_1,a_2,\ldots)$ הגבול $\lim_{n\to\infty}\frac{p_n}{q_n}$ קיים, וקיים θ עבורו הסדרה הנתונה מתקבלת מנוסחאות הנסיגה של θ.

למה. נניח $\theta=[a_1,\ldots,a_n,a_{n+1},\ldots]$ ו- $\theta'=[a_1,\ldots,a_n,b_{n+1},\ldots]$. אזי $|\theta-\theta'|<2^{-(n-2)}$.

הוכחה. נסמן ב- $\frac{p_k}{q_k}$, $k=1,\ldots,n+1$ את הקירובים המתקבלים מנוסחאות הנסיגה. אז $\frac{p_{n+1}}{q_{n+1}}$ הוא קירוב טוב ביותר של θ וגם של θ'. הסימנים של $q_{n+1}\theta-p_{n+1}$ ושל $q_{n+1}\theta'-p_{n+1}$ זהים. נניח בה"כ ש- θ רחוק יותר מ- $\frac{p_{n+1}}{q_{n+1}}$ מאשר θ'. (ידוע ש- $\frac{p_{n+1}}{q_{n+1}}$ נמצא מאותו צד של θ,θ' ולכן לא ביניהם). לכן:

$$|\theta-\theta'|\le\left|\theta-\frac{p_{n+1}}{q_{n+1}}\right|\le\frac{1}{q_{n+1}^{2}}$$

אבל

$$q_{n+1}=a_nq_n+q_{n-1}\ge 2q_{n-1}\overset{\text{By induction on } n}{\ge} 2^{\frac{n-2}{2}}$$

ולכן

$$|\theta-\theta'|\le 2^{-(n-2)}$$

משל.

טענה. לכל סדרה $(a_1, a_2, \ldots) \in \mathcal{S}$, אינסופית או סופית עם איבר אחרון גדול מ-1, יש θ כך ש-$\theta = [a_1, a_2, \ldots]$.

הוכחה. אם הסדרה סופית, $(a_1, \ldots, a_N)$, נסמן $\theta_{N+1} = 0$ ונשתמש בנוסחת הנסיגה $\frac{1}{\theta_n} = a_n + \theta_{n+1}$ "בכיוון ההפוך" כדי להגדיר את $\{\theta_N, \theta_{N-1}, \ldots, \theta_1\}$. מנוסחת הנסיגה מקבלים

$$\theta = \theta_1 = \frac{1}{a_1 + \theta_2} = \frac{1}{a_1 + \frac{1}{a_2 + \theta_3}} = \ldots = \frac{1}{a_1 + \frac{1}{a_2 + \ddots \frac{1}{a_N}}} = [a_1, \ldots, a_N]$$

כנדרש.

במקרה שהסדרה אינה סופית, נרשום לכל N, $\theta^{(N)} = [a_1, \ldots, a_N]$. (לפי החלק הקודם של ההוכחה, ידוע שיש מספר כזה.) לפי הלמה, הסדרה $\theta^{(N)}$ היא סדרת קושי, ולכן קיים לה גבול θ. רוצים להראות ש-

$$\theta = [a_1, a_2, \ldots]$$

נסמן

$$\theta_n^{(N)} = [a_n, a_{n+1}, \ldots, a_N]$$

הגבול $\lim_{N \to \infty} \theta_n^{(N)}$ קיים (לפי הלמה), נסמנו θ_n.

לכל N, לפי הבנייה,

$$\frac{1}{\theta_n^{(N)}} = a_n + \theta_{n+1}^{(N)}, \quad \frac{1}{\theta_n} = a_n + \theta_{n+1}$$

כלומר, נוסחת הנסיגה $\frac{1}{\theta_n} = a_n + \theta_{n+1}$ מתקיימת עבור θ_n לכל n, ו-$\theta = \theta_1 = [a_1, a_2, \ldots]$.

משל.

טענה.

$$\frac{1}{a_n {q_n}^2} > \left| \theta - \frac{p_n}{q_n} \right| > \frac{1}{(a_n + 2) {q_n}^2}$$

(בשיעור הבא.)

2013-03-13

טענה.

$$\frac{1}{a_n {q_n}^2} > \left| \theta - \frac{p_n}{q_n} \right| > \frac{1}{(a_n + 2) {q_n}^2}$$

הוכחה. הוכחנו בשיעור הקודם ש-$q_{n+1} \langle q_n \theta \rangle + q_n \langle q_{n+1} \theta \rangle = 1$. לכן,

$$\langle q_n\theta\rangle < \frac{1}{q_{n+1}} = \frac{1}{a_nq_n+q_{n-1}} < \frac{1}{a_nq_n}$$

ומכאן, $\left|\theta-\frac{p_n}{q_n}\right| < \frac{1}{a_nq_n^2}$. מצד שני,

$$1 = q_{n+1}\langle q_n\theta\rangle + q_n\langle q_{n+1}\theta\rangle < (q_n+q_{n+1})\langle q_n\theta\rangle$$

ומכאן

$$\left|\theta-\frac{p_n}{q_n}\right| > \frac{1}{q_n(q_n+q_{n+1})} = \frac{1}{q_n((a_n+1)q_n+q_{n-1})} > \frac{1}{(a_n+2)q_n^2}$$

מש"ל.

טענה. אם $\left|\theta-\frac{p}{q}\right| < \frac{1}{2q^2}$ אזי $\frac{p}{q}=\frac{p_n}{q_n}$ לאיזשהו n.

הוכחה. נבחר n כך ש-$q_{n-1}\le q<q_n$. נראה שאם $\frac{p}{q}\ne\frac{p_n}{q_n}$ אז $q<q_{n-1}$ (סתירה).

הערה: ברור שיש n כזה אם $\theta\notin\mathbb{Q}$. אם $\theta=\frac{p_N}{q_N}$, כדי לדעת שיש n כזה, די להראות ש-$q<q_N$. ואכן,

$\frac{1}{q_N} \le \frac{|qp_N-q_Np|}{q_N} = |q\theta-p| < \frac{1}{2q} \Rightarrow 2q<q_N$, ובפרט $q<q_N$.

עפ"י הבחירה של n כך ש-$q_{n-1}\le q<q_n$, מתקיים $\langle q_{n-1}\theta\rangle \le \langle q\theta\rangle < \frac{1}{2q}$. לכן

$$\frac{1}{qq_{n-1}} \le \frac{|qp_{n-1}-pq_{n-1}|}{qq_{n-1}} = \left|\frac{p_{n-1}}{q_{n-1}}-\frac{p}{q}\right| \le \overbrace{\left|\frac{p_{n-1}}{q_{n-1}}-\theta\right|}^{\frac{1}{q_{n-1}}\langle q_{n-1}\theta\rangle} + \left|\theta-\frac{p}{q}\right| < \frac{1}{2qq_{n-1}}+\frac{1}{2q^2}$$

ע"י העברת אגפים וצמצום q מקבלים: $q<q_{n-1}$ - סתירה.

מש"ל.

מספרים מקורבים רע ומספרי Liouville

תזכורת. θ נקרא <u>מקורב רע</u> (BA) אם יש $C>0$ כך שלכל p,q, $\left|\theta-\frac{p}{q}\right| \ge \frac{C}{q^2}$ $(**)$.

טענה. $\theta=[a_0;a_1,\dots]$ מקורב רע $\Leftrightarrow$ $\sup a_n<\infty$.

הוכחה. לפי הטענה הקודמת, אפשר לבדוק את $(**)$ רק עבור המספרים p,q שהם קירובים p_n,q_n הניתנים ע"י פיתוח θ כשבר משולב.

לפי הטענה שלפני הקודמת,

$$\frac{1}{(a_n+2)q_n^2} < \left|\theta-\frac{p_n}{q_n}\right| < \frac{1}{a_nq_n^2}$$

אם $\sup a_n = \infty$, נבחר סדרה של a_n-ים עבורה $a_n \to \infty$ ונקבל מאי-השוויון הימני סתירה ל-$(**)$ לכל C. מאידך אם $\sup a_n = K < \infty$, נבחר $C = \frac{1}{K+2}$ ונשתמש באי-השוויון השמאלי.
מש"ל.

מסקנה. BA אינה בת-מניה.
הסבר. כל מילה אינסופית בספרות $\{1,\dots,k\}$ לאיזשהו k מתאימה למספר שהוא BA, ע"י שבר משולב.

טענת עזר. אם θ אלגברי מדרגה $d > 1$ (כלומר, שורש אי-רציונלי של פולינום במקדמים שלמים מדרגה d)
אז יש קבוע C כך ש- $\left|\theta - \frac{p}{q}\right| \ge \frac{C}{q^d}$ לכל p,q.

הערה. לפי משפט Roth (1956) ניתן למעשה להחליף באגף ימין את החזקה d ב-$2+\varepsilon$, ללא תלות ב-d.

הוכחה. נניח בשלילה שיש $\frac{p_n}{q_n}$ כך ש-$q_n^d\left|\theta - \frac{p_n}{q_n}\right| \xrightarrow{n\to\infty} 0$. נסמן את הפולינום המינימלי של θ ב-$P(x) = a_0 + a_1x + \dots + a_dx^d$.

אז $0 \ne q_n^d P\left(\frac{p_n}{q_n}\right)$, כי ל-$P$ אין שורשים רציונליים, ומצד שני $q_n^d P\left(\frac{p_n}{q_n}\right) \in \mathbb{Z}$ (כי יש מכנה משותף q_n^d בהצבת $\frac{p_n}{q_n}$ בפולינום). לכן (נסמן ב-$\theta_1,\dots,\theta_d$ את הצמודים האלגבריים של $\theta = \theta_1$):

$$1 \le q_n^d\left|P\left(\frac{p_n}{q_n}\right)\right| = q_n^d\left|a_d\right|\prod_{i=1}^{d}\left|\frac{p_n}{q_n} - \theta_i\right| \overset{\text{For large enough } n}{\le} q_n^d\left|a_d\right|\left|\frac{p_n}{q_n} - \theta\right| \cdot 2^{d-1}\max_{i>1}\left|\theta - \theta_i\right|$$

הסבר למעבר האחרון: לכל $i > 1$, $\left|\frac{p_n}{q_n} - \theta_i\right| \xrightarrow{n\to\infty} \left|\theta - \theta_i\right|$, ולכן עבור n מספיק גדול,

$$\left|\frac{p_n}{q_n} - \theta_i\right| \le 2\max_{i>1}\left|\theta - \theta_i\right| \qquad \forall i$$

באגף ימין הכל קבוע חוץ מ-$q_n^d\left|\frac{p_n}{q_n} - \theta\right|$ ששואף לאפס עפ"י הנחת השלילה, אבל מצד שני אגף ימין גדול מ-1. סתירה. **מש"ל.**

מסקנה (Liouville, 1844). יש מספרים טרנסצנדנטיים.
הערה. ההוכחה "המודרנית" לכך שיש מספרים טרנסצנדנטיים היא פשוט שהאלגבריים הם בני-מניה. אבל בתקופה שבה Liouville הוכיח זאת, שיקולי עוצמות לא היו ידועים לו, וההוכחה הזו ממש קונסטרוקטיבית.

הוכחה. לפי טענת העזר, די לבנות מספר θ כך ש-$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{nq_n^n}$ $(***)$ (אפשר גם לכתוב באגף ימין $\frac{1}{q_n^n}$ למשל). מספר זה לא יוכל להיות אלגברי, כי זה יסתור את טענת העזר. למעשה, נראה שאפשר לבנות מספרים שקצב ההתכנסות שלהם גבוה כרצוננו.

לפי טענה קודמת: $\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{a_nq_n^2}$. נבנה את $\theta=[a_0;a_1,\dots]$ ע"י כך שנבנה את הסדרה a_n באינדוקציה.

נניח ש-$(***)$ מתקיים עבור $q_1,\dots,q_{n-1}$, כלומר $a_1,\dots,a_{n-1}$ נבחרו, ולפי נוסחת הנסיגה, ידוע q_n. כעת נבחר את a_n כך ש-$\frac{1}{nq_n^n}<\frac{1}{a_nq_n^2}$ (כלומר $a_n>nq_n^{n-2}$).

מש"ל.

הערה. מספרים x שיש להם אינסוף פתרונות ל-$0<\left|x-\frac{p}{q}\right|<\frac{1}{q^n}$ נקראים מספרי Liouville.

משפט. לכל $\theta\notin\mathbb{Q}$ יש אינסוף פתרונות לאי-השוויון $\left|\theta-\frac{p}{q}\right|\le\frac{1}{\sqrt{5}q^2}$.

תזכורת. הראינו שעבור $\theta=\phi$ (יחס הזהב), אם $C<\frac{1}{\sqrt{5}}$ אז יש רק מספר סופי של פתרונות לאי-השוויון $\left|\theta-\frac{p}{q}\right|\le\frac{C}{q^2}$.

הערה. לכל θ, מגדירים $m(\theta):=\liminf_{q\to\infty}q\langle q\theta\rangle$. לפי המשפט הזה, לכל $\theta\in\mathbb{R}$ מתקיים $m(\theta)\le\frac{1}{\sqrt{5}}$.

לפי מה שראינו, $m(\phi)=\frac{1}{\sqrt{5}}$. לכל $\theta\in\mathrm{BA}$, $m(\theta)>0$. הקבוצה $\{m(\theta):\theta\in\mathbb{R}\}$ נקראת הספקטרום של Markov (שבין השאר, פיתח את שרשראות Markov כדי להבין את הקבוצה הזו). הקבוצה הזו מעניינת: בחלק הימני שלה (ממספר כלשהו עד $\frac{1}{\sqrt{5}}$) זו קבוצה דיסקרטית. בחלק השמאלי (מ-0 עד מספר כלשהו) יש קטע. באמצע בין שני החלקים הנ"ל, יש קבוצה סגורה שאינה דיסקרטית ואינה קטע (פרקטל כלשהו) ויש בעיות פתוחות הקשורות בהבנת הקבוצה.

הערה. לא ידוע הקבוע הקטן ביותר C כך שלכל $\vec{\theta}\in\mathbb{R}^2$ יש אינסוף $\vec{p}\in\mathbb{Z}^2$, $q\in\mathbb{N}$ כך ש-

$$\left\|\vec{\theta}-\frac{1}{q}\vec{p}\right\|\le\frac{C}{q^{3/2}}$$

(בנורמת ∞ או בנורמה אוקלידית.)

הוכחה של המשפט.

נסמן $A_n=q_n\langle q_n\theta\rangle$. רוצים להראות $\liminf_{n\to\infty}A_n\le\frac{1}{\sqrt{5}}$. נראה שלכל n לפחות אחד מהמספרים $A_k\in\{A_n,A_{n+1},A_{n+2}\}$ מקיים $A_k\le\frac{1}{\sqrt{5}}$.

נקבע n, ונסמן $\lambda=\frac{q_{n-1}}{q_n}$, $\mu=\frac{q_{n+1}}{q_n}$. נשתמש בזהות $q_{n+1}\langle q_n\theta\rangle+q_n\langle q_{n+1}\theta\rangle=1$. נכתוב אותה עם A_n:

$$\underbrace{\frac{q_n}{q_{n+1}}}_{\mu^{-1}} A_{n+1} + \underbrace{\frac{q_{n+1}}{q_n}}_{\mu} A_n = 1$$

כמו-כן, ע"י החלפת n ב-$n-1$ נקבל

$$\underbrace{\frac{q_{n-1}}{q_n}}_{\lambda} A_n + \underbrace{\frac{q_n}{q_{n-1}}}_{\lambda^{-1}} A_{n-1} = 1$$

לכן:

$$(1) \qquad \lambda^2 A_n - \lambda + A_{n-1} = 0$$

$$(2) \qquad \mu^2 A_n - \mu + A_{n+1} = 0$$

$$(3) \qquad \mu - \lambda = \frac{q_{n+1} - q_{n-1}}{q_n} = a_n$$

נחסר את (2) מ-(1) ונשתמש ב-(3):

$$0 = \left(\lambda^2 - \mu^2\right) A_n + \left(\mu - \lambda\right) + A_{n+1} - A_{n-1} = -a_n \left(\lambda + \mu\right) A_n + a_n + A_{n-1} - A_{n+1}$$

מכאן:

$$(4) \qquad a_n A_n \left(\lambda + \mu\right) = a_n + A_{n-1} - A_{n+1}$$

נעלה את (3), (4) בריבוע ונחבר.

$$(5) \qquad 2a_n^2 A_n^2 \left(\lambda^2 + \mu^2\right) = a_n^2 A_n^2 \left(\left(\lambda + \mu\right)^2 + \left(\lambda - \mu\right)^2\right) = \left(a_n + A_{n-1} - A_{n+1}\right)^2 + a_n^4 A_n^2$$

נחבר את (1) ו-(2) ונשתמש ב-(5),(4):

$$0 = \left(\mu^2 + \lambda^2\right) A_n - \left(\lambda + \mu\right) + A_{n-1} + A_{n+1}$$

כופלים ב- $2a_n^2 A_n$:

$$\begin{aligned} 0 &= 2a_n^2 A_n^2 \left(\mu^2 + \lambda^2\right) - 2a_n^2 A_n \left(\lambda + \mu\right) + 2a_n^2 A_n \left(A_{n-1} + A_{n+1}\right) \overset{(4),(5)}{=} \\ &= a_n^4 A_n^2 + \left(a_n + A_{n-1} - A_{n+1}\right)^2 - 2a\left(a_n + A_{n-1} - A_{n+1}\right) + 2a_n^2 A_n \left(A_{n-1} + A_{n+1}\right) = \\ &= a_n^4 A_n^2 + \left(a_n + A_{n-1} - A_{n+1}\right)\left(A_{n-1} - A_{n+1} - a_n\right) + 2a_n^2 A_n \left(A_{n-1} + A_{n+1}\right) = \\ &= a_n^4 A_n^2 + 2a_n^2 A_n \left(A_{n+1} + A_{n-1}\right) + \left(A_{n+1} - A_{n-1}\right)^2 - a_n^2 \end{aligned}$$

נעביר אגף, נחלק ב- a_n^2 ונקבל:

$$a_n^2 A_n^2 + 2A_n \left(A_{n+1} + A_{n-1}\right) = 1 - \frac{\left(A_{n-1} - A_{n+1}\right)^2}{a_n^2}$$

ומכאן:

$$(6) \qquad a_n^2 A_n^2 + 2A_n \left(A_{n+1} + A_{n-1}\right) \le 1$$

אם נסמן $A = \min\left\{A_{n-1}, A_n, A_{n+1}\right\}$ אז צד שמאל של (6) הוא לפחות $a_n^2 A^2 + 4A^2$, לכן:

$$A^2 \left(a_n^2 + 4\right) \le 1$$

כעת, מכיוון ש- a_n טבעי, נקבל $A \le \frac{1}{\sqrt{5}}$.

מש"ל.

שימוש נוסף של שברים משולבים, בתורת החבורות:

$$\Gamma = \mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : \det = \pm 1 \right\}$$

כשחבורה פועלת על מרחב (למשל $\mathrm{GL}_2(\mathbb{Z})$ על $\mathbb{R}^2$) היא מגדירה באופן טבעי יחס שקילות באמצעות המסלולים של החבורה. Γ פועלת על $\mathbb{R}^2$ ע"י כפל מטריצה בוקטור.

דוגמה אחרת של פעולה היא הפעולה על $\mathbb{C}$ ע"י העתקת מביוס:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

לחילופין נראה ש- Γ פועלת על מרחב הישרים דרך הראשית ב- $\mathbb{R}^2$ ($\mathbb{RP}^1$) ע"י העתקות מביוס:

נניח $\ell = \mathrm{Span}\left\{ \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right\}$ כאשר $y_0 \neq 0$. אז $\ell = \mathrm{Span}\left\{ \begin{pmatrix} \frac{x_0}{y_0} \\ 1 \end{pmatrix} \right\}$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ell = \mathrm{Span}\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{x_0}{y_0} \\ 1 \end{pmatrix} \right\} = \mathrm{Span}\left\{ \begin{pmatrix} \frac{ax_0}{y_0} + b \\ \frac{cx_0}{y_0} + d \end{pmatrix} \right\} \overset{\frac{cx_0}{y_0}+d \neq 0}{=} \mathrm{Span}\left\{ \begin{pmatrix} \frac{\frac{ax_0}{y_0}+b}{\frac{cx_0}{y_0}+d} \\ 1 \end{pmatrix} \right\}$$

כפי שרצינו להראות.

מכיוון ש- $\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\} \cong \mathcal{S}^1$, קיבלנו פעולה של חבורה על המעגל. הפעולה הזו לא פשוטה.

נסמן בתור $\sim$ את יחס השקילות הנובע מהפעולה של החבורה: $x \sim y$ אם קיים $\gamma \in \Gamma$ כך ש- $\gamma x = y$.

משפט. נסמן $x = [a_0; a_1, a_2, \ldots]$ ו- $y = [b_0; b_1, b_2, \ldots]$. אז $x \sim y \iff$ קיימים N_1, N_2 כך שלכל $n \ge 1$, $a_{N_1+n} = b_{N_2+n}$.

ניסוח אחר: $x \sim y$ ביחס ל- $\Gamma \iff$ בפיתוח לשברים משולבים יש ל- x, y את אותו הזנב.

הוכחה. הכיוון הקל, $\Rightarrow$: נסמן $\theta_1 = \theta = [a_1, a_2, \ldots]$, $\theta_n = [a_n, a_{n+1}, \ldots]$. אזי

$$\theta_n = \frac{1}{a_n + \theta_{n+1}} = \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \theta_{n+1}$$

לכן $\theta_n \sim \theta_{n+1}$ לכל n. מטרנזיטיביות ובאינדוקציה, $\theta \sim \theta_n$ לכל n, ולכן $x \sim y$.

הכיוון $\Leftarrow$: ידוע ש- $y = \gamma x$ כאשר $\gamma \in \Gamma$.

נכתוב $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ עם $r, s, t, u \in \mathbb{Z}$. אזי $\det \gamma = \pm 1$ ולכן $\gamma^{-1} = \pm \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$.

<u>טענת עזר.</u> קיים n_0 כך שלכל $n \ge n_0$ ולכל זוג $\frac{p_n}{q_n},\frac{p_{n+1}}{q_{n+1}}$ של קירובים עוקבים של y, גם $\frac{p'_n}{q'_n},\frac{p'_{n+1}}{q'_{n+1}}$ קירובים עוקבים של x, כאשר

$$\begin{pmatrix} p' \\ q' \end{pmatrix} = \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} pu-qs \\ -pt+rq \end{pmatrix} = \pm\gamma^{-1}\begin{pmatrix} p \\ q \end{pmatrix}$$

כלומר

$$\pm\begin{pmatrix} p \\ q \end{pmatrix} = \gamma\begin{pmatrix} p' \\ q' \end{pmatrix} = \begin{pmatrix} p'r+q's \\ p't+q'u \end{pmatrix}$$

במילים אחרות, אם $y=\gamma x$, $\frac{p_n}{q_n}$ הם קירובי שבר משולב של y ו- $\frac{\tilde{p}_n}{\tilde{q}_n}$ הם קירובי שבר משולב של x, אז קיימים $n_0 \in \mathbb{N}, k_0 \in \mathbb{Z}$ כך שלכל $n \ge n_0$, $\frac{\tilde{p}_{k_0+n}}{\tilde{q}_{k_0+n}} = \frac{p'_n}{q'_n} = \gamma\begin{pmatrix} p_n \\ q_n \end{pmatrix}$.

הוכחת טענת העזר תתפרסם בהמשך באתר הקורס.

<u>הוכחת המשפט בעזרת טענת העזר.</u>

כזכור, סימנו $x=[a_0;a_1,a_2,\ldots]$ ו- $y=[b_0;b_1,b_2,\ldots]$. מטענת העזר, מתקיים לכל $n \ge n_0$:

$$\begin{aligned}\tilde{q}_{k_0+n} &= q'_n = rq_n - tp_n = \\ &= r\left(b_{n-1}q_{n-1}+q_{n-2}\right) - t\left(b_{n-1}p_{n-1}+p_{n-2}\right) = \\ &= b_{n-1}\left(rq_{n-1}-tp_{n-1}\right)+rq_{n-2}-tp_{n-2} = \\ &= b_{n-1}\tilde{q}_{k_0+n-1}+\tilde{q}_{k_0+n-2}\end{aligned}$$

מצד שני, $\tilde{q}_{k_0+n} = a_{k_0+n-1}\tilde{q}_{k_0+n-1}+\tilde{q}_{k_0+n-2}$ לכל $n \ge n_0$.

מכאן, $a_{k_0+n-1} = b_{n-1}$ לכל $n \ge n_0$. **מש"ל.**

(אחרי פסח, נעבור למשפט חינצ'ין.)

הוכחת טענת העזר מהשיעור האחרון (הקלדת ההוכחה שפורסמה באתר הקורס בכתב יד).

סימונים. $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, $x \in \mathbb{R}\setminus\mathbb{Q}$, $y=\gamma x = \frac{rx+s}{tx+u}$.

לכל $p,q \in \mathbb{Z}$ נסמן $\begin{pmatrix} p' \\ q' \end{pmatrix} = \begin{pmatrix} pu-qs \\ -pt+qr \end{pmatrix} = \pm\gamma^{-1}\begin{pmatrix} p \\ q \end{pmatrix}$.

קירובי השברים המשולבים של y: $\frac{p_n}{q_n}$; של x: $\frac{\tilde{p}_n}{\tilde{q}_n}$.

טענה. קיימים N_1,N_2 כך שלכל $m \ge 1$, $\begin{pmatrix} p'_{N_1+m} \\ q'_{N_2+m} \end{pmatrix} = \begin{pmatrix} \tilde{p}_{N_2+m} \\ \tilde{q}_{N_2+m} \end{pmatrix}$.

כלומר, החל ממקום מסוים, תמונתם תחת $\pm\gamma^{-1}$ של קירובי השברים המשולבים של y הם קירובי השברים המשולבים של x, וההתאמה $\begin{pmatrix} p_n \\ q_n \end{pmatrix} \mapsto \begin{pmatrix} p'_n \\ q'_n \end{pmatrix}$ מעבירה קירובים עוקבים לקירובים עוקבים (החל משם).

הוכחה. ע"י החלפת סימני (כל) המספרים r,s,t,u אפשר להניח בה"כ ש-$r-ty>0$.
לכל p,q, $q'=qr-pt$, ולכן אפשר לרשום

$$q'=q\left(r-ty\right)+t\left(qy-p\right) \qquad (*)$$

מ-$(*)$ ומההנחה $r-ty>0$ נובע:

$$\text{אם } \left|qy-p\right|<\frac{r-ty}{|t|}\text{, אז ל-}q\text{ ול-}q'\text{ יש אותו סימן} \qquad (**)$$

(זאת מפני ש-$|q|\geq 1$, ולכן אם $\left|t\left(qy-p\right)\right|<r-ty$ אז $t\left(qy-p\right)$ לא מספיק גדול כדי להשפיע על הסימן של $q\left(r-ty\right)$.)

עבור n מספיק גדול, התנאי בצד ימין של $(**)$ מתקיים עבור $\left(p,q\right)=\left(p_n,q_n\right)$ (כי $\left|q_n y-p_n\right|\to 0$).
לכן ל-q_n ו-q'_n אותו סימן, כלומר המספרים $q_n,q_{n+1},q'_n,q'_{n+1}$ חיוביים ($q_n>0$ לפי הגדרת קירוב לפי שבר משולב...). באופן דומה, עבור n מספיק גדול אפשר להפעיל את $(**)$ עבור
$\left(p,q\right)=\left(p_{n+1}-p_n,q_{n+1}-q_n\right)$, ולקבל ש-$q'_{n+1}-q'_n$ ו-$q_{n+1}-q_n$ שווי-סימן. אבל $q_{n+1}>q_n$, ולכן $q'_{n+1}>q'_n$. נבחר N_1 כך שלכל $n\geq N_1$, מתקיים $0<q'_n<q'_{n+1}<q'_{n+2}<\ldots$.

נראה שאם $n\geq N_1$ ו-$\frac{p_n}{q_n},\frac{p_{n+1}}{q_{n+1}}$ הם קירובים עוקבים של y, אז $\frac{p'_n}{q'_n},\frac{p'_{n+1}}{q'_{n+1}}$ הם הקירובים עוקבים של x.

נשים לב שלכל זוג מספרים p,q, מתקיים (לפי כך ש-$y=\frac{rx+s}{tx+u}$):

$$\begin{aligned}\left|q'x-p'\right|&=\left|\left(-pt+qr\right)x-\left(pu-qs\right)\right|=\left|\left(rx+s\right)q-\left(tx+u\right)p\right|=\\&=\left|\left(tx+u\right)yq-\left(tx+u\right)p\right|=\left|tx+u\right|\left|qy-p\right|\end{aligned}$$

ולכן מתקיים: $\left|q'_n x-p'_n\right|>\left|q'_{n+1}x-p'_{n+1}\right|$ (מכיוון ש-$\left|q_n y-p_n\right|>\left|q_{n+1}y-p_{n+1}\right|$).

עתה, נניח שיש שלמים P',Q' כך ש-$0<Q'<q'_{n+1}$ וגם $\left|Q'x-P'\right|\leq\left|q'_n x-p'_n\right|$.
אז אם נגדיר $\begin{pmatrix} P \\ Q \end{pmatrix}=\gamma\begin{pmatrix} P' \\ Q' \end{pmatrix}$, נקבל

$$\left|Qy-P\right|=\left|tx+u\right|\left|Q'x-P'\right|\leq\left|tx+u\right|\left|q'_n x-p'_n\right|=\left|q_n y-p_n\right|$$

מכיוון ש-n מספיק גדול, נקבל מכך ש-$\left(P,Q\right)$ מקיימים את התנאי בצד ימין של $(**)$, ולכן Q,Q' שווי סימן. באותו אופן, גם $\left(p_{n+1}-P,q_{n+1}-Q\right)$ מקיימים את התנאי בצד ימין של $(**)$, ולכן $q_{n+1}-Q,q'_{n+1}-Q'$ שווי סימן. לכן, מ-$0<Q'<q'_{n+1}$ נקבל $0<Q<q_{n+1}$.

קיבלנו ש- $0<Q<q_{n+1}$ וגם $\left|Qy-P\right|\le\left|q_ny-p_n\right|$, ולכן (מכיוון ש- $\frac{p_n}{q_n}$ קירובי y ע"י שברים משולבים) מתקיים $Q=q_n$ ו- $P=p_n$, כלומר $Q'=q_n'$ ו- $P'=p_n'$. לכן, $\frac{p_n'}{q_n'}$ הם קירובי שברים משולבים של x (לפי ההגדרה של הקירובים הטובים ביותר). **מש"ל.**

2013-04-03

משפט חינצ'ין

סימונים: $\varphi:\mathbb{N}\to\mathbb{R}_+$ (פונקציית שגיאה). λ - מידת לבג על $\mathbb{R}$.

הגדרה. נאמר ש- $\theta\in\mathbb{R}$ הוא φ-מקורב ($\theta\in\varphi\text{-approx}$) אם יש אינסוף פתרונות $(p,q)\in\mathbb{Z}^2$, $q>0$ לאי-השוויון $\left|\theta-\frac{p}{q}\right|<\varphi(q)$.

הערות.

א. המוסכמה כאן היא ש<u>לא דורשים</u> ש- $\frac{p}{q}$ מצומצם. לכן אם $\theta\in\mathbb{Q}$ אז θ הוא φ-מקורב לכל φ.

ב. ע"י הכפלה ב- q מקבלים את הצורה הבאה: $\langle q\theta\rangle<\psi(q)$, כאשר $\psi(q)=q\varphi(q)$.

[משפט (חינצ'ין / Khinchin, 1926).](#)

א. אם $\sum_{q=1}^{\infty}\psi(q)<\infty$ אז $\lambda(\varphi\text{-approx})=0$.

ב. אם $\psi(q)$ מונוטונית יורדת ו- $\sum_{q=1}^{\infty}\psi(q)=\infty$ אז $\lambda(\mathbb{R}\setminus\varphi\text{-approx})=0$.

דוגמה. כל המספרים הם $\frac{1}{q^2}$-מקורבים, לפי משפט דיריכלה, ואכן זה מסתדר עם משפט חינצ'ין, מכיוון שהטור $\sum\frac{1}{q}$. עם זאת, אם נרצה לחזק את התנאי ולהתבונן במספרים $\frac{1}{q^{2+\varepsilon}}$-מקורבים, אז לפי מקרה א' של משפט חינצ'ין, קבוצת המספרים האלה היא ממידת לבג אפס (למרות שהיא G_δ וצפופה ובפרט מקטגוריית Baire גדולה, כפי שראינו בתחילת הקורס). מספרים $\frac{1}{q^2\log q}$-מקורבים – שוב לפי תנאי ב', כמעט כל $\mathbb{R}$.

מסקנה. BA ממידת לבג אפס.

הסבר. $\theta\in\mathrm{BA}$ $\Leftrightarrow$ לכל c, θ אינו $\frac{c}{q^2}$-מקורב $\Leftarrow$ θ אינו $\frac{1}{q^2\log q}$-מקורב. כלומר $\mathrm{BA}\subset\mathbb{R}\setminus\left(\frac{1}{q^2\log q}\text{-approx}\right)$, ולכן ממידה אפס לפי חלק ב' של משפט חינצ'ין.

מקרה ההתכנסות

להוכחת חלק א' של משפט חינצ'ין, נשתמש בלמה של בורל-קנטלי:

למה (Borel-Cantelli, מקרה התכנסות).

נניח ש-$(X,\mathcal{B},\mu)$ מרחב הסתברות (מרחב מידה עם $\mu(X)=1$), ו-$A_1,A_2,\ldots\in\mathcal{B}$.

נסמן $A_\infty=\limsup_{n\to\infty}A_n=\{x : x\in A_n \text{ for } \infty \text{ values of } n\}=\bigcap_{N\ge1}\bigcup_{n\ge N}A_n$.

אם $\sum_{n=1}^{\infty}\mu(A_n)<\infty$ אז $\mu(A_\infty)=0$.

הוכחה (Borel-Cantelli, מקרה התכנסות).

$$\mu(A_\infty)=\mu\left(\bigcap_{N\ge1}\bigcup_{n\ge N}A_n\right)\overset{\text{for all } N}{\le}\mu\left(\bigcup_{n\ge N}A_n\right)\le\sum_{n=N}^{\infty}\mu(A_n)\xrightarrow[\text{Tail of convergent series}]{N\to\infty}0$$

מש"ל.

הוכחה (משפט חינ'צין, חלק א').

נניח ש-$\sum_{q=1}^{\infty}\psi(q)<\infty$.

כדי להוכיח ש-$\lambda(\varphi\text{-approx})=0$, די להוכיח שלכל $k\in\mathbb{Z}$, $\lambda(\varphi\text{-approx}\cap[k,k+1])=0$.

לפי הגדרתה, הקבוצה φ-approx היא אינווריאנטית להזזות בשלמים: $\theta\in\varphi\text{-approx}$ $\Leftrightarrow$ $\theta+k\in\varphi\text{-approx}$ לכל $k\in\mathbb{Z}$. לכן, די להוכיח ש-$\lambda(\varphi\text{-approx}\cap[0,1])=0$.

נפעיל את הלמה של בורל-קנטלי במרחב ההסתברות שהוא הקטע $[0,1]$ עם מידת לבג.

$\theta\in\varphi\text{-approx}$ $\Leftrightarrow$ $\left|\theta-\frac{p}{q}\right|<\varphi(q)$ עבור אינסוף p,q $\Leftrightarrow$ יש אינסוף p,q כך ש-

$\theta\in\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)$. עבור $\theta\in(0,1)$, מאחר ש-$\varphi(q)\to0$, אם $\theta\in\varphi\text{-approx}$ אז יש

אינסוף p,q כך ש-$\frac{p}{q}\in(0,1)$ ו-$\theta\in\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)$.

לכן, בסימונים של בורל-קנטלי: $\varphi\text{-approx}\cap[0,1]=A_\infty$, כאשר

$$A_1,A_2,\ldots=\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)\quad\left(p,q\in\mathbb{Z},q>0,\frac{p}{q}\in(0,1)\right).$$

$$\sum_{n=1}^{\infty}\lambda(A_n)=\sum_{q=1}^{\infty}\sum_{\substack{0\le p<q\\ p\text{ integer}}}\lambda\left([0,1]\cap\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)\right)\le$$

$$\le\sum_{q=1}^{\infty}\sum_{\substack{0\le p<q\\ p\text{ integer}}}2\varphi(q)=2\sum_{q=1}^{\infty}q\varphi(q)<\infty$$

ולכן מבורל-קנטלי, $\lambda(A_\infty)=\lambda(\varphi\text{-approx}\cap[0,1])=0$.

מש"ל.

מקרה ההתבדרות

להוכחת חלק ב', נזדקק למקרה ההתבדרות בלמה של בורל-קנטלי.
מקרה ההתבדרות הוא לא משפט אחד אלא אוסף של משפטים מהצורה הבאה:

$\sum_{n=1}^{\infty}\mu(A_n)=\infty$ + תנאי נוסף $\Leftarrow$ $\mu(A_\infty)>0$ (בתנאים מסויימים) או $\mu(A_\infty)=1$ (בתנאים מסויימים).

דוגמה שמראה שמקרה ההתבדרות אינו נכון ללא הנחות נוספות: המרחב שלנו – הקטע $[0,1]$ עם מידת לבג, ו-$A_n=\left(0,\frac{1}{n}\right)$. אז $A_\infty=\varnothing$ ולכן $\mu(A_\infty)=0$. אבל $\sum_{n=1}^{\infty}\mu(A_n)=\infty$.

נוכיח את שתי הגרסאות הבאות של מקרה ההתבדרות בלמה של בורל-קנטלי:

משפט (Rényi).
נניח ש-$(X,\mathcal{B},\mu)$ מרחב הסתברות, $A_1,A_2,\ldots\in\mathcal{B}$, ונסמן $A_\infty=\limsup_{n\to\infty}A_n$.
אם $\sum_{n=1}^{\infty}\mu(A_n)=\infty$, וקיים $C\geq 1$ כך שלכל $n\neq m$, $\mu(A_n\cap A_m)\leq C\mu(A_n)\mu(A_m)$, אזי $\mu(A_\infty)\geq\frac{1}{C}$.

הערה. לתנאי $\mu(A_n\cap A_m)\leq C\mu(A_n)\mu(A_m)$ קוראים לפעמים "אי-תלות חלשה".

הגרסה הבאה היא הכללה של משפט Rényi:

משפט (Paley-Zigmund).
נניח ש-$(X,\mathcal{B},\mu)$ מרחב הסתברות, $A_1,A_2,\ldots\in\mathcal{B}$, ונסמן $A_\infty=\limsup_{n\to\infty}A_n$.
אם $\sum_{n=1}^{\infty}\mu(A_n)=\infty$, וקיים $C\geq 1$ כך שיש אינסוף ערכים של N עבורם $\sum_{n,m=1}^{N}\mu(A_m\cap A_n)\leq C\left(\sum_{n=1}^{N}\mu(A_n)\right)^2$, אז $\mu(A_\infty)\geq\frac{1}{C}$.

הוכחה (משפט Rényi כמסקנה ממשפט Paley-Zigmund).
אם C כמו בהנחת משפט Rényi, ניקח $C_0>C$. נראה מיד שהנחות משפט Paley-Zigmund מתקיימות עבור C_0, ואז נסיק $\mu(A_\infty)\geq\frac{1}{C_0}$. מכיוון ש-$C_0$ שרירותי נקבל $\mu(A_\infty)\geq\frac{1}{C}$.

$$\sum_{n,m=1}^{N}\mu(A_n\cap A_m)=\sum_{n=1}^{N}\mu(A_n)+\sum_{\substack{n\neq m\\1\leq n,m\leq N}}\mu(A_n\cap A_m)\leq$$

$$\leq\sum_{n=1}^{N}\mu(A_n)+C\sum_{\substack{n\neq m\\1\leq n,m\leq N}}\mu(A_n)\mu(A_m)\leq$$

$$\leq\underbrace{\sum_{n=1}^{N}\mu(A_n)}_{I_N}+C\sum_{n,m=1}^{N}\mu(A_n)\mu(A_m)=I_N+CI_N^2=I_N^2\left(C+\frac{1}{I_N}\right)$$

אבל מהנתון, $I_N \xrightarrow{N\to\infty} \infty$, ולכן עבור N מספיק גדול,

$$\sum_{n,m=1}^{N} \mu\left(A_n \cap A_m\right) \le C_0 I_N^{\,2} = C_0\left(\sum_{n=1}^{N}\mu\left(A_n\right)\right)^2$$

וממשפט Paley-Zigmund נקבל $\mu\left(A_\infty\right) \ge \frac{1}{C_0}$.

מש"ל.

הוכחה (משפט Paley-Zigmund).

נסמן: $A_{M,N} = \bigcup_{n=M}^{N} A_n$; $S_{M,N} = \sum_{n=M}^{N} \mathbf{1}_{A_n}$ (סכום של פונקציות אינדיקטור); $S_N = S_{1,N}$. מתקיים:

$$\mu\left(A_\infty\right) = \mu\left(\bigcap_{M\ge 1}\bigcup_{n\ge M} A_n\right) = \lim_{M\to\infty}\mu\left(\bigcup_{n\ge M} A_n\right) = \lim_{M\to\infty}\lim_{N\to\infty}\mu\left(A_{M,N}\right)$$

לכן, רוצים להעריך מלמטה את $\mu\left(A_{M,N}\right)$. ליתר דיוק, רוצים להוכיח שלכל M, $\lim_{N\to\infty}\mu\left(A_{M,N}\right) \ge \frac{1}{C}$.

$$\left(\int_X S_{M,N}\,d\mu\right)^2 \overset{\text{When } x\notin A_{M,N} \text{ we have } S_{M,N}(x)=0}{=} \left(\int_X \mathbf{1}_{A_{M,N}} S_{M,N}\,d\mu\right)^2 \overset{\text{Cauchy-Schwarz}}{\le}$$

$$\le \int_X \mathbf{1}_{A_{M,N}}^{\,2}\,d\mu \cdot \int_X S_{M,N}^{\,2}\,d\mu = \mu\left(A_{M,N}\right)\int_X S_{M,N}^{\,2}\,d\mu$$

לכן:

$$\mu\left(A_{M,N}\right) \ge \frac{\left(\int_X S_{M,N}\,d\mu\right)^2}{\int_X S_{M,N}^{\,2}\,d\mu}$$

נסמן:

$$V_N = V_{1,N} \qquad V_{M,N} = \int_X S_{M,N}^{\,2}\,d\mu = \sum_{M\le m,n\le N}\mu\left(A_m \cap A_n\right)$$

$$E_N = E_{1,N} \qquad E_{M,N} = \int_X S_{M,N}\,d\mu = \sum_{n=M}^{N}\mu\left(A_n\right)$$

כלומר, בסימונים אלה, הוכחנו: $\mu\left(A_{M,N}\right) \ge \frac{E_{M,N}^{\,2}}{V_{M,N}}$. בפרט ($M=1$): $E_N^{\,2} \le V_N$.

עפ"י הנתון, עבור אינסוף ערכי N, $\sum_{n,m=1}^{N}\mu\left(A_m \cap A_n\right) \le C\left(\sum_{n=1}^{N}\mu\left(A_n\right)\right)^2$.

בסימונים שלנו, זה אומר שעבור אינסוף ערכי N, מתקיים $\frac{E_N^{\,2}}{V_N} \ge \frac{1}{C}$. לכן:

$$\frac{E_{M,N}^{\,2}}{V_{M,N}} \overset{V_{M,N}\le V_N}{\ge} \frac{\left(E_N - E_{M-1}\right)^2}{V_N} \overset{E_{M-1}\ge 0}{\ge} \frac{E_N^{\,2}}{V_N} - \frac{2E_N E_{M-1}}{V_N} = \frac{E_N^{\,2}}{V_N} - \frac{2E_N^{\,2}}{V_N}\cdot\frac{E_{M-1}}{E_N}$$

כעת: לאורך תת-סדרה של N-ים, $\frac{E_N^2}{V_N} \geq \frac{1}{C}$; הביטוי $\frac{2E_N^2}{V_N}$ חסום; והביטוי $\frac{E_{M-1}}{E_N}$ שואף לאפס, כאשר M קבוע ו-$N \to \infty$. לכן בהינתן M קבוע, $\liminf_{N\to\infty} \frac{E_{M,N}^2}{V_{M,N}} \geq \frac{1}{C}$, ולכן $\lim_{N\to\infty} \mu\left(A_{M,N}\right) \geq \frac{1}{C}$ כנדרש.

מש"ל.

בעזרת משפט Paley-Zigmund ניתן להוכיח את מקרה ההתבדרות במשפט חינצ'ין:

הטענה שיש להוכיח: אם $\psi(q)$ מונוטונית יורדת ו-$\sum_{q=1}^{\infty} \psi(q) = \infty$ אז $\lambda(\mathbb{R} \setminus \varphi\text{-approx}) = 0$.

הוכחה (משפט חינ'צין, חלק ב').

ראשית, מספר רדוקציות:

- כמו בחלק א', מספיק להוכיח ש-$\lambda\left(\left[0,1\right] \cap \left(\varphi\text{-approx}\right)^c\right) = 0$.
- אפשר להניח ש-$\psi(q) \leq \frac{1}{2}$ לכל q. זאת מפני שאם $\psi(q) > \frac{1}{2}$ לאינסוף q-ים אז $\psi(q) \geq \frac{1}{2}$ לכל q כי ψ מונוטונית, וממשפט דיריכלה, כל θ הוא φ-מקורב. לכן נותר המקרה ש-$\psi(q) \leq \frac{1}{2}$ כמעט לכל q, ונשפר זאת ל-"לכל q" ע"י לקיחת מינימום בין ψ ל-$\frac{1}{2}$ (מכיוון שגם ככה כמעט לכל q מתקיים $\psi(q) \leq \frac{1}{2}$, זה לא משנה את קבוצת ה-φ-מקורבים).

ההוכחה מורכבת מ-2 שלבים:

- שלב ראשון: נוכיח באמצעות משפט Paley-Zigmund ש-$\lambda\left(\left[0,1\right] \cap \varphi\text{-approx}\right) > 0$.
- שלב שני (בשיעור הבא): נוכיח באמצעות טענת ארגודיות ש-$\lambda\left(\left(\varphi\text{-approx}\right)^c\right) = 0$.

שלב ראשון – הוכחה ש-$\lambda\left(\left[0,1\right] \cap \varphi\text{-approx}\right) > 0$

סימון: $\phi(q)$ פונקציית אוילר (Euler totient function), כלומר סדר החבורה הכפלית מודולו q.

<u>טענת עזר 1.</u> יש $C > 0$ כך שאם $\psi(q)$ פונקציה מונוטונית יורדת, $\sum_{q=1}^{N} \frac{\phi(q)}{q} \psi(q) \geq C \sum_{q=1}^{N} \psi(q)$.

<u>הערה.</u> בטענת העזר הזו משתמשים בצורה הכי רצינית בהנחה ש-ψ מונוטונית יורדת. יש בעיה פתוחה, **<u>השערת Duffin-Schaeffer (1941)</u>**, שאם היא נכונה אז ניתן לוותר על ההנחה ש-ψ מונוטונית יורדת, אם מחליפים במשפט חינצ'ין את התנאי $\sum \psi(q) = \infty$ בתנאי $\sum \frac{\phi(q)}{q} \psi(q) = \infty$.

<u>טענת עזר 2.</u> לכל $A \geq 1$ ולכל $q, s \in \mathbb{N}$, מספר הזוגות $(p, r) \in \mathbb{Z}^2$ המקיימים $0 < |ps - rq| < A \quad (*)$, $0 < r < s$, $0 < p < q$ הוא לכל היותר $2A$.

<u>פירוש גיאומטרי לטענת עזר 2.</u> ברגע שקובעים q, s, ניתן להסתכל על הישר $xs - yq = 0$. הטענה חוסמת את כמות נקודות השריג $\mathbb{Z}^2$ הקרובות לישר הזה.

<u>הוכחת טענת עזר 2.</u> נסמן $n=\gcd(q,s)$, $q'=\frac{q}{n}$, $s'=\frac{s}{n}$. אז מ-$(*)$, נובע $0<|ps'-rq'|<\frac{A}{n}$, לכן יש a שלם המקיים $0<|a|<\frac{A}{n}$ כך ש- $ps'=rq'+a$, כלומר $ps'\equiv a \pmod{q'}$. מכיוון ש- s',q' זרים, בהינתן a יש פתרון יחיד עבור p לקונגרואנציה הזו, כלומר פתרון יחיד עבור $0<p<q'$, ולכן n פתרונות עבור $0<p<q$. אם a,p ידועים אז גם r נקבע ע"י $ps'=rq'+a$, לכן יש לכל היותר n פתרונות (p,r). מכיוון שיש לכל היותר $\frac{2A}{n}$ ערכים אפשריים של a, מספר כל הפתרונות הוא לכל היותר $\frac{2A}{n}\cdot n=2A$. <u>מש"ל.</u>

נשלים את הוכחת הצעד הראשון (בהינתן טענת עזר 1 שטרם הוכחנו ו-2 שהוכחנו).

יהי C כמו בטענת עזר 1, ונגדיר $A_q=\bigcup_{\substack{0\le p\le q\\ \gcd(p,q)=1}}\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)$.

נוכיח שתנאי משפט Paley-Zigmund מתקיימים (עם $\frac{2}{C^2}$ במקום C), ומכך נקבל מיד את הדרוש.

נשים לב ש- A_q הוא <u>איחוד של קטעים זרים</u>; זאת מפני שעבור $p\neq p'$, המרחק בין המרכזים של הקטעים הוא לפחות $\frac{1}{q}$, ומכיוון שהנחנו ש- $\psi(q)\le\frac{1}{2}$, רדיוס הקטעים הוא לכל היותר $\frac{1}{2q}$. לכן:

$$\lambda(A_q)=2\varphi(q)\cdot\#\{p:0\le p\le q,\gcd(p,q)=1\}=2\phi(q)\varphi(q)$$

$$\sum_{q=1}^{N}\lambda(A_q)=2\sum_{q=1}^{N}\phi(q)\varphi(q)=2\sum_{q=1}^{N}\frac{\phi(q)}{q}\psi(q)\overset{\text{Proposition 1}}{\ge}2C\sum_{q=1}^{N}\psi(q)\xrightarrow{N\to\infty}\infty$$

לכן התנאי הראשון ב-Paley-Zigmund מתקיים. לבדיקת התנאי השני, צריך להעריך את $\sum_{1\le q,s\le N}\lambda(A_q\cap A_s)$:

נניח $q\neq s$ ונניח שאחד הקטעים בהגדרת A_q נחתך עם אחד הקטעים בהגדרת A_s.

כלומר, $\left(\frac{p}{q}-\varphi(q),\frac{p}{q}+\varphi(q)\right)\cap\left(\frac{r}{s}-\varphi(s),\frac{r}{s}+\varphi(s)\right)\neq\varnothing$ כאשר $0<r<s$, $0<p<q$, $1=\gcd(r,s)=\gcd(p,q)$. לכן $\frac{p}{q}\neq\frac{r}{s}$ (אחרת אחד השברים לא היה מצומצם...) ומתקיים:

$$0<\left|\frac{p}{q}-\frac{r}{s}\right|<\varphi(q)+\varphi(s)$$

(צד ימין כי אלה מרכזים של שני קטעים נחתכים עם רדיוסים $\varphi(q),\varphi(s)$). כלומר, ע"י הכפלה ב- qs:

$$0<|ps-rq|<qs(\varphi(q)+\varphi(s))$$

ולכן, לפי טענת עזר 2, מספר הזוגות של קטעים שנחתכים הוא לכל היותר $2A$, כאשר

$$2A=2qs(\varphi(q)+\varphi(s))=2s\psi(q)+2q\psi(s)\le 4\max\{s\psi(q),q\psi(s)\}$$

והאורך של כל חיתוך הוא לכל היותר האורך של הקטע הקצר מבין השניים, שהוא $2\min\left\{\varphi(s),\varphi(q)\right\}$, או $2\min\left\{\frac{\psi(s)}{s},\frac{\psi(q)}{q}\right\}$. לכן:

$$\lambda\left(A_q\cap A_s\right)\le 8\max\left\{s\psi(q),q\psi(s)\right\}\min\left\{\frac{\psi(s)}{s},\frac{\psi(q)}{q}\right\}=8\psi(q)\psi(s)$$

(את השוויון האחרון ניתן להוכיח ע"י חלוקה למקרים ושימוש במונוטוניות של ψ.) לכן:

$$\sum_{1\le q\ne s\le N}\lambda\left(A_q\cap A_s\right)\le 8\sum_{q,s=1}^{N}\psi(q)\psi(s)\le 8\left(\sum_{q=1}^{N}\psi(q)\right)^2\le$$

$$\le 8\left(\frac{1}{C}\sum_{q=1}^{N}\frac{\phi(q)}{q}\psi(q)\right)^2\le\frac{2}{C^2}\left(\sum_{q=1}^{N}\lambda\left(A_q\right)\right)^2$$

נוסיף את האלכסון להערכה ונקבל:

$$\sum_{1\le q,s\le N}\lambda\left(A_q\cap A_s\right)\le\sum_{q=1}^{N}\lambda\left(A_q\right)+\frac{2}{C^2}\left(\sum_{q=1}^{N}\lambda\left(A_q\right)\right)^2$$

אבל $\sum_{q=1}^{\infty}\lambda\left(A_q\right)=\infty$. לכן לכל $\tilde{C}>\frac{2}{C^2}$ מתקיים $\sum_{1\le q,s\le N}\lambda\left(A_q\cap A_s\right)\le\tilde{C}\left(\sum_{q=1}^{N}\lambda\left(A_q\right)\right)^2$ עבור N מספיק גדול; המסקנה מ-Paley-Zigmund תהיה נכונה לכל $\tilde{C}>\frac{2}{C^2}$ שרירותי ולכן גם עבור $C=\frac{2}{C^2}$.

בזאת סיימנו את כל הצעד הראשון בהוכחה של חלק ב' במשפט חינצ'ין, פרט לטענת עזר 1:

<u>טענת עזר 1.</u> יש $C>0$ כך שאם $\psi(q)$ פונקציה מונוטונית יורדת, $\sum_{q=1}^{N}\frac{\phi(q)}{q}\psi(q)\ge C\sum_{q=1}^{N}\psi(q)$.

<u>הוכחת טענת עזר 1.</u>
ניעזר בפונקציית מביוס:

$$\mu(d)=\begin{cases}(-1)^s & d=p_1\cdots p_s \text{ product of distinct primes}\\ 0 & \text{otherwise}\end{cases}$$

מ<u>נוסחת ההיפוך של מביוס</u>, נובע:

$$\frac{\phi(q)}{q}=\sum_{0<d\mid q}\frac{\mu(d)}{d}$$

מכאן:

$$\frac{1}{Q}\sum_{1\le q\le Q}\frac{\phi(q)}{q}=\frac{1}{Q}\sum_{1\le q\le Q}\sum_{\substack{d\mid q\\0<d}}\frac{\mu(d)}{d}\overset{\substack{\text{Exchange order}\\\text{of summation}}}{=}\frac{1}{Q}\sum_{1\le d\le Q}\frac{\mu(d)}{d}\sum_{\substack{1\le q\le Q\\d\mid q}}1=\frac{1}{Q}\sum_{1\le d\le Q}\frac{\mu(d)}{d}\left\lfloor\frac{Q}{d}\right\rfloor\overset{\lfloor x\rfloor=x+O(1)}{=}$$

$$=\sum_{d=1}^{Q}\frac{\mu(d)}{d^2}+\frac{1}{Q}\sum_{d=1}^{Q}\left(\frac{\mu(d)}{d}O(1)\right)\xrightarrow{Q\to\infty}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$$

לכן קיים $\lim_{Q\to\infty}\frac{1}{Q}\sum_{1\le q\le Q}\frac{\phi(q)}{q}$, ולכן קיים $C_1>0$ כך שלכל Q, $\sum_{1\le q\le Q}\frac{\phi(q)}{q}\ge C_1Q$.

נכתוב: $\chi(Q)=\sum_{q=1}^{Q}\frac{\phi(q)}{q}\ge C_1Q$. כעת, בהינתן ψ מונוטונית יורדת,

$$\begin{aligned}\sum_{q=1}^{Q}\frac{\phi(q)}{q}\psi(q)&=\sum_{q=1}^{Q}\psi(q)\big(\chi(q)-\chi(q-1)\big)\overset{\text{Abel transformation}}{=}\\&=\left(\sum_{q=1}^{Q-1}\chi(q)\big(\psi(q)-\psi(q+1)\big)\right)+\chi(Q)\psi(Q)\ge\\&\ge\left(\sum_{1\le q<Q}C_1q\big(\psi(q)-\psi(q+1)\big)\right)+C_1Q\psi(Q)\overset{\text{Abel transformation}}{=}\\&=C_1\psi(2)+C_1\sum_{1<q\le Q}\psi(q)\end{aligned}$$

כנדרש בטענת העזר (עד כדי בחירה נכונה של C עבור הערכים הראשונים).
<u>מש"ל.</u>

2013-04-17

תזכורת מהשיעור שעבר – משפט חינצ'ין.

<u>הגדרה:</u> תהי $\varphi:\mathbb{N}\to\mathbb{R}_+$ ונסמן $\psi(q)=q\varphi(q)$. אז $\theta\in\mathbb{R}$ הוא φ-מקורב אם יש אינסוף פתרונות שונים ב- $p\in\mathbb{Z},q\in\mathbb{N}$ לאי-השוויון $\left|\theta-\frac{p}{q}\right|<\varphi(q)\iff\theta\in B\left(\frac{p}{q},\varphi(q)\right)\iff|q\theta-p|<\psi(q)$.

נסמן ב- λ את מידת לבג ב- $\mathbb{R}$.

<u>משפט חינצ'ין:</u>

א. אם $\sum_{q=1}^{\infty}\psi(q)<\infty$ אז $\lambda(\varphi\text{-approx})=0$.

ב. אם $\sum_{q=1}^{\infty}\psi(q)=\infty$ וגם ψ פונקציה יורדת אז $\lambda\left((\varphi\text{-approx})^C\right)=0$.

בשיעור שעבר התחלנו וכמעט סיימנו להוכיח את משפט חינצ'ין. השלבים בהוכחה:

לסעיף א' (מקרה ההתכנסות), משתמשים בכך ש-θ הוא φ-מקורב $\iff$ המאורע $\theta\in B\left(\frac{p}{q},\varphi(q)\right)$ מתרחש אינסוף פעמים, ובמשתמשים בלמה של Borel-Cantelli.

לסעיף ב' (מקרה ההתבדרות), יש להשתמש בגרסת התבדרות של Borel-Cantelli המשתמשת בגרסה כלשהי של אי-תלות, למשל משפט Rényi או (כמו בהוכחה שראינו) משפט Paley-Zigmund.

ראינו שמתקיים:

$$\sum_{q=1}^{\infty}\sum_{p=0}^{q}\lambda\left(\frac{p}{q},\varphi(q)\right)\simeq\sum_{q=1}^{\infty}\frac{\phi(q)}{q}\psi(q)\overset{\text{Assuming }\psi\text{ is decreasing}}{\simeq}\sum_{q=1}^{\infty}\psi(q)$$

בשלב הראשון של ההוכחה, הוכחנו: $\lambda(\phi\text{-approx})>0$. נותר להוכיח: $\lambda\left((\varphi\text{-approx})^C\right)=0$.

שלב שני – הוכחה ש- $\lambda\left(\left(\varphi\text{-approx}\right)^C\right)>0$

לצורך השלב הזה בהוכחה, נזדקק לטענה הבאה:

טענה (הארגודיות של פעולת $\mathbb{Q}$ על $\mathbb{R}$).
תהי $A\subset\mathbb{R}$ מדידה, $\lambda(A)>0$, ונניח ש- $A=A+\mathbb{Q}$. אזי $\lambda\left(A^C\right)=0$.

נוכיח את הטענה בהמשך. כעת נסיים את הוכחת משפט חינצ'ין.
ידוע כבר מהשלב הראשון ש- $\lambda\left(\varphi\text{-approx}\right)>0$, ולכן אם נוכיח שהקבוצה $\varphi\text{-approx}$ אינווריאנטית להזזות ברציונליים, נקבל מהארגודיות של פעולת $\mathbb{Q}$ על $\mathbb{R}$ ש- $\lambda\left(\left(\varphi\text{-approx}\right)^C\right)=0$ כנדרש.

בהינתן $\frac{p_0}{q_0}\in\mathbb{Q}$, נבדוק מה הקשר בין θ לבין $\theta+\frac{p_0}{q_0}$ ביחס ל- $\varphi\text{-approx}$:
$\theta\in\varphi\text{-approx}$ $\Leftrightarrow$
$\Leftrightarrow$ לאי-השוויון $\left|\theta-\frac{p}{q}\right|<\varphi(q)$ יש אינסוף פתרונות ב- $p\in\mathbb{Z},q\in\mathbb{N}$ $\Leftrightarrow$
$\Leftrightarrow$ לאי-השוויון $\left|\left(\theta+\frac{p_0}{q_0}\right)-\left(\frac{p}{q}+\frac{p_0}{q_0}\right)\right|<\varphi(q)$ יש אינסוף פתרונות ב- $p\in\mathbb{Z},q\in\mathbb{N}$.

אבל באי-השוויון האחרון, מקרבים את $\theta+\frac{p_0}{q_0}$ ע"י מספר רציונלי שהמכנה שלו הוא qq_0, ולא q. כלומר צריך אינסוף פתרונות להערכה $<\varphi(qq_0)$, ולא להערכה $<\varphi(q)$.
ניעזר בתרגיל הבא:

תרגיל.
תהי $\psi(q)$ כך ש- $\sum_{q=1}^{\infty}\psi(q)=\infty$ ו- ψ יורדת, ונסמן $\varphi(q)=\frac{\psi(q)}{q}$.
אזי קיימת $\psi_0(q)$ כך ש-

א. $\sum_{q=1}^{\infty}\psi_0(q)=\infty$.

ב. ψ_0 יורדת.

ג. אם נסמן $\varphi_0(q)=\frac{\psi_0(q)}{q}$, אז לכל q_0, החל ממקום מסוים מתקיים $\varphi_0(q)<\varphi(qq_0)$.

(**הערה:** התרגיל הזה נובע מיידית מתרגיל 10 בדף התרגילים ולמעשה שקול לו.)
בהינתן התרגיל, אם $\theta\in\varphi_0\text{-approx}$ אז לכל $\frac{p_0}{q_0}$, $\theta+\frac{p_0}{q_0}\in\varphi\text{-approx}$. לפי החלק הראשון של ההוכחה (עם φ_0 במקום φ), $\lambda\left(\varphi_0\text{-approx}\right)>0$. נסמן $A=\varphi_0\text{-approx}+\mathbb{Q}\subset\varphi\text{-approx}$.
אז בבירור A אינווריאנטית להזזות $\mathbb{Q}$ ו- $\lambda(A)>0$, ולכן $\lambda\left(\left(\varphi\text{-approx}\right)^C\right)\le\lambda\left(A^C\right)=0$.

מש"ל.

הארגודיות של פעולת $\mathbb{Q}$ על $\mathbb{R}$

כעת נוכיח את טענת הארגודיות שהשתמשנו בה במהלך השלב האחרון של ההוכחה:

טענה (הארגודיות של פעולת $\mathbb{Q}$ על $\mathbb{R}$).
תהי $A \subset \mathbb{R}$ מדידה, $\lambda(A) > 0$, ונניח ש- $A = A + \mathbb{Q}$. אזי $\lambda(A^C) = 0$.

ניתן שתי הוכחות לטענה. ההוכחה הראשונה – בעזרת המשפט הבא:

<u>משפט הצפיפות של לבג.</u> אם $\lambda(A) > 0$ אז יש $x_0 \in A$ כך שלכל $\varepsilon > 0$ יש r_0 כך שלכל קטע פתוח I המכיל את x_0 ואורכו לכל היותר r_0 מתקיים $\frac{\lambda(I \cap A)}{\lambda(I)} \geq 1 - \varepsilon$.

<u>הערה.</u> נקודה $x_0 \in A$ המקיימת את האמור נקראת <u>נקודת צפיפות</u> של A. למעשה, המשפט מתקיים כמעט בכל מקום ביחס ל- $x_0 \in A$.

הוכחה 1 לטענת הארגודיות.
תהי x_0 נקודת צפיפות של A. נניח בשלילה ש- $\lambda(A^C) > 0$, ותהי x_1 נקודת צפיפות של A^C. ניקח $\varepsilon < \frac{1}{2}$, וניקח r_0 כמו במשפט הצפיפות של לבג, עבור $x_0 \in A$ ו- $x_1 \in A^C$.
נבחר קטע I פתוח סביב x_0 עם אורך קטן מ- r_0, ו- $t \in \mathbb{Q}$ כך ש- $t + I$ קטע סביב x_1. נקבל:

$$\frac{1}{2} < \frac{\lambda(A \cap I)}{\lambda(I)} \overset{\lambda \text{ is translation invariant}}{=} \frac{\lambda((A+t) \cap (I+t))}{\lambda(I+t)} \overset{A=A+t}{=} \frac{\lambda(A \cap (I+t))}{\lambda(I+t)}$$

אבל גם $\frac{1}{2} > \frac{\lambda(A^C \cap (I+t))}{\lambda(I+t)}$. סתירה.

מש"ל.

ההוכחה השנייה – בעזרת משפט ההצגה של Riesz:

יהי X מרחב האוסדורף קומפקטי-מקומית, μ מידת בורל ב- X, והיא מידה רגולרית/מידת Radon, כלומר:

א. אם $K \subset X$ קומפקטית אז $\mu(K) < \infty$.
ב. לכל A מדידה, $\mu(A) = \inf\{\mu(U) : A \subset U \text{ open}\}$.
ג. לכל U פתוחה, $\mu(U) = \sup\{\mu(K) : U \supset K \text{ compact}\}$

<u>הערה.</u> אם $X = \mathbb{R}$ אז כל מידת בורל היא Radon אם ורק אם דרישה א' מתקיימת. (כלומר ב' וג' נובעות מזה.)

<u>סימון.</u>

- $C_C(X)$ פונקציות רציפות בעלות תומך קומפקטי ב- X.
  (כאן, תומך – הסגור של הקבוצה בה הפונקציה לא מתאפסת.)

- פונקציונל לינארי $\Lambda : C_C(X) \to \mathbb{R}$ נקרא <u>חיובי</u> אם לכל $\varphi \geq 0$, $\Lambda(\varphi) \geq 0$.

<u>משפט ההצגה של Riesz</u> (לפעמים Riesz-Markov-Katkutani).
ההעתקה $\mu \mapsto \Lambda_\mu(\varphi) = \int_X \varphi d\mu$ היא התאמה חח"ע ועל בין מידות בורל שהן מידות Radon על X לבין פונקציונלים לינאריים חיוביים על $C_C(X)$.

<u>מסקנה.</u> אם μ_1, μ_2 מידות בורל ו-Radon כך ש- $\int_X \varphi d\mu_1 = \int_X \varphi d\mu_2$ לכל $\varphi \in C_C(X)$ אזי $\mu_1 = \mu_2$.
<u>הסבר.</u> נובע מיידית ממשפט Riesz (חח"ע).

<u>מסקנה.</u> תהי μ מידת בורל ו-Radon על $\mathbb{R}$. נסמן ב- $\mathbb{R}_\mu$ את <u>המייצב</u> של המידה:

$$\mathbb{R}_\mu = \left\{ x \in \mathbb{R} : \mu(A+x) = \mu(A) \quad \forall A \in \text{Borel}(\mathbb{R}) \right\}$$

אז $\mathbb{R}_\mu$ חבורה <u>סגורה</u>.

<u>הערה.</u> זה נכון גם לכל פעולה של חבורה טופולוגית על מרחב האוסדורף קומפקטי-מקומית.

<u>הוכחת המסקנה השנייה.</u>
נניח $x_1, x_2, \ldots$ סדרה ב- $\mathbb{R}_\mu$ המתכנסת לגבול x_∞; צ"ל $x_\infty \in \mathbb{R}_\mu$.
כלומר, צריך להוכיח שלכל קבוצת בורל $A \subset \mathbb{R}$, $\mu(A + x_\infty) = \mu(A)$.
לפי משפט Riesz, די להוכיח שלכל $\varphi \in C_C(\mathbb{R})$, $\int_{\mathbb{R}} \varphi(t + x_\infty) d\mu(t) = \int_{\mathbb{R}} \varphi(t) d\mu(t)$.

$$\int_{\mathbb{R}} \varphi(t + x_\infty) d\mu(t) = \int_{\mathbb{R}} \varphi\left(\lim_{n\to\infty}(t + x_n)\right) d\mu(t) \overset{\varphi \text{ is continuous}}{=} \int_{\mathbb{R}} \lim_{n\to\infty} \varphi(t + x_n) d\mu(t) \overset{\text{DCT}}{=}$$

$$= \lim_{n\to\infty} \int_{\mathbb{R}} \varphi(t + x_n) d\mu(t) \overset{x_n \in \mathbb{R}_\mu}{=} \lim_{n\to\infty} \int_{\mathbb{R}} \varphi(t) d\mu(t) = \int_{\mathbb{R}} \varphi(t) d\mu(t)$$

בשימוש במשפט ההתכנסות הנשלטת לעיל, משתמשים בכך שהפונקציה φ רציפה ובעלת תומך קומפקטי, לכן כמעט כל ההזזות $\varphi(t + x_n)$ נתמכות ע"י תומך משותף שהוא הזזה בקצת של התומך של φ (כי x_n סדרת קושי), ואפשר לקחת בתור פונקציה שולטת אינטגרבילית את הפונקציה השווה ל- $\sup \varphi$ בתומך ו- 0 מחוץ לתומך.
<u>מש"ל.</u>

הוכחה 2 לטענת הארגודיות.
נגדיר מידת בורל: $\mu(B) = \lambda(A \cap B)$ לכל קבוצת בורל B.
לכל B, $\mu(B) \leq \lambda(A)$ ולכן μ מידה סופית, ובפרט סופית על קבוצות קומפקטיות, ולכן מידת Radon.
לכל $t \in \mathbb{Q}$,

$$\mu(B+t) = \lambda(A \cap (B+t)) \overset{A+t=A}{=} \lambda((A+t) \cap (B+t)) =$$

$$= \lambda((A \cap B) + t) \overset{\text{Lebesgue measure is translation-invariant}}{=} \lambda(A \cap B) = \mu(B)$$

לכן $\mathbb{R}_\mu$ מכילה את $\mathbb{Q}$. ומאחר ש- $\mathbb{R}_\mu$ סגורה, $\mathbb{R}_\mu = \mathbb{R}$.
כלומר, $\mu(B+x) = \mu(B)$ לכל $x \in \mathbb{R}$ ו- B בורל.

אבל יש רק מידת ראדון אחת שאינווריאנטית להזזות ב- $\mathbb{R}$ (עד כדי כפל בסקלר) והיא מידת לבג.
לכן: $\mu(B)=c\lambda(B)$ לכל B בורל.
נציב $B=A$ ונקבל $\lambda(A)=\lambda(A\cap A)=\mu(A)=c\lambda(A)$ ומכיוון ש- $\lambda(A)>0$ נקבל $c=1$.
כלומר, $\mu=\lambda$. מכאן:

$$\lambda\left(A^C\right)=\mu\left(A^C\right)=\lambda\left(A^C\cap A\right)=\lambda(\varnothing)=0$$

מש"ל.

כיוון להוכחה שלישית. לוקחים את פונקציית האינדיקטור של A ומתבוננים בטרנספורם פורייה שלה. משתמשים בכך שזה גם טרנספורם פורייה של האינדיקטור של $A+t$ לכל $t\in\mathbb{Q}$.

משפט חינצ'ין-גרושב – הגרסה הרב-מימדית של משפט חינצ'ין

הבעיה. תהי $X=\left(x_{ij}\right)\in M_{m,n}(\mathbb{R})$. עבור $q\in\mathbb{Z}^m$ שכתוב כוקטור שורה (כך ש- qX הגיוני), נסמן:

$$\langle qX\rangle=\operatorname{dist}\left(qX,\mathbb{Z}^n\right)$$

נאמר ש- X הוא ψ-מקורב אם יש אינסוף פתרונות $q\in\mathbb{Z}^m$ לאי-השוויון $\langle qX\rangle<\psi(\|q\|)$.

הערות.

- אנו נשתמש בנורמה $\|q\|=\|q\|_\infty$. גם המרחק $\operatorname{dist}\left(qX,\mathbb{Z}^n\right)$ הוא ביחס לנורמת המקסימום.
- להיזהר לא להתבלבל בניסוח "ψ-מקורב", שאינו אותו הניסוח כמו במקרה החד-מימדי. במקרה החד-מימדי דיברנו על "φ-מקורב" (ו- $\psi(q)=q\varphi(q)$).
- לפעמים דורשים תנאי נוסף, ש- q וקטור פרימיטיבי, כלומר $\gcd\left(q_1,q_2,\ldots,q_m\right)=1$. יותר נוח לנו להגדיר ללא תנאי זה.
- לעיתים נניח ש- q וקטור עמודה ונכתוב ${}^{\text{tr}}qX$. בכל מקרה צריך להתייחס ל- q כוקטור שורה או עמודה כך שהמכפלה qX הגיונית...

נסמן ב- λ_m את מידת לבג על $\mathbb{R}^m$, ו- $\lambda_{m,n}$ על $M_{m,n}(\mathbb{R})$.

משפט (חינצ'ין-גרושב, Khinchine-Groshev).
בהינתן m,n, X ו- ψ כמו בסימונים לעיל,

א. אם $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n<\infty$ אז $\lambda_{m,n}(\psi\text{-approx})=0$.

ב. אם $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n=\infty$ ו- $r^{m-1}\psi(r)^n$ סדרה יורדת ב- r אז $\lambda_{m,n}\left((\psi\text{-approx})^C\right)=0$.

הערות.

- הוכחנו את המקרה $m=n=1$ (משפט חינצ'ין החד-מימדי).
- חינצ'ין הוכיח את המקרה $m=1$, n כללי. ההוכחה לכך כמעט זהה למה שנתנו, ונדלג עליה.
- גרושב הוכיח את המקרה $m\geq 2$. נוכיח מקרה זה. נראה שכאשר $m\geq 2$ ההוכחה יותר קלה.

הוכחת מקרה ההתכנסות

אפשר להניח בה"כ ש- $X \in \mathbb{T}^{m\cdot n} = \mathbb{R}^{m\cdot n}/\mathbb{Z}^{m\cdot n} \cong M_{m,n}(\mathbb{R})/M_{m,n}(\mathbb{Z})$.

זאת מפני שאם $A \in M_{m,n}(\mathbb{Z})$ ו- $X_1 = X + A$ אז

$$\langle qX_1 \rangle = \mathrm{dist}(qX_1, \mathbb{Z}^n) = \mathrm{dist}(qX + qA, \mathbb{Z}^n) = \mathrm{dist}(qX, \mathbb{Z}^n)$$

לכן נצמצם את מידת לבג $\lambda_{m,n}$ לטורוס $\mathbb{T}^{m\cdot n}$ (ונמשיך לסמן אותה כ- $\lambda_{m,n}$).

כעת, $\lambda_{m,n}(\mathbb{T}^{m\cdot n}) = 1$, כלומר זו מידת הסתברות, וניתן להשתמש בלמה של Borel-Cantelli.

מתקיים: $\psi\text{-approx} = A_\infty$, כאשר $A_1, A_2, \ldots$ הוא סידור של הקבוצות:

$W_q = \left\{ X \in \mathbb{T}^{m\cdot n} : \langle qX \rangle < \psi(\|q\|) \right\}$.

<u>טענת עזר.</u> $\lambda_{m,n}(W_q) = 2^n \psi(\|q\|)^n$.

נוכיח את מקרה ההתכנסות של המשפט בעזרת טענת העזר: נסכום את $\sum_q \lambda_{m,n}(W_q)$ לפי סדר עולה של $\|q\|$. נשים לב שמכיוון שאנו משתמשים בנורמת סופרמום, $\|q\| \in \mathbb{N}$ כאשר $q \neq 0$.

$$\sum_q \lambda_{m,n}(W_q) = \sum_{r=1}^{\infty} \#\left\{ q \in \mathbb{Z}^m : \|q\| = r \right\} 2^n \psi(r)^n \leq \underbrace{C}_{\text{Constant depending on } m,n} \cdot \sum_{r=1}^{\infty} r^{m-1} \psi(r)^n < \infty$$

<u>הערה:</u> $\#\left\{ q \in \mathbb{Z}^m : \|q\| = r \right\} \leq C r^{m-1}$, כי אם $q \in \mathbb{Z}^m$, $\|q\| = r$, אז יש $1 \leq i_0 \leq m$ כך ש- $q_0 = \pm r$, ועבור $j \neq i_0$, $q_j \in [-r, r]$, כלומר מספר הוקטורים בהם הנורמה מתקבלת ברכיב i_0 הוא $2(2r+1)^{m-1}$; לכן $\#\left\{ q \in \mathbb{Z}^m : \|q\| = r \right\} \leq 2m(2r+1)^{m-1}$.

מכאן נובע ש- $\sum_q \lambda_{m,n}(W_q) < \infty$, ומ-Borel-Cantelli נובע סעיף א' של המשפט.

נותר רק להוכיח את טענת העזר:

<u>הוכחה (טענת העזר).</u> נסתכל על ההעתקה $T_q : \mathbb{T}^{m\cdot n} \to \mathbb{T}^n$ המוגדרת ע"י $T_q(X) = qX \mod \mathbb{Z}^n$.

יש דיאגרמה קומוטטיבית:

$$\begin{array}{ccc} M_{m,n}(\mathbb{R}) = \mathbb{R}^{m\cdot n} & \xrightarrow{X \mapsto qX - p} & \mathbb{R}^n \\ \downarrow \text{mod } \mathbb{Z}^{m\cdot n} & & \downarrow \text{mod } \mathbb{Z}^n \\ \mathbb{T}^{m\cdot n} & \xrightarrow{T_q} & \mathbb{T}^n \end{array}$$

מתקיים:

$\langle qX \rangle < \psi(\|q\|) \Leftrightarrow$

$\Leftrightarrow$ קיים $p \in \mathbb{Z}^n$ כך ש- $\|qX - p\|_\infty < \psi(\|q\|) \Leftrightarrow$

$\Leftrightarrow$ תמונת X תחת T_q היא בהיטל ל- $\mathbb{T}^n$ של הקוביה $B_\infty^n(0, \psi(\|q\|))$ (כדור ב- $(\mathbb{R}^n, \|\ \|_\infty)$).

לכן, די להוכיח שלכל קבוצה $B\subset\mathbb{T}^n$, מתקיים $\lambda_{m,n}\left(T_q^{-1}\left(B\right)\right)=\lambda_n\left(B\right)$ $(*)$.

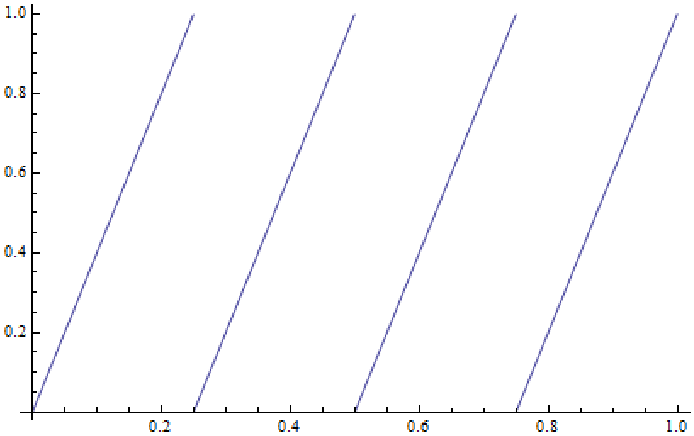
נוכיח את $(*)$ בשלבים: תחילה, נניח $q=e_1$ (הוקטור הראשון של הבסיס הסטנדרטי ב-$\mathbb{R}^m$).

אז $T_q\left(X\right)$ זו השורה הראשונה של X (נסמנה X_{1*}), ולכן $T_q^{-1}\left(B\right)=\left\{X:\ X_{1*}\in B\right\}\cong B\times\mathbb{T}^{(m-1),n}$.

ומכאן מתקיים $(*)$.

שלב שני: אם $q=re_1$,$r\in\mathbb{N}$, אז $T_q^{-1}\left(B\right)=\left\{x:rX_{1*}\in B\right\}$.

נשים לב ש-$\left\{Y\in\mathbb{T}^n:rY\in B\right\}$ הוא איחוד של r קבוצות זרות שכל אחת מהן מתקבלת מ-B ע"י כיווץ ביחס של $\frac{1}{r}$:



הגרף של $x\mapsto rx\bmod 1$ על $\mathbb{T}^1\cong{[0,1]}\big/{0\sim 1}$, כאשר $r=4$

בשבוע הבא נשלים את הוכחת הטענה, ונוכיח גם <u>טענת אי-תלות</u>: אם $q,q'\in\mathbb{Z}^m$ בלתי תלויים לינארית אז

$$\lambda_{m,n}\left(W_{q'}\cap W_q\right)=\lambda_{m,n}\left(W_q\right)\lambda_{m,\mathrm{n}}\left(W_{q'}\right)$$

הטענה הראשונה מוכיחה שהתכנסות הטור $\sum_{r=1}^{\infty}r^{m-1}\psi\left(r\right)^n$ שקולה להתכנסות הטור $\sum\lambda\left(A_i\right)$, $\left\{A_i\right\}=\left\{W_q\right\}_q$. מהטענה השנייה (טענת אי-התלות) מקבלים את האי-תלות שניתן באמצעותה להשתמש במשפט Rényi, עם $C=1$, ומכך ניתן להסיק את מקרה ההתבדרות, $\lambda\left(\left(\psi\text{-approx}\right)^C\right)=0$.

2013-04-24

הוכחת מקרה ההתבדרות

<u>תזכורת מהשיעור הקודם:</u>

משפט חינצ'ין-גרושב.

נקבע $n\geq 1$ ו-$m\geq 2$.

בהינתן $\psi:\mathbb{N}\to\mathbb{R}_+$, $X\in M_{m,n}(\mathbb{R})$ נקרא ψ-מקורב אם יש אינסוף פתרונות $q\in\mathbb{Z}^m$ לאי-השוויון $\operatorname{dist}_\infty\left({}^{\mathrm{tr}}qX,\mathbb{Z}^n\right)\le\psi\left(\|q\|_\infty\right)$. (או qX אם q וקטור שורה.)

נסמן ב-λ את מידת לבג ב-$\mathbb{R}^{mn}\cong M_{m,n}(\mathbb{R})$.

- אם $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n<\infty$ אז $\lambda(\psi\text{-approx})=0$.
- אם $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n=\infty$ וגם $r^{m-1}\psi(r)^n$ סדרה יורדת ב-r, אז $\lambda\left((\psi\text{-approx})^c\right)=0$.

<u>**רעיון ההוכחה**</u>

לכל $q\in\mathbb{Z}^m$, הגדרנו:

$$W_q=\left\{X\in\mathbb{T}^{mn}:T_q(X)\in\pi\left(\left[-\psi(\|q\|),\psi(\|q\|)\right]^n\right)\right\}$$

כאשר $\pi:\mathbb{R}^n\to\mathbb{T}^n$ היא ההטלה הסטנדרטית (מודולו 1 בכל קואורדינטה), ו-$T_q(X)=\pi\left({}^{\mathrm{tr}}qX\right)$.

נובע מיידית מההגדרות: $\pi(\psi\text{-approx})\subset\mathbb{T}^{mn}$ היא A_∞ (כלומר $\limsup_{n\to\infty}A_n$) כאשר A_n היא מנייה של W_q: $\{A_1,A_2,\dots\}=\{W_q\}_{q\in\mathbb{Z}^m}$.

כדי להוכיח את סעיף א' של המשפט, נראה: אם $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n<\infty$ אז $\sum_{q\in\mathbb{Z}^m}\lambda_{m,n}(W_q)<\infty$. ואז נקבל את הנדרש מ-Borel-Cantelli. ננמק מיד מדוע מתקיים $\lambda_{m,n}(W_q)=2^n\psi(\|q\|)^n$ ומכך נובע הדרוש.

כדי להוכיח את סעיף ב' של המשפט, נשתמש במשפט Rényi: אם לכל $i\ne j$ מתקיים $\mu(A_i\cap A_j)\le C\mu(A_i)\mu(A_j)$ אז $\mu(A_\infty)\ge\frac{1}{C}$. נשתמש עם $C=1$.

ננמק מיד מדוע: $\lambda_{mn}(W_{q_1}\cap W_{q_2})=\lambda(W_{q_1})\lambda(W_{q_2})$ כאשר q_1,q_2 <u>בלתי תלויים לינארית</u>.

נשתמש ב-Rényi כאשר $\{A_1,A_2,\dots\}=\{W_q:q\in\mathbb{Z}^m\text{ is a }\textit{primitive}\text{ vector}\}$.

וקטור $q=\begin{pmatrix}q_1\\ \vdots\\ q_m\end{pmatrix}\in\mathbb{Z}^m$ נקרא <u>פרימיטיבי</u> אם $\gcd(q_1,\dots,q_m)=1$, או באופן שקול, אם $q=cq'$ כאשר $q'\in\mathbb{Z}^m$ אז $c=\pm1$. באופן אינטואיטיבי: הוקטורים הפרימיטיביים הם הנקודות ב-$\mathbb{Z}^m$ שניתן לראות אותן אם מסתכלים מראשית הצירים (כלומר, הן לא מוסתרות ע"י נקודות $\mathbb{Z}^m$ אחרות).

צריך לבדוק שהקבוצה A_∞ המתקבלת מאוסף זה והקבוצה ψ-approx נבדלות בקבוצה בעלת מידה אפס (נשאר כתרגיל, בדף התרגילים).

צריך להוכיח גם שאם $\sum_{r=1}^{\infty} r^{m-1}\psi\left(r\right)^{n}=\infty$ אז גם $\sum_{\substack{q\in\mathbb{Z}^m \text{ primitive}\\ q_1\geq 1}} \lambda_{m,n}\left(W_q\right)=\infty$.

<u>הערה.</u> התנאי $q_1\geq 1$ בסך הכל מונע לספור זוגות וקטורים מנוגדים. ניתן לראות ש-$\lambda_{m,n}\left(W_q\right)=\lambda_{m,n}\left(W_{-q}\right)$ ולכן התנאי הזה לא משפיע על ההתבדרות. מצד שני, לא נקבל אי-תלות בין W_q לבין W_{-q} ולכן התנאי הזה מבטיח שאנו סוכמים רק על וקטורים בלתי תלויים לינארית, כך שנוכל להפעיל את משפט Rényi.

הגדרה. בהינתן $A\subset\mathbb{Z}^m$, <u>הצפיפות</u> של A היא

$$\mathrm{fr}\left(A\right):=\lim_{N\to\infty}\frac{\#A\cap\left[-N,N\right]^m}{\#\mathbb{Z}^m\cap\left[-N,N\right]^m}$$

בתנאי שהגבול קיים.

טענה. אם $m\geq 2$ ואם A קבוצת הוקטורים הפרימיטיביים ב-$\mathbb{Z}^m$ אזי

$$\mathrm{fr}\left(A\right)=\frac{1}{\zeta\left(m\right)}$$

כאשר $\zeta\left(s\right)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ פונקציית זטא של רימן.

הערה. למעשה זה נכון גם עבור $m=1$, כי $\zeta\left(1\right)=\infty$ ויש רק שני וקטורים פרימיטיביים ב-$\mathbb{Z}$ (±1), ובאופן טריוויאלי $\mathrm{fr}\left(\left\{\pm1\right\}\right)=0$.

לא נוכיח את הטענה הזו. זו טענה קלאסית בתורת המספרים וההוכחה בספרות ומשתמשת בהכלה והפרדה, פונקציית מביוס וכו'.

ניתן הסבר חלקי לטענה: נניח ש-$p=\mathrm{fr}\left(A\right)$, כלומר שהגבול קיים (ואת זה לא נוכיח).

לכל $r\in\mathbb{N}$, rA הוא אוסף הוקטורים $q\in\mathbb{Z}^m$ עבורם $\gcd\left(q_1,\ldots,q_m\right)=r$. כלומר:

$$\mathbb{Z}^m\setminus\left\{0\right\}=\bigcup_{r\geq1}rA$$

וזהו איחוד זר.

בבירור $\mathrm{fr}\left(\mathbb{Z}^m\setminus\left\{0\right\}\right)=1$, ולכל קבוצה A בעלת צפיפות, ניתן לראות מההגדרה ש-$\mathrm{fr}\left(rA\right)=r^{-m}\,\mathrm{fr}\left(A\right)$.

כמו-כן, אם A,B זרות ובעלות צפיפות אז מההגדרה, $\mathrm{fr}\left(A\cup B\right)=\mathrm{fr}\left(A\right)+\mathrm{fr}\left(B\right)$ (נראה שזה לא בהכרח נכון לאיחוד בן-מניה, אבל גם זה פרט בהוכחה שנדלג עליו). לכן:

$$1=\mathrm{fr}\left(A\right)\sum_{r=1}^{\infty}r^{-m}=\mathrm{fr}\left(A\right)\zeta\left(m\right)$$

ומכאן $\mathrm{fr}\left(A\right)=\frac{1}{\zeta\left(m\right)}$.

נותר להוכיח שתי טענות על נפחים:

טענה.

נסמן בתור π את העתקת המנה $\mathbb{R}^k\to\mathbb{T}^k$ (עבור ערכים שונים של k, תלוי בהקשר).

עבור $q\in\mathbb{Z}^m$ נגדיר $T_q:\mathbb{T}^{mn}\to\mathbb{T}^n$ ע"י $T_q\left(\pi\left(X\right)\right)=\pi\left({}^{\mathrm{tr}}qX\right)$ (בדקנו שמוגדר היטב).

נגדיר $W_q=T_q^{-1}\left(\pi\left[-\psi\left(\|q\|\right),\psi\left(\|q\|\right)\right]^n\right)$. אזי:

1. $\lambda_{m,n}\left(W_q\right)=2^n\psi\left(\|q\|\right)^n$. כלומר, אותו הנפח כמו $\left[-\psi\left(\|q\|\right),\psi\left(\|q\|\right)\right]^n$.
2. אם q_1,q_2 בלתי תלויים לינארית אז $\lambda_{m,n}\left(W_{q_1}\cap W_{q_2}\right)=\lambda_{m,n}\left(W_{q_1}\right)\lambda_{m,n}\left(W_{q_2}\right)$.

הוכחה.

<u>שלב ראשון:</u> נניח בלי הגבלת הכלליות ש-$n=1$. אפשר להניח זאת, כי אם $n>1$:

$$\Leftrightarrow\quad X\in T_q^{-1}\left(\left[-s,s\right]^n\right)$$

$\Leftrightarrow$ לכל $k=1,\dots,n$, $\mathrm{dist}\left(\left({}^{\mathrm{tr}}qX\right)_k,\mathbb{Z}\right)\le r$ $\Leftrightarrow$

$\Leftrightarrow$ לכל $k=1,\dots,n$, ${}^{\mathrm{tr}}q\left(X\right)_k\in\left[-r,r\right]$ כאשר $\left(X\right)_k$ העמודה ה-k של X.

$$T_q^{-1}\left(\left[-s,s\right]\right)=\left(\left\{v\in\mathbb{R}^m:{}^{\mathrm{tr}}qv\in\left[-s,s\right]\right\}\right)^n$$

לכן די להראות ש-$\left\{v\in\mathbb{R}^m:{}^{\mathrm{tr}}qv\in\left[-s,s\right]\right\}$ ממידה $2s$, כלומר הצטמצמנו למקרה $n=1$.

<u>שלב שני:</u> נוכיח את הטענה הראשונה תחת ההנחה ש-$q=re_1$, $r\in\mathbb{N}$, e_1 הוקטור הראשון בבסיס הסטנדרטי. (עשינו בשיעור שעבר.)

בטענה השניה מוכיחים קודם תחת ההנחה ש-q_1,q_2 וקטורים מהצורה $q_1=\begin{pmatrix}*\\0\\0\\\vdots\\0\end{pmatrix},q_2=\begin{pmatrix}*\\*\\0\\\vdots\\0\end{pmatrix}$, כלומר $q_1=re_1$ ו-$\mathrm{Span}_{\mathbb{R}}\left\{q_1,q_2\right\}=\mathrm{Span}_{\mathbb{R}}\left\{e_1,e_2\right\}$. הוכחה זו נשארת כתרגיל (נעשה משהו דומה אחר כך).

<u>עובדה:</u> לכל $q\in\mathbb{Z}^m$ יש $A\in\mathrm{SL}_m\left(\mathbb{Z}\right)$ כך ש-${}^{\mathrm{tr}}qA=re_1$, כאשר $r=\gcd\left(q_1,\dots,q_m\right)$.

במילים אחרות, כל הוקטורים השלמים עם אותו $\gcd$ הם מסלול אחד של החבורה $\mathrm{SL}_m\left(\mathbb{Z}\right)$.

(זה תרגיל פשוט באלגברה לינארית.)

נזכיר ש-$A\in\mathrm{SL}_m\left(\mathbb{Z}\right)$ מטריצה <u>הפיכה מעל השלמים</u>.

מתקיים: ${}^{\mathrm{tr}}q=re_1A^{-1}\quad\Leftrightarrow\quad{}^{\mathrm{tr}}qA=re_1$, ולכן, אם נסמן $s=\psi\left(\|q\|\right)$:

$$W_q=\left\{X:\pi\left({}^{\mathrm{tr}}qX\right)\in\left[-s,s\right]\right\}=\left\{X:\pi\left(re_1A^{-1}X\right)\in\left[-s,s\right]\right\}\overset{A^{-1}X=Y\Leftrightarrow X=AY}{=}$$
$$=A\left\{Y:\pi\left(re_1Y\right)\in\left[-s,s\right]\right\}$$

לכן A פועלת על הטורוס $\mathbb{T}^m$ ע"י $A\pi\left(X\right)=\pi\left(AX\right)$.

זו פעולה מוגדרת היטב כי ל-A מקדמים שלמים. פעולת A לא משנה מידות של קבוצות כי $\det A=1$ (ולכן לפי נוסחת היעקוביאן...) ולכן $\lambda\left(W_q\right)=\lambda\left(\left\{Y:\pi\left(re_1Y\right)\in\left[-s,s\right]\right\}\right)$.

__עובדה נוספת:__ לכל $q_1,q_2\in\mathbb{Z}^m$ יש $A\in\mathrm{SL}_m(\mathbb{Z})$ כך ש-$\begin{pmatrix} * \\ * \\ 0 \\ \vdots \end{pmatrix}$, ${}^{\mathrm{tr}}q_2A=\begin{pmatrix} * \\ 0 \\ 0 \\ \vdots \end{pmatrix}$ ${}^{\mathrm{tr}}q_1A=$.

לכן ניתן לקבל מסקנה דומה לגבי הטענה השנייה.

עוד שימושים של Borel-Cantelli

קירוב דיופנטי לא-הומוגני (חד-מימדי).

בהינתן (θ,δ) ובהנתן פונקציה $\psi:\mathbb{Z}\to\mathbb{R}_+$ (הפעם מוגדרת ב-$\mathbb{Z}$), אם יש אינסוף פתרונות $q\in\mathbb{Z}$ לאי-השוויון $\langle q\theta-\delta\rangle<\psi(q)$, אז אומרים ש-$(\theta,\delta)$ הוא ψ-מקורב (לא הומוגנית), ונרשום $(\theta,\delta)\in\psi\text{-inh.-approx}$. נשים לב ש-$\psi\text{-inh.-approx}\in\mathbb{R}^2$.

מבחינה גיאומטרית, מסובבים את θ על המעגל $\mathbb{T}$, ורוצים למדוד את כמות הפעמים שהסיבוב קרוב ל-$\delta\in\mathbb{T}$ עד כדי $\psi(q)$.

משפט (האנלוג המתאים של משפט חינצ'ין).

נניח ש-$0\le\psi(q)<\frac{1}{2}$ לכל q. נסמן ב-λ את מידת לבג ב-$\mathbb{R}^2$. אזי:

- אם $\sum_{q\in\mathbb{Z}}\psi(q)<\infty$ אזי $\lambda(\psi\text{-inh.-approx})=0$.
- אם $\sum_{q\in\mathbb{Z}}\psi(q)=\infty$ אזי $\lambda\left((\psi\text{-inh.-approx})^c\right)=0$.

הערה. יש הכללה רב-מימדית (עם אותה ההוכחה): $\theta,\delta\in\mathbb{R}^n$, $q\in\mathbb{Z}$, ומשתמשים בטור $\sum_{q\in\mathbb{Z}}\psi(q)^n$.

הוכחה.

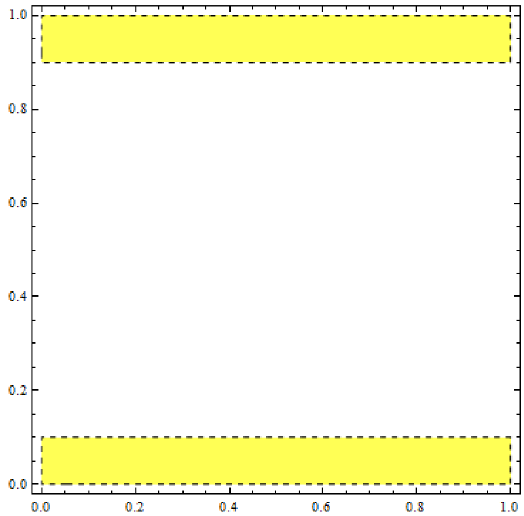
נגדיר $A_q=\pi\{(\theta,\delta):\langle q\theta-\delta\rangle<\psi(q)\}$ ($\pi:\mathbb{R}^2\to\mathbb{T}^2$ פונקציית המנה).

נראה שמתקיים:

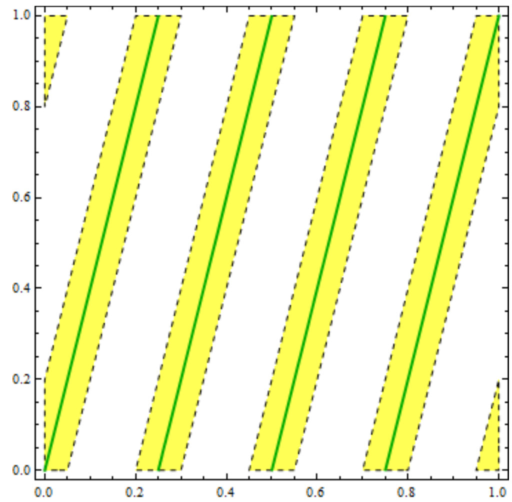
- $\lambda(A_q)=2\psi(q)$.
- אם $q_1\ne q_2$ אז $\lambda(A_{q_1}\cap A_{q_2})=\lambda(A_{q_1})\lambda(A_{q_2})$.

כמו בהוכחות הקודמות, מכאן המשפט נובע (ההתכנסות לפי Borel-Cantelli, ההתבדרות לפי Rényi).

לשם המחשה, נתבונן בשני האיורים הבאים: באיור הראשון ניתן לראות את השטח של A_0; הציר האופקי הוא θ והאנכי הוא δ. כאן אין תלות ב-δ כי $A_0=\pi\{(\theta,\delta):\langle\delta\rangle<\psi(0)\}$.



באיור השני ניתן לראות את השטח של A_4. הקו הירוק הוא הקו $\langle 4\theta-\delta\rangle=0$, והשטח הצהוב הוא הקבוצה $A_4=\{(\theta,\delta):\langle 4\theta-\delta\rangle<\psi(4)\}$, כאשר כמו קודם, הציר האופקי הוא θ והאנכי הוא δ.



מהאיורים ניתן לראות שהטענות מתקיימות:

ב- A_0, השטח של המלבן התחתון הוא $\psi(0)$ וגם השטח של המלבן העליון הוא $\psi(0)$ ובסה"כ $2\psi(0)$.

ב- A_q, השטח "מעל" כל אחד מ- $|q|$ הקטעים הוא $\frac{\psi(q)}{|q|}$ וגם מתחת. בסה"כ, $2\psi(q)$.

בחיתוך של $A_0\cap A_q$ ניתן לראות מהאיור שהשטח המשותף הוא מכפלת השטחים.

בחיתוך של $A_{q_1}\cap A_{q_2}$ ניתן לכתוב $q_1=q_2+s$ (עם $s\in\mathbb{Z}$) ואז $q_1\theta=q_2\theta+s\theta$. בעזרת החלפת משתנים ניתן לראות שהשטח לא משתנה ולמעשה עושים רדוקציה לחיתוך מהצורה הקודמת.

הערה. נשים לב שאם יש שני סיבובים של θ שמאוד קרובים זה לזה, אז כבר היה סיבוב של θ שמאוד קרוב לאפס. זאת מפני ש- $\operatorname{dist}(i\theta,j\theta)=\operatorname{dist}((i-j)\theta,0)$. לכן הבעיה ההומוגנית טמונה בבעיה הלא-הומוגנית.

ממשפט דיריכלה נובע שלכל Q יש $q<Q$ כך ש- $\langle q\theta\rangle<\frac{1}{Q}$.

<u>לא יכול להיות</u> משפט דיריכלה לא-הומוגני: "לכל Q יש $q<Q$ כך ש- $\langle q\theta-\delta\rangle<f(Q)$, f כלשהי."

לדוגמה אם θ רציונלי, אז יש רק מספר סופי של נקודות במעגל ש- $q\theta$ יכול להיות עליהן. אם θ אי-רציונלי, אז עדיין יכול להיות ש- $q\theta$ מתרכז במספר סופי של אזורים במעגל (למשל אם θ מספר בעל קירוב טוב מאוד?).

קירובים טובים מאוד

הגדרה. θ נקרא <u>בעל קירובים טובים מאוד</u> (VWA, very well approximated) אם קיים $\varepsilon>0$ וקיימים אינסוף פתרונות p,q לאי-השוויון $\left|\theta-\frac{p}{q}\right|<\frac{1}{q^{2+\varepsilon}}$.

במילים אחרות, $\mathrm{VWA}=\bigcup_{\varepsilon>0}\left(\frac{1}{q^{2+\varepsilon}}\text{-approx}\right)$.

לפי משפט חינצ'ין, $\lambda(\mathrm{VWA})=0$.

תהי $\mathcal{C}\subset[0,1]$ קבוצת קנטור – המספרים שניתנים להצגה עם הספרות $0,2$ בלבד בפיתוח לפי בסיס 3.

נסמן ב- μ את מידת ההסתברות בה מגרילים את הספרות $0,2$ בהסתברות $\frac{1}{2},\frac{1}{2}$, ולכל סדרה אינסופית שמקבלים מתאימים מספר לפי פיתוח בבסיס 3. אזי $\operatorname{supp}\mu=\mathcal{C}$.

μ נקראת לפעמים <u>מידת קנטור-לבג</u>.

תיאור אלמנטרי של μ: אפשר לקבל את μ באמצעות משפט Carathéodory (מידה על אלגברה ניתנת להרחבה יחידה למידה על σ-אלגברה). נבנה את קבוצת קנטור:

$$K_0=[0,1]$$

$$K_1=\left[0,\frac{1}{3}\right]\cup\left[\frac{2}{3},1\right]$$

$$\vdots$$

K_n הוא איחוד של 2^n קטעים סגורים זרים באורך 3^{-n}, וכל קטע ב- K_n מתפצל לשני קטעים בקצוות שלו, שהם ב- K_{n+1}; ו- $\mathcal{C}=\bigcap_{n=1}^{\infty}K_n$.

נכתוב $K_n=\bigcup_{j=1}^{2^n}I_j^{(n)}$ ונגדיר $\mu\left(I_j^{(n)}\right)=2^{-n}$ לכל j,n. מכאן ניתן להגדיר באופן יחיד את μ על האלגברה של האיחודים והחיתוכים הסופיים של הקבוצות $I_j^{(n)}$. ממשפט Carathéodory יש הרחבה יחידה ל- σ-אלגברה של בורל ב- $\mathcal{C}$, ולכן זו מידת בורל על $\mathcal{C}$.

נראה ש- $\mu(\mathrm{VWA})=0$.

הגדרה (שתי תכונות של מידות).

- נאמר ש-μ מקיימת <u>חוק חזקה</u> עם חזקה α אם יש קבועים C_1,C_2 כך שלכל $x\in\operatorname{supp}\mu$ ולכל $0<r<1$, מתקיים $C_1r^\alpha\le\mu\left(B(x,r)\right)\le C_2r^\alpha$.
- נאמר ש-μ מקיימת <u>תנאי דעיכה</u> עם חזקה α, אם יש C כך שלכל x ולכל $r<1$, $\varepsilon>0$, מתקיים $\mu\left(B(x,\varepsilon r)\right)\le C\varepsilon^\alpha\mu\left(B(x,r)\right)$.

טענה. אם μ מקיימת חוק חזקה עם חזקה α אז μ מקיימת תנאי דעיכה עם חזקה α.
(הכיוון ההפוך לא נכון.)

הוכחה.
אם $B(x,\varepsilon r)$ לא נחתך עם $\operatorname{supp}\mu$ אז אין מה להוכיח (צד שמאל מתאפס).
אחרת, אם $x_1\in B(x,\varepsilon r)\cap\operatorname{supp}\mu$, אז:

$$\mu\left(B(x,\varepsilon r)\right)\le\mu\left(B(x_1,2\varepsilon r)\right)\overset{\text{Power rule, upper bound}}{\le}C_2(2\varepsilon r)^\alpha=\tilde{C}\varepsilon^\alpha\cdot C_1\left(\frac{r}{2}\right)^\alpha\overset{\text{Power rule, lower bound}}{\le}$$

$$\le\tilde{C}\varepsilon^\alpha\mu\left(B\left(x_1,\frac{r}{2}\right)\right)\le\tilde{C}\varepsilon^\alpha\mu\left(B(x,r)\right)$$

מש"ל.

טענה. מידת קנטור-לבג מקיימת את תנאי החזקה עם חזקה $\alpha=\dfrac{\log 2}{\log 3}$. (נשאיר כתרגיל.)

משפט. אם μ מקיימת תנאי דעיכה עם חזקה α, ואם $\psi:\mathbb{N}\to\mathbb{R}$ כך ש-$\sum_{q=1}^{\infty}q^{\alpha-1}\psi(q)^\alpha<\infty$ ואם ψ יורדת, אז $\mu(\varphi\text{-approx})=0$ כאשר $\varphi(q)=\dfrac{\psi(q)}{q}$.

הערה. בהכרח $\alpha\le1$ כי אחרת $\dim\operatorname{supp}\mu>1$ (מימד האוסדורף), אבל $\operatorname{supp}\mu\subset\mathbb{R}$. (לא נפרט על כך.)

שאלה. האם התנאי ש-ψ יורדת באמת נחוץ? עד כמה אפשר להחליש אותו?

מסקנה. אם μ מידת קנטור-לבג אז $\mu(\mathrm{VWA})=0$.

הוכחת המסקנה. נפעיל את המשפט עם $\psi(q)=\dfrac{1}{q^{1+\varepsilon}}$. נראה שהתנאי על הטור מתקיים:

$$\sum_{q=1}^{\infty}q^{\alpha-1}\left(\frac{1}{q^{1+\varepsilon}}\right)^\alpha=\sum_{q=1}^{\infty}\frac{1}{q^{1+\alpha\varepsilon}}<\infty$$

ולכן $\mu\left(\dfrac{1}{q^{2+\varepsilon}}\text{-approx}\right)=0$. מכיוון שניתן לכתוב את VWA כאיחוד <u>בן-מנייה</u> של $\dfrac{1}{q^{2+\varepsilon}}$-approx, גם $\mu(\mathrm{VWA})=0$.
מש"ל.

הוכחת המשפט.

נשתמש במבחן העיבוי: ψ מונוטונית יורדת ו-$\alpha \le 1$ ולכן $\frac{\psi(q)^\alpha}{q^{1-\alpha}}$ גם יורדת. לפי משפט העיבוי, התכנסות הטור $\sum_{q=1}^{\infty} q^{\alpha-1}\psi(q)^\alpha$ שקולה להתכנסות הטור $2^{\alpha Q}\sum_{Q=1}^{\infty}\psi(2^Q)^\alpha = \sum_{Q=1}^{\infty} 2^Q(2^Q)^{\alpha-1}\psi(2^Q)^\alpha$.

בפרט, $2^{\alpha Q}\psi(2^Q)^\alpha \xrightarrow{q\to\infty} 0$ ולכן $\psi(2^Q)2^Q \to 0$, ולכן $\varphi(2^Q)2^{2Q} \to 0$.

בשביל בורל-קנטלי, נרצה: $\sum_{\substack{q=1\\0\le p\le q}}^{\infty} \mu\left(B\left(\frac{p}{q},\varphi(q)\right)\right) < \infty$. אבל לא נקבל את זה בסכימה על <u>כל</u> q.

נקבץ לקבוצות שבהן $2^Q \le q \le 2^{Q+1}$. מדובר בבערך 2^{2Q} רציונליים והם מפוזרים במרחקים בערך אחידים.

לבסוף מכיוון ש-$\frac{\varphi(2^Q)}{2^{-2Q}} \to 0$, נוכל לקבל את התכנסות הטור.

בה"כ אפשר להניח שמתעניינים במספרים θ שהם φ-מקורבים, עבורם יש סדרה $\frac{p_n}{q_n} \to \theta$ כך ש-$\left|\theta - \frac{p_n}{q_n}\right| < \varphi(q_n)$ ו-$\gcd(p_n,q_n)=1$.

לפי מקרה ההתכנסות של Borel-Cantelli, די להראות $\sum_{\substack{q\in\mathbb{N}\\0\le p\le q\\\gcd(p,q)=1}} \mu\left(B\left(\frac{p}{q},\varphi(q)\right)\right) < \infty$.

לכל $q,q',p,p' \in \mathbb{Z}$ כך ש-$2^Q \le q,q' < 2^{Q+1}$, $0 \le \frac{p'}{q'} \ne \frac{p}{q} \le 1$, נראה:

$$B\left(\frac{p}{q},2^{-2(Q+2)}\right) \cap B\left(\frac{p'}{q'},2^{-2(Q+2)}\right) = \varnothing$$

אכן, אם $s \in B\left(\frac{p}{q},2^{-2(Q+2)}\right) \cap B\left(\frac{p'}{q'},2^{-2(Q+2)}\right)$ אז:

$$2^{-2(Q+1)} \le \frac{1}{qq'} \le \frac{|pq'-p'q|}{qq'} = \left|\frac{p}{q}-\frac{p'}{q'}\right| < 2\cdot 2^{-2(Q+2)}$$

סתירה.

לכן:

$$\sum_{\substack{2^Q\le q\le 2^{Q+1}\\0\le p\le q\\\gcd(p,q)=1}} \mu\left(B\left(\frac{p}{q},2^{-2(Q+2)}\right)\right) = \mu\left(\bigcup_{\dots} B\left(\frac{p}{q},2^{-2(Q+2)}\right)\right) \underset{\mu\text{ is a probability measure}}{\le} 1$$

ומכאן:

$$\sum_{\substack{q\in\mathbb{N}\\0\le p\le q\\\gcd(p,q)=1}} \mu\left(B\left(\frac{p}{q},\varphi(q)\right)\right)=\sum_{Q=0}^{\infty}\sum_{\substack{2^Q\le q<2^{Q+1}\\0\le p\le q\\\gcd(p,q)=1}}\mu\left(B\left(\frac{p}{q},\frac{\psi(q)}{q}\right)\right)\le$$

$$\le\sum_{Q=0}^{\infty}\sum_{\substack{2^Q\le q<2^{Q+1}\\0\le p\le q\\\gcd(p,q)=1}}C\left(\frac{\psi(q)/q}{2^{-2(Q+2)}}\right)^{\alpha}\mu\left(B\left(\frac{p}{q},2^{-2(Q+2)}\right)\right)\le$$

$$\le C_1\sum_{Q=0}^{\infty}\frac{\psi\left(2^Q\right)^{\alpha}}{2^{\alpha Q}2^{-2(Q+2)}}\sum_{\substack{2^Q\le q<2^{Q+1}\\0\le p\le q\\\gcd(p,q)=1}}\mu\left(B\left(\frac{p}{q},2^{-2(Q+2)}\right)\right)\le$$

$$\le C_2\sum_{Q=0}^{\infty}2^Q2^{Q(\alpha-1)}\psi\left(2^Q\right)^{\alpha}<\infty$$

מש"ל.

[הערה: יש קובץ pdf באתר/ספריית הקורס עם תיקונים והשלמות לשיעור של היום.]

2013-05-01

משחקי שמידט ותכונות הקבוצה BA

(מבוסס על מאמר של שמידט משנות ה-60.)

תזכורת: $\mathrm{BA}=\left\{\theta\in\mathbb{R}:\exists c>0\ \ \forall p,q\in\mathbb{Z}\ \left|\theta-\frac{p}{q}\right|\ge\frac{c}{q^2}\right\}=\left\{\theta=[a_1,a_2,\dots]:\sup a_i<\infty\right\}$.

ממשפט חינצ'ין, $\lambda(\mathrm{BA})=0$. מתרגיל בשיעורי הבית, BA קבוצה מקטגוריה ראשונה (היא איחוד בן-מניה של קבוצות סגורות דלילות).

<u>חידה.</u> האם יש $X_0\subset\mathbb{R}$, $\lambda(X_0)=0$, כך שלכל $c_1,c_2,\dots$ מתקיים $\bigcap_{i=1}^{\infty}(X_0+c_i)\ne\varnothing$?

<u>תשובה.</u> כל קבוצה מקטגוריה שניה בעלת מידה אפס תעבוד, למשל:

$$\mathrm{VWA}=\left\{\theta:\exists\varepsilon>0,\frac{p_n}{q_n}:\ \left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{q_n^{2+\varepsilon}}\quad\forall n\right\}$$

כי חיתוך בן מניה של קבוצות מקטגוריה שניה היא קבוצה מקטגוריה שניה. במקום הזזות יכולנו לבחור כל $f_i:\mathbb{R}\to\mathbb{R}$ עם התנאי שהן שומרות קבוצות ממידה אפס.

<u>חידת המשך.</u> האם יש $X_0\subset\mathbb{R}$, $\lambda(X_0)=0$, מקטגוריה ראשונה, כך שלכל $c_1,c_2,\dots$, $\bigcap_{i=1}^{\infty}(X_0+c_i)\ne\varnothing$?

<u>תשובה:</u> כן. נראה בהמשך ש- BA היא קבוצה כזו.

הגדרה (משחק שמידט, Wolfgang Schmidt game).

נתונים: (X,d) מרחב מטרי שלם; $S \subset X$ קבוצת המטרה; פרמטרים $0<\alpha<1$ ו-$0<\beta<1$; שני שחקנים, אורנה ובועז.
חוקי המשחק:

1. בועז בוחר $x_0 \in X$ ו-$r_0 > 0$. נסמן $B_0 = B(x_0, r_0)$ כדור סגור.
2. אורנה בוחרת $y_1 \in B_0$ כך ש-$A_1 = B(y_1, \alpha r_0) \subset B_0$.
3. בועז בוחר $x_1 \in A_1$ כך ש-$B_1 = B(x_1, \alpha\beta r_0) \subset A_1$.
4. נמשיך כך אינסוף צעדים. קיבלנו אוסף יורד: $B_0 \supset A_1 \supset B_1 \supset A_2 \supset \dots$. מכיוון שהכדורים סגורים והמרחב המטרי שלם, בחיתוך שלהם יש נקודה יחידה: $\{z_\infty\} = \bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} B_i$.
5. אם $z_\infty \in S$ אז אורנה ניצחה; אם $z_\infty \notin S$ אז בועז ניצח.

אסטרטגיה לאחד השחקנים היא פונקציה שלכל $n \geq 0$, בהינתן השתלשלות חוקית של המשחק עד צעד n, מתאימה בחירה של צעד חוקי במשחק. כלומר, אסטרטגיה לאורנה מתאימה לכל סדרת כדורים $B_0 \supset A_1 \supset B_1 \supset \dots \supset B_n$ שעשויים להיבחר בצעדים חוקיים, כדור $A_n \supset B_n$ שאפשר לבחור בצעד ה-n.

הגדרה (קבוצה מנצחת).

- קבוצה $S \subset X$ נקראת **קבוצה (α,β)-מנצחת** אם יש לאורנה אסטרטגיה כך ש-$z_\infty \in S$ לכל סדרת צעדים חוקיים של בועז.
- S נקראת **קבוצה α-מנצחת** אם היא (α,β)-מנצחת לכל $\beta > 0$.
- S נקראת **קבוצה מנצחת** אם היא α-מנצחת לאיזשהו α.

תכונות של קבוצות מנצחות

טענה א'. אם S היא (α,β)-מנצחת לאיזשהם α,β אז S צפופה ב-X.

הוכחה.
אם $\mathcal{U} \subset X$ פתוחה, בועז יכול לבחור $B_0 \subset \mathcal{U}$. לאורנה יש אסטרטגיה מנצחת, ולכן $z_\infty \in B_0 \cap S$, ובפרט $S \cap B_0 \neq \varnothing$, כלומר S נחתכת עם כל קבוצה פתוחה.

דרך אחרת לנסח זאת: אילו S לא צפופה, בועז יכול לבחור בצעד הראשון כדור זר ל-S, בסתירה לכך שלאורנה יש אסטרטגיה מנצחת.
מש"ל.

טענה ב'. אם $X = \mathbb{R}$ ו-S היא (α,β)-מנצחת עם $\beta < \frac{1}{2}$ אז S לא בת-מניה.

הוכחה.
בהינתן α,β כאשר $\beta < \frac{1}{2}$ ובהינתן אסטרטגיה מנצחת עבור אורנה, נגדיר העתקה <u>חח"ע</u> $\{0,1\}^{\mathbb{N}} \to S$, ונסיק ש-$S$ לא בת-מניה.

לכל סדרה אינסופית $\bar{a} = \{a_1, a_2, \dots\} \in \{0,1\}^{\mathbb{N}}$ נגדיר אסטרטגיה לבועז: B_0 נבחר באופן שרירותי (בחירה שאינה תלויה ב-$\bar{a}$). הצעדים הבאים: אם נבחרו $B_0 \supset A_1 \supset B_1 \supset \dots \supset B_{n-1} \supset A_n$, אז A_n הוא קטע. אם

$a_n = 0$ (לחילופין $a_n = 1$) אז B_n יהיה תת-הקטע השמאלי ביותר (לחילופין הימני ביותר) של A_n. הקטעים האלה <u>זרים</u> כי $\beta < \frac{1}{2}$.

זוהי אסטרטגיה לבועז; האסטרטגיה של אורנה נקבעה, ולכן לכל $\overline{a}$ מקבלים נקודה $z_\infty \in S$ (כי האסטרטגיה של אורנה מנצחת). לכן קיבלנו העתקה $z_\infty : \{0,1\}^N \to S$ המתאימה לכל סדרה $\overline{a}$ את נקודת הגבול z_∞ המתקבלת מהמשחק.
נראה שההעתקה הזו היא חח"ע:
נניח ש- $\overline{a} \neq \overline{b}$ שתי סדרות שונות, ויהי k המקום הראשון בו הם לא מסכימים: $a_k \neq b_k$.
אז הכדורים $B_0 \supset A_1 \supset \ldots \supset A_k$ הם אותם כדורים אם בועז ישחק לפי $\overline{a}$ או לפי $\overline{b}$. בשלב ה- k, הוא ישחק לפי אסטרטגיות שונות ולכן הכדורים $B_k(\overline{a})$, $B_k(\overline{b})$ <u>זרים</u> (כי $\beta < \frac{1}{2}$). אבל $z_\infty(\overline{a}) \in B_k(\overline{a})$ ו- $z_\infty(\overline{b}) \in B_k(\overline{b})$ ולכן $z_\infty(\overline{a}) \neq z_\infty(\overline{b})$.
מש"ל.

הערה. השתמשנו כאן במבנה של $\mathbb{R}$ (תת-קטע ימני/שמאלי). אפשר לתת הוכחה דומה למרחב מטרי אוקלידי. בהמשך נראה שהטענה אינה בהכרח נכונה במרחב מטרי כללי; אך אפשר במקום זה להוכיח טענה יותר חזקה: אם $S \subset \mathbb{R}^d$ מנצחת, אז $\dim S = d$ (מימד האוסדורף).

טענה ג'. חיתוך בן-מניה של קבוצות α-מנצחות היא α-מנצחת.

הוכחה.
האינטואיציה: "שח סימלוטני". שוזרים את כל המשחקים ביחד, משחקים בכולם במקביל ומנצחים בכולם.
יהיו $S_1, S_2, \ldots$ קבוצות α-מנצחות. נחלק את $\mathbb{N}$ לאיחוד בן-מניה של סדרות חשבוניות זרות $P_k = \{n : n \equiv a_k \pmod{d_k}\}$, כך:

$$P_1 = \{1,3,5,7,9,\ldots\}$$
$$P_2 = \{2,6,10,14,18,\ldots\}$$
$$P_3 = \{4,12,20,28,\ldots\}$$

כלומר $a_k = 2^{k-1}$ ו- $d_k = 2^k$.

המטרה: להגדיר אסטרטגיה מנצחת לאורנה על $\bigcap_{k=1}^{\infty} S_k$ עבור α, β נתונים, בהינתן אסטרטגיות מנצחות של אורנה על S_k עבור α, β_k כאשר את β_k אפשר לבחור כתלות ב- k. נגדיר $\beta_k = \alpha^{d_k - 1}\beta^{d_k}$.
נתאר את האסטרטגיה של אורנה: בצעד הראשון, אחרי שבועז בחר B_0, אורנה משתמשת באסטרטגיה הנתונה עבור S_1 כדי לבחור את A_1. אם בועז בחר B_{n-1}, ו- $n \in P_k$ אז אורנה בוחרת $A_n \subset B_{n-1}$ לפי האסטרטגיה למשחק (α, β_k) על S_k.
כלומר, אורנה מתייחסת לכל הצעדים שנעשו על-ידה ע"י בועז, מאז הפעם האחרונה שנבחר אינדקס ב- P_k, כצעד אחד אפשרי של בועז במשחק (α, β_k) על S_k. הבחירה של β_k מבטיחה שזהו צעד חוקי, לכן האסטרטגיה של אורנה קובעת את הצעד הבא. לכן $z_\infty \in S_k$ לכל k כנדרש.
מש"ל.

טענה ד'. יהיו X,Y מרחבים מטריים שלמים, תהי $f:X\to Y$ העתקה C-בי-ליפשיץ (כלומר לכל $x_1,x_2\in X$ שונים זה מזה, $\frac{1}{C}\le\frac{d_Y\left(f\left(x_1\right),f\left(x_2\right)\right)}{d_X\left(x_1,x_2\right)}\le C$) ותהי $S\subset X$ קבוצה α-מנצחת.

אזי $f\left(S\right)\subset Y$ היא α_0-מנצחת כאשר $\alpha_0=\frac{\alpha}{C^2}$.

הערה. ניתן לנסח את הטענה עם המושג של דחיפה קדימה. זוהי דחיפה קדימה של אסטרטגיה מנצחת.

הוכחה.
בהינתן β_0 עלינו להגדיר אסטרטגיה במשחק $\left(\alpha_0,\beta_0\right)$ על Y עם קבוצת מטרה $f\left(S\right)$. נגדיר $\beta=C^2\beta_0$.
נניח ש-$\beta<1$ (נטפל אח"כ במקרה $\beta\ge1$).
לפי בחירתנו, $\alpha_0\beta_0=\alpha\beta$. עלינו לקבוע אסטרטגיה לאורנה, על $f\left(S\right)\subset Y$ למשחק $\left(\alpha_0,\beta_0\right)$, בהינתן אסטרטגיה לאורנה על $S\subset X$ למשחק $\left(\alpha,\beta\right)$.
אם בועז בוחר $B_0\subset Y$ מרדיוס r_0, אז מתנאי בי-ליפשיץ של f, $f^{-1}\left(B_0\right)\subset X$ מכילה כדור ברדיוס $\frac{r_0}{C}=\tilde{r}_0$. נסמן את הכדור הזה כ-$\tilde{B}_0$. אורנה מפעילה את האסטרטגיה שלה כאילו $\tilde{B}_0$ היה הצעד הראשון של בועז במשחק $\left(\alpha,\beta\right)$ על X. לכן יש בחירה של $\tilde{A}_1\subset\tilde{B}_0$, ברדיוס $\frac{r_0}{C}\alpha$. נתבונן ב-$f\left(\tilde{A}_1\right)$. שוב מתנאי בי-ליפשיץ, $f\left(\tilde{A}_1\right)$ מכילה כדור ברדיוס $r_0\alpha_0=\frac{1}{C}\left(\frac{r_0}{C}\alpha\right)$.
עתה ממשיכים. נניח שנבחרו $B_0\supset A_1\supset\ldots\supset B_n=B\left(x_n,\left(\alpha\beta\right)^n r_0\right)$. אז $f^{-1}\left(B_n\right)$ מכיל כדור $\tilde{B}_n$ מרדיוס $\left(\alpha_0\beta_0\right)^n\frac{r_0}{C}=\frac{\left(\alpha\beta\right)^n r_0}{C}$. כלומר $\tilde{B}_n$ צעד חוקי עבור בועז במשחק $\left(\alpha,\beta\right)$ על המרחב X. יש $\tilde{A}_{n+1}\subset\tilde{B}_n$ (לפי האסטרטגיה של אורנה על X) כדור ברדיוס $\alpha\left(\alpha\beta\right)^n\tilde{r}_0$. $f\left(\tilde{A}_{n+1}\right)$ מכילה כדור ברדיוס $\frac{\alpha\left(\alpha\beta\right)^n\tilde{r}_0}{C}=\frac{\alpha}{C^2}\left(\alpha_0\beta_0\right)^n r_0=\alpha_0^{n+1}\beta_0^{\,n}r_0$, ואורנה תבחר אותו במשחק $\left(\alpha_0,\beta_0\right)$ על Y. בגלל הבחירות שהתקבלו, החיתוך $z_\infty\in Y$ הוא התמונה תחת f של החיתוך $\bigcap_{n=1}^{\infty}\tilde{B}_n$, ולכן $z_\infty\in f\left(S\right)$.
מש"ל.

מסקנה. אם $X_0\subset\mathbb{R}$ מנצחת, אז לכל $c_1,c_2,\ldots$, $\bigcap_{i=1}^{\infty}\left(X_0+c_i\right)$ לא בת-מניה.
הוכחה.
לפי טענה ד, מאחר שההעתקה $x\mapsto x+c_i$ היא בי-ליפשיץ עם $C=1$, כל הקבוצות X_0+c_i הן α-מנצחות עם אותו α. לכן גם $\bigcap_{i=1}^{\infty}\left(X_0+c_i\right)$ היא α-מנצחת לפי טענה ג. בפרט מטענה ב, היא מעוצמת הרצף.
מש"ל.

הערה. יתר על כן, $\bigcap_{i=1}^{\infty}\left(X_0+c_i\right)$ היא ממימד האוסדורף 1.

דוגמה (שמראה שטענה ב' לא נכונה עבור מרחב מטרי כללי).

נבחר $Y=\{0,1,2\}^{\mathbb{N}}$ ו- $X_1=\{0,1\}^{\mathbb{N}}\subset Y$, ו- $X_1\subset X=\left\{\bar{a}=\left(a_1,a_2,\dots\right)\in Y: a_n=2\Rightarrow a_{n+1}=2\right\}$.

כלומר:

$$X=X_1\cup\underbrace{\left\{\text{Sequences of the form }\left(a_0,a_1,a_2,\dots,2,2,2,\dots\right):a_i\in\{0,1\}\right\}}_{\text{Countable}}$$

נסמן $X_2=X\setminus X_1$, כלומר כל הסדרות שהן קבועות 2 החל ממקום מסויים ושונות מ- 2 לפני המקום הזה.

מטריקה על Y שהופכת אותה למרחב מטרי שלם:

$$d\left(\bar{a},\bar{b}\right)=\begin{cases}0 & \bar{a}=\bar{b}\\ 2^{-k\left(\bar{a},\bar{b}\right)} & k\left(\bar{a},\bar{b}\right)=\inf\left\{j:a_j\neq b_j\right\}\end{cases}$$

תרגיל. Y מרחב מטרי שלם ו- X תת-קבוצה סגורה בו, ובפרט X עם אותה המטריקה מרחב מטרי שלם.

טענה. אם $\alpha<\frac{1}{2}$ אז X_2 היא קבוצה α-מנצחת.

הוכחה.

בהינתן B_0,r_0 בחירות של בועז, אורנה "מחכה" (מבצעת צעדים שרירותיים) עד ש- $r_n=\left(\alpha\beta\right)^n r_0<1$.

$B_n=B\left(\bar{a},r_n\right)$. קיים k כך ש- $2^{-(k+1)}<r_n\le 2^{-k}$. לפי הגדרת המטריקה,

$$B_n=\left\{\bar{c}:c_1=a_1,c_2=a_2,\dots,c_k=a_k\right\}$$

בפרט B_n מכיל נקודה כלשהי $\omega=\left(a_1,a_2,\dots,a_k,2,2,\dots\right)$.

מכיוון ש- $\alpha<\frac{1}{2}$, $\alpha r_n\le 2^{-(k+1)}$.

אורנה תבחר את $A_{n+1}=B\left(\omega,\alpha r_n\right)\subset\left\{\bar{c}:c_1=\omega_1=a_1,\dots,c_{k+1}=\omega_{k+1}=2\right\}=\{\omega\}$.

מרגע זה ואילך, $B_{n+1}=A_{n+1}=\dots=\{\omega\}$. לכן $z_\infty=\omega\in X_2$.

מש"ל.

תרגיל. אם $\alpha<1$ ולאורנה אסטרטגיה $\left(\alpha,\beta\right)$-מנצחת לכל $\beta<\varepsilon_0$ אז לאורנה יש אסטרטגיה מנצחת לכל $\beta<1$. (רמז: צעדי סרק). (**הערה:** זה תרגיל 13 בדף התרגילים.)

בטענה ד' לעיל הראינו שלאורנה אסטרטגיה מנצחת עם α_0, ולכל $\beta_0<\frac{1}{C^2}$. לפי התרגיל, לאורנה אסטרטגיה מנצחת עם α_0, לכל β.

BA היא קבוצה מנצחת

משפט. BA היא α-מנצחת עם כל $\alpha<\frac{1}{2}$ למשחק שמידט על $X=\mathbb{R}$.

הוכחה. נסמן $\mathrm{BA}^{(c)}=\left\{\theta\in\mathbb{R}:\forall\frac{p}{q}\in\mathbb{Q},\ \left|\theta-\frac{p}{q}\right|\geq\frac{c}{q^2}\right\}$. ואז $\mathrm{BA}=\bigcup_{c>0}\mathrm{BA}^{(c)}$ (וגם איחוד בן-מניה).

בהינתן $\alpha<\frac{1}{2}$, $0<\beta<1$, r_0 רדיוס של הכדור ההתחלתי של הבחירה הראשונה B_0 של בועז, נגדיר $c>0$ ונגדיר אסטרטגיה לאורנה כך שנקבל $z_\infty\in\mathrm{BA}^{(c)}$.

נסמן $R=\frac{1}{\sqrt{\alpha\beta}}$, $c_1<\frac{1}{4R^2}$.

בהתחלה אורנה תבצע צעדי סרק עד ש- $r_{n_0}=\left(\alpha\beta\right)^{n_0}r_0<\frac{1}{4R^2}$. נמספר מחדש את הצעדים כדי להניח $r_{n_0}=r_0<\frac{1}{4R^2}$ ונגדיר $c=\min\left\{c_1,\left(1-2\alpha\right)r_0\right\}$. עלינו להציג אסטרטגיה שבאמצעותה הנקודה z_∞ תהיה ב- $\mathrm{BA}^{(c)}$.

נאמר שרציונלי $\frac{p}{q}$ מסוכן בשלב ה- n אם יש $\theta\in B_n$ כך ש- $\left|\theta-\frac{p}{q}\right|<\frac{c_1}{q^2}$.

<u>טענת עזר.</u> לכל n יש לכל היותר רציונלי אחד שהוא מסוכן בשלב n ומקיים $R^n\leq q<R^{n+1}$.

<u>הוכחת טענת העזר.</u> נניח בשלילה שיש שניים כאלה, $\frac{p_1}{q_1}\neq\frac{p_2}{q_2}$, המקיימים את אי-השוויון $R^n\leq q_i<R^{n+1}$.

אז $\left|\frac{p_1}{q_1}-\frac{p_2}{q_2}\right|\geq\frac{1}{q_1q_2}>\frac{1}{R^{2(n+1)}}$. מצד שני, מאי-שוויון המשולש ומכך ש- $\frac{p_1}{q_1},\frac{p_2}{q_2}$ שניהם מסוכנים בשלב ה- n, יש $\theta_1,\theta_2\in B_n$ כך ש:

$$\left|\frac{p_1}{q_1}-\frac{p_2}{q_2}\right|\leq\left|\frac{p_1}{q_1}-\theta_1\right|+\left|\frac{p_2}{q_2}-\theta_2\right|+\left|\theta_1-\theta_2\right|\leq\frac{c_1}{q_1^2}+\frac{c_1}{q_2^2}+\overbrace{2\left(\alpha\beta\right)^n r_0}^{\operatorname{diam}B_n}\leq$$

$$\leq\frac{2c_1}{R^{2n}}+\frac{2r_0}{R^{2n}}=\frac{2\left(c_1+r_0\right)}{R^{2n}}<\frac{4}{4R^{2n+2}}=\frac{1}{R^{2(n+1)}}$$

סתירה. <u>מש"ל (טענת העזר).</u>

עתה נמשיך עם הוכחת המשפט.

בשלב ה- n, אם ב- B_n אין רציונליים מסוכנים $\frac{p}{q}$ עם $R^n\leq q<R^{n+1}$, אורנה תבחר $A_{n+1}\subset B_n$ באופן שרירותי. אם יש רציונלי מסוכן כזה, אז לפי טענת העזר יש רק אחד. אם הוא משמאל למרכז B_n, אורנה תבחר את A_{n+1} בתור תת-הקטע הימני של B_n, ולהיפך.

כעת, $z_\infty\in\bigcap_n B_n$. צריך להוכיח ש- $z_\infty\in\mathrm{BA}^{(c)}$. אם לא, אז יש $\frac{p}{q}\in\mathbb{Q}$ כך ש- $\left|z_\infty-\frac{p}{q}\right|<\frac{c}{q^2}\leq\frac{c_1}{q^2}$ ולכן $\frac{p}{q}$ מסוכן בשלב ה- n לכל n. נבחר את n עבורו $R^n\leq q<R^{n+1}$. אז $z_\infty\in A_{n+1}$ ו-

$$\left|z_\infty - \frac{p}{q}\right| \geq \left|\left(\text{center of } B_n\right) - \left(\text{edge of } A_{n+1} \text{ closer to the center}\right)\right| =$$

$$= \left(1-2\alpha\right) r_n = \left(1-2\alpha\right)\left(\alpha\beta\right)^n = \frac{1-2\alpha}{R^{2n}} \geq \frac{c_1}{q^2}$$

סתירה. **מש"ל.**

לפני שמידט: (Cassels, Davenport)

לכל N קיימים מספרים x עבורם $x, x^2, \ldots, x^N \in \mathrm{BA}$.

שימוש במשחק שמידט: קיים x (כעוצמת הרצף ואפילו ממימד האוסדורף 1) כך ש- $x, x^2, x^3, \ldots \in \mathrm{BA}$.

הכללה רב-מימדית: נסמן

$$\mathrm{BA}_d = \left\{ x \in \mathbb{R}^d : \exists c > 0\ \forall p \in \mathbb{Z}^d, q \in \mathbb{N},\ \left\| x - \frac{p}{q} \right\|_\infty \geq \frac{c}{q^{1+(1/d)}} \right\}$$

לפני שמידט: $\mathrm{BA}_d \neq \varnothing$ (בקושי).

בעזרת התוצאות של שמידט: אם $y_1, \ldots, y_n \in \mathbb{R}^d$ אז $\bigcap_{i=1}^{n} \left(\mathrm{BA}_d + y_i\right) \neq \varnothing$.

שמידט הוכיח: BA_d קבוצה מנצחת ב- $\mathbb{R}^d$. מסקנה: אם $\Lambda_1, \Lambda_2, \ldots : \mathbb{R}^d \to \mathbb{R}^d$ העתקות אפיניות הפיכות אז $\bigcap_{i=1}^{\infty} \Lambda_i\left(\mathrm{BA}_d\right)$ מעוצמת הרצף (ובעלת מימד האוסדורף d).

נעיר שכאשר $d > 1$ אין פיתוח לשברים משולבים ולכן קשה להבין את הקבוצה BA_d. (מאידך, $x \in \mathrm{BA}_1$ $\Leftrightarrow$ הפיתוח של x כשבר משולב הוא בעל סדרת מקדמים חסומה.)

משפט (פישמן, 2008). תהי $\mathcal{C}$ קבוצת קנטור הסטנדרטית (דוגמה אחת מני רבות). אז $\mathrm{BA} \cap \mathcal{C}$ היא קבוצה מנצחת למשחק שמידט על $\mathcal{C}$.

מסקנה. אם $c_1, \ldots \in \mathbb{R}$ אז $\dim\left[\mathcal{C} \cap \bigcap_i \left(c_i + \mathrm{BA}\right)\right] = \dim \mathcal{C} = \frac{\log 2}{\log 3}$.

2013-05-08

[לא הייתי בשיעור, הסיכומים למטה הם השלמה עפ"י הסיכומים של רון ברק ושל יותם סמילנסקי]

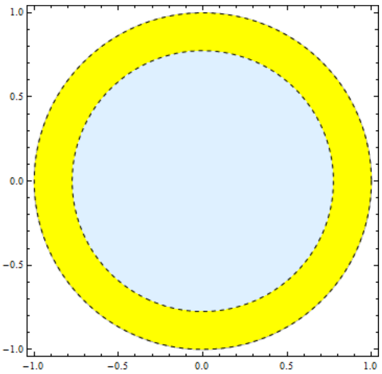
מידות ידידותיות לחלוטין

הגדרה. תהי μ מידת בורל סופית על $\mathbb{R}^d$.

- נאמר ש- μ **מקיימת תנאי פדרר (Federer condition)** אם קיים D כך שלכל $x \in \operatorname{supp} \mu$, ולכל $0 < r < 1$, מתקיים:

$$\mu\left(B\left(x, \frac{5}{6} r\right)\right) \geq D \cdot \mu\left(B\left(x, r\right)\right)$$

כלומר, לכדור הפנימי מידה לא קטנה בהרבה מהכדור החיצוני; לחילופין, אין ריכוז מידה על הטבעת:



הערה: אפשר גם לקחת קבוע אחר, קטן מ-1, במקום $\frac{5}{6}$.

- נאמר ש- μ **מקיימת תנאי דעיכה עם חזקה** a אם יש C כך שלכל $x \in \operatorname{supp} \mu$, לכל $0 < \varepsilon \le r < 1$, ולכל על-מישור אפיני L, מתקיים:
$$\mu\left(B(x,r) \cap L^{(\varepsilon)}\right) \le C\left(\frac{\varepsilon}{r}\right)^a \mu\left(B(x,r)\right)$$
כאשר $L^{(\varepsilon)} = \left\{x : \operatorname{dist}(x,L) < \varepsilon\right\}$.

- נאמר ש- μ **ידידותית לחלוטין (absolutely friendly)** אם היא מקיימת תנאי פדרר וכן תנאי דעיכה עם חזקה $a > 0$ כלשהי.

משפט (פישמן, 2009).
תהי μ ידידותית לחלוטין; נסמן $\mathcal{C} = \operatorname{supp} \mu$.
אז יש $0 < \alpha < 1$, $\alpha = \alpha(D, C, a)$ כך שלכל העתקה אפינית הפיכה $\Lambda : \mathbb{R}^d \to \mathbb{R}^d$, $\mathcal{C} \cap \Lambda(\mathrm{BA}_d)$ היא α-מנצחת במשחק שמידט על $\mathcal{C}$.

הערה. פישמן הוכיח שאם μ ידידותית לחלוטין אז $\mathcal{C} \cap S$ מנצחת על $\mathcal{C}$ $\Leftarrow$ $\dim \mathcal{C} = \dim S$.

מסקנות.

א. $\dim\left(\mathcal{C}_0 \cap \mathrm{BA}\right) = \dim \mathcal{C}_0 = \frac{\log 2}{\log 3}$ כאשר $\mathcal{C}_0$ קבוצת קנטור הקלאסית.
(אפריורית, לא ברור בכלל שקבוצת קנטור מכילה BA.)

ב. אם $a_1, a_2, \ldots$ מספרים שונים מאפס ו- $b_1, b_2, \ldots$ מספרים, אז
$$\dim\left[\mathcal{C} \cap \bigcap_{i=1}^{\infty}\left\{a_i x + b_i : x \in \mathrm{BA}\right\}\right] = \frac{\log 2}{\log 3}$$
בפרט, זו קבוצה לא ריקה.
נעיר שאם μ ידידותית לחלוטין אז $\operatorname{supp} \mu$ מפולג במובן מסויים במידה שווה.

ג. אם $\mathcal{C}$ פתית השלג של Koch או השטיח של Sierpiński או פרקטל אחר "המושך למערכת העתקות דמיון מכווצות המקיימות תנאי Hutchinson", אז לכל $\Lambda_1, \Lambda_2, \ldots$, $\Lambda_i : \mathbb{R}^d \to \mathbb{R}^d$ העתקות אפיניות הפיכות,

$$\varnothing \neq \mathcal{C} \cap \bigcap_{i=1}^{\infty} \Lambda_i\left(\mathrm{BA}_d\right)$$

(ולמעשה בעל המימד של $\mathcal{C}$.)

הלמה של Davenport

סימונים.

יהי $d \geq 1$. נסמן $c_d = \frac{1}{(r_d \cdot d!)^{1/d}}$ כאשר $r_d = \operatorname{vol} B_2^d$ נפח כדור היחידה האוקלידי ב- $\mathbb{R}^d$.

נקבע $R > 1$ והעתקה אפינית הפיכה $\Lambda : \mathbb{R}^d \to \mathbb{R}^d$.

בהינתן Λ, R כאלה, לכל $k \geq 1$ נסמן $\mathcal{U}_k = \left\{ \Lambda\left(\frac{p}{q}\right) : p \in \mathbb{Z}^d, q \in \mathbb{N}, R^{k-1} \leq q < R^k \right\}$.

למה (הלמה של Davenport).

אם $0 < \rho_0 < c_d \left|\det L_\Lambda\right|^{1/d} R^{-\left(1+\frac{1}{d}\right)}$, כאשר L_Λ החלק הלינארי של Λ, אז לכל $x \in \mathbb{R}^d$ ולכל $k \geq 1$ קיים על-מישור אפיני L כך ש- $L \supset \mathcal{U}_k \cap B\left(x, R^{-(k-1)\left(1+\frac{1}{d}\right)} \rho_0\right)$.

במילים אחרות, יש כדור קטן מספיק כך שאם נחתוך את תמונות הרציונליים $\mathcal{U}_k$ עם הכדור הזה, נקבל שכולם בתוך על-מישור אחד.

הוכחת הלמה.

נסמן ב- B את הכדור $B\left(x, R^{-(k-1)\left(1+\frac{1}{d}\right)} \rho_0\right)$.

נניח בשלילה שהתוצאה לא מתקיימת, כלומר יש $x \in \mathbb{R}^d$, $k \geq 1$ ו- $v_0, \ldots, v_d \in \mathcal{U}_k \cap B$ כך ש- $\Delta = \operatorname{conv}\{v_0, \ldots, v_d\}$ סימפלקס עם פנים לא-ריק (מימד מלא ב- $\mathbb{R}^d$).

לכל $0 \leq i \leq d$ נסמן $v_i = \Lambda\left(\frac{\vec{p}_i}{q_i}\right)$, כאשר $\vec{p}_i \in \mathbb{Z}^d$, $q_i \in \mathbb{N}$, $R^{k-1} \leq q_i < R^k$ לכל i.

הנפח של הסימפלקס הוא: $\lambda_d(\Delta) = \frac{1}{d!}\left|\det L_\Lambda\right|\left|\det L'\right|$, כאשר

$$L' = \begin{pmatrix} \frac{\vec{p}_1}{q_1} - \frac{\vec{p}_0}{q_0} \\ \frac{\vec{p}_2}{q_2} - \frac{\vec{p}_0}{q_0} \\ \vdots \\ \frac{\vec{p}_d}{q_d} - \frac{\vec{p}_0}{q_0} \end{pmatrix}_{d \times d}$$

נחשב את הדטרמיננטה של L':

$$\det L' = \det\begin{pmatrix} 1 & \frac{\vec{p}_0}{q_0} \\ 0 & \\ \vdots & \left(L'\right) \\ 0 & \end{pmatrix}_{(d+1)\times(d+1)} = \det\begin{pmatrix} 1 & \frac{\vec{p}_0}{q_0} \\ 1 & \frac{\vec{p}_1}{q_1} \\ \vdots & \vdots \\ 1 & \frac{\vec{p}_d}{q_d} \end{pmatrix}_{(d+1)\times(d+1)} = \frac{1}{q_0 q_1 \cdots q_d}\det\begin{pmatrix} q_0 & \vec{p}_0 \\ \vdots & \vdots \\ q_d & \vec{p}_d \end{pmatrix}_{(d+1)\times(d+1)}$$

לכן, מכיוון שהנחנו ש- $\lambda_d(\Delta) > 0$ (הסימפלקס בעל נפח) והמטריצה האחרונה היא מטריצה עם איברים שלמים, נקבל שהדטרמיננטה שלה היא לפחות 1 בערך מוחלט, כלומר:

$$\left|\det L'\right| \geq \frac{1}{q_0 \cdots q_d}$$

ומכאן:

$$\lambda_d(\Delta) \geq \frac{\left|\det L_\Lambda\right|}{d!\, q_0 \cdots q_d}$$

ומכיוון ש- $R^{k-1} \leq q_i < R^k$:

$$\lambda_d(\Delta) > \frac{\left|\det L_\Lambda\right|}{d!} R^{-k(d+1)}$$

מצד שני, מכיוון ש- Δ קמור ו- $v_i \in B$ לכל i, נקבל $\Delta \subset B$, ולכן:

$$\lambda_d(\Delta) \leq \lambda_d(B) = \lambda_d\left(B\left(x, R^{-(k-1)\left(1+\frac{1}{d}\right)}\rho_0\right)\right) = r_d R^{-(k-1)(d+1)} {\rho_0}^d \overset{\text{Assumption about } \rho_0}{<}$$

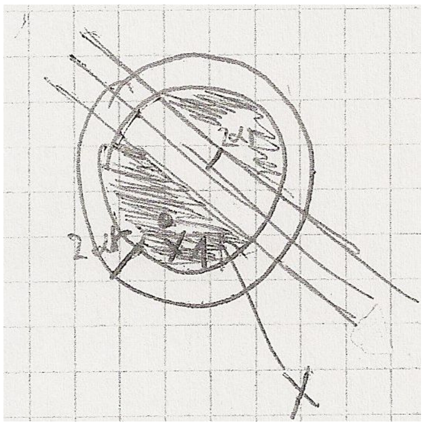
$$< r_d R^{-(k-1)(d+1)} {c_d}^d \left|\det L_\Lambda\right| R^{-(d+1)} = \frac{\left|\det L_\Lambda\right|}{d!} R^{-k(d+1)}$$

וזו סתירה לכך ש- Λ בעל פנים לא ריק.
מש"ל.

הוכחת משפט פישמן

נראה שאם μ ידידותית לחלוטין, אז יש α כך שלכל $x \in \mathcal{C}(=\operatorname{supp}\mu)$, לכל $0 < r < 1$ ולכל על-מישור אפיני L, מתקיים

$$(*) \qquad 0 < \mu\underbrace{\left\{x_1 \in B(x,r) \setminus L^{(2\alpha)} : B(x_1, \alpha r) \subset B(x, (1-\alpha) r)\right\}}_{X}$$



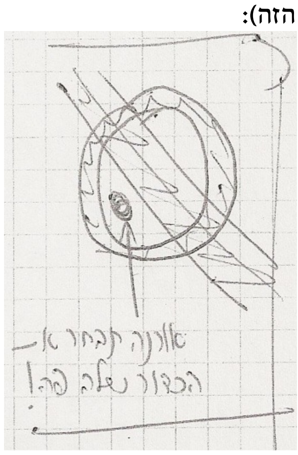
במילים אחרות, x_1 כנ"ל יקיים את התנאי שלכל $y \in B\left(x_1, \alpha r\right)$, $\operatorname{dist}\left(y, L\right) \ge \alpha r$ וכן $\operatorname{dist}\left(y, \partial B\left(x, r\right)\right) \ge \alpha r$. נוכיח את $(*)$:

$$\frac{\mu(X)}{\mu\left(B(x,r)\right)} \ge \frac{\mu\left(B\left(x,(1-2\alpha)r\right)\right)}{\mu\left(B(x,r)\right)} - \frac{\mu\left(B(x,r)\cap L^{(2\alpha r)}\right)}{\mu\left(B(x,r)\right)} \ge$$

$$\ge D - C\left(2\alpha\right)^{a} \ge \frac{D}{2}$$

(לפי תנאי פדרר ותנאי דעיכה אם α מספיק קטן: $\alpha < \frac{1}{12} \;\Leftrightarrow\; 1-2\alpha \ge \frac{5}{6}$).

נתאר אסטרטגיה עבור אורנה (עם ה-α הזה):



נסמן:

$$\alpha\beta = R^{-\left(1+\frac{1}{d}\right)} \qquad \Leftrightarrow \qquad R = \left(\alpha\beta\right)^{\frac{-d}{d+1}}.$$

נסמן $\tilde{\mathcal{U}}_k = \mathcal{U}_k \cap B_{k-1}$, כאשר $B_0, B_1, \ldots$ הם הכדורים שבועז בוחר, ו-

$$\mathcal{U}_k = \left\{ \Lambda\left(\frac{\vec{p}}{q}\right) : q \in \mathbb{N}, \vec{p} \in \mathbb{Z}^d, R^{k-1} \le q < R^k \right\}$$

בה"כ, אורנה יכולה להניח ש-r_0 , הרדיוס ההתחלתי שבועז בוחר, מקיים $r_0 < \min\left\{\rho_0, 1\right\}$ (ו-ρ_0 כמו בלמה). אחרת, אורנה מבצעת צעדי סרק עד שזה מתקיים.

לפי הלמה, לכל k ולכל בחירה אפשרית של בועז, יש על-מישור אפיני L_k כך ש- $\mathcal{U}_k \cap B_{k-1} \subset L_k$.

אורנה בוחרת:

$$A_k = B\left(y, \alpha r_k\right) \subset B_{k-1}$$

כאשר $r_k = r_0\left(\alpha\beta\right)^k$ ו- y שייכת לקבוצה X שהוכחנו ב-$(*)$ שיש לה מידה חיובית. כלומר:

$$\operatorname{dist}\left(y, L_k\right) \geq 2\alpha r_{k-1}$$

$$\operatorname{dist}\left(y, \partial B_k\right) \geq 2\alpha r_{k-1}$$

ואז אם $z_\infty \in \bigcap B_k$ ואם $\vec{p} \in \mathbb{Z}^d$, $q \in \mathbb{N}$, נבחר k כך ש- $R^{k-1} \leq q < R^k$, ומאחר ו- $z_\infty \in A_k$, מתקיימת אחת מהאלטרנטיבות הבאות:

(i) $\Lambda\left(\frac{\vec{p}}{q}\right) \notin B_k$ ואז $\operatorname{dist}\left(z_\infty, \Lambda\left(\frac{\vec{p}}{q}\right)\right) \geq \alpha r_{k-1}$

(ii) $\Lambda\left(\frac{\vec{p}}{q}\right) \in B_k$ ואז $\Lambda\left(\frac{\vec{p}}{q}\right) \in L_k$ ולכן $\operatorname{dist}\left(z_\infty, \Lambda\left(\frac{\vec{p}}{q}\right)\right) \geq \alpha r_{k-1}$

ובסה"כ, מתקיים:

$$\operatorname{dist}\left(z_\infty, \Lambda\left(\frac{\vec{p}}{q}\right)\right) \geq \alpha r_{k-1} = \alpha r_0 R^{-(k-1)\left(1+\frac{1}{d}\right)} \geq \alpha r_0 \left(Rq\right)^{-\left(1+\frac{1}{d}\right)}$$

כעת, אם נבחר $z'_\infty \in \Lambda^{-1}\left(z_\infty\right)$ אז מתקיים

$$\operatorname{dist}\left(z'_\infty, \frac{\vec{p}}{q}\right) \geq \underbrace{\frac{\alpha r_0}{R^{1+\frac{1}{d}}} C}_{\text{Const for } \mathrm{BA}_d} q^{-\left(1+\frac{1}{d}\right)}$$

כאשר C קבוע ליפשיץ של Λ. לכן, $z'_\infty \in \mathrm{BA}_d$ ומכאן $z_\infty \in \Lambda\left(\mathrm{BA}_d\right)$.

מש"ל (משפט פישמן).

קבוצות מקורבות טוב מאוד ממימד גבוה

תזכורת. הוכחנו את המשפט הבא:

אם μ מידת קנטור-לבג ($\operatorname{supp}\mu = \mathcal{C}_0$) אז $\mu\left(\mathrm{VWA}\right) = 0$, כאשר

$$\mathrm{VWA} = \left\{ x \in \mathbb{R} : \exists \varepsilon > 0, p_n, q_n \to \infty \ \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^{2+\varepsilon}} \right\}$$

למעשה, הוכחנו משפט יותר כללי: אם μ מידת בורל סופית על $\mathbb{R}$ עבורה קיימים C, α כך ש-

$$\mu\left(B\left(x, \varepsilon r\right)\right) \leq C\varepsilon^\alpha \mu\left(B\left(x, r\right)\right) \qquad \forall x \in \mathbb{R},\ r < 1,\ \varepsilon > 0$$

ואם ψ סדרה יורדת המקיימת $\sum_{q=1}^{\infty} q^{\alpha-1}\psi\left(q\right)^\alpha < \infty$, אזי $\mu\left\{x : \exists p_n, q_n : \left|q_n x - p_n\right| < \psi\left(q_n\right)\right\} = 0$.

כעת נכליל את העובדה הזו למימדים גבוהים יותר:

הגדרה. $\mathrm{VWA}_d := \left\{ x \in \mathbb{R}^d : \exists \varepsilon > 0, p_n \in \mathbb{Z}^d, q_n \in \mathbb{N}, \left\| x - \frac{p_n}{q_n} \right\| < \frac{1}{q_n^{1+\frac{1}{d}+\varepsilon}} \right\}$.

משפט. אם μ ידידותית לחלוטין אז $\mu\left(\mathrm{VWA}_d\right)=0$.

המשפט ינבע ממשפט חזק יותר: אם μ מידה סופית על $\mathbb{R}^d$, ידידותית לחלוטין, עם פרמטר a בתנאי הדעיכה, ו- $\varphi:\mathbb{N}\to\mathbb{R}_+$ מקיימת $\sum_{r=1}^{\infty} r^{\left(1+\frac{1}{d}\right)a-1}\varphi(r)^a<\infty$ ו- $r^{\left(1+\frac{1}{d}\right)a-1}\varphi(r)^a$ סדרה יורדת ב- r, אזי $\mu(\varphi\text{-approx})=0$, כאשר $\varphi\text{-approx}=\left\{x\in\mathbb{R}^d:\exists p_n,q_n\ \left\|x-\frac{p_n}{q_n}\right\|\le\varphi(q_n)\right\}$.

להוכחת המשפט, נזדקק ללמה הבאה:

למת כיסוי $3r$.
יהי (X,d) מרחב מטרי, $\mathcal{B}$ אוסף כל הכדורים בעלי אותו הרדיוס r עם מרכזים בקבוצה קומפקטית. אז יש $B_1,\dots,B_n\in\mathcal{B}$ זרים, כך ש- $\bigcup_{B\in\mathcal{B}}B\subset\bigcup_{i=1}^{n}3B_i$ (כאשר $3B_i=B(x_i,3r)$).

הערה. אפשר לנסח גרסה של הלמה מבלי להניח שכל הכדורים בעלי אותו הרדיוס או שהמרכזים שלהם בקבוצה קומפקטית.

הוכחה. יהי $B_1,\dots,B_n\in\mathcal{B}$ אוסף מקסימלי של כדורים זרים (יש כזה אוסף כי אלה כדורים זרים בעלי אותו רדיוס עם מרכזים בתוך קבוצה קומפקטית). כלומר אם $B\in\mathcal{B}$ ולא אחד מ- $B_1,\dots,B_n$, אז יש איזשהו j כך ש- $B_j\cap B\ne\varnothing$. נסמן $B=B(x_0,r)$ ו- $B_j=B(x_j,r)$. מתקיים $d(x_0,x_j)<2r$ מאי-שוויון המשולש, ולכן $B\subset B_j(x_j,3r)=3B_j$. **מש"ל.**

הוכחת המשפט.
הנחנו ש- $\sum_{r=1}^{\infty} r^{\left(1+\frac{1}{d}\right)a-1}\varphi(r)^a<\infty$, וסדרת המחוברים לא עולה. לפי מבחן העיבוי,

$$\sum_{n=1}^{\infty}\left(2^{n\left(1+\frac{1}{d}\right)}\varphi(2^n)\right)^{\alpha}<\infty \quad \text{ובפרט} \quad 2^{n\left(1+\frac{1}{d}\right)}\varphi(2^n)\xrightarrow{n\to\infty}0.$$

לכן קיים c_1 כך שלכל n מספיק גדול, $\dfrac{\varphi(2^n)}{2^{-n\left(1+\frac{1}{d}\right)}}\le c_1$.

נסמן $\mathcal{C}=\operatorname{supp}\mu$. בה"כ $\mathcal{C}$ קומפקטית.

מהלמה של Davenport, יש c_2 כך שלכל n, אם B כדור ברדיוס $c_2 2^{-\left(1+\frac{1}{d}\right)(n+1)}$, אז כל הנקודות $\frac{\vec{p}}{q}$, $\vec{p}\in\mathbb{Z}^d$, $2^n\le q<2^{n+1}$, $B\left(\frac{p}{q},\sqrt{d}\varphi(q)\right)\cap 3B\ne\varnothing$ מצויות על אותו על-מישור אפיני, L_B.

לכל n, נפעיל את למת הכיסוי עבור $\mathcal{B}$ - כל הכדורים עם רדיוס $c_2 2^{-\left(1+\frac{1}{d}\right)(n+1)}$ עם מרכז ב- $\mathcal{C}$.

נסמן $\mathcal{B} \supset \{B_1,\dots,B_n\} = \mathcal{D}_n$ כך ש: $\operatorname{supp}\mu \subset \bigcup_{B\in\mathcal{D}_n} 3B$.

כעת:

$$\sum_{B\in\mathcal{D}_n}\mu(3B) \overset{\text{Federer}}{\leq} c_3\sum_{B\in\mathcal{D}_n}\mu(B) \overset{\text{Disjoint}}{\leq} c_3\mu\left(\mathbb{R}^d\right) \overset{\text{Finite measure}}{=} c_4$$

כעת, נסמן $L_i := L_{B_i}$ לכל $B_i \in \mathcal{D}_n$, ונגדיר:

$$A_n := \bigcup_{2^n\leq q<2^{n-1}}\ \bigcup_{\vec{p}\in\mathbb{Z}^d} B\left(\frac{\vec{p}}{q},\sqrt{d}\varphi(q)\right)$$

($\sqrt{d}$ - השוואה בין נורמות.)

עבור בחירה זו, $\varphi\text{-approx} \subset A_\infty$, כאשר $A_\infty = \limsup_{n\to\infty} A_n$ כמו בלמה של בורל-קנטלי.

כעת, אם נסמן $\varepsilon = \sqrt{d}\varphi\left(2^n\right)$, נקבל:

$$\mu(A_n) = \mu\left(A_n \cap \bigcup_{B\in\mathcal{D}_n} 3B\right) \leq \sum_{B\in\mathcal{D}_n}\mu\left(3B\cap\mathcal{L}_B^{(\varepsilon)}\right) \overset{\text{Decay with parameter } a}{\leq}$$

$$\leq c_5\left(2^{n\left(1+\frac{1}{d}\right)}\varphi\left(2^n\right)\right)^a \sum_{B\in\mathcal{D}_n}\mu(3B) \leq c_6\left(2^{n\left(1+\frac{1}{d}\right)}\varphi\left(2^n\right)\right)^a$$

ומכאן:

$$\sum_{n=1}^{\infty}\mu(A_n) \leq c_6\sum_{n=1}^{\infty}\left(2^{n\left(1+\frac{1}{d}\right)}\varphi\left(2^n\right)\right)^a < \infty$$

ומשתמשים בלמה של בורל-קנטלי (מקרה ההתכנסות) לקבל ש- $\mu(A_\infty) = 0$, ולכן $\mu(\varphi\text{-approx}) = 0$.

מש"ל.

2013-05-22

[לא הייתי בשעה הראשונה – הושלמה על פי סיכומים של יותם סמילנסקי]

משפט Roth

$\alpha\in\mathbb{C}$ נקרא **אלגברי מדרגה** d אם יש פולינום $P\in\mathbb{Z}[x]$, $\deg P = d$, $P(\alpha)=0$, ואין פולינום כזה עם $\deg P < d$.

משפט (Roth, 1955). אם α אלגברי אי-רציונלי, אז לכל $\delta > 0$ יש מספר סופי לכל היותר של פתרונות $p,q\in\mathbb{Z}$ לאי-השוויון $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}$.

היסטוריה של תוצאות קשורות

בהינתן d, אפשר לשאול עבור איזה $\mu_0=\mu_0(d)$ מינימלי מתקיים שלכל $\mu>\mu_0$ ולכל אלגברי α מדרגה d יש מספר סופי לכל היותר של פתרונות לאי-השוויון $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^\mu}$.

- **Liouville (ככה"נ ~1844):** $\mu_0\le d$.
- **Thue (1909):** $\mu_0\le\frac{d}{2}+1$.
- **Siegel (1921):** $\mu_0\le 2\sqrt{d}$.
- **Dyson (1947):** $\mu_0\le\sqrt{2d}$.
- **Roth (1955) – המשפט שנוכיח:** $\mu_0=2$.

הערה Lang (1968): לכל אלגברי אי-רציונלי α ולכל $\delta>0$ יש מספר סופי לכל היותר של פתרונות לאי-השוויון $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2(\log p)^{1+\delta}}$.

עובדות על מספרים אלגבריים

א. אם α שורש של פולינום ב-$\mathbb{Q}[x]$ אז הוא אלגברי.

ב. אם α אלגברי מדרגה d אז יש פולינום $P\in\mathbb{Z}[x]$ כך שאם $Q\in\mathbb{Z}[x]$, $Q(\alpha)=0$ אז $P\mid Q$.
יתר על כן, אם נדרוש שלמקדמים של P אין מחלק משותף, והמקדם המוביל חיובי, אז P נקבע ביחידות ונקרא <u>הפולינום המינימלי</u> של α.

ג. השורשים האחרים של P נקראים <u>צמודי גלואה</u> של α, והם שורשים של כל פולינום ב-$\mathbb{Z}[x]$ ש-α שורש שלו.

ד. אם P הפולינום המינימלי של α אז $P'(\alpha)\neq 0$.

ה. אם $Q\in\mathbb{Z}[x]$, $Q(\alpha)=Q'(\alpha)=\ldots=Q^{(i)}(\alpha)=0$, אז לכל צמוד גלואה β של α גם מתקיים $Q(\beta)=Q'(\beta)=\ldots=Q^{(i)}(\beta)=0$.

משפט (Liouville). בהינתן α אלגברי מדרגה d, קיים קבוע $C>0$ כך שלכל p,q, $\left|\alpha-\frac{p}{q}\right|\ge\frac{C}{q^d}$.

הוכחה.
יהי $P\in\mathbb{Z}[x]$ הפולינום המינימלי של α. נפתח את P פיתוח טיילור סביב α.

$$P(x)=\underbrace{P(\alpha)}_{=0}+P'(\alpha)(x-\alpha)+\ldots+\frac{P^{(d)}(\alpha)(x-\alpha)^d}{d!}$$

אם $\frac{p}{q}\in\mathbb{Q}$, בה"כ $\left|\alpha-\frac{p}{q}\right|\le 1$, ואז

$$\left|P\left(\frac{p}{q}\right)\right|\le\left|P'(\alpha)\right|\left|\alpha-\frac{p}{q}\right|+\ldots+\left|\frac{P^{(d)}(\alpha)}{d!}\right|\left|\alpha-\frac{p}{q}\right|^d\le C(\alpha)\left|\alpha-\frac{p}{q}\right|$$

המעבר האחרון מוצדק מפני ש- $\left|\alpha-\frac{p}{q}\right|^i \le \left|\alpha-\frac{p}{q}\right|$, ושאר הביטויים לא תלויים ב- p,q אלא רק ב- P,α.

עבור המקרים $\left|\alpha-\frac{p}{q}\right|$ מספיק לקחת $C=1$ ולכן לוקחים את המקסימום של $C(\alpha)$ לעיל ו-1.

אבל $P\left(\frac{p}{q}\right)\neq 0$ כי P מינימלי, ולכן $q^d P\left(\frac{p}{q}\right)=q^d\left(a_0+a_1\frac{p}{q}+\ldots+a_d\frac{p^d}{q^d}\right)\in\mathbb{Z}\setminus\{0\}$, ולכן $\left|P\left(\frac{p}{q}\right)\right|\ge\frac{1}{q^d}$. כלומר:

$$\frac{1}{q^d}\le\left|P\left(\frac{p}{q}\right)\right|\le C(\alpha)\left|\alpha-\frac{p}{q}\right|$$

והטענה מתקבלת על ידי העברת אגפים ושינוי תפקיד C.
מש"ל.

כעת, נניח $F\in\mathbb{Z}[x,y]$ הומוגני מדרגה m, כלומר $F(x,y)=\sum_{k=0}^{m}a_k x^k y^{m-k}$.

$$\frac{1}{y^m}F(x,y)=\sum_{k=0}^{m}a_k\left(\frac{x}{y}\right)^k=a_m\prod_{k=1}^{m}\left(\frac{x}{y}-\lambda_k\right)$$

ולכן:

$$F(x,y)=a_m\prod_{k=1}^{m}(x-\lambda_k y)$$

ו- λ_k אלגברי מדרגה לכל היותר m (שורשים של פולינום במקדמים רציונליים).

באופן זה אפשר להציג כל תבנית מדרגה m בשני משתנים בתור $F(x,y)=b\prod_{i=1}^{m}(\gamma_i x+\delta_i y)$ $(*)$ כאשר $\gamma_i=1$ או $\gamma_i=0$ ואם $\gamma_i=0$ אז $\delta_i=1$, ו- δ_i אלגברי מדרגה לכל היותר m.

משפט (Thue). אם F תבנית בשני משתנים מדרגה $m\ge 3$ עם מקדמים שלמים, ונניח שבפירוק $(*)$ לפחות 3 מהתבניות הלינאריות שונות זו מזו, אז לכל $0\neq r\in\mathbb{Z}$ יש לכל היותר מספר סופי של פתרונות שלמים $(x,y)\in\mathbb{Z}^2$ למשוואה $F(x,y)=r$.

הוכחה.

נסמן $z=\begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{Z}^2$. נוכיח $F(z)\xrightarrow{z\to\infty}\infty$. אם לא, אז יש סדרה אינסופית של z-ים עבורם $F(z)$ חסומה, ובהוכחה נעבור לתתי-סדרות ונקבל סתירה.

נרשום $F(x,y)=b|\gamma_1 x+\delta_1 y|^{e_1}\cdot|\gamma_2 x+\delta_2 y|^{e_2}\cdot\ldots\cdot|\gamma_\ell x+\delta_\ell y|^{e_\ell}$, $\ell\ge 3$, ונניח ש- $(\gamma_1,\delta_1),(\gamma_2,\delta_2)$ בת"ל ב- $\mathbb{R}^2$ (יש לפחות 3 אז אפשר להניח).

נעבור לתת-סדרה ונשנה את סדר האינדקסים כך שהסדרה מקיימת $F(z)\neq 0$ וכן

$$0<|\gamma_1 x+\delta_1 y|\le|\gamma_2 x+\delta_2 y|\le\ldots\le|\gamma_\ell x+\delta_\ell y|$$

$\left(\gamma_1,\delta_1\right),\left(\gamma_2,\delta_2\right)$ בת"ל ב- $\mathbb{R}^2$ ולכן

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \left|\gamma_1 x+\delta_1 y\right|+\left|\gamma_2 x+\delta_2 y\right|$$

נורמה על $\mathbb{R}^2$. לכן יש C כך ש- $\left|\gamma_1 x+\delta_1 y\right|+\left|\gamma_2 x+\delta_2 y\right| \ge C\|z\|$. לכן:

$$C\|z\| \le \frac{\left|\gamma_1 x+\delta_1 y\right|+\left|\gamma_2 x+\delta_2 y\right|}{2} \le \left|\gamma_2 x+\delta_2 y\right| \le \ldots \le \left|\gamma_\ell x+\delta_\ell y\right|$$

$$\left\|F\left(z\right)\right\| \ge c_0\|z\|^{m-e_1}\left|\gamma_1 x+\delta_1 y\right|^{e_1}$$

נניח $\gamma_1=1$, $\delta_1 \notin \mathbb{Q}$: לכל δ יש c_2 כך ש:

$$\left|\gamma_1 x+\delta_1 y\right| = y\left|\frac{x}{y}+\delta_1\right| \overset{\text{Roth}}{\ge} c_2 y^{-(1+\delta)}$$

לכן

$$\left\|F\left(z\right)\right\| \ge c_2 c_0\|z\|^{m-e_1}\left|y\right|^{-(1+\delta)e_1} \ge c_2 c_0\left|y\right|^{m-(2+\delta)e_1} \xrightarrow{z\to\infty} 0$$

אם $e_1=1$ $m\ge 3$.

אם $e_1>1$ $m\ge 3e_1$ כי כל צמודי גלואה של δ_1 מופיעים בריבוי e_1 לפחות.

אם $\delta_1\in\mathbb{Q}$ אז $\left|\frac{x}{y}+\delta_1\right| \ge \frac{c}{y}$ זהו רציונלי שהמכנה שלו הוא y כפול המכנה של c ולא יכול להיות אפס.

ואז:

$$\left\|F\left(z\right)\right\| \ge c\left(\frac{c}{y}\right)^{e_1}\|z\|^{m-e_1} \xrightarrow{z\to\infty} \infty$$

מש"ל.

הוכחת משפט Roth

למות קומבינטוריות

למה 1. יהיו $r_1,\ldots,r_m\in\mathbb{N}$, $0<\varepsilon<1$.

מספר ה- m-יות $\left(i_1,\ldots,i_m\right)\in\mathbb{Z}^m$ המקיימות $0\le i_1\le r_1,\ldots,0\le i_j\le r_j$, $\left|\left(\sum_{j=1}^{m}\frac{i_j}{r_j}\right)-\frac{m}{2}\right|\ge\varepsilon m$, הוא

לכל היותר $\left(r_1+1\right)\cdots\left(r_m+1\right)\cdot 2e^{-\frac{1}{4}\varepsilon^2 m}$.

נקבל את למה 1 כמסקנה מלמה 2 שננסח ונוכיח לאחר טענת העזר הבאה:

טענת עזר. יהיו $n,r\in\mathbb{Z}_+$, $n\ge 1$.

אזי מספר ה- n-יות $\left(i_1,\ldots,i_n\right)\in\mathbb{Z}_+^n$ המקיימות $\sum_{j=1}^{r} i_j=r$ הוא $\binom{r+n-1}{r}$.

הוכחה. לכל בחירה של r מספרים מבין המספרים $1,\dots,r+n-1$ נתאים n-יה כזו באופן חח"ע ועל: לדוגמה,

<u>O O X O X O O O X X O O</u>

המספרים מבין $1,\dots,r+n-1$ שבחרנו מסומנים ב-X והמספרים שלא בחרנו ב-O. חושבים על ה-O-ים בתור מחיצות, ובסה"כ יש $n+1$ מחיצות. בתור $i_1,\dots,i_n$ נבחר את כמות המספרים בכל מחיצה, כלומר $i_j=k_j-k_{j-1}$ כאשר k_j המיקום של המחיצה ה-j בסדר עולה.
מש"ל.

למה 2. יהיו $r_1,\dots,r_m$ טבעיים, $0<\varepsilon<1$, $n\geq 2$ טבעי.

אז מספר ה-nm-יות $\begin{pmatrix} i_{11} & \cdots & i_{1n} \\ \vdots & \ddots & \vdots \\ i_{m1} & \cdots & i_{mn} \end{pmatrix}_{m\times n}$ של מספרים שלמים אי-שליליים המקיימים $\sum_{k=1}^{n} i_{jk}=r_j$ לכל $j=1,\dots,m$, וכן $\left|\left(\sum_{j=1}^{m}\frac{i_{j1}}{r_j}\right)-\frac{m}{n}\right|\geq\varepsilon m$, הוא לכל היותר $\binom{r_1+n-1}{r_1}\cdots\binom{r_m+n-1}{r_m}\cdot 2e^{-\frac{1}{4}\varepsilon^2 m}$.

הוכחת למה 1 כמסקנה מלמה 2.
ניקח $n=2$. הצורה הכללית של ה-$2m$-יות מלמה 2 (מכיוון שהסכום של השורה ה-j הוא r_j) היא:

$$\begin{pmatrix} i_1 & r_1-i_1 \\ \vdots & \vdots \\ i_m & r_m-i_m \end{pmatrix}_{m\times 2}$$

מכאן, יש התאמה חח"ע ועל בין ה-$2m$-יות המקיימות את תנאי למה 2 לבין ה-m-יות המקיימות את תנאי למה 1. לבסוף, המקדם של האקספוננט בלמה 2 הוא בדיוק $(r_1+1)\cdots(r_m+1)=\binom{r_1+1}{r_1}\cdots\binom{r_m+1}{r_m}$.

מש"ל.

הוכחת למה 2.

נסמן ב-M_+ את מספר ה-nm-יות המקיימות $\sum_{k=1}^{n} i_{jk}=r_j$ לכל $1\leq j\leq m$ וגם $\left(\sum_{j=1}^{m}\frac{i_{j1}}{r_j}\right)-\frac{m}{n}\geq\varepsilon m$.

נסמן ב-M_- את מספר ה-nm-יות המקיימות $\sum_{k=1}^{n} i_{jk}=r_j$ לכל $1\leq j\leq m$ וגם $\left(\sum_{j=1}^{m}\frac{i_{j1}}{r_j}\right)-\frac{m}{n}\leq-\varepsilon m$.

צ"ל: $M_+ + M_- \leq \binom{r_1+n-1}{r_1}\cdots\binom{r_m+n-1}{r_m}\cdot 2e^{-\frac{1}{4}\varepsilon^2 m}$.

נניח שנתונים $c_\ell\in\{0,\dots,r_\ell\}$, לכל $\ell=1,\dots,m$ (בחירות של ערכים ל-$i_{\ell 1}$), ונסמן ב-$f_\ell(c_\ell)$ את מספר ה-$(n-1)$-יות של שלמים אי-שליליים $i_{\ell 2},\dots,i_{\ell n}$ המקיימים $i_{\ell 2}+\ldots+i_{\ell n}=r_\ell-c_\ell$.
לפי הגדרת M_+,M_-, מתקיים

$$M_{\pm} = \sum_{\vec{c} \in \mathcal{A}_{\pm}} f_1(c_1) \cdots f_m(c_m)$$

כאשר $\vec{c} = (c_1, \ldots, c_m) \in \mathcal{A}_+$ אם $\left(\sum_{j=1}^{m} \frac{c_j}{r_j} \right) - \frac{m}{n} \geq \varepsilon m$, וכן $\vec{c} \in \mathcal{A}_-$ אם $\left(\sum_{j=1}^{m} \frac{c_j}{r_j} \right) - \frac{m}{n} \leq -\varepsilon m$.

לכן מתקיים:

$$M_{\pm} e^{\frac{1}{2}\varepsilon^2 m} \leq \sum_{c_1=0}^{r_1} \cdots \sum_{c_m=0}^{r_m} f_1(c_1) \cdots f_m(c_m) \exp\left(\pm \frac{\varepsilon}{2} \left(\left(\sum_{j=1}^{m} \frac{c_j}{r_j} \right) - \frac{m}{n} \right) \right)$$

הסבר: אם $\vec{c} \in \mathcal{A}_+$ אז משתמשים באי-השוויון $\varepsilon m \leq (\cdots)$ ואם $\vec{c} \notin \mathcal{A}_+$ אז הוספנו מספר חיובי. כך במקרה ה- $+$ וכנ"ל במקרה ה-$-$.

את אגף ימין אפשר לכתוב כך:

$$\prod_{\ell=1}^{m} \left(\sum_{c_\ell=0}^{r_\ell} f_\ell(c_\ell) \exp\left(\pm \frac{\varepsilon}{2} \left(\frac{c_\ell}{r_\ell} - \frac{1}{n} \right) \right) \right)$$

ונרצה להעריך את כל אחד מהגורמים במכפלה. כעת,

$$\sum_{c=0}^{r_\ell} f_\ell(c) = \sum_{\substack{c, i_2, \ldots, i_n \\ c + i_2 + \ldots + i_n = r_\ell}} 1 = \binom{r_\ell + n - 1}{r_\ell}$$

אפשר להוכיח בקלות שלכל $x \in [-1,1]$ מתקיים $e^x \leq 1 + x + x^2$, לכן:

$$\sum_{c=0}^{r_\ell} f_\ell(c) \exp\left(\pm \frac{\varepsilon}{2} \left(\frac{c}{r_\ell} - \frac{1}{n} \right) \right) \leq \sum_{c=0}^{r_\ell} f_\ell(c) \left(1 \pm \frac{\varepsilon}{2} \left(\frac{c}{r_\ell} - \frac{1}{n} \right) + \frac{\varepsilon^2}{4} \underbrace{\left(\frac{c}{r_\ell} - \frac{1}{n} \right)^2}_{\leq 1} \right) \leq$$

$$\leq \sum_{c=0}^{r_\ell} f_\ell(c) \left(1 + \frac{\varepsilon^2}{4} \right) \pm \frac{\varepsilon}{2 r_\ell} \underbrace{\left(\sum_{c=0}^{r_\ell} c f_\ell(c) - \frac{r_\ell}{n} \sum_{c=0}^{r_\ell} f_\ell(c) \right)}_{(*)}$$

אבל למעשה $(*) = 0$. נראה זאת:

$$f_\ell(c) = \sum_{\substack{i_2, \ldots, i_n \\ i_2 + \ldots + i_n = r_\ell - c}} 1 = \sum_{\substack{i_1, i_2, \ldots, i_n \\ i_1 + i_2 + \ldots + i_n = r_\ell \\ i_1 = c}} 1$$

$$c \cdot f_\ell(c) = \sum_{\substack{i_1, i_2, \ldots, i_n \\ i_1 + i_2 + \ldots + i_n = r_\ell \\ i_1 = c}} i_1$$

$$\sum_{c=0}^{r_\ell} c \cdot f_\ell(c) = \sum_{\substack{i_1, i_2, \ldots, i_n \\ i_1 + i_2 + \ldots + i_n = r_\ell}} i_1 = \frac{1}{n} \sum_{\substack{i_1, i_2, \ldots, i_n \\ i_1 + i_2 + \ldots + i_n = r_\ell}} (i_1 + \ldots + i_n) = \frac{r_\ell}{n} \sum_{\substack{i_1, i_2, \ldots, i_n \\ i_1 + i_2 + \ldots + i_n = r_\ell}} 1 = \frac{r_\ell}{n} \sum_{c=0}^{r_\ell} f_\ell(c)$$

והשוויון האחרון הוא בדיוק $(*) = 0$. מכך, נקבל:

$$\sum_{c=0}^{r_\ell} f_\ell(c)\exp\left(\pm\frac{\varepsilon}{2}\left(\frac{c}{r_\ell}-\frac{1}{n}\right)\right)\le\left(1+\frac{\varepsilon^2}{4}\right)\sum_{c=0}^{r_\ell} f_\ell(c)=\left(1+\frac{\varepsilon^2}{4}\right)\binom{r_\ell+n-1}{r_\ell}$$

ולכן:

$$M_\pm e^{\frac{1}{2}\varepsilon^2 m}\le\prod_{\ell=1}^{m}\left[\binom{r_\ell+n-1}{r_\ell}\left(1+\frac{\varepsilon^2}{4}\right)\right]=\left(1+\frac{\varepsilon^2}{4}\right)^m\prod_{\ell=1}^{m}\binom{r_\ell+n-1}{r_\ell}$$

ומכך ש- $e^{\frac{\varepsilon^2}{4}}\ge 1+\frac{\varepsilon^2}{4}$, מקבלים

$$M_\pm e^{\frac{1}{2}\varepsilon^2 m}\le e^{\frac{1}{4}\varepsilon^2 m}\prod_{\ell=1}^{m}\binom{r_\ell+n-1}{r_\ell}$$

כעת מעבירים אגפים, ומקבלים את הנדרש.

מש"ל.

טענות עזר על פולינומים

נדון בפולינומים במקדמים שלמים ב- m משתנים. ראשית, סימונים והגדרות:

סימון מולטי-אינדקס: $P(X_1,\dots,X_m)=\sum_J C_J\mathcal{X}^J$, כאשר $J=(j_1,\dots,j_m)$ ו- $\mathcal{X}^J=X_1^{j_1}\cdots X_m^{j_m}$.
לכל J $C_J\in\mathbb{Z}$, ו- $C_J=0$ פרט למספר סופי של J-ים.

גובה של פולינום: $\lceil P\rceil:=\max_J|C_J|$.

אופרטור גזירה: אם $I=(i_1,\dots,i_m)$, נגדיר $P_I=\frac{1}{i_1!\cdots i_m!}\frac{\partial^{i_1+\dots+i_m}}{\partial X_1^{i_1}\cdots\partial X_m^{i_m}}P$.

למה. גם ל- P_I מקדמים שלמים.
כמו-כן, אם ל- P דרגה לכל היותר r_j במשתנה X_j, אז $\lceil P_I\rceil\le 2^{r_1+\dots+r_m}\lceil P\rceil$.

הוכחה.
נסכים ש- $\binom{m}{n}=0$ כאשר $n>m$. אז נכתוב במפורש את הגזירה:

$$P(X_1,\dots,X_m)=\sum_{j_1=0}^{r_1}\cdots\sum_{j_m=0}^{r_m}C_J X^{j_1}\cdots X^{j_m}$$

$$P_I(X_1,\dots,X_m)=\sum_{j_1=0}^{r_1}\cdots\sum_{j_m=0}^{r_m}\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}C_J X^{j_1-i_1}\cdots X^{j_m-i_m}$$

זה מוכיח שהמקדמים שלמים. כעת נחסום את המקדמים:

$$\left|\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}C_J\right|\le 2^{j_1}\cdots 2^{j_m}|C_J|\le 2^{r_1+\dots+r_m}\lceil P\rceil$$

ע"י לקיחת $\max_J$ על אגף שמאל נקבל $\lceil P_I \rceil \le 2^{r_1+\ldots+r_m} \lceil P \rceil$.
מש"ל.

הלמה של זיגל (Siegel).
יהיו $N > M$ טבעיים, ולכל $j=1,\ldots,M$, יהי L_j פונקציונל לינארי:

$$L_j\left(z_1,\ldots,z_N\right)=\sum_{k=1}^{N} a_{jk} z_k$$

עם $a_{jk} \in \mathbb{Z}$ לכל j,k. (כלומר נתונות M תבניות לינאריות במקדמים שלמים על N משתנים.)

נניח ש- $A \in \mathbb{N}$ מקיים $\left|a_{jk}\right| \le A$ לכל j,k. אז יש $z=\left(z_1,\ldots,z_N\right)\in\mathbb{Z}^N$ המאפס את כל התבניות: $0=L_1\left(z\right)=\ldots=L_m\left(z\right)$, והרכיבים שלו חסומים ע"י: $0<\|z\|_\infty \le \left\lfloor (NA)^{\frac{M}{N-M}} \right\rfloor$.

הוכחה.
ההוכחה היא לפי עקרון שובך היונים. נסמן: $T=\left\lfloor (NA)^{\frac{M}{N-M}} \right\rfloor$. אזי

$$\begin{aligned} & T+1>(NA)^{\frac{M}{N-M}} \\ \Rightarrow\quad & NA<(T+1)^{\frac{N-M}{M}} \\ \Rightarrow\quad & NAT+1 \le NA(T+1)<(T+1)^{\frac{N}{M}} \\ \Rightarrow\quad & (NAT+1)^M<(T+1)^N \end{aligned}$$

באי-השוויון האחרון נשתמש בהפעלת עקרון שובך היונים.
לכל $z=\left(z_1,\ldots,z_N\right)$ כך ש- $0 \le z_i \le T$ לכל i, מתקיים

$$-B_j T \le L_j\left(z\right) \le C_j T$$

כאשר $-B_j, C_j$ סכומי המקדמים החיוביים והשליליים בהתאמה של L_j.
מכיוון ש- $\left|a_{jk}\right| \le A$, מתקיים $B_j+C_j \le NA$ (חסם על סכום N הערכים המוחלטים באותה השורה).
לכן כל המספרים $L_j\left(z\right)$, עבור הצבות שונות של z, הם בקטע (ב- $\mathbb{R}$) שאורכו NAT, כלומר כל $L_j\left(z\right)$ מקבל לכל היותר $NAT+1$ ערכים. מכאן, ה- M-יה $\left(L_1\left(z\right),\ldots,L_M\left(z\right)\right)$ מקבלת לכל היותר $\left(NAT+1\right)^M$ ערכים על קבוצת z-ים בגודל $\left(T+1\right)^N$. אבל ראינו ש- $\left(NAT+1\right)^M<\left(T+1\right)^N$, ולכן מעקרון שובך היונים יש $z_1 \ne z_2$ כך ש- $L_j\left(z_1\right)=L_j\left(z_2\right)$ לכל $j=1,\ldots,m$, וההפרש z_1-z_2 יקיים את הנדרש.
מש"ל.

הגדרה. מספר אלגברי α נקרא <u>שלם אלגברי</u> אם לפולינום המינימלי שלו (במקדמים שלמים) מקדם מוביל 1.
זה שקול, לפי הלמה של גאוס, לכך שקיים פולינום המאפס את α עם מקדמים שלמים עם מקדם מוביל 1.

הערה. אם α אלגברי כלשהו: $a_0+a_1\alpha+\ldots a_d\alpha^d=0$, עבור $a_0,\ldots,a_d\in\mathbb{Z}$, אז המספר $\beta=a_d\alpha$ הוא שלם אלגברי:

$$\begin{aligned}&\beta^d+a_{d-1}\beta^{d-1}+a_{d-2}a_d\beta^{d-2}+\ldots+a_0{a_d}^{d-1}=\\&=\left(a_d\alpha\right)^d+a_{d-1}\left(a_d\alpha\right)^{d-1}+\ldots+a_0{a_d}^{d-1}=\\&={a_d}^{d-1}\left(a_d\alpha^d+a_{d-1}\alpha^{d-1}+\ldots+a_0\right)=0\end{aligned}$$

מסקנה. מספיק להוכיח את משפט Roth רק לשלמים אלגבריים. זאת מפני שאם β מקיים את מסקנת משפט Roth, כלומר יש מספר סופי של פתרונות ל- $\left|\beta-\frac{p}{q}\right|<\frac{1}{q^{2+\delta}}$, נראה שגם α מקיים זאת: לכל פתרון לאי-השוויון $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^{2+\delta}}$, מתקיים $\left|\beta-\frac{a_d p}{q}\right|<\frac{|a_d|}{q^{2+\delta}}$, ויש רק מספר סופי של פתרונות כאלה בהנחת נכונות המשפט לשלמים אלגבריים.

2013-05-29

הראינו בשיעור הקודם שמספיק להוכיח את משפט Roth רק לשלמים אלגברים והמקרה הכללי נובע מכך.
נניח α שלם אלגברי, עם פולינום מינימלי $Q(x)=a_0+a_1x+\ldots+a_{d-1}x^{d-1}+x^d$.

טענה. לכל שלם $\ell\geq 0$, יש שלמים $a_1^{(\ell)},\ldots,a_d^{(\ell)}$ כך ש- $\alpha^\ell=a_d^{(\ell)}\alpha^{d-1}+\ldots+a_2^{(\ell)}\alpha+a_1^{(\ell)}$.
כלומר, α^ℓ צירוף לינארי של $1,\alpha,\ldots,\alpha^{d-1}$ עם מקדמים שלמים, ומתקיים $\left|a_i^{(\ell)}\right|\leq\left(\lceil Q\rceil+1\right)^\ell$, כאשר $\lceil Q\rceil:=\max\left|a_i\right|$.

הוכחה. באינדוקציה על ℓ. אם $\ell\leq d-1$ זה ברור. נוכיח $\ell=d$ על סמך נכונות עבור $\ell\leq d-1$:

$$\begin{aligned}\alpha^\ell&=\alpha\cdot\alpha^{\ell-1}=\alpha\left(a_d^{(\ell-1)}\alpha^{d-1}+\ldots+a_1^{(\ell-1)}\right)=\\&=a_d^{(\ell-1)}\alpha^d+a_{d-1}^{(\ell-1)}\alpha^{d-1}+\ldots+\alpha a_1^{(\ell-1)}=\\&=a_d^{(\ell-1)}\left(-a_0-a_1\alpha-\ldots-a_d\alpha^{d-1}\right)+a_{d-1}^{(\ell-1)}\alpha^{d-1}+\ldots+\alpha a_1^{(\ell-1)}\end{aligned}$$

כלומר הבענו את α^ℓ על ידי צירוף לינארי של $1,\alpha,\ldots,\alpha^{d-1}$, עם המקדמים:

$$a_i^{(\ell)}=a_{i-1}^{(\ell-1)}-a_{d-1}^{(\ell-1)}a_i$$

ואכן:

$$\left|a_i^{(\ell)}\right|\overset{\text{induction hypothesis}}{\leq}\left(\lceil Q\rceil+1\right)^{\ell-1}+\lceil Q\rceil\left(\left(\lceil Q\rceil+1\right)^{\ell-1}\right)=\left(\lceil Q\rceil+1\right)^\ell$$

מש"ל.

אינדקס של פולינום

האינדקס של פולינום בנקודה נתונה מודד "עד כמה הפולינום מתאפס" שם, עם משקל שונה למשתנים השונים בפולינום.

יהיו $P\in\mathbb{Z}\left[x_1,\ldots,x_m\right]$, $\vec{r}=\left(r_1,\ldots,r_m\right)\in\mathbb{N}^m$, $\vec{\alpha}=\left(\alpha_1,\ldots,\alpha_m\right)\in\mathbb{R}^m$.
האינדקס של P ביחס ל- $\vec{r},\vec{\alpha}$ הוא $\min\left\{\frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m}:\frac{\partial^{i_1+\ldots+i_m}P}{\partial x_1^{i_1}\cdots\partial x_m^{i_m}}\left(\vec{\alpha}\right)\neq 0\right\}$, או $+\infty$ אם $P\equiv 0$.

סימון. $\operatorname{Ind} P$ או $\operatorname{Ind}_{\vec{\alpha},\vec{r}} P$.

נזכיר שסימנו בהינתן מולטי-אינדקס I את הנגזרת החלקית המנורמלת $P_I = \frac{1}{i_1!\cdots i_m!}\frac{\partial^{i_1+\ldots+i_m} P}{\partial x_1^{i_1}\cdots\partial x_m^{i_m}}$.

תכונות.
עבור $\vec{\alpha},\vec{r}$ כנ"ל, מתקיים:

א. $\operatorname{Ind} P_I \geq \operatorname{Ind} P - \sum_{k=1}^{m}\frac{i_k}{r_k}$

ב. $\operatorname{Ind}(P+Q) \geq \min\{\operatorname{Ind} P, \operatorname{Ind} Q\}$

ג. $\operatorname{Ind}(PQ) = \operatorname{Ind} P + \operatorname{Ind} Q$

הערה. תכונות ב' וג' אומרות שאינדקס הוא הערכה (valuation) בחוג הפולינומים. בפרט, אם $0<\lambda<1$, אז $P \mapsto \lambda^{\operatorname{Ind} P}$ נורמה אולטרה-מטרית.

הוכחה.
א': נסמן $T = P_I$. אם $T_J(\vec{\alpha}) \neq 0$ אז $P_{I+J}(\vec{\alpha}) \neq 0$ ולכן $\frac{i_1+j_1}{r_1}+\ldots+\frac{i_m+j_m}{r_m} \geq \operatorname{Ind} P$. ע"י העברת אגפים נקבל $\frac{j_1}{r_1}+\ldots+\frac{j_m}{r_m} \geq \operatorname{Ind} P - \sum_{k=1}^{m}\frac{i_k}{r_k}$. על ידי לקיחת מינימום על אגף שמאל נקבל את הנדרש.

ב': אם $P_J(\vec{\alpha})+Q_J(\vec{\alpha}) = (P+Q)_J(\vec{\alpha}) \neq 0$ אז לפחות אחד מבין $P_J(\vec{\alpha})$, $Q_J(\vec{\alpha})$ לא מתאפס. כלומר, $\frac{j_1}{r_1}+\ldots+\frac{j_m}{r_m} \geq \min\{\operatorname{Ind} P, \operatorname{Ind} Q\}$. נקח מינימום על אגף שמאל ונקבל את הנדרש.

ג': נדלג על ההוכחה.
מש"ל.

משפט האינדקס

יהי α אלגברי מדרגה $d \geq 2$. אז יש $B = B(\alpha) > 0$ כך שלכל $\varepsilon > 0$, $m \in \mathbb{N}$ עם $m > \frac{16}{\varepsilon^2}\log(4d)$, ו-$r_1,\ldots,r_m \in \mathbb{N}$, יש $P \in \mathbb{Z}[x_1,\ldots,x_m]$ בעל התכונות:

א. הדרגה של P במשתנה x_j היא לכל היותר r_j.

ב. $\operatorname{Ind}_{\vec{\alpha},\vec{r}} P \geq \frac{m}{2}(1-\varepsilon)$.

ג. $\lceil P \rceil \leq B^{r_1+\ldots+r_m}$.

הוכחה. יהי Q הפולינום המינימלי של α, ונסמן $B = 4(\lceil Q \rceil + 1)$.
אנו מחפשים פולינום P מהצורה $P(X) = \sum_J c_J X^J$ (סימון מולטי-אינדקס, $c_J \in \mathbb{Z}$).

נסמן $N = (r_1+1)\cdots(r_m+1)$. זהו מספר המקדמים ב-P שאינם אפס לפי הדרישה הראשונה. רוצים לבחור אותם כך שתכונות ב' ו-ג' יתקיימו.

הפירוש של תכונה ב' הוא שאם $\frac{-\varepsilon m}{2} > \frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m}-\frac{m}{2}$ אז $P_I(\vec{\alpha})=0$.

לפי "למה ו" שהוכחנו בשיעור שעבר, מספר הבחירות של I שיקיימו $\left(\sum_{k=1}^{m}\frac{i_k}{r_k}\right)-\frac{m}{2}<\frac{-\varepsilon m}{2}$ אינו עולה על $2N\exp\left(\frac{-\varepsilon^2 m}{16}\right)<\frac{N}{2d}$ (ה-ε מהלמה הוא $\frac{\varepsilon}{2}$ כאן, ולכן הקבוע 4 הוחלף ב-16).

נחשוב על כל אחד מהתנאים $P_I(\vec{\alpha})=0$, I כנ"ל, כתנאי לינארי על המקדמים c_J.

$$P_I(\vec{\alpha})=\sum_J c_J\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}\alpha^{j_1-i_1}\cdots\alpha^{j_m-i_m}$$

המשוואות $P_I(\vec{\alpha})=0$ הן משוואות לינאריות עבור c_J-ים, עם מקדמים שהם חזקות של α.

את החזקות של α אפשר להחליף בצירופים לינאריים עם מקדמים שלמים של $1,\alpha,\ldots,\alpha^{d-1}$.

התנאי יתקיים אם הכופל של α^i במשוואות הנ"ל יהיה 0 לכל i. לכן יש לנו לכל היותר $\frac{dN}{2d}=\frac{N}{2}$ משוואות. נסמן את מספר המשוואות ב-M, $M\le\frac{N}{2}$, ואלה משוואות בנעלמים (c_J) עם מקדמים שלמים.

נסמן ב-A את המקסימום של הערכים המוחלטים של המקדמים (השלמים) במשוואות האלה.
לכל J, המקדם ה-J במשוואה $P_I(\vec{\alpha})=0$ לא עולה על

$\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}\left(\lceil Q\rceil+1\right)^{\ell}\le 2^{j_1+\ldots+j_m}\left(\lceil Q\rceil+1\right)^{\ell}$, כאשר $\ell=(j_1-i_1)+\ldots+(j_m-i_m)$.

לכן: $A\le\left(2\left(\lceil Q\rceil+1\right)\right)^{r_1+\ldots+r_m}$.

לפי הלמה של זיגל, למערכת המשוואות הנ"ל יש פתרון לא טריוויאלי (c_J), $c_J\in\mathbb{Z}$, המקיים את ההערכה:

$$\sup_J|c_J|\overset{\text{Siegel's lemma}}{\le}(NA)^{\frac{M}{N-M}}\overset{M\le\frac{N}{2}}{\le}NA=2^{r_1+\ldots+r_m}\left(2\left(\lceil Q\rceil+1\right)\right)^{r_1+\ldots+r_m}=B^{r_1+\ldots+r_m}$$

מש"ל.

מעתה ואילך, α שלם אלגברי מדרגה $d\ge2$.

משפט. קיים $D=D(\alpha)>0$ כך שלכל

- $\varepsilon>0$,
- $m>\frac{16}{\varepsilon^2}\log(4d)$ טבעי,
- $P\in\mathbb{Z}[x_1,\ldots,x_m]$ פולינום המקיים את התכונות ממשפט האינדקס,
- $\delta>0$ המקיים $0<\varepsilon<\frac{\delta}{36}$,

- $\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\in\mathbb{Q}$ כך שלכל $j=1,\dots,m$ מתקיים
  - $\left|\alpha-\frac{p_j}{q_j}\right|<\frac{1}{q^{2+\delta}}$,
  - $q_j^{\delta}>D$,
  - $r_1\log q_1\le r_j\log q_j\le(1+\varepsilon)r_1\log q_1$,

אז האינדקס של P ביחס ל-$\overbrace{(r_1,\dots,r_m)}^{\vec{r}},\overbrace{\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)}^{\vec{\alpha}}$ הוא לפחות εm.

הוכחה. יהי $B=B(\alpha)$ כמו במשפט האינדקס, ונסמן $C=8B\max\{1,|\alpha|\}$, $D=(2C)^4$.

יהי J מולטי-אינדקס המקיים $\frac{j_1}{r_1}+\ldots+\frac{j_m}{r_m}<\varepsilon m$. עלינו להראות $T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)=0$ כאשר $T=P_J$

(כאשר $P,\frac{p_i}{q_i}$ הם לפי בתנאי המשפט).

לפי בחירת P, $\lceil P\rceil\le B^{r_1+\ldots+r_m}$ ולכן $\lceil T\rceil\le(2B)^{r_1+\ldots+r_m}$.

יהי I מולטי-אינדקס. אז $\lceil T_I\rceil\le(4B)^{r_1+\ldots+r_m}$.

לכן כשמעריכים את $T_I(\vec{\alpha})$, $\vec{\alpha}=(\alpha,\dots,\alpha)$, לכל מחובר ערך מוחלט של לכל היותר $(4B)^{r_1+\ldots+r_m}\max\{1,|\alpha|\}^{r_1+\ldots+r_m}$.

מספר המחוברים ב-T_I הוא לכל היותר $(r_1+1)\cdots(r_m+1)\le 2^{r_1+\ldots+r_m}$. לכן

$$\left|T_I(\vec{\alpha})\right|\le\left(8B\max\{1,|\alpha|\}\right)^{r_1+\ldots+r_m}=C^{r_1+\ldots+r_m}$$

לפי בחירת P, האינדקס של P ביחס ל-$\vec{\alpha},\vec{r}$ הוא לפחות $\frac{m}{2}(1-\varepsilon)$. לכן בפרט

$$\mathrm{Ind}_{\vec{\alpha},\vec{r}}(T)\ge\frac{m}{2}(1-\varepsilon)-\sum_{k=1}^{m}\frac{j_k}{r_k}\ge\frac{m}{2}(1-3\varepsilon)$$

נפתח את T כפולינום טיילור סביב $\vec{\alpha}$, ונעריך ב-$\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)$:

$$T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)=\sum_I T_I(\vec{\alpha})\left(\frac{p_1}{q_1}-\alpha\right)^{i_1}\cdots\left(\frac{p_m}{q_m}-\alpha\right)^{i_m}$$

לפי החישוב הקודם $T_I(\vec{\alpha})=0$, אלא אם כן $\sum_k\frac{i_k}{r_k}>\frac{m}{2}(1-3\varepsilon)$.

לפי אי-השוויונות $\left|\alpha-\frac{p_i}{q_i}\right|<\frac{1}{q_i^{2+\delta}}$ וההערכות הנ"ל על $T_I(\vec{\alpha})$, מקבלים:

$$\left|T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right|\le\sum_{I\in\mathcal{A}}C^{r_1+\ldots+r_m}\left(q_1^{\ i_1}\cdots q_m^{\ i_m}\right)^{-(2+\delta)}$$

כאשר $\mathcal{A}=\left\{I:\sum_{k=1}^{m}\frac{i_k}{r_k}>m\left(\frac{1}{2}-2\varepsilon\right),\ i_j\le r_j\right\}$.

כעת, אם $I\in\mathcal{A}$, אז

$$q_1^{i_1}\cdots q_m^{i_m}=q_1^{\ r_1\left(\frac{i_1}{r_1}\right)}\cdots q_m^{\ r_m\left(\frac{i_m}{r_m}\right)}\ge q_1^{\ r_1\left(\frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m}\right)}\ge q_1^{\ r_1m\left(\frac{1}{2}-2\varepsilon\right)}\ge\left(q_1^{\ r_1}\cdots q_m^{\ r_m}\right)^{\left(\frac{1}{2}-2\varepsilon\right)/(1+\varepsilon)}>$$
$$>\left(q_1^{\ r_1}\cdots q_m^{\ r_m}\right)^{\frac{1}{2}(1-6\varepsilon)}$$

נציב זאת בהערכה האחרונה. מספר האינדקסים ב- $\mathcal{A}$ חסום מלמעלה ע"י החסם הטריוויאלי $2^{r_1+\ldots+r_m}$. מכאן:

$$\left|T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right|\le\prod_{j=1}^{m}\left(2Cq_j^{\ -\frac{1}{2}(1-6\varepsilon)(2+\delta)}\right)^{r_j}$$

מבחירת ε מקבלים:

$$\frac{1}{2}(1-6\varepsilon)(2+\delta)>1+\frac{\delta}{4}$$
$$2Cq_j^{\ -\frac{1}{2}(1-6\varepsilon)(2+\delta)}<2Cq_j^{\ -\left(1+\frac{\delta}{4}\right)}$$

אם $a_j^{\delta}>D=(2C)^4$ אז הביטוי הנ"ל חסם מלמעלה ע"י $\frac{1}{q_j}$. ובסיכומו של דבר:

$$\left|T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right|<\frac{1}{q_1^{\ r_1}\cdots q_m^{\ r_m}}$$

אבל $\left|T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right|\in\frac{1}{q_1^{\ r_1}\cdots q_m^{\ r_m}}\mathbb{Z}_+$. האפשרות היחידה היא $T\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)=0$.

משל.

הורונסקיאן המוכלל (Generalized Wronskian)

תזכורת. אם f פונקציה וקטורית, $f=(\varphi_1,\dots,\varphi_k):\mathbb{R}\to\mathbb{R}^k$, הורונסקיאן של f הוא

$$\det\begin{pmatrix}\varphi_1&\varphi_2&\cdots&\varphi_k\\ \varphi_1'&\varphi_2'&\cdots&\varphi_k'\\ \vdots&\vdots&\ddots&\vdots\\ \varphi_1^{(k-1)}&\varphi_2^{(k-1)}&\cdots&\varphi_k^{(k-1)}\end{pmatrix}$$, פונקציה של t. זהו אופרטור דיפרנציאלי לינארי.

הכללה. $\varphi_1,\dots,\varphi_k$ פונקציות רציונליות ב- m משתנים. לכל $I=(i_1,\dots,i_m)$, נסמן $\Delta=\Delta_I=\frac{\partial^{i_1+\ldots+i_m}}{\partial x_1^{i_1}\cdots\partial x_m^{i_m}}$. זהו אופרטור דיפרנציאלי לינארי מסדר $i_1+\ldots+i_m$.

ורונסקיאן מוכלל הוא ביטוי מהצורה $\det\left(\Delta_i\varphi_j\right)_{1\le i,j\le m}$, כאשר Δ_i אופרטור גזירה מסדר קטן ממש מ- i.

הורונסקיאן הרגיל הוא הורונסקיאן המוכלל היחיד הלא טריוויאלי כאשר $m=1$.

למה. אם ל- $\varphi_1,\ldots,\varphi_k$ מקדמים ממשיים, והם בת"ל מעל $\mathbb{R}$, אז יש לפחות ורונסקיאן מוכלל אחד של $\varphi_1,\ldots,\varphi_k$ שאינו זהותית אפס.

הערה. הכיוון ההפוך קל.

הוכחה. באינדוקציה על k. אם $k=1$ אז הורונסקיאן המוכלל היחיד הוא פשוט הפונקציה עצמה, מיידי.
נניח $k\ge 2$. נסמן ב- Ω פונקציה רציונלית כלשהי ב- m משתנים, $\Omega\not\equiv 0$. נסמן ב- $\varphi_i^*=\Omega\cdot\varphi_i$.
$\varphi_i\mapsto\varphi_i^*$ טרנספורמציה לינארית של מרחב הפונקציות הרציונליות. היא הפיכה (אפשר לכפול ב- Ω^{-1}) ולכן גם $\varphi_1^*,\ldots,\varphi_k^*$ בת"ל.
כל ורונסקיאן מוכלל של $\varphi_1^*,\ldots,\varphi_k^*$ הוא צירוף לינארי של ורונסקיאנים מוכללים של $\varphi_1,\ldots,\varphi_k$ (לפי כלל המכפלה בגזירה). לכן די להוכיח שאחד הורונסקיאנים המוכללים של $\varphi_1^*,\ldots,\varphi_k^*$ לא מתאפס.
נבחר $\Omega=\varphi_1^{-1}$. אז $\varphi_1^*\equiv 1$, כלומר אפשר להניח בה"כ ש- $\varphi_1\equiv 1$. נסמן

$$V=\operatorname{Span}\{\varphi_1,\ldots,\varphi_k\}$$

זהו תת-מרחב ממימד k במרחב כל הפונקציות הרציונליות ב- m משתנים.
$k>1$, $\varphi_1\equiv 1$ ולכן φ_2 לא קבועה. לכן יש משתנה j כך ש- $\frac{\partial\varphi_2}{\partial x_j}\ne 0$.

ע"י פרמוטציה נניח בה"כ $j=1$, ז"א $\frac{\partial\varphi_2}{\partial x_1}\ne 0$.

נסמן $W=\left\{\psi\in V:\frac{\partial\psi}{\partial x_1}\equiv 0\right\}$.

אז $W\ne\{0\}$ כי $\varphi_1\in W$ ו- $W\ne V$ כי $\varphi_2\notin W$.
לכן אם $t=\dim W$ אז $1\le t\le k-1$.
נבחר בסיס $\{\psi_1,\ldots,\psi_k\}$ ל- V כך ש- $\{\psi_1,\ldots,\psi_t\}$ בסיס ל- W.

לפי הנחת האינדוקציה, יש אופרטורים דיפרנציאליים $\Delta_1^*,\ldots,\Delta_t^*$ כך שהסדר של Δ_i^* קטן ממש מ- i, ו- $\mathcal{W}_1:=\det\left(\Delta_i^*\psi_j\right)_{1\le i,j\le t}\not\equiv 0$.

אם $c_{t+1},\ldots,c_k$ ממשיים שלא כולם אפס, אז $\frac{\partial}{\partial x_1}\left(c_{t+1}\psi_{t+1}+\ldots+c_k\psi_k\right)\ne 0$ כי $\{0\}=W\cap\operatorname{Span}\{\psi_{t+1},\ldots,\psi_k\}$.

כלומר, $j=t+1,\ldots,k$, $\frac{\partial}{\partial x_1}\psi_j$ בת"ל. לפי הנחת האינדוקציה יש $\Delta_{t+1}^*,\ldots,\Delta_n^*$ כך שהסדר של Δ_j^* הוא לכל היותר $j-(t+1)$, כך ש- $\mathcal{W}_2:=\det\left(\Delta_i^*\frac{\partial}{\partial x_1}\psi_j\right)_{i,j=t+1,\ldots,k}\not\equiv 0$.

נסמן $\Delta_i = \begin{cases} \Delta_i^* & i=1,\dots,t \\ \Delta_i^* \circ \frac{\partial}{\partial x_i} & i=t+1,\dots,k \end{cases}$. אז הסדר של Δ_i קטן ממש מ-i, ו-

$$\det\left(\Delta_i \psi_j\right)_{1\le i,j\le k} = \det\begin{pmatrix} \left(\Delta_i^* \psi_j\right) & \left(\Delta_i^* \psi_j\right) \\ 0 & \left(\Delta_i^* \frac{\partial}{\partial x_1} \psi_j\right) \end{pmatrix} = \mathcal{W}_1 \mathcal{W}_2 \not\equiv 0$$

$\left(\psi_j\right)_{j=1}^k$ התקבלו מ-$\left(\varphi_j\right)_{j=1}^k$ ע"י טרנספורמציה לינארית (עם מקדמים קבועים, הפיכה) ולכן $\det\left(\Delta_i \varphi_j\right)_{1\le i,j\le k} \not\equiv 0$.

משל.

2013-06-05

סקירת ההוכחה של משפט Roth.

רוצים להוכיח שלכל אלגברי α ולכל $\delta > 0$ יש רק מספר סופי של פתרונות לאי-השוויון $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}$.

בדרך להוכחה הגדרנו:

- פולינום $P \in \mathbb{Z}\left[x_1,\dots,x_m\right]$ כאשר m מאוד גדול.
- $\lceil P \rceil$ - "הגובה" של פולינום, המקסימום של הערכים המוחלטים של המקדמים.
- האינדקס של P ביחס ל-$\left(\vec{\alpha},\vec{r}\right) \in \mathbb{R}^m \times \mathbb{N}^m$ הוגדר ע"י

$$\operatorname{Ind}_{\vec{\alpha},\vec{r}} P := \min\left\{\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} : I = \left(i_1,\dots,i_m\right);\ P_I\left(\vec{\alpha}\right) \ne 0\right\}$$

באופן אינטואיטיבי, האינדקס "מחפש" את הסדר הראשון של נגזרת (סביב הנקודה $\vec{\alpha}$) של הפולינום שאינה מתאפסת, לפי משקל כלשהו.

הלמה של Roth

משפט (הלמה של Roth).

יהי $0 < \varepsilon < \frac{1}{12}$, $m \in \mathbb{N}$, ונגדיר $w = w\left(m,\varepsilon\right) = \frac{24}{2^m}\left(\frac{\varepsilon}{12}\right)^{2^{m-1}}$.

יהיו $\frac{p_1}{q_1},\dots,\frac{p_m}{q_m} \in \mathbb{Q}, r_1,\dots,r_m \in \mathbb{N}$ המקיימים:

$$wr_j \ge r_{j+1} \qquad \gcd\left(p_j,q_j\right)=1$$

$$q_j > 0 \qquad q_j^{\,w} \ge 2^{3m} \qquad q_j^{\,r_j} \ge q_1^{\,r_1}$$

יהי $P \in \mathbb{Z}\left[x_1,\dots,x_m\right]$ כך שהדרגה של P במשתנה x_j אינו עולה על r_j, ו-$\lceil P \rceil \le q_1^{\,wr_1}$.

אזי: האינדקס של P ביחס ל- $\left(\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right),\left(r_1,\ldots,r_m\right)\right)$ הוא לכל היותר ε.

הערה 1. נשים לב שמתקיימת הנוסחה הרקורסיבית הבאה:

$$w(m,\varepsilon)=\begin{cases}\varepsilon & m=1\\ \frac{1}{2}w\left(m-1,\frac{\varepsilon^2}{12}\right) & m>1\end{cases}$$

וכן $w(m,\varepsilon)\xrightarrow{m\to\infty}0$ עבור ε קבוע.

הערה 2. מההנחות על הפרמטרים נובע: $r_1\ge wr_1\ge r_2\ge wr_2\ge\ldots\ge r_m$.

נשתמש במהלך ההוכחה בלמה של גאוס, שנזכיר אותה כעת:

הלמה של גאוס. יהי $P\in\mathbb{Z}\left[x_1,\ldots,x_m\right]$ פריק מעל $\mathbb{Q}$. יהיו $R_1,R_2\in\mathbb{Q}\left[x_1,\ldots,x_m\right]$ כך ש- $P=R_1R_2$.
אזי יש $\lambda\in\mathbb{Q}$ כך ש- $\lambda R_1\in\mathbb{Z}\left[x_1,\ldots,x_m\right]$ וכן $\lambda^{-1}R_2\in\mathbb{Z}\left[x_1,\ldots,x_m\right]$.

הוכחת הלמה של Roth.
ההוכחה היא באינדוקציה על m.

מקרה $m=1$: נכתוב $P(x)=\left(x-\frac{p_1}{q_1}\right)^\ell R_1(x)$ כאשר $\ell\ge 0$ ו- $R_1\left(\frac{p_1}{q_1}\right)\neq 0$.

ע"י הכפלה ב- ${q_1}^\ell$ נקבל את הפירוק $P(x)=\left(q_1x-p_1\right)^\ell R(x)$, $R=\frac{R_1}{{q_1}^\ell}$.

מכיוון ש- $\gcd\left(p_1,q_1\right)=1$, לא ניתן להכפיל את $\left(q_1x-p_1\right)^\ell$ ברציונלי לא שלם ולקבל פולינום במקדמים שלמים, ולכן לפי הלמה של גאוס, ל- R יש מקדמים שלמים. לכן המקדם המוביל של P מתחלק ב- ${q_1}^\ell$, ולכן

${q_1}^\ell\le\lceil P\rceil\overset{\text{assumption}}{\le}{q_1}^{wr_1}\overset{m=1}{=}{q_1}^{\varepsilon r_1}$.

ע"י השוואה של החזקות, נקבל $\frac{\ell}{r_1}\le\varepsilon$. אבל לפי ההגדרה P $\frac{\ell}{r_1}=\operatorname{Ind}_{\left(\left(\frac{p_1}{q_1}\right),\left(r_1\right)\right)}$. מש"ל ($m=1$).

מעבר האינדוקציה – $m>1$ כלשהו בהינתן $m-1$:
נתבונן בפירוקים של P מהצורה הבאה:

$$P\left(x_1,\ldots,x_m\right)=\sum_{j=1}^{k}\varphi_j\left(x_1,\ldots,x_{m-1}\right)\psi_j\left(x_m\right)$$

כאשר φ_j,ψ_j פולינומים עם מקדמים ב- $\mathbb{Q}$.

קיים לפחות פירוק אחד כזה, מכיוון שניתן לבחור $\psi_j\left(x_m\right)={x_m}^j$ ולקבל פירוק שבו $k\le r_m+1$ (כי r_m הוא הדרגה של הפולינום ביחס ל- x_m). כמו-כן בפירוק הזה המקדמים הם ב- $\mathbb{Z}$.

נאפשר למקדמים להיות ב- $\mathbb{Q}$ ונבחר את הפירוק בעל ה- k המינימלי. כמובן $k_{\min}\le r_m+1$.
נראה ש- $\varphi_1,\ldots,\varphi_k$ בת"ל מעל $\mathbb{R}$: אחרת,

$$V=\left\{\begin{pmatrix}c_1\\ \vdots\\ c_k\end{pmatrix}\in\mathbb{R}^k : c_1\varphi_1+\ldots+c_k\varphi_k=0\right\}$$

הוא מרחב וקטורי לא טריוויאלי. אבל V מרחב וקטורי מוגדר מעל $\mathbb{Q}$ (כל המקדמים של φ_j הם רציונליים), ולכן יש $(c_1,\ldots,c_k)\in\mathbb{Q}^k\setminus\{0\}$ כך ש- $c_1\varphi_1+\ldots+c_k\varphi_k=0$.

בה"כ נניח שהמשוואה הזו היא $\varphi_k=c_1\varphi_1+\ldots+c_{k-1}\varphi_{k-1}$ (כלומר בה"כ $c_k=-1$). אזי

$$P=\sum_{j=1}^{k-1}\varphi_j\psi_j+\left(c_1\varphi_1+\ldots+c_{k-1}\varphi_{k-1}\right)\psi_k=\sum_{j=1}^{k-1}\varphi_j\left(\psi_j+c_j\psi_k\right)$$

בסתירה למינימליות של k.

באותו אופן, מראים ש- $\psi_1,\ldots,\psi_k$ בת"ל מעל $\mathbb{R}$.

נסמן:

$$\mathcal{U}\left(x_m\right)=\det\left(\frac{1}{(i-1)!}\frac{\partial^{i-1}}{\partial {x_m}^{i-1}}\psi_j\left(x_m\right)\right)_{1\le i,j\le k}\not\equiv 0$$

זהו הורונסקיאן (הרגיל) של $\psi_1,\ldots,\psi_k$, ומכיוון שהם בת"ל, הוא לא זהותית אפס.

נעשה את אותו דבר עם ורונסקיאן מוכלל עבור $\varphi_1,\ldots,\varphi_k$:

לפי הלמה שהוכחנו בשיעור שעבר על ורונסקיאנים מוכללים, קיימים אופרטורים דיפרנציאליים $\Delta_1',\ldots,\Delta_k'$ כאשר אם $I_t=\left(i_1,\ldots,i_{m-1}\right)$,

$$\Delta_t'=\frac{1}{i_1!\cdots i_{m-1}!}\frac{\partial^{i_1+\ldots+i_{m-1}}}{\partial {x_1}^{i_1}\cdots\partial {x_{m-1}}^{i_{m-1}}}\qquad t=1,\ldots,k$$

אז $(*)$ $i_1+\ldots+i_{m-1}\le t-1\le k-1\le r_m$, וכן

$$\mathcal{V}\left(x_1,\ldots,x_m\right):=\det\left(\Delta_t'\varphi_j\left(x_1,\ldots,x_{m-1}\right)\right)_{1\le t,j\le k}\not\equiv 0$$

נגדיר:

$$\mathcal{W}\left(x_1,\ldots,x_m\right):=\det\left(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial {x_m}^{j-1}}\Delta_i'P\right)_{1\le i,j\le k}$$

נפשט את הביטוי על ידי כך ש- $P=\sum_j\varphi_j\psi_j$, כאשר האופרטורים Δ' פועלים רק על הפולינומים φ_j והאופרטורים $\frac{\partial}{\partial x_m}$ פועלים רק על הפולינומים ψ_j, ונקבל:

$$\mathcal{W}\left(x_1,\ldots,x_m\right)=\det\left(\sum_{r=1}^{k}\left(\Delta_i'\varphi_r\right)\left(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial {x_m}^{j}}\psi_r\right)\right)_{1\le i,j\le k}\overset{\text{Matrix product formula}}{=}$$

$$=\det\left(\left(\Delta_i'\varphi_r\right)_{1\le i,r\le k}\cdot\left(\frac{\partial^{j}}{\partial {x_m}^{j}}\psi_r\right)_{1\le r,j\le k}\right)=\mathcal{U}\cdot\mathcal{V}\not\equiv 0$$

מכאן, ניתן להניח בה"כ $\mathcal{U},\mathcal{V}$ עם מקדמים שלמים: מהנוסחה שמגדירה את $\mathcal{W}$ ניתן לראות ש-$\mathcal{W}$ הוא פולינום במקדמים שלמים, והוא מתפרק ל-$\mathcal{U}\cdot\mathcal{V}$ שידוע שיש להם מקדמים רציונליים, אז ניתן להפעיל את הלמה של גאוס ולהכפיל/לחלק את $\mathcal{U},\mathcal{V}$ ברציונלי ולקבל מקדמים שלמים. נשתמש בעובדה זו כדי להעריך.

נתייחס בהמשך ל-$\mathcal{W}$ גם כך:

$$\mathcal{W}=\det\left(P_{I_{t,j}}\right)_{1\le t,j\le n}$$

כאשר מולטי-אינדקסי הגזירה $I_{t,j}$ ניתנים ע"י Δ_i' ו- $\frac{\partial^j}{\partial {x_m}^j}$, וכן נכתוב $\mathcal{W}=\mathcal{U}\cdot\mathcal{V}$ לא עם ההגדרות לעיל של $\mathcal{U},\mathcal{V}$ אלא עם $\mathcal{U},\mathcal{V}$ בעלי מקדמים שלמים כך ש-$\mathcal{U}$ פולינום של x_m, $\mathcal{V}$ פולינום של $x_1,\ldots,x_{m-1}$ ואף אחד מהם אינו פולינום האפס.

למה. נסמן ב-$\overline{\theta}$ את האינדקס של $\mathcal{W}$ ביחס ל-$\left(\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right),(r_1,\ldots,r_m)\right)$. אז $\overline{\theta}\le\frac{k\varepsilon^2}{6}$.

הוכחת הלמה.

נשתמש בהנחת האינדוקציה עבור $\mathcal{U},\mathcal{V}$. נעריך את הגובה של $\mathcal{U},\mathcal{V}$. נסמן $I=(i_1,\ldots,i_{m-1},j)$.

$$\lceil P_I\rceil\le 2^{r_1+\ldots+r_m}\lceil P\rceil\le 2^{r_1+\ldots+r_m}q^{wr_1}$$

הפולינום $\mathcal{W}$ הוא מהצורה: סכום של $k!$ מחוברים, שכל אחד מהם הוא מכפלה של k ביטויים מהצורה $P_I(x_1,\ldots,x_m)$. נשתמש בהערכה (הבזבזנית) הבאה: $k!\le k^{k-1}\le k^{r_m}\le 2^{kr_m}$. לכן:

$$\lceil\mathcal{W}\rceil\le 2^{kr_m}\cdot\begin{pmatrix}\text{Height of product of } k\\ \text{factors of the form } P_I\end{pmatrix}\le$$

$$\le 2^{kr_m}\cdot\left(\underbrace{2^{r_1+\ldots+r_m}}_{\substack{\text{Bound on \# of}\\ \text{coefficients of } P_I}}\cdot\underbrace{2^{r_1+\ldots+r_m}q_1^{wr_1}}_{\substack{\text{Bound on every}\\ \text{coefficient of } P_I}}\right)^k\overset{r_1\ge\ldots\ge r_m}{\le}\left(2^{3mr_1}q^{wr_1}\right)^k$$

ומכיוון שנתון $q_1^{\,w}\ge 2^{3m}$, מתקיים $\lceil\mathcal{W}\rceil\le q^{2wr_1k}$.

ולכן $\mathcal{W}=\mathcal{U}\cdot\mathcal{V}$ $\lceil\mathcal{U}\rceil,\lceil\mathcal{V}\rceil\le q_1^{\,2wr_1k}$ (כאן משתמשים בכך שאין חיתוך בין המשתנים שמרכיבים את $\mathcal{U},\mathcal{V}$, ולכן במכפלה $\mathcal{W}$ לא יכולים להיות "צמצומים" – כל מקדם ב-$\mathcal{W}$ הוא מכפלה של מקדם ב-$\mathcal{U}$ ומקדם ב-$\mathcal{V}$).

לפי הנחת האינדוקציה, נשתמש בלמה של Roth עם $m-1$ במקום m, עם $kr_1,\ldots,kr_{m-1}$ במקום $r_1,\ldots,r_m$, ועם $\frac{\varepsilon^2}{12}$ במקום ε. בדיקה מראה שכל התנאים של הלמה מתקיימים. לכן:

- האינדקס של $\mathcal{V}$ ביחס ל-$\left(\left(\frac{p_1}{q_1},\ldots,\frac{p_{m-1}}{q_{m-1}}\right),(kr_1,\ldots,kr_{m-1})\right)$ הוא לכל היותר $\frac{\varepsilon^2}{12}$.
- האינדקס של $\mathcal{U}$ ביחס ל-$\left(\left(\frac{p_m}{q_m}\right),(kr_m)\right)$ הוא לכל היותר $\frac{\varepsilon^2}{12}$.

נחשוב על $\mathcal{U},\mathcal{V}$ כעל פולינומים במשתנים $(x_1,\ldots,x_m)$, כשלא כל המשתנים מופיעים. זה לא משפיע על האינדקס; כלומר האינדקס של $\mathcal{U}$ או של $\mathcal{V}$ ביחס ל- $\left(\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right),(kr_1,\ldots,kr_m)\right)$ אינו עולה על $\frac{\varepsilon^2}{12}$.

כעת נשתמש בטענה משיעורים קודמים, ש- $\operatorname{Ind}_{\bar{\alpha},\bar{r}}(PQ)=\operatorname{Ind}_{\bar{\alpha},\bar{r}}(P)+\operatorname{Ind}_{\bar{\alpha},\bar{r}}(Q)$. כמו-כן, קל לראות ש- $\operatorname{Ind}_{\bar{\alpha},k\bar{r}} P=\frac{1}{k}\operatorname{Ind}_{\bar{\alpha},\bar{r}} P$. נקבל:

$$\begin{aligned}\operatorname{Ind}_{\left(\frac{p_i}{q_i},r_i\right)}\mathcal{W}&=\operatorname{Ind}_{\left(\frac{p_i}{q_i},r_i\right)}\mathcal{U}+\operatorname{Ind}_{\left(\frac{p_i}{q_i},r_i\right)}\mathcal{V}=\\&=k\left(\operatorname{Ind}_{\left(\frac{p_i}{q_i},kr_i\right)}\mathcal{U}+\operatorname{Ind}_{\left(\frac{p_i}{q_i},kr_i\right)}\mathcal{V}\right)\le k\left(\frac{\varepsilon^2}{12}+\frac{\varepsilon^2}{12}\right)=\frac{k\varepsilon^2}{6}\end{aligned}$$

מש"ל (למה).

המשך הוכחת הלמה של Roth.

נסמן ב-θ את האינדקס של P ביחס ל- $\left(\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right),(r_1,\ldots,r_m)\right)$. לכל $I_{t,j}=\left(i_1,\ldots,i_{m-1},\overbrace{j-1}^{i_m}\right)$

כמו בהגדרת $\mathcal{W}$, מתקיים (לפי הערכה שראינו לפני כמה שיעורים על אינדקס של נגזרת של פולינום):

$$\begin{aligned}\operatorname{Ind} P_I&\ge\theta-\left(\frac{i_1}{r_1}+\ldots+\frac{i_{m-1}}{r_{m-1}}+\frac{j-1}{r_m}\right)\overset{r_1\ge\ldots\ge r_m}{\ge}\\&\ge\theta-\left(\frac{i_1+\ldots+i_{m-1}}{r_{m-1}}+\frac{j-1}{r_m}\right)\overset{\text{By }(*),\ i_1+\ldots+i_m\le r_m}{\ge}\\&\ge\theta-\left(\frac{r_m}{r_{m-1}}+\frac{j-1}{r_m}\right)\overset{wr_{m-1}\ge r_m}{\ge}\\&\ge\theta-\left(w+\frac{j-1}{r_m}\right)\overset{m\ge2}{\ge}\theta-\left(\frac{\varepsilon^2}{24}+\frac{j-1}{r_m}\right)\end{aligned}$$

ומכיוון שהאינדקס אי-שלילי, נכתוב:

$$\operatorname{Ind} P_I\ge\max\left\{0,\theta-\frac{\varepsilon^2}{24}-\frac{j-1}{m}\right\}$$

כעת נרצה להעריך את האינדקס של $\mathcal{W}$. נשתמש בתכונות הכלליות של האינדקס שהופיעו לפני כמה שיעורים:

$$\operatorname{Ind}(PQ)=\operatorname{Ind}P+\operatorname{Ind}Q$$
$$\operatorname{Ind}(P+Q)\ge\min\{\operatorname{Ind}P,\operatorname{Ind}Q\}$$

כאמור, $\mathcal{W}$ הוא סכום של $k!$ ביטויים שכל אחד מהם הוא מכפלה של k ביטויים מהצורה P_I. לכן:

$$\overline{\theta}=\operatorname{Ind}\mathcal{W}\geq\sum_{j=1}^{k}\max\left\{0,\theta-\frac{\varepsilon^2}{24}-\frac{j-1}{m}\right\}\geq$$

$$\geq\frac{-k\varepsilon^2}{24}+\sum_{j=1}^{k}\max\left\{0,\theta-\frac{j-1}{m}\right\}=\frac{-k\varepsilon^2}{24}+\sum_{i=0}^{k-1}\max\left\{0,\theta-\frac{i}{m}\right\}$$

מכאן:

$$\sum_{i=0}^{k-1}\max\left\{0,\theta-\frac{i}{m}\right\}\leq\overline{\theta}+\frac{k\varepsilon^2}{24}\leq\frac{k\varepsilon^2}{6}+\frac{k\varepsilon^2}{24}\leq\frac{k\varepsilon^2}{4}\qquad(**)$$

נפריד לשני מקרים:

א. $\theta>\frac{k-1}{r_m}$, ואז $(**)$ הופך ל-

$$k\theta-\frac{k(k-1)}{2r_m}=\frac{1}{2}k\left(\theta+\theta-\frac{k-1}{r_m}\right)<\frac{k\varepsilon^2}{4}$$

כלומר: $\varepsilon>\frac{\varepsilon^2}{2}>\left(\theta-\frac{k-1}{r_m}\right)+\theta>\theta$, וסיימנו.

ב. $\theta\leq\frac{k-1}{r_m}$. ואז $(**)$ הופך ל-

$$\sum_{i=0}^{[\theta r_m]}\left(\theta-\frac{i}{r_m}\right)<\frac{k\varepsilon^2}{4}$$

$$\frac{1}{2}\theta^2 r_m<\frac{1}{2}\theta\left(\left[\theta r_m\right]+1\right)<\frac{k\varepsilon^2}{4}\overset{k\leq r_m+1\leq 2r_m}{\leq}\frac{1}{2}\varepsilon^2 r_m$$

ומכאן שוב נקבל $\theta<\varepsilon$.

משל (הלמה של Roth).

סיום הוכחת משפט Roth

נזכיר שני משפטים שהוכחנו בשיעורים קודמים, שנזדקק להם בסיום ההוכחה:

משפט האינדקס. יהי α אלגברי מדרגה $d\geq 2$, אז יש $B=B(\alpha)>0$ כך שאם נתונים $\varepsilon>0$, $m\in\mathbb{N}$ עם $m>\frac{16}{\varepsilon^2}\log(4d)$, ו- $r_1,\ldots,r_m\in\mathbb{N}$; אז קיים $P\in\mathbb{Z}[x_1,\ldots,x_m]$ בעל התכונות

א. הדרגה של P במשתנה x_j היא לכל היותר r_j

ב. $\operatorname{Ind}_{\vec{\alpha},\vec{r}}P=\operatorname{Ind}_{(\alpha,\alpha,\ldots,\alpha),(r_1,\ldots,r_m)}P\geq\frac{m}{2}(1-\varepsilon)$ ($\vec{\alpha}=\left(\underbrace{\alpha,\ldots,\alpha}_{m\text{ times}}\right)$)

ג. $\lceil P\rceil\leq B^{r_1+\ldots+r_m}$

משפט 1. נניח ש- α,ε,m,P כמו במשפט האינדקס; אז קיים $D=D(\alpha)>0$ בעל התכונה: לכל $\delta>0$,

$0<\varepsilon<\frac{\delta}{36}$, $\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\in\mathbb{Q}$ פותרים את $\left|\alpha-\frac{p_j}{q_j}\right|<\frac{1}{q^{2+\delta}}$, $q_j^{\delta}>D$, ו- $q_1^{r_1}\approx q_j^{r_j}$ ($\approx$ מתפרש כך:

$r_1\log q_1\le r_j\log q_j\le(1+\varepsilon)r_1\log q_1$), אז $\operatorname{Ind}P\ge\varepsilon m$ ביחס ל- $(r_1,\dots,r_m)$, $\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)$.

הוכחת משפט Roth.

צ"ל: מספר סופי לכל היותר של פתרונות ל- $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^{2+\delta}}$ $(*)$ כאשר α אלגברי, $\delta>0$.

בה"כ α שלם אלגברי (הסברנו לפני כמה שיעורים מדוע זה לא מגביל את הכלליות).

בה"כ $\delta<1$.

נבחר $\frac{1}{12}<\frac{\delta}{36}>\varepsilon$, ונבחר m כך ש- $m>\frac{16}{\varepsilon^2}\log(4d)$.

נסמן $w=w(m,\varepsilon)$ כמו בלמה של Roth.

נבחר B,D כמו במשפט האינדקס ומשפט 1.

יהי $\frac{p_1}{q_1}$ המקיים את $(*)$ עם $q_1^{w}>B^m$, ו- $q_1^{w}\ge 2^{3m}$, ו- $q_1^{\delta}>D$.

עתה נבחר $\frac{p_2}{q_2},\dots,\frac{p_m}{q_m}$ פתרונות נוספים ל- $(*)$ באינדוקציה, כך שיתקיים $w\log q_{i+1}\ge 2\log q_i$.

נבחר r_1 כך שיתקיים אי-השוויון $\varepsilon r_1\log q_1\ge\log q_m$.

עבור $i=2,\dots,m$ נבחר $r_i=\left(\frac{r_1\log q_1}{\log q_i}\right)+1$.

כעת יש שלב של בדיקה שכל התנאים של כל המשפטים מתקיימים, שלא נפרט את החישובים בו:

התנאים של משפט האינדקס מתקיימים ולכן ניתן לבחור פולינום P כפי שמתקבל ממשפט האינדקס עם חסם עליון על הגובה.

ממשפט 1 מקבלים חסם תחתון על האינדקס שהוא εm.

מהלמה של רות מקבלים חסם עליון על האינדקס שהוא ε.

מכיוון ש- $m>1$, זו סתירה.

מש"ל.

הערה. בעזרת משפט Roth ניתן להוכיח הרבה תוצאות על טרנסצנדנטיות של מספרים <u>ספציפיים</u>. כמו במשפט Liouville, כדי להוכיח שמספר הוא טרנסצנדנטי מספיק להראות שיש לו קירובים "טובים מדי" על ידי רציונליים. בעזרת משפט Roth ניתן להסתפק בקירובים טובים מדי "פחות טובים" מאשר, למשל, מספרי Liouville.

דוגמה. האם עבור $k\in\mathbb{N}$, יש הצגה פשוטה של $\zeta(k)$?

השאלה קלה עבור k זוגי (מתקבלת דרך תורת פורייה ושוויון פרסבל בחישוב קצר).

השאלה קשה מאוד עבור k אי-זוגי.

Apéry הוכיח לראשונה בשנות ה-70, בדרך זו, ש- $\zeta(3)$ הוא אי-רציונלי.

משפט תת-המרחב של שמידט ← הכללה רב-מימדית למשפט Roth

שמידט הוכיח את ההכללה הבאה של משפט Roth:

משפט (Schmidt, 1970). נניח $\alpha_1,\dots,\alpha_n$ אלגבריים כך ש- $1,\alpha_1,\dots,\alpha_n$ בת"ל מעל $\mathbb{Q}$. (כלומר, לא ניתן למצוא $a_1,\dots,a_n\in\mathbb{Z}$ שלא כולם אפס כך ש- $\sum_{i=1}^{n}a_i\alpha_i\in\mathbb{Z}$.)

אז לכל $\delta>0$, יש מספר סופי לכל היותר של פתרונות $p=\left(p_i\right)\in\mathbb{Z}^n$, $q\in\mathbb{N}$ לאי-השוויון

$$\left\|\vec{\alpha}-\frac{\vec{p}}{q}\right\|_\infty<\frac{1}{q^{1+\frac{1}{n}+\delta}}$$

יתרה מזו, יש מספר סופי לכל היותר של פתרונות q לאי-השוויון $\langle q\alpha_1\rangle\langle q\alpha_2\rangle\dots\langle q\alpha_n\rangle<\frac{1}{q^{1+\delta}}$.

הניסוח השני נקרא "הגרסה הכפלית" והיא הרבה יותר חזקה; הניסוח הראשון נובע מהגרסה הכפלית. נראה שאכן, כל פתרון לניסוח הראשון נותן פתרון לניסוח השני (ולכן מספר סופי של פתרונות לניסוח השני גורר מספר סופי של פתרונות לניסוח הראשון): נניח ש- $\vec{p},q$ פתרון לניסוח הראשון, אז לכל i,

$$\left|\alpha_i-\frac{p_i}{q}\right|<\frac{1}{q^{1+\frac{1}{n}+\delta}}$$

$$\langle q\alpha_i\rangle\le\left|q\alpha_i-p\right|<\frac{1}{q^{\frac{1}{n}+\delta}}$$

$$\langle q\alpha_1\rangle\cdots\langle q\alpha_n\rangle\le\frac{1}{q^{1+n\delta}}$$

משפט תת-המרחב (Schmidt, 1972).

יהיו $L_1\left(\vec{x}\right),\dots,L_n\left(\vec{x}\right)$ תבניות לינאריות ב- n משתנים, כלומר $L_i:\mathbb{R}^n\to\mathbb{R}$ טרנספורמציה לינארית, עם מקדמים ממשיים או מרוכבים.

אזי לכל $\delta>0$, יש מספר סופי של תתי-מרחבים ממש $\{0\}\underset{\neq}{\subset}T_1,\dots,T_r\underset{\neq}{\subset}\mathbb{R}^n$, כך שלכל $\vec{x}\in\mathbb{Z}^n$ המקיים

$$\left|L_1\left(\vec{x}\right)\cdots L_n\left(\vec{x}\right)\right|\le\|x\|^{-\delta}$$

אזי $\vec{x}$ שייך לאחד מתתי המרחבים T_j.

בלי הגבלת הכלליות, T_i מוגדרים מעל $\mathbb{Q}$.

הוכחת משפט Schmidt כמסקנה ממשפט תת-המרחב.

בהינתן q המקיים $\langle q\alpha_1\rangle\cdots\langle q\alpha_n\rangle<\frac{1}{q^{1+\delta}}$, נבחר p_i כך ש- $\langle q\alpha_i\rangle=\left|q\alpha_i-p_i\right|$.

נסמן $N=n+1$, $\vec{x}=\begin{pmatrix}p_1\\ \vdots\\ p_n\\ q\end{pmatrix}$. מתקיים $\|\vec{x}\|\le C|q|$ כאשר C תלוי ב- $\alpha_1,\dots,\alpha_n$.

נגדיר תבניות לינאריות:

$$L_i\left(\vec{x}\right)=\alpha_i x_N - x_i \qquad i=1,\dots,n$$
$$L_N\left(\vec{x}\right)=x_N$$

אזי עבור ה- $\vec{x}$ הספציפי שבחרנו,

$$\left|L_1\left(\vec{x}\right)\cdots L_N\left(\vec{x}\right)\right|<\left\|\vec{x}\right\|^{-\delta/2} \qquad (*)$$

אם q מספיק גדול (מסקנה מיידית מכך ש- $\left\langle q\alpha_1\right\rangle\cdots\left\langle q\alpha_n\right\rangle<\frac{1}{q^{1+\delta}}$). לפי משפט תת-המרחב, הפתרונות $\vec{x}$ הם במספר סופי של תתי-מרחבים ממש, רציונליים, אשר נסמן אחד מהם ב- T. אם על T מתקיימת המשוואה $c_1y_1+\ldots+c_ny_n+c_Ny_N=0$ ($c_i\in\mathbb{Z}$), אז עבור $\vec{y}=\vec{x}$,

$$c_1\left(\alpha_1q-p_1\right)+\ldots+c_n\left(\alpha_nq-p_n\right)=\left(c_1\alpha_1+\ldots+c_n\alpha_n+c_N\right)q$$

(הוספנו $\sum_{i=1}^{n}c_i\alpha_iq$ לשני האגפים.)

לכן לפי אי-שוויון המשולש:

$$\sum\left|c_i\right|\geq\left|c_1\right|\left\langle q\alpha_1\right\rangle+\ldots+\left|c_n\right|\left\langle q\alpha_n\right\rangle\geq\gamma q$$

כאשר

$$\gamma:=\left|c_1\alpha_1+\ldots+c_n\alpha_n+c_N\right|>0$$

כי $1,\alpha_1,\ldots,\alpha_n$ בת"ל מעל $\mathbb{Q}$.

קיבלנו חסם מלמעלה $\frac{\sum\left|c_i\right|}{\gamma}$ על q, ולכן יש מספר סופי של פתרונות כנדרש.

מש"ל.