קורס : קודים לתיקון שגיאות ושימושיהם במדעי המחשב
מרצה : ד״ר קלים יפרמנקו
סמסטר סתיו תשפ״א
20/12/2020

הרצאה 17:

Johnson Bound

מבוא :

במתמטיקה יישומית, הגבול של ג׳ונסון (על שם סלמר מרטין ג׳ונסון) הוא מגבלה על גודל הקודים לתיקון שגיאות, כפי שמשמשים בתורת הקידוד להעברת נתונים או לתקשורת.

ראינו שניתן להפוך כל קוד עם מרחק יחסי δ לקוד הניתן לפענוח-רשימה עם אורך רשימה קצר (אורך הרשימה אחד, למעשה), אך מספר השגיאות שיכולנו לתקן היה רק $\frac{\delta}{2}$. כלומר, אנחנו כבר יודעים שאפשר לעשות List-decoding מ- $\frac{\delta}{2}$, למען האמת פענוח כזה אפשר לעשות אפילו מ-Unique -decoding .

חסם ג׳ונסון (Johnson Bound) מבטיח חסם טוב יותר על מספר השגיאות, בעוד משמר את אורך הרשימה קטן או לא יותר מדי גדול, כלומר אורך הרשימה יהיה ריבועי באורך הרשימה. (פולינומי ב-n).

Johnson Bound אומר שניתן לעשות List-decoding לכל קוד, כך שכמות השגיאות בו היא יותר גדולה מכמות השגיאות שיש ב- List-decoding והדבר היחיד שנצטרך לדעת זה את המרחק של הקוד. על כן, נראה השיעור שאם נתון לנו קוד במרחק d אז הקוד הזה הוא List Decodable .

תזכורת : בהינתן שהמרחק של הקוד הוא d. קוד יכול לתקן, כלומר לפענח : $\left\lfloor\frac{\mathrm{d}-1}{2}\right\rfloor$ שגיאות.

עכשיו נעסוק בשאלה אם ניתן לפענח יותר מ-$\left\lfloor\frac{\mathrm{d}-1}{2}\right\rfloor$ שגיאות עבור קוד כללי במרחק d ?

משפט : לכל קוד $C \subseteq \sum^n$ באורך L ומרחק d מתקיים : קוד C הוא: List Decodable-$(J_q\left(\frac{1}{n}\right), qnd)$

כאשר List-Decodable - $J_q(\delta)=\left(1-\frac{1}{q}\right) \cdot\left(1-\sqrt{1-\frac{q}{q-1} \cdot \delta}\right)$

הערה: qnd זה האורך של הרשימה וה-$J_q\left(\frac{1}{n}\right)$ זה המרחק שממנו אפשר לפענח.

הסבר: משפט זה אומר שאם לקוד יש מרחק d אז הוא List-Decodable. כלומר לא רק שניתן לפענח אותו עם שגיאה אחת אלא, ניתן לפענח אותו עם qnd שגיאות וזה נותן לנו בעצם לפענח כמות יותר גדולה של שגיאות. ומאיזה מרחק אפשר לעשות לקוד List-decoding ? יש לנו פונקצייה של ג׳ונסון שמוגדרת פה.
בהמשך נראה כי $J_q(\delta)>\frac{\delta}{2}$ עבור כמעט כל דלתא.

הערה: אם הינו מוסיפים פה אפסילון כך : List Decodable-$(J_q\left(\frac{1}{n}\right)-\varepsilon, qnd)$ אז היה אפשר להוריד את אורך הרשימה, qnd להיות יותר קטן. אך אנחנו לא נעשה זאת.

הוכחה :

נוכיח מקרה פרטי של המשפט, עבור א״ב בינארי, מכיוון שנשתמש ב- Johnson Bound רק עבור q=2 : כלומר
$J_2(\delta) = \frac{1}{2}\cdot\left(1-\sqrt{1-2\cdot\delta}\right)$

*תרגיל בית להוכיח עבור כל q .

השיטה שבה נוכיח את המשפט נקראת ספירה כפולה.

מה אנחנו בעצם צריכים להוכיח?

שלכל מילת קוד w , הכדור שניצור סביב w במרחק $J_2(\delta)\cdot n$ חיתוך עם c (כלומר כל מילות הקוד שנמצאות במרחק $J_2(\delta)\cdot n$ מ- w) יהיה קטן מאורך הרשימה qnd , פורמלית :

$$|B(w,J_2(\delta)\cdot n)\cap c| \le qnd$$

נתבונן על כל מילות הקוד שנמצאות בחיתוך : $B(w,J_2(\delta)\cdot n)\cap c = \{c_1,c_2...c_L\}$

נביע את זה באמצעות מטריצה עם L שורות ו-n עמודות :

בשורה ראשונה נכתוב את תוצאת $c_1\oplus w$ וכך הלאה... עד השורה ה-L שבה נכתוב את תוצאת $c_L\oplus w$:

$$\begin{pmatrix} & \cdots & \to c_1\oplus w \\ \vdots & \ddots & \vdots \\ & \cdots & \to c_L\oplus w \end{pmatrix}$$

מה אנחנו יודעים על המטריצה הזאת?

(1) בכל שורה יש לכל היותר $J_2(\delta)\cdot n$ אחדות.

הסבר: לקחנו את כל המילים $\{c_1,c_2...c_L\}$ שהן במרחק $J_2(\delta)\cdot n$ מ-w . אם נבצע עליהן XOR עם המילה w, נקבל שמספר האחדות הוא לכל היותר המרחק, כלומר לכל היותר $J_2(\delta)\cdot n$. למעשה, עובדה זאת אומרת לנו שבכל שורה אין יותר מדיי אחדות.

(2) לכל שתי שורות במטריצה מתקיים: $d(r_i,r_j)\ge d$

הסבר: ידוע כי : $x\oplus y = z\oplus y \Leftrightarrow x=y$ ולכן נקבל ש : $d(r_i,r_j)=d(c_i\oplus w,c_j\oplus w)=d(c_i,c_j)$

ומכיוון שהמרחק של הקוד הוא d , כלומר המרחק בין כל שתי מילים של הקוד הוא לפחות d (מהגדרת מרחק). למעשה, נקבל שהמרחק בין כל שתי שורות הוא לפחות d :

$$d(r_i,r_j)=d(c_i\oplus w,c_j\oplus w)=d(c_i,c_j)\ge d$$

הערה: נשים לב שגם כל השורות במטריצה הן גם בת״ל.

כעת נרצה לחסום את מספר השורות במטריצה : נראה שלא יכול להיות שיהיו יותר מדיי שורות במטריצה, כלומר שלא יכולה להיות מטריצה עם יותר מדיי שורות שמקיימת את שני התנאים הנ״ל.

אז איך אנחנו הולכים להראות את זה? באמצעות סכום המרחקים בין כל השורות, כלומר : $\sum_{i\ne j} d(r_i,r_j)$

<u>נחסום את סכום המרחקים בין כל השורות בשתי דרכים:</u>

<u>דרך ראשונה-</u> $\sum_{i<j} d(r_i,r_j) \geq d \cdot \binom{L}{2}$

כלומר, סכום המרחקים בין כל השורות הוא לפחות המרחק כפול כל הדרכים לבחור שתי שורות.

נתבונן שוב על המטריצה שלנו, ונסמן את מספר האחדות בעמודה ה-i כ-m_i.

במטריצה יש L שורות ומעובדה (1) בכל שורה יש לכל היותר $J_2(\delta)\cdot n$ אחדות, ולכן בכל המטריצה יש לכל היותר $J_2(\delta)\cdot n\cdot L$ אחדות.

נשים לב שסכום של מספר האחדות בכל העמודות, זהה לסכום האחדות בכל המטריצה, זהה לסכום האחדות בכל העמודות ולכן נקבל:

$$\frac{\sum_{i=1}^{n} m_i}{L} \leq \frac{J_2(\delta)\cdot n\cdot L}{L} = J_2(\delta)\cdot n$$

<u>דרך שנייה-</u> נרצה "לספור" את סכום המרחקים לפי סדר השורות.

לספור סכום בין מרחקים, זה בעצם אומר מה המרחק בין השורה הראשונה לשנייה וכן הלאה, שזה כמה פעמים הקורדינאטה הראשונה היא שונה ועוד כמה פעמים הקורדינאטה השנייה היא שונה וכן הלאה, כלומר כמה פעמים יש שוני באיבר (0/1) שהוא באותה העמודה רק בשורה אחרת. פורמלית:

מספר הדרכים לבחור i ו-j שונים כך ש: $m[i,k] \neq m[j,k]$ כלומר באחד מהם יש אפס ובשני אחד:

$$\sum_{i<j} d(r_i,r_j) =^{*} \sum_{i<j}\sum_{k=1}^{n} r_i[k]\oplus r_j[k] =^{*} \sum_{k=1}^{n}\sum_{i<j} r_i[k]\oplus r_j[k] =^{*} \sum_{k=1}^{n} m_i\cdot(L-m_i) \geq d\cdot\binom{L}{2}$$

*כאשר $r_i[k] \neq r_j[k]$ אז תוצאת ה-XOR בניהם תהיה 1, ואם $r_i[k] = r_j[k]$ אז תוצאת ה-XOR בניהם תהיה אפס ולכן זה נותן לנו את הסכימה של כל המקומות ששונים(כי האפסים לא משפיעים על הסכימה).

*נחליף את סדר הסכימה

*הסכימה היא כל ה- {i,j} כך ש $i<j$ כך ש: $(r_i[0]\hat{}r_j[1]) \mid (r_i[1]\hat{}r_j[0])$ ולכן זה כמו לבחור שאחד מהם יהיה אחד, שזה בעצם m_i והשני אפס שזה היתר כלומר $L-m_i$.

<u>סיכום ביניים:</u>

1. בדרך הראשונה קיבלו כי:

$$\frac{\sum_{i=1}^{n} m_i}{L} \le J_2(\delta)\cdot n \quad\Rightarrow\quad \sum_{i=1}^{n} m_i \le J_2(\delta)\cdot n\cdot L \quad\Rightarrow\quad \sum_{i=1}^{n} m_i\cdot L \le J_2(\delta)\cdot n\cdot L^2$$

2. בדרך השנייה קיבלו כי:

$$\sum_{i<j} d(r_i,r_j) \le \sum_{i=1}^{n} m_i\cdot(L-m_i) = \sum_{i=1}^{n} m_i\cdot L - \sum_{i=1}^{n} {m_i}^2$$

נמשיך לפתח את האי-שיוון השני, באמצעות מציאת חסם לביטוי: $\sum_{i=1}^{n} m_i\cdot L - \sum_{i=1}^{n} {m_i}^2$. מכיוון שהביטוי מורכב משני חלקים, השיטה שלנו תהיה למצוא חסם לכל חלק בנפרד.

נשים לב שמ-1. יש לנו חסם על החלק הראשון של הביטוי, שהוא: $\sum_{i=1}^{n} m_i\cdot L \le J_2(\delta)\cdot n\cdot L^2$

<u>כעת נרצה לחסום את החלק השני של הביטוי:</u>

<u>תזכורת- אי-שוויון קושי-שוורץ:</u> אם V הוא מרחב מכפלה פנימית, אז לכל $x, y \in V$ מתקיים:

$|\langle x\,,y\rangle| \le \|x\|\cdot\|y\|$. כאשר $\|x\| = \sqrt{|\langle x\,,x\rangle|}$ מסמן את הנורמה המושרית על V מהמכפלה הפנימית.

מסקנה: $\langle x\,,y\rangle^2 \le \|x\|^2\cdot\|y\|^2$

נבחר: $x=(m_1,\dots,m_n)\,,y=(\frac{1}{n},\dots,\frac{1}{n})$, נציב במסקנה הנ״ל שנובעת מאי-השוויון קושי-שוורץ נקבל מכפלה פנימית של וקטור x ב-y שזה שווה ל:

$$\left(\frac{\sum_{i=1}^{n} m_i}{n}\right)^2 \le \sum_{i=1}^{n} {m_i}^2\cdot\sum_{i=1}^{n}\left(\frac{1}{n}\right)^2 = \sum_{i=1}^{n} {m_i}^2\cdot\sum_{i=1}^{n}\frac{1}{n^2} = \sum_{i=1}^{n} {m_i}^2\cdot n\cdot\frac{1}{n^2} = \frac{1}{n}\cdot\sum_{i=1}^{n} {m_i}^2$$

כלומר נקבל כי:

$$\frac{(\sum_{i=1}^{n} m_i)^2}{n^2} \le \frac{1}{n}\cdot\sum_{i=1}^{n} {m_i}^2 \quad\Rightarrow\quad \sum_{i=1}^{n} {m_i}^2 \ge \frac{(\sum_{i=1}^{n} m_i)^2}{n}$$

נחזור לאי-שוויון שלנו ובשלב הראשון נציב את החסם שמצאנו לחלק השני של הביטוי:

$$\sum_{i<j} d(r_i,r_j) \le \sum_{i=1}^{n} m_i\cdot(L-m_i) = \sum_{i=1}^{n} m_i\cdot L - \sum_{i=1}^{n} {m_i}^2 \le \sum_{i=1}^{n} m_i\cdot L - \frac{(\sum_{i=1}^{n} m_i)^2}{n}$$

נסמן: $\frac{\sum_{i=1}^{n} m_i}{L} = e$, ונציב את $\sum_{i=1}^{n} m_i = e\cdot L$ חזרה באי-שוויון ונקבל:

$$\sum_{i<j} d(r_i, r_j) \leq \sum_{i=1}^{n} m_i \cdot L - \frac{(\sum_{i=1}^{n} m_i)^2}{n} = e \cdot L \cdot L - \frac{e^2 \cdot \mathrm{L}^2}{n} = L^2 (e - \frac{e^2}{n})$$

חסמנו את סכום המרחקים בין כל השורות מלמעלה ומלמטה ולכן נקבל ש :

$$d \cdot \binom{L}{2} \leq \sum_{i<j} d\left(r_i, r_j\right) \leq L^2 \left(e - \frac{e^2}{n}\right)$$

$$\Downarrow$$

$$d \cdot \binom{L}{2} = d \cdot \frac{L(L-1)}{2} \leq L^2 \left(e - \frac{e^2}{n}\right)$$

$$\Downarrow$$

$$d \cdot L - d \leq 2 \cdot L \cdot \left(e - \frac{e^2}{n}\right)$$

$$\Downarrow$$

נעביר אגפים ונקבל:

$$d \geq L \cdot (d - 2 \cdot (e - \frac{e^2}{n}))$$

$$\Downarrow$$

נכפיל ב- n ונקבל:

$$d \cdot n \geq L \cdot (d \cdot n - 2 \cdot e \cdot n + 2 \cdot e^2)$$

<u>טענה :</u> $d \cdot n - 2 \cdot e \cdot n + 2 \cdot e^2 > 0$

מכאן נובע ש : $2 \cdot e \cdot n - 2 \cdot e^2 < d \cdot n$ כלומר : $e \cdot (2 \cdot n - 2 \cdot e) < d \cdot n$

<u>הוכחה:</u>

נוכיח ש: $e\cdot(2\cdot n - 2\cdot e) < d\cdot n$ ונקבל ש: $d\cdot n - 2\cdot e\cdot n + 2\cdot e^2 > 0$

ראשית נשים לב ש$e\cdot(2\cdot n - 2\cdot e)$ זוהי פונקצייה מונוטונית עולה עבור: $e \le \frac{n}{2}$.

נזכיר ש: $\frac{\sum_{i=1}^{n} m_i}{L} \le J_2(\delta)\cdot n$ ולכן מתקיים כי: $e \le J_2(\delta)\cdot n = \frac{1}{2}\cdot\left(1-\sqrt{1-2\cdot\delta}\right)\cdot n$.

נציב:

$$e\cdot(2\cdot n-2\cdot e) \le J_2(\delta)\cdot n\cdot(2\cdot n-2\cdot J_2(\delta)\cdot n) = J_2(\delta)\cdot n^2\cdot\left(2-2\cdot J_2(\delta)\right) =$$

$$=\frac{1}{2}\cdot\left(1-\sqrt{1-2\cdot\frac{d}{n}}\right)\cdot\left(1+\sqrt{1-2\cdot\frac{d}{n}}\right)\cdot n^2 = \frac{1}{2}\cdot\left(1-\left(1-2\cdot\frac{d}{n}\right)\right)\cdot n^2 = \frac{d}{n}\cdot n^2 = d\cdot n$$

ולכן, בעצם הוכחנו ש $d\cdot n - 2\cdot e\cdot n + 2\cdot e^2 > 0$

נחזור לאי-שיוון שלנו: $d\cdot n \ge L\cdot(d\cdot n - 2\cdot e\cdot n + 2\cdot e^2)$ אז כעת נקבל ש:

$$L \le \frac{d\cdot n}{d\cdot n - 2\cdot e\cdot n + 2\cdot e^2} \le^{*} d\cdot n$$

*הוכחנו בעצם שהמכנה: $d\cdot n - 2\cdot e\cdot n + 2\cdot e^2$ חיובי ומספר שלם.

<u>לסיכום:</u> החסם שקיבלנו על מספר השורות במטריצה הוא: $L \le d\cdot n$

חסם זה אומר לנו שלא יכול להיות שיהיו יותר מדיי שורות במטריצה. בעצם, שלא יכולה להיות מטריצה עם יותר מדיי שורות שמקיימת את שני התנאים שהצגנו בתחילת השיעור ולכן ניתן לעשות List-decoding לכל קוד במרחק d.

הערה1: כעיקרון Johnson Bound הוא הדוק. במובן הזה שיש קודים ממרחק d כך שיש מילת קוד עם מספר אקפוננציאלי של מילים מסביב לאיזשהי נקודה שכאשר אנחנו עוברים את ה-Johnson Bound.

הערה2: עבור q גדול, כלומר מעל א"ב גדול, נשתמש בחסם: $e \le n - \sqrt{n\cdot(n-d)}$

שיעור הבא נראה שימושים ב-Johnson Bound ושאפשר באמצעות Johnson Bound לקבל חסמים על משהו שבכלל לא קשור לפענוח- אלא על היחס בין δ ל-R. בנוסף, נשפר את החסם שמצאנו.