בדיקה הסתברותית של הוכחות | 67790

הרצאות | פרופ' גיא קינדלר

כתיבה | נמרוד רק

תשפ"ג סמסטר ב'

השבוע הראשון הושלם באדיבותו (הרבה) של דויד קיסר-שמידט וסיכומו.

תוכן העניינים

שבוע $\mathbb{I}$ | מבוא

הגדרה מכונת טיורינג היא אוטומט עם סרט זיכרון שהיא יכולה לנוע עליו. מ"ט M מקבלת שפה $L \subseteq \Sigma^*$ אם היא מסיימת במצב מקבל על x אם"ם $x \in L$.

הגדרה מ"ט חישוב זו מ"ט שיש לה מצב עוצר שכשהיא מגיעה אליו הערך שרשום על הסרט הוא הפלט שלה.

הגדרה $\mathsf{P} = \{L :$ קיימת מ"ט המכריעה את L בזמן פולי' $\}$.

הגדרה נאמר כי $L \in \mathsf{NP}$ אם קיימת שפה L^π כך ש:

1. $L^\pi \in \mathsf{P}$.
2. המילים ב-L^π הן מהצורה (x, w) כאשר $x \in L$ ו-$|w| \leq \mathsf{poly}(x)$.
3. לכל $x \in L$ קיים w כך ש-$(x, w) \in L^\pi$.

הערה בעיות הכרעה של שפה L הן למעשה חלוקה של Σ^* ל-$(\mathcal{Y}, \mathcal{N})$.

הגדרה בעיית הבטחה (promise problem) היא חלוקה $L = (\mathcal{Y}, \Sigma^* \setminus (\mathcal{Y} \cup \mathcal{N}), \mathcal{N})$ של Σ^*. מ"ט שמזהה את L מקבלת ודוחה נכונה מילים ב-$\mathcal{Y}, \mathcal{N}$ בהתאמה (מבטיחה את התשובה עליהם) ומילים ב-$\Sigma^* \setminus (\mathcal{Y} \cup \mathcal{N})$ יכולות להתקבל, להדחות או שהמ"ט לא תעצור (אין ערובה לתוצאת הריצה).

הערה בעיית הכרעה של שפה L היא בעיית הבטחה מהצורה $(L, \varnothing, \Sigma^* \setminus L)$.

הערה רדוקציה חשיבה לבעיות הבטחה מוגדרת בדומה לרדוקציה בבעיות הכרעה.

הגדרה נאמר כי $L \in \mathsf{NPH}$ אם לכל $L' \in \mathsf{NP}$ קיימת רדוקציה פולי' מ-L' ל-L (כאשר L בעיית הבטחה).

הגדרה נאמר כי $L \in \mathsf{NPC}$ אם $L \in \mathsf{NPH}$ וגם $L \in \mathsf{NP}$.

הגדרה בעיית $\mathsf{MAX} - \mathsf{3SAT}$ מקבלת קלט חוקי $I \in \mathsf{3CNF}$ (נוסחה המורכבת מהסגרים) והמטרה היא לתת השמה שתספק כמה שיותר הסגרים.

עבור קלט חוקי I נגדיר $\mathrm{opt}(I)$ (מסומן לעתים $\mathrm{val}(I)$) האחוז המקסימלי של הסגרים שניתן לספק ב-I.

הערה $\mathsf{3SAT} \in \mathsf{NP}$ היא שפת כל הקלטים החוקיים שהערך שלהם הוא 1 (נוסחה הניתנת לסיפוק במלואה).

הערה $\mathsf{MAX} - \mathsf{3SAT}$ אינה בעיית הכרעה או הבטחה ולכן לעת עתה ההוכחה (העד) אינה מוגדרת היטב.

הערה ל-$\mathsf{3SAT}$ יש כמה מאפיינים מיוחדים מבחינת בדיקת הוכחות. ראשית ניתן לבדוק הוכחה במקביל על כל ההסגרים אם נתון לנו כוח חישוב מקבילי מספיק. ניתן לנצל מנגנון זה לצורכי בדיקה הסת' של השמה: אם $I \in \mathsf{3SAT}$ אז בהגרלת הסגרת, ההסת' שיסופק היא $P(\mathcal{Y}) = 1$ אבל אם $I \notin \mathsf{3SAT}$ אז $P(\mathcal{Y}) \leq 1 - \frac{1}{m}$ (לפחות הסגר אחד לא מסופק). כלומר ניתן להגדיר מוודא הסת' לבעיה.

הגדרה מוודא הסת' לבעיית הבטחה הוא מ"ט שמקיים את התנאים הבאים:

- (לוקליות) המ"ט מבצעת מספר גישות קבוע לעד (3 ביטים בלבד מתוך העד).
- (רנדומיות) המ"ט מגרילה $\mathcal{O}\left(\log n\right)$ ביטים.
- (שלמות) המ"ט מקבלת קלט בשפה בהסת' 1 (המוודא מושלם).
- (תקפות, Soundness) קיים חסם מלעל להסת' לקבלת קלט שאינו בשפה (במקרה שלנו $1-\Theta\left(\frac{1}{n}\right)$).

טענה לכל $L\in$ NP קיים מוודא הסת' עם פרמטרים כמו שכתבנו למעלה.

הוכחה: ממשפט קוק-לוין, יש רדוקציה מ-L ל-3SAT ולכן מספיק לבדוק הסת' את הקלט המתקבל ל-3SAT. ■

משפט (PCP בניסוח 3SAT) לכל $L\in$ NP קיים מוודא הסת' עם פרמטרים כנ"ל ו-$1 <$ const $<$ soundness (ישנו חסם מלעל קבוע קטן ממש מאחד לתקפות).

הערה כדי לקיים את הדרישה על התקפות צריך שהרדוקציה מהשפה לנוסחה ב-3CNF תיתן נוסחה שהיא בהסת' נמוכה ספיקה.

הגדרה $[c,s]$ gap − MAX − 3SAT היא בעיית ההבטחה עם

$$\mathcal{Y}=\{I:\text{3SAT קלט חוקי לבעיית } I\ \wedge\ \mathrm{val}\left(I\right)\geq c\}$$

$$\mathcal{N}=\{I:\text{3SAT קלט חוקי לבעיית } I\ \wedge\ \mathrm{val}\left(I\right)\leq s\}$$

הערה אינטואטיבית, c הוא המשלים (אחד פחות-) אחוז ה-false negative שאנחנו מוכנים לסבול ו-s הוא אחוז ה-false postiive שאנחנו מוכנים לסבול.

משפט (ניסוח מחדש של PCP עם gap − MAX − 3SAT) קיים $s<1$ כך ש-NPH $\in [1,s]$ gap − MAX − 3SAT.

הערה נראה שהניסוח החדש גורר את PCP המקורי על $L=$ gap − MAX − 3SAT $[1,s]$ ומשם עם רדוקציה מכל שפה אחרת נקבל את משפט ה-PCP המקורי. לכן מספיק שנציג מוודא הסת' עם תקפות s ל-L ונסיים. חשוב לשים לב ש-L כאן היא רק מתווכת לכל שפה והקושי הוא בהוכחת הקשיות שלה ב-NP, ואילו המוודא ההסת' הוא טריוויאלי (והנה הוא).

המוודא ההסת' מקבל $I=c_1\wedge\ldots\wedge c_m$ נוסחה חוקית ו-f השמה (העד), מגריל $i\in[m]$ ובודק האם c_i מסופקת ע"י f (צריך לבדוק את שלושת הביטים ב-f המתאימים לליטרלים ב-c_i). אם הפסוקית מסופקת יענה $\mathcal{Y}$ ואחרת $\mathcal{N}$.

- אם $I\in\mathcal{Y}$ אז יש השמה מספקת ולכן המוודא יענה $\mathcal{Y}$ על איזשהו עד (לכן תמיד נסווג נכון $I\in\mathcal{Y}$).
- אם $I\in\mathcal{N}$ אז $s\cdot m$ פסוקיות לכל היותר מסופקות ע"י כל השמה ולכן ההסת' שניפול על אחת מסופקת (שתגרום לנו לחשוב ש-I כן ספיקה) היא s.

הגדרה אלג' α-מקרב ל-MAX − 3SAT (עבור $\alpha\in[0,1]$) הוא אלג' שמקבל כקלט נוסחת 3CNF חוקית I ומחזיר מספר b שמקיים $\alpha\,\mathrm{val}\left(I\right)\leq b\leq\mathrm{val}\left(I\right)$.

מסקנה (ממשפט ה-PCP) אם $\mathsf{NP} \neq \mathsf{P}$ אז לא קיים אלג' α-מקרב פוליונמי ל-$\mathsf{MAX}-\mathsf{3SAT}$ עבור $s < \alpha$ (כאשר s הקבוע ממשפט ה-PCP).

הערה או במילים, אם אפשר לקרב את 3SAT עד כדי s בזמן פולינומי, אז אפשר לפתור את $\mathsf{gap}-\mathsf{MAX}-\mathsf{3SAT}\,[1,s]$ בזמן פולינומי (באמצעות אלג')

הוכחה: נניח בשלילה שקיים אלג' כזה. תהי $L \in \mathsf{NP}$, לכן קיימת רדוקציה f מ-L ל-$[1,s]$ $\mathsf{gap}-\mathsf{MAX}-\mathsf{3SAT}$. יהי קלט w לבעיית ההכרעה L. נריץ את אלג' הקירוב על $f\,(w)$ ונקבל

$$\alpha\,\mathrm{val}\,(f\,(w)) \le b \le \mathrm{val}\,(f\,(w))$$

- אם $w \in L$ אז $b \ge \alpha \underbrace{\mathrm{val}\,(f\,(w))}_{\ge 1} \ge \alpha > s$.
- אם $w \notin L$ אז $b \le \mathrm{val}\,(f\,(w)) \le s$.

כלומר השוואה של b ל-s תכריע האם $w \in L$ ולכן מ"ט דטר' פולי' בזמן יכולה להכריע את L כלומר $L \in \mathsf{P}$, ולכן $\mathsf{NP} = \mathsf{P}$ סתירה. ■

מסקנה אם $\mathsf{gap}-\mathsf{MAX}-\mathsf{3SAT}\,[c,s] \in \mathsf{NPH}$ וגם $\mathsf{NP} \neq \mathsf{P}$ אז אין אלג' קירוב עם פרמטר גדול מ-$\frac{s}{c}$.

הוכחה: כנ"ל. ■

דוגמאות לאלג' קירוב לבעיות קשות ב-NP

- ראינו באלגו' אלג' $\frac{7}{8}$-מקרב ל-3SAT (מגרילים הרבה השמות עד שאחת מספקת לפחות $\frac{7}{8}$ מהפסוקיות).
- בעיית $\mathsf{MAX}-\mathsf{Exact3}-\mathsf{LIN2}$ היא בעיית האופטימיזציה מעל מערכת n משוואות, בכל אחת שלושה משתנים (שניתן לשים בהם $0,1$) שערכה הוא המספר המקס' של משוואות שניתן לספק במערכת.

  אלג' $\frac{1}{2}$-מקרב לבעיה (שראינו באלגו') בודק לכל משתנה איזו השמה עדיפה (לפי תוחלת סיפוק המשוואה) ובוחר באופן חמדני את ההשמה העדיפה.

  ידוע כי $\mathsf{gap}-\mathsf{MAX}-\mathsf{E3}-\mathsf{LIN2}\left[1-\epsilon,\frac{1}{2}+\epsilon\right]$ היא בעיה קשה ב-NP לכל $\epsilon > 0$ (כלומר אינטואיטיבית ממש קשה להבדיל בין מערכות משוואות שניתן לספק כמעט את כל המשוואות בהן לבין מערכות שניתן לספק קצת יותר מחצי ממשוואותיהן).
- בעיית $\mathsf{MAX}-\mathsf{IS}$ לכל גרף מחזירה את גודל קבוצת הקודקודים הבת"ל (אף שני קודקודים בקבוצה אינם מחוברים בצלע) המקסימלית.

  ידוע כי $\mathsf{gap}-\mathsf{MAX}-\mathsf{IS}\left[1-\frac{1}{\sqrt{2}}-\epsilon,\epsilon\right]$ קשה ב-NP לכל $\epsilon > 0$ (ראו הסבר אינטואיטיבי לעיל).

קווים לדמותו של PCP - משחק עם שני שחקנים חזקים ומוודא חלש

נתונים שני שחקנים (חזקים חישובית) שמשחקים משחק: בהינתן נוסחה, הם מתאמים עמדות (בוחרים השמה) ואז מופרדים.

שחקן אחד מקבל פסוקית c_i ושחקן נוסף משתנה בפסוקית x_j. הראשון מחזיר השמה לכל המשתנים ב-c_i והאחרון השמה רק ל-x_J.

הם מנצחים אם ההשמה של הראשון מספקת את c_i ואם שני השחקנים מסכימים על הערך המושם ב-x_j.

הערה הרעיון מאחורי המשחק הזה הוא שקילות ה-PCP למצב בו שני שחקנים חזקים חישובית מנסים להראות הסת' למוודא חלש מאוד שניתן לספק את נוסחה מסוימת.

טענה בהינתן $\text{val}\left(I\right)\leq\alpha$ (שיעור הפסוקיות שניתנות לסיפוק בו זמנית המקסימלי), ההסת' שינצחו היא $P\left(\text{success}\right)\leq1-\frac{1-\alpha}{3}$.

הוכחה: נניח שהשחקנים משחקים באסטרטגיה עם שיעור הצלחה β. לכן

$$
\begin{aligned}
E_{c\in I}\left[\mathbb{1}_{\{\text{מפסידים על } c\}}\right] & \overset{(*)}{\leq} E_{c\in I}\left[\mathbb{1}_{s_1(c)\neq s_2(c)}\right]\\
& \overset{(**)}{\leq} 3\cdot E_{c\in I}\left[\frac{\sum_{i=1}^{3}\mathbb{1}_{s_1(c_i)\neq s_2(c_i)}}{3}\right]\\
& \overset{(***)}{=} 3\cdot\left(1-\beta\right)
\end{aligned}
$$

$(*)$ מונוטוניות ההסת': השחקנים אידאליים ולכן אם c מסופקת ע"י ההשמה (אסטרטגיה) שהוסכמה בהתחלה, שניהם יחזירו את האחרונה. אם היא לא מסופקת תחת ההשמה שחקן 1 ידע את זה וישנה את ההשמה (שתספק ובתקווה תהיה זהה להשמת שחקן 2 למשתנה). לכן אם הם מפסידים הם בהכרח לא מסכימים על ההשמה לפסוקית (של שחקן 1 זו החדשה שהמציא עכשיו ממנ,sc,ה הוא חושף 3 ערכים למוודא ושל 2 היא המוסכמת במקור ממנה הוא חושף ערך אחד למוודא). $s_1\left(c\right),s_2\left(c\right)$ הן וקטורים ב-$\left\{0,1\right\}^3$.

$(**)$ הכפלה וחלוקה ב-3 וגם חסם האיחוד על אי ההסכמה על ההסגר (לפחות אחד מהליטרלים לא מוסכם).

$(***)$ הצלחה היא לשכנע את המוודא שניתן לספק את הפסוקית (במרמה או לאו), ואי הסכמה יש רק כשההשמה המקורית לא מספקת את הפסוקית (כלומר הנוסחה לא ספיקה). לכן ההסת' לכישלון $1-\beta$ היא ההסת' לאי הסכמה בין השחקנים, שזה בדיוק תוחלת ממוצע אי ההסכמה במשוואה למעלה.

ולכן

$$
P\left(\text{success}\right)=\beta\leq1-\frac{E_{c\in I}\left[\mathbb{1}_{\{\text{לא מסופק } c\}}\right]}{3}\leq1-\frac{1-\alpha}{3}
$$

■

הגדרה משחק בין שני שחקנים עם סיבוב אחד (2 Player 1 Round Game) הוא שלשה $G=\left\langle V,P_1,P_2\right\rangle$ כאשר:

- $P_1=\left\langle Q_1,\Sigma_1\right\rangle,P_2=\left\langle Q_2,\Sigma_2\right\rangle$ הם השחקנים כאשר Q_1,Q_2 אוסף שאלות ו-Σ_1,Σ_2 אוסף תשובות.

• $V=\langle D,P\rangle$ הוא מוודא כאשר D התפלגות מעל $Q_1\times Q_2$ (לא בהכרח ב"ת) ו-P "פרדיקט" שהוא פ' $Q_1\times Q_2\times\Sigma_1\times\Sigma_2\mapsto\{0,1\}$.

ערך ההצלחה של המשחק הוא $\text{val}\left(G\right)=\sup_{\text{strategies}}P\left(\text{success}\right)$.

טענה נניח שאנחנו משחקים את המשחק למעלה עם שני השחקנים והנוסחה I שעבורה מתקיים $\text{val}\left(I\right)=\alpha$. אז ניתן לחשב את $\text{val}\left(G\right)$ בזמן סופי.

הוכחה: תוחלת ההצלחה במשחק היא α (ההסת' שניפול על פסוקית שסופקה ע"י ההשמה המקסימלית שלנו) כלומר

$$\alpha=E\left[\mathbb{1}_{\text{success}}\right]=E_{r_1,r_2}\left[E_{\text{strategies}}\left[\mathbb{1}_{\text{success}}\right]\right]$$

כאשר r_1,r_2 סרטי ביטים אקראיים (ככה ממודלת גישה לערכים אקראיים), והאסטרטגיות בתוחלת הפנימית למעשה עוברות דטרמיניזציה כי בהינתן סרט עם הערכים האקראיים שלו, האסטרטגיה נהפכת לדטר'. מתכונות התוחלת, יש לפחות אסטרטגיה אחת (א"ד שנהיית דטר' תחת סרט מקרי כלשהו) עם לפחות ערך α, שזה הכי הרבה שאנחנו יכולים להשיג. לכן מספיק שנעבור על כל האסטרטגיות הדטר' ונקבל $\text{val}\left(G\right)=\max_{\text{det' strategies}}P\left(\text{success}\right)$ כלומר שהאסטרטגיה שמשיגה sup היא מתוך קבוצה סופית. ■

שבוע $\mathbb{III}$ | קודים לתיקון שגיאות

כל טענה מתמטית ניתן לקודד באופן שמחשב יוכל להבין אותו (מעל א"ב כלשהו), ולכן בהינתן טענה S, נוכל לכתוב הוכחה π שגם אותה נוכל לקודד. מעבר לכך ישנו אלג' שרץ בזמן פולי' (באורך הטענה וההוכחה) שמוודא את ההוכחה. עם זאת מציאת הוכחה לטענה נתונה היא לא כריעה.

טענה בהינתן טענה S וסטרינג אונרי 1^n, הבעיה האם יש תווים שמחליפים את 1^n כך שהם מהווים הוכחה חוקית ל-S, היא ב-NP (אפשר לוודא עד פולי'), ובפרט היא שלמה ב-NP.

מסקנה ממשפט ה-PCP, נוכל לבנות מוודא הסת' שדוגם מספר קבוע של ביטים מהוכחה לטענה מתמטית כלשהי (לא רק נוסחת 3SAT) וקובע האם היא תקינה או לא. כלומר הבדיקה הלוקאלית היא להוכחות כלליות ולא לבעיה ספציפית!

הערה קידוד הוא מחרוזת מוארכת מהמקורית שכולל יתירות כדי שיהיה אפשר לשחזר אותו לאחר שהושחת. קודים הם אוסף הקידודים של המילים (לאחר שקודדו), שמהם אפשר לבחור אחד שיעזור לשחזר תוכן מקורי וכו'.

הגדרה יהי Σ אלפבית. קוד מעל Σ הוא $C\subseteq\Sigma^n$ ויש לו ארבעה פרמטרים (n,d,R,q):

• n - אורך המילים המקודדות (block length).

• d - המרחק של הקוד, שערכו $\min_{u\neq w\in C}\left\{h\left(u,w\right)\right\}$ כאשר $h\left(u,w\right)=P_{i\in[n]}\left(u_i\neq w_i\right)$ (חלקיות הקוורדינטות עליהן הוקטורים לא מסכימים).

• R - הקצב (rate) שערכו $\frac{\log|C|}{\log|\Sigma^n|}$.

- q - גודל הא"ב, $q=|\Sigma|$.

הערה נתסכל על u ו-w בקוד מאוד רחוקות אחת מהשנייה לפי מרחק האמינג. אם נשדר את u וחלק מהמידע מושחת כך שהתקבל u', נוכל לשחזר אותה ל-u כי כל מילה אחרת בקוד יותר רחוק מ-u' מאשר u. למעשה כל מרחק פחות מ-$\frac{d}{2}$ ניתן לשחזר נכונה.

הערה הקצב מגדיר את יעילות הקוד - כמה גדול הניפוח ממספר הביטים של האותיות שאנחנו רוצים לייצג ($\log_{|\Sigma|}|C|$) לאורך הקוד שלנו בסוף ($\log_{|\Sigma|}|\Sigma|^n=n$). לכן, R גבוה הוא תכונה רצויה.

הגדרה בהינתן קוד C, $B_w^n(\alpha)=\{u\in\Sigma^n : h(u,w)\leq\alpha\}$ הוא אוסף המילים במרחק (האמינג) לכל היותר α.

הגדרה עבור $\Sigma=\mathbb{F}_q$ (שדה מודולו מעל q ראשוני), $C\subseteq\Sigma^n=\mathbb{F}_q^n$ הוא קוד לינארי אם C הוא מרחב וקטורי (ת"מ של Σ^n).

הערה במקרה כזה,

$$d(C)=\min_{u\neq w\in C}\{h(u,w)\}\overset{(*)}{=}\min_{u\in C\setminus\{0\}}\{h(u,0)\}\overset{(**)}{=}\min_{u\in C\setminus 0}|u|$$

$(*)$ $h(u,w)=h(u-w,0)$.

$(**)$ כך נגדיר ערך מוחלט.

בנוסף, $R=\frac{\dim C}{n}$ כי כל איבר של C ניתן לייצג ע"י $\dim C$ מספרים (שהם הקוורדינטות של וקטורי בסיס של C).

הגדרה בהינתן בסיס $\{M_1,\ldots,M_{Rn}\}$ (של וקטורים עומדים) לקוד C, $M=(M_1\ \ldots\ M_{Rn})$ נקראת המטריצה היוצרת של C.

הערה באמצעות המטריצה היוצרת ניתן לקודד בקלות וביעילות ע"י Mx מפני שתמונת M היא C.

טענה לכל קוד C עם פרמטרים (n,d,R,q) מתקיים $1\geq R+\frac{d}{2}+o_{|\Sigma|}(1)$.

הוכחה:

$$|\Sigma|^n\overset{(i)}{\geq}|C|\cdot\left|B_0\left(\frac{d}{2}\right)\right|\overset{(ii)}{\geq}|C|\binom{n}{\frac{1}{2}dn-1}|\Sigma|^{\frac{dn}{2}}\overset{(iii)}{\geq}|\Sigma|^{Rn+\frac{dn}{2}}2^{\mathcal{O}(n)}\overset{|\Sigma|\to\infty}{=}|\Sigma|^{Rn+\frac{dn}{2}+o(n)}$$

(i) כל מילה ב-w נמצאת בכדור ברדיוס $\frac{d}{2}$ שבו היא נמצאת ללא מילים אחרות בקוד (מהגדרת המרחק). לכן נוכל למלא את $|\Sigma|^n$ בכדורים ברדיוס $\frac{d}{2}$ סביב כל המילים ב-C ועדיין לא למלא את כל Σ^n (או בדיוק כן למלא). כדור סביב 0 מתנהג בדיוק כמו כדור סביב מילה בקוד ולכן לפשטות נשתמש בראשון.

(ii) המילים ב-$B_0\left(\frac{d}{2}\right)$ הם המילים עם לכל היותר $\frac{d}{2}n$ אותיות שאינן 0. לכן קומבינטורית, נבחר את $\frac{1}{2}dn$ האותיות שנשנה (אחד פחות כדי למנוע התנגשויות), ונקבע בהם את הערכים החדשים (בפרט יכולים להיות גם 0, כי 0 גם בכדור של עצמו).

(iii) $\log|C|=Rn$ וחסם עליון ל-choose מהצורה $\binom{n}{\frac{1}{2}dn}$ הוא $2^{\mathcal{O}(n)}$.

ומשם ניקח $\log_{|\Sigma|}$ על שני האגפים, נחלק ב-n ונקבל את הנדרש. ■

קודי Reed-Solomon

בהינתן שתי פרבולות, אנחנו יודעים שהן נפגשות לכל היותר בשתי נקודות, ולכן מבחינת הערכים שלהן הן די שונות. באותו האופן פולינומים ממעלה נמוכה גם כן כשאינם זהים אינם חולקים ערכים רבים.

הגדרה נקבע את דרגת הפולינומים מעל $\mathbb{F}_q$ (q ראשוני כי זה שדה) איתה נעבוד להיות $d \le n \le q$ ונבחר $a_1, \ldots, a_n \in \mathbb{F}_q$. הקוד של ריד-סולומון הוא

$$RS_{d,a_1,\ldots,a_n,q} = \left\{ f\left(a_1\right), \ldots, f\left(a_n\right) \mid \deg f \le d \text{ פוליונום עם } f : \mathbb{F}_q \to \mathbb{F}_q \right\}$$

הערה זהו קוד לינארי כי $\mathbb{F}_q\left[x\right]$ מרחב וקטורי ופולינומים מדרגה $\ge d$ סגורים לחיבור וכפל בסקלר.

נחשב את הפרמטרים של הקוד.

- אורך הקוד הוא n.
- מרחק הקוד הוא $1 - \frac{d}{n}$ כי שני פולינומים שונים מסכימים על לכל היותר d נקודות.
- קצב הקוד הוא $\frac{d+1}{n}$ כי $\dim C = d + 1$ וזהו קוד לינארי.
- גודל הא"ב הוא $q = |\Sigma| = |\mathbb{F}_q|$.

אם נבחר $d \le \frac{n}{2}$ נקבל קצב ומרחק $\frac{1}{2}$ שכאמור מאפשר לנו לשחזר קוד מושחת תמיד, וגודל א"ב בין n ל-$2n$ (שם בהכרח יש ראשוני).

הערה כרגע יש לנו n^n מילים ב-$|\Sigma|^n$. נרצה משהו עם משמעותית פחות אותיות. אם נבחר קוד C_2 עם n מילים ונייצג כל אות ב-Σ באמצעות מילה מ-C_2, נוכל לייצג קודים ב-C_1 באמצעות מילים מהקוד הקטן יותר (באמצעות הצמדה), ובתקווה עדיין לשמר את אותן התכונות (כבר ניתן לראות שהקצב ירד).

הרכבת קודים

הגדרה יהיו C_1 קוד $\left(n_1, d_1, r_1, q_1\right)$ מעל Σ ו-C_2 קוד $\left(n_2, d_2, r_2, q_2\right)$ מעל Σ' עבורם $q_1 \gg q_2$, $|C_2| \ge q_1$ וקיימת העתקה $E : \Sigma \overset{\text{חח"ע}}{\to} C_2$ (קידוד אותיות ב-Σ למילים בקוד C_2). נגדיר את <u>ההרכבה של הקודים</u> C_1, C_2 להיות

$$C_1 \circ C_2 = \left\{ \left(E\left(x_1\right) || \ldots || E\left(x_{n_1}\right)\right) : x_1 \ldots x_{n_1} \in C_1 \right\}$$

פרמטרים של הרכבה

- אורך הקוד הוא $n_1 \cdot n_2$ (יש לנו n_1 מילים משורשות, כל אחת באורך n_2).

- מרחק הקוד הוא $d\left(C_1 \circ C_2\right) \geq d_1 \cdot d_2$ כי כשנדגום קוורדינטה מקרית נדגום קודם קוורדינטה מהמילים המקוריות ב-C_1 לפני שתורגמו, שם הסיכוי לשוויון הוא d_1, ואז לאחר שנתרגם הסיכוי לשוויון בקוורדינטה הוא d_2 (אין התנגשויות ב-E כי היא חח"ע).

- קצב הקוד הוא $R_1 \cdot R_2$ (עד כדי קבוע קטן) מהחישוב

$$\begin{aligned} R\left(C_1 \circ C_2\right) &= \frac{\log\left|C_1\right|}{\log\left(q_2^{n_1 \cdot n_2}\right)} \\ &= \frac{\log\left|C_1\right|}{\log\left(q_1^{n1}\right)} \cdot \frac{\log\left(q_1^{\cancel{n1}}\right)}{\log\left(q_2^{\cancel{n1} \cdot n_2}\right)} \\ &\approx R_1 \cdot R_2 \end{aligned}$$

כאשר באופן אופטימלי $\left|C_2\right|$ קרוב כמה שיותר (מלמעלה) ל-q_1, כלומר אין לנו יותר מדי מילים שלא מייצגות אות ב-Σ_1.

טענה הרכבת קידודים לינאריים עם E לינארית היא קוד לינארי.

השגת קוד עם פרמטרים קבועים וא"ב בגודל 2

משפט קיים קוד מעל הא"ב $\{0,1\}$ עם מרחק וקצב קבוע ב-n (אורך המילים שנקודד) ואורך מילה $\log\log\log n$.

הוכחה: נבחר C_1 קוד עם פרמטרים $\left(n, \frac{1}{2}, \frac{1}{2}, n\right)$ (לצורך עניינו, ריד-סולומון עם $d = \frac{n}{2}, q = n$). כל $\frac{n}{2}$-יה של ערכים ב-$\mathbb{F}_q$ ניתנת להשגה ע"י פולינום ממשפט האינטרפולציה ולכן $\left|C_1\right| = n^{\frac{n}{2}}$.

נבחר C_2 עם פרמטרים $\left(\log n, \frac{1}{2}, \frac{1}{2}, \log n\right)$ (ריד סולומון עם $q = k$ ו-$d = \frac{k}{2}$ עבור $k = \log n$) ולכן בדומה $k^{\frac{k}{2}} = \left|C_2\right| \geq n$.

עתה $C = C_1 \circ C_2$ הוא קוד עם פרמטרים $(n, d, R, q) = \left(n\log n, \frac{1}{4}, \frac{1}{4}, \log n\right)$.

נבחר C_3 עם פרמטרים $\left(\log\log n, \frac{1}{2}, \frac{1}{2}, \log\log n\right)$ ונקבל של-$C \circ C_3$ יש את הפרמטרים $\left(n\log n\log\log n, \frac{1}{8}, \frac{1}{8}, \log\log n\right)$.

בראייה כוללת, אנחנו מאבדים ביצועים (קצב ומרחק יורדים) ולא מתקרבים ל-$q = 2$ אלא רק משיגים q לוג' ב-n. נצטרך גישה אחרת.

אם קיים קוד C_4 עם פרמטרים $\left(\log\log\log n, \frac{1}{100}, \frac{1}{100}, 2\right)$ ואז נוכל להרכיב את $C \circ C_3$ עליו ולקבל קוד עם קצב, מרחק וגודל א"ב קבוע, ואורך מילים בקוד קרוב מאוד ל-n, שזו המטרה הסופית שלנו.

בנוסף, מספר תתי הקבוצות של מילים באורך $\log\log\log n$ מתוך $\{0,1\}^*$ הוא $2^{2^{\log\log\log n}} = \log n$ כלומר נוכל לעבור על כל הקבוצות עד שנגיע לאחת שהיא קוד עם פרמטרים מספקים בזמן $\operatorname{polylog} n$. כל שנותר הוא להוכיח שיש קוד כזה. ■

טענה לכל $N \in \mathbb{N}$ קיים קוד מעל $\{0,1\}^N$ עם פרמטרים $\left(N, \frac{1}{100}, c, 2\right)$ כאשר $c \in [0,1]$ קבוע.

הוכחה: נראה אלג' שמוצא קוד שמוכל ב-$\{0,1\}^N$. נבחר $w_1 \in \{0,1\}^N$ ונוציא מ-$Q = \{0,1\}^N$ את המילים שבכדור ברדיוס $\frac{1}{100}$ שלה. נבחר מילה נוספת זמינה ונשלול מ-Q את מה שברדיוס שלה, וחוזר חלילה. האלג' יפסיק כשאין עוד מילים זמינות.

ברור שלקוד מרחק $\frac{1}{100}$ לפחות. נוכיח שיש לקוד קצב קבוע. נניח שמצאנו k מילות קוד ואז נתקענו. מתקיים $2^N \leq k \cdot \left|B_0\left(\frac{1}{100}\right)\right|$ כי בכל פעם לכל היותר שללנו $\left|B_0\left(\frac{1}{100}\right)\right|$ מילים, ולכן

$$k \geq \frac{2^N}{\left|B_0\left(\frac{1}{100}\right)\right|} \geq \frac{2^N}{\binom{N}{\frac{N}{100}-1}} \overset{(*)}{\geq} 2^{c\cdot N}$$

$(*)$ מתקיים $\binom{N}{\alpha N} \approx 2^{N\left(\log_2 \frac{1}{\alpha} + \log_2 \frac{1}{1-\alpha}\right)}$.

לכן $R = \frac{\log k}{\log 2^N} = c$ כאשר c קבוע. ■

שבוע $\mathbb{III}$ | בודקים-מקומיים

הערה נשתמש בקודים כדי לעשות PCP בגרסתו הפשוטה יותר: בהינתן וקטור בגודל n (שהוא אסימפטוטית גדול), נרצה להחליט האם הוא מילת קוד או לא באמצעות דגימת מספר קבוע של ביטים מתוכו.

הערה ב-PCP אנחנו עושים בדיקה לוקאלית (הסת') של "נכונות הוכחה" (בעצם בודקים את נכונות הטענה: בהינתן טענה, אם היא ספיקה אז בסבירות גבוהה הביטים שנדגום יספקו הסגר ב-3SAT, אבל זה לא אומר שההוכחה הספציפית הזו דווקא נכונה).

בדקן-מקומי לקוד

לכאורה אפשר לדחות מילה $w \in \Sigma^n$ אם הרישא שלה (בגודל קבוע) לא נכללת מבין רישאות מילות הקוד. זה לא עובד כי מספיק שנחליף אות אחת מקוד חוקי מקרית ובהסת' גבוהה (אסימפטוטית) נחליף ביט שאנחנו לא בודקים ובגלל שהמרחק בין קודים גדול הרי שהשינוי לא יהיה ב-C אבל כן נאשר אותו.

הגדרה יהי $n \in \mathbb{N}$ ו-$C \subseteq \Sigma^n$ קוד. T אלג' רנדומי הוא (ϵ, δ, h) $-$local $-$ tester ל-C אם:

1. הוא מבצע h גישות אורקל למילה נתונה w (שאילתות מהצורה "תן לי את האות באינדקס i").
2. לכל $w \in C$ מתקיים $P\left(w \text{ מקבל את } T\right) = 1$ (שלמות היא 1 במונחי PCP).
3. לכל w כך ש-$\Delta\left(w, C\right) \geq \epsilon$ מתקיים $P\left(w \text{ דוחה את } T\right) \geq \delta$ (התקפות היא לכל היותר $1-\delta$).

הערה T תלוי ב-C ו-C יכול להשתנות לפי n (כי כל קוד הוא למעשה משפחת Expander-ים) אבל נתעלם מהפער הזה.

הערה עם $h=1$ אין אלג' שנותנים שלמות 1, $h=2$ יש אלג' עם כמעט שלמות 1 ו-$h=3$ כבר יש שלמות 1.

local $-$ tester עבור קוד ריד-סולומון

יהי קוד $C = RS_{d,a_1,\ldots,a_n,q} \subseteq \mathbb{F}_q^n$ כאשר $d < n \leq q$.

דוגמה קודים עם $d=2$ הם שערוך פרבולה ב-n הנקודות. עם $q=4$ אפשר לדגום שלושה ערכים, הם מגדירים לנו את פרבולה (כשאם מדובר במילת קוד, היא הפולינום שמשרה את המילה) ואז נקודה רביעית, ונבדוק האם הפרבולה שחזינו זהה לערך במילה, ונקבל אם כן. זה יתקיים לכל מילת קוד (וגם למילים שהן לא מילות קוד שבמקרה הנקודות שדגמנו חוזות נכונה את הנקודה האחרונה).

במקרה הכללי עם $d+2$ נקודות אפשר לבנות בדקן-מקומי ע"י דגימת $d+1$ נקודות שקובעות את הפולינום המשרה את המילה (לכאורה) ואז חיזוי האות ה-$d+1$ עם הפולינום ולסיום בדיקת שוויון מול מה הערך המופיע במילה (מקבלים אם כן, דוחים אחרת). נקרא למבחן זה מבחן האינטרפולציה.

טענה "מבחן האינטרפולציה" הוא בוחן לוקאלי עבור C עם פרמטרים $(\epsilon,\delta,h)=(2\delta,\delta,d+2)$ כאשר $\delta<\frac{1}{4(d+1)^2}$.

הערה הקשר הפרופורציוני בין ϵ ל-δ הוא הגיוני כי ככל שהמילים המטעות שלנו יותר קרובות למילות קוד אמיתיות, הסיכוי שנדגום אותיות שחושפות את היות המילה לא בקוד יורד (כי רוב האותיות משותפות עם מילת קוד אמיתית).

הוכחה: ברור שאנחנו מבצעים רק $h=d+2$ בקשות וברור שאם $w\in C$ אז נקבל בהסת' 1.

1. אם הסיכוי לקבל את w הוא 1 אז $w\in C$ (נכונות הפרמטרים עבור $\delta=0$).

   נבחר $\{a_1,\ldots,a_n\} \subseteq b_1\neq\ldots\neq b_{d+1}$. יהי $g:\mathbb{F}_q\to\mathbb{F}_q$ הפולינום היחיד מדרגה $\leq d$ שמסכים עם w על $b_1,\ldots,b_{d+1}$ (קל להוכיח יחידות). לכל $a\in\{a_1,\ldots,a_n\}$:

   - אם $a\in\{b_1,\ldots,b_{d+1}\}$ אז g מסכים עם w על a מהגדרתו.
   - אם $a\notin\{b_1,\ldots,b_{d+1}\}$ אז g מסכים עם w על a (כי מקבלים בהסת' 1).

   ולכן g הוא פולינום מדרגה $\leq d$ שמשרה את w כלומר $w\in C$.

2. אם $\Delta(w,C)=\delta$ אז ההסת' לדחות את w היא לפחות $0<$ (נכונות התכונה השלישית).

   נניח שהבדיקה בוחרת $\{a_1,\ldots a_n\} \in b_0\neq\ldots\neq b_{d+1}$ ועושה אינטרפולציה לערך b_0 לפי שאר הערכים. תהי $w\in\Sigma^n$ כך ש-$\Delta(w,C)=\delta>0$. נביט במאורע

$$E=\{\exists w\in C:w(b_0)\neq w'(b_0)\wedge w(b_i=w'(b_i)\quad\forall i\in[d+1])\}$$

   במקרה כזה המבחן ידחה.

$$P(E)\geq\delta(1-(d+1)\delta)$$

כי ראשית נדגום את b_0 שהוא בהסת' δ (בדיוק) נקודת שוני בין w,w', ואז נטען שההסת' ש-b_i אחד לפחות הוא נקודת שוני היא לכל היותר $(d+1)\delta$ (ואז נסתכל על המשלים). זה נכון מחסם האיחוד כי ההסת' לכל אחד מה-b_i (בנפרד) להיות נקודת שוני היא δ.

זה לא מסיים את ההוכחה כי אם המילים מאוד שונות אי אפשר לבצע את אותו הניתוח כי אי אפשר להניח שנוכל להשיג $\{b_i\}_{i=1}^{d+1}$ שכן יסכימו עם מילת קוד כלשהי.

■

הגדרה יהי קוד $C = RS_{d,0,\ldots,(n-1),q}$ כאשר $d < n = q$ כלומר $\{a_i\} = \mathbb{F}_q$. מבחן האינטרפולציה האריתמטי הוא המבחן הבא: נבחר $b_0 \in \mathbb{F}_q$ מקרי ו-$r \in \mathbb{F}_q \setminus \{0\}$ ונעשה אינטרפולציה בנקודה b_0 בעזרת הנקודות $b_0 + r, b_0 + 2r, \ldots, b_0 + (d+1)r$ (ונקבל אם החיזוי נכון ואחרת לא).

הערה המשפט נכון עם מבחן האינטרפולציה האריתמטי ולא המבחן הרגיל, ואת ההוכחה לכך נראה לאחר שנוכיח נכונות של בדקן-מקומי לקודי הדמארד.

הערה המבחן הזה לא טוב כי כדי לקודד מילים באורך k צריך קוד עם $d \approx k$, והקוד ריד-סולומון שראינו עם תכונות טובות היה לו $d = \frac{n}{2}$ או איזשהו אחוז קבוע מ-n כלומר הלוקאליות שלנו היא לא משהו, כי אנחנו קוראים אחוז קבוע של המילה שהיא באורך n, שהוא אסימפטוטית גדול מאוד.

קודי ריד-מולר והדמארד

הגדרה יהיו $m, d < q \in \mathbb{N}$ קוד ריד-מולר הוא

$$RM_{m,d,q} = \left\{ \left(f\left(v_1,\ldots,v_m\right)\right)_{(v_1,\ldots,v_m)\in\mathbb{F}_q^m} \mid d \geq \text{פולי' ממעלה טוטאלית } f : \mathbb{F}_q^m \to \mathbb{F}_q \right\} \subseteq \mathbb{F}_q^{q^m}$$

הערה מילת הקוד פשוט כוללת את כל הערכים של פולינום רב-משתנים כלשהו. נשערך לפי

$$f\left(x_1,\ldots,x_m\right) = \sum_{\vec{i}:i_1+\ldots+i_m\leq d} c_{\vec{i}} x^{\vec{i}}$$

כאשר $x^{\vec{i}} = x_1^{i_1}\cdot\ldots\cdot x_m^{i_m}$ ו-d המעלה הטוטאלית של f.

הפרמטרים של הקוד הם $(n,d,R,q) = \left(q^m, 1-\frac{d}{q}, \frac{\binom{d+m+1}{d}}{q^m}, q\right)$ כאשר המרחק נכון כי שני פולינומים שונים ב-m משתנים ממעלה טוטאלית d בשדה בגודל q מסכימים על לכל היותר $\frac{d}{q}$ ערכים ממשפט שוורץ-זיפל. הקצב נובע מהיות הקוד לינארי וכן ש-$\left\{x^{\vec{i}}\right\}_{\vec{i}}$ הוא בסיס למרחב המולטינומים והעובדה שיש $\binom{d+m+1}{d}$ מונומים כי יש לנו $m-1$ מחיצות (המפרידות בין חזקות x_i) שביניהן אנחנו מחלקים d כדורים (כל כדור מייצג אינסטנס אחד של אחד המשתנים).

הערה אם נבחר $d = q$ אז נוכל לקודד מספר אקספ' של מילים ב-d ולכן נקבל ביצועים טובים לבדקן-לוקאלי אבל הפרמטרים של הקוד יהיו לא טובים.

המבחן שלנו יהיה בחירת ישר אפיני מקרי מתוך הקוביה שהיא מילת הקוד (ממימד m), והרצת המבחן של ריד-סולומון כרגיל (נבחר $d+1$ נקודות ואז נחזה את הנקודה הבאה ונבדוק שוויון למילה הנבחנת). זאת משום שהישר נותן לנו q נקודות מהצורה $\{v + tu : t \in \mathbb{F}_q\}$ כאשר

$u,v\in\mathbb{F}_q^m$ והצבת $v+tu$ בפולינום רב-משתני נותן פולינום במשתנה אחד t, הלא הוא הפולינום המשרה את הישר האפיני אם הקוביה היא מילת קוד.

הוכחת הנכונות של המבחן מתבססת על נכונות המבחן לסולומון-ריד יחד עם התכונה הגאומטרית לפיה לשתי נקודות סיכוי שווה להיות על ישר אפיני מקרי מתוך קוביה n-ממדית.

הגדרה קוד הדמארד הוא קוד ריד-מולר עם $q=2,d=1$ ובלי המקדם החופשי, כלומר $H_m=\left\{f:f\left(x\right)=\sum_{i=1}^{m}a_ix_i,\ a_i\in\mathbb{F}_q\right\}$.

הערה עתה הקוד מכיל פ' ולא וקטורים כי זה שקול לחלוטין כי ב-RM דוגמים את כל ערכי הפ' (כלומר הוקטור פשוט מייצג את הפ') ולכן נשתמש בשמות לחלופין מעתה.

הערה נבחר m גדול כרצוננו כדי שמבילת קוד יהיו הרבה אותיות ביחס למספר האותיות שנדגום במבחן וכך נקבל לוקאליות טובה. עם זאת נקבל קצב נורא, שהוא $\frac{m}{2^m}$ כי ייצוג של מילה דורש 2^m ביטים (ערך לכל קלט לפ'), אפילו שמילות קוד מושרות מוקטור עם m ביטים (אחת לכל וקטור ב-$M_{1\times m}\left(\mathbb{F}_2\right)$).

הפרמטרים של קוד האדמארד הם $\left(n,d,R,q\right)=\left(2^m,\frac{1}{2},\frac{m}{2^m},2\right)$ כאשר הקצב נובע מהיות הקוד לינארי (הוא הרחבה של קוד ריד-מולר שהוא הרחבה של קוד ריד-סולומון שהוא לינארי).

שבוע $\mathbb{IV}$ | הבודק הלינארי לקודי הדמארד וריד-סולומון

מעתה נתייחס רק לקודי ריד-סולומון עם $\mathbb{F}_q=\{a_1,\ldots,a_n\}$, כלומר נסמן $RS_{d,q}$ כשנתכוון $RS_{d,0,\ldots,q-1,q}$ עבור q ראשוני.

הערה נרשום מחדש את שלושת הקודים שלמדנו, עתה עם פ' כאיברים במקום השיערוכים בהן

$$\begin{aligned}RS_{d,q}&=\{f:\mathbb{F}_q\to\mathbb{F}_q:\deg f\le d\}\\RM_{m,d,q}&=\left\{f:\mathbb{F}_q^m\to\mathbb{F}_q:\deg f\le d\right\}\\H_m&=\{f:\mathbb{F}_2^m\to\mathbb{F}_2:\exists M\in M_{1\times m}\left(\mathbb{F}_2\right),f\left(x\right)=Mx,\forall x\}\end{aligned}$$

הערה לפ' אין דרגה, גם אם הן ניתנות לייצוג ע"י פולינום, ולכן $\deg f$ משמעו דרגת הפולינום מהדרגה הנמוכה ביותר שמייצג את הפ' (במקרה שלנו אין כמה פולינומים אבל עקרונית זו ההגדרה).

הערה אמנם נדמה שהקצב לעתים הוא גרוע (דועך אקספ' ב-d), אבל d לא אמור לעניין אותנו יותר מדי. יותר מעניין להסתכל על הקצב כפ' של n, שמייצג את מספר המילים שאנחנו מקודדים.

דוגמה עבור קוד ריד-מולר עם $m=d,q\approx 2d$, נקבל (מפיתוח לא ברור) קצב שהוא פולינומי קטן ב-m.

לעומת זאת קוד הדמארד נותן קצב $\frac{m}{2^m}$ שהוא אקספוננציאלי קטן ב-m, שהוא גודל המילים שמילות הקוד מייצגות, שזה רע מאוד.

בדקן-מקומי לקודי הדמארד

הערה אי אפשר להכליל את מה שאמרנו על ריד-מולר (שם בחרנו ישר דרך הקוביה והרצנו את הבדקן של ריד-סולומון על הישר) להדמארד כי כדי לעשות מבחן אינטרפולציה צריך לפחות 3 נקודות על אותו ישר, וב-$\mathbb{F}_2$ יש רק שני איברים ולכן אין שלושה איברים על אותו ישר.

נבדוק שהפ' מקיימת $f(x) = f(y) + f(x+y)$ (בגלל שאנחנו ב-$\mathbb{F}_q$ + ו-− מבצעים את אותה הפעולה). f היא מילת קוד חוקית אם"ם המשוואה מתקיימת בהסת' 1 על פני $x, y \in_R \mathbb{F}_2^m$ (כאשר ההגרלה היא אחידה, כלומר מתקיים לכל x, y).

הגדרה נאמר כי פ' f היא random-self-reducable אם לכל x, מתקיים $f(x) = f(y) + f(x+y)$ בהסת' גבוהה כאשר y מוגרל באקראי.

הערה התכונה שימושית כי אם נרצה לחשב את $f(x)$ כאשר ידועים לנו ערכים אחרים של הפ', נגריל y אקראי ונחשב $f(x) = f(y) + f(x+y)$ כאשר אמנם $y, x+y$ תלויים אחד בשני מאוד, כל אחד מהם בנפרד מתפלג אחיד.

הגדרה הבודק הלינארי בוחר באקראי $x, y \in \mathbb{F}_2^m$ ומחזיר

$$B(x,y) = B_f(x,y) = \mathbb{1}_{\{x,y: f(x) = f(y) + f(x+y)\}}(x,y)$$

טענה הבודק הלינארי הוא בודק-לוקאלי עם פרמטרים $(\epsilon, \delta, h) = (\epsilon, 2\epsilon, 3)$ עבור H_n כאשר $\epsilon < \frac{1}{8}$.

הערה לצורך הוכחת המשפט נשתמש באינטואיציה הבאה: אם במקרה ידוע לנו ש-f היא פ' ϵ-קרובה לפ' g לינארית, אז $f(x) = f(y) + f(x+y)$ בהסת' גבוהה כי $P(f(y) = g(y)) \geq 1 - \epsilon$ וכך גם עבור $x+y$ ולכן $P(f(x) = g(x)) \geq 1 - 2\epsilon$ מחסם האיחוד. אם לא ידוע לנו ש-f קרובה לפ' לינארית, נצטרך לפעול בצורה אחרת.

הוכחה: ברור שהבודק מקבל מילים בקוד ושהוא דוגם רק שלושה ערכים. נוכיח את התכונה השלישית בקונטרה פוזיטיב, כלומר שאם מילה עוברת את המבחן בהסת' גבוהה, אז היא קרובה למילה בקוד. תהי $f : \mathbb{F}_2^m \to \mathbb{F}_2$ כך ש-$P_{x,y}(B_f(x,y)) \geq 1 - \epsilon$. נרצה למצוא את $g : \mathbb{F}_2^m \to \mathbb{F}_2$ הלינארית הקרובה ל-f. נגדיר את g לכל $x \in \mathbb{F}_2^m$ ע"י

$$g(x) = \operatorname*{Maj}_{y \in \mathbb{F}_2^m} \left(f(y) + f(x+y)\right)$$

כאשר הרעיון הוא שבגלל שרוב הערכים של f מתנהגים כמו פ' לינארית, אז חישוב ערכו של g באמצעות דעת הרוב של f (על ערכים שונים מ-x אמנם) ייתן תוצאות מיטיבות. נוכיח כי $\text{dist}(f,g) \leq 2\epsilon$,

$$
\begin{aligned}
1-\epsilon &\leq P_{x,y}\left(f\left(x\right)=f\left(y\right)+f\left(x+y\right)\right)\\
\text{התוחלת השלמה} &= E_x\left[P_y\left(B_f\left(x,y\right)\mid x\right)\right]\\
(*) &\leq P_x\left(M\right)\cdot 1+\left(1-P_x\left(M\right)\right)\frac{1}{2}\\
&=\frac{1}{2}+\frac{1}{2}P_x\left(M\right)
\end{aligned}
$$

$(*)$ נסמן $M=\left\{x:P_y\left(B_f\left(x,y\right)\right)\geq\frac{1}{2}\right\}$ ונשתמש בנוסחת ההסת' השלמה (משמאל כל הסת' קטנה מ-1 ומימין ההסת' תחת M^C ל-$B_f\left(x,y\right)$ היא לכל היותר $\frac{1}{2}$ מהגדרת M).

ומהעברת אגפים נקבל $\frac{1}{2}P_x\left(M\right)\geq\frac{1}{2}-\epsilon$ כלומר

$$
P_x\left(f\left(x\right)=g\left(x\right)\right)=P_x\left(M\right)\geq 1-2\epsilon
$$

כלומר של-$1-2\epsilon$ מה-x-ים לפחות חצי מה-y-ים מקיימים את המבחן, ומכך נובע שהמרחק אכן חסום ע"י 2ϵ.

נשים לב שיש לנו qualifier חלקיות גם ל-x-ים וגם ל-y-ים, נרצה לחזק את המשוואה הנ"ל כדי להוכיח הוכחת התכונה השלישית.

נאמר כי $\left(x,y,x+y\right)$ <u>חופשית</u> אם $x,y\in_R\mathbb{F}_2^m$, <u>מעוגנת</u> אם x קבוע ו-$y\in_R\mathbb{F}_2^m$ <u>וקבועה</u> אם x,y קבועים.

טענת ביניים קטנה לכל x,

$$
\star=P_{y^1,y^2}\left(f\left(y^1\right)+f\left(x+y^1\right)=f\left(y^2\right)+f\left(x+y^2\right)\right)\geq 1-2\epsilon
$$

הוכחה: $\left(y_1,y_2,y_1+y_2\right)$ היא שלשה חופשית, וכך גם $\left(x+y_1,x+y_2,y_1+y_2\right)$ ולכן מהתנאי שדרשנו לעצמנו בתחילת ההוכחה הכללית, ההסת' שכל אחת מהמשוואות הבאות לא מתקיימות הוא לכל היותר ϵ

$$
\begin{aligned}
f\left(y^1\right)&=f\left(y^2\right)+f\left(y^1+y^2\right)\\
f\left(x+y^1\right)&=f\left(x+y^2\right)+f\left(y^1+y^2\right)
\end{aligned}
$$

ולכן השוויון הבא מתקיים בהסת' לפחות $1-\epsilon-\epsilon=1-2\epsilon$ (המשלים להסת' שאחד האי שוויונות לא מתקיים, שנחסם מחסם האיחוד)

$$
\begin{aligned}
f\left(y^1\right)+f\left(x+y^1\right)&=f\left(y^1\right)+f\left(x+y^2\right)+f\left(y^1+y^2\right)\\
&=f\left(y^2\right)+f\left(y^1+y^2\right)+f\left(x+y^2\right)+f\left(y^1+y^2\right)\\
&=f\left(y^2\right)+f\left(x+y^2\right)
\end{aligned}
$$

$\blacksquare$

טענת ביניים גדולה לכל x (לא רק $1-2\epsilon$ מתוך כולם),

$$P_y\left(g\left(x\right)=f\left(x+y\right)+f\left(y\right)\right)\geq1-2\epsilon$$

כלומר יש רוב מוחץ של y-ים שנותנים ערך $f\left(x\right)=g\left(x\right)$.

הוכחה: יהי $x\in\mathbb{F}_2^m$. נסמן

$$p=P_y\left(f\left(y\right)+f\left(x+y\right)=0\right)$$

ולכן $g\left(x\right)=0$ אם $p>\frac{1}{2}$ ואחרת $g\left(x\right)=1$. לכן מתקיים

$$1-2\epsilon\leq\star\overset{(*)}{=}p^2+\left(1-p\right)^2=1-2p\left(1-p\right)$$

כלומר $p\left(1-p\right)\leq\epsilon$. אם $p<\frac{1}{2}$ אז $\frac{1}{2}p<p\left(1-p\right)$ כלומר $p\leq2\epsilon$ ואחרת $1-p\leq2\epsilon$. זה אומר ש-$p\geq1-2\epsilon$ או ש-$1-p\geq1-2\epsilon$. המקרה הראשון משמעו שברוב של $1-2\epsilon$ האינטרפולציה תיתן 0 והשני שבאותו רוב היא נקבל 1, כך שכך או כך, חישוב g הוא ברוב מוחץ על פני האינטרפולציות. $\blacksquare$

נסיים את הוכחת הטענה הכללית ע"י הוכחה ש-$g\left(x\right)=g\left(z\right)+g\left(x+z\right)$ לכל x,z, כלומר ש-g אכן לינארית. נביט בנקודות הבאות

$$\begin{array}{ccc}
x & y^1 & x+y^1\\
z & y^2 & z+y^2\\
x+z & y^1+y^2 & x+z+y^1+y^2
\end{array}$$

עבור y^1,y^2 מקריים, שלושת השורות הן שלשות מעוגנות (סכום ביטים מתפלגים אחיד מתפלג אחיד) ושתי העמודות הימניות הן שלשות חופשיות. לכן בהסת' לפחות $0<1-8\epsilon=1-\left(2\epsilon+2\epsilon+\epsilon+\epsilon+2\epsilon\right)$

$$\begin{aligned}
g\left(z\right)+g\left(x+z\right) & =f\left(y^2\right)+f\left(z+y^2\right)+g\left(x+z\right)\\
 & =f\left(y^2\right)+f\left(z+y^2\right)+f\left(y^1+y^2\right)+f\left(x+z+y^1+y^2\right)\\
 & =f\left(y^1\right)+f\left(x+y^1\right)\\
 & =g\left(x\right)
\end{aligned}$$

כאשר כל מעבר מתקיים לא בהסת' 1 אלא בהסת' נמוכה מ-1 ולכן לכאורה השוויון מתקיים בהסת' נמוכה מ-1, אבל מאחר שאין לנו פה הסת' לנוסחה הסופית (שכוללת רק את x,z שהם קבועים), הרי שהמשוואה מתקיימת תמיד ולכן g לינארית. לסיום הראנו ש-f 2ϵ-קרובה ל-g שהיא לינארית, כלומר מילת קוד חוקית. $\blacksquare$

הערה ההוכחה היא הדרגתית: קודם הוכחנו ש-f קרובה ל-g בהסת' גבוהה לשלשות חופשיות, ואז בהסת' גבוהה לשלשות מעוגנות ואז בהסת' 1 לשלשות קבועות.

נספק הוכחה בראשי פרקים (אנלוגית לחלוטין להוכחה הנ"ל) לכך שבדקן לריד סולומון עם מבחן האינטרפולציה האריתמטי הוא אכן בדקן-מקומי.

נגדיר לכל x, $g(x)=\operatorname*{plur}_{r\in_R\mathbb{F}_q}\sum a_i f(x+r\cdot i)$. ניתן להוכיח כי g $d\epsilon$-קרוב ל-f. משם נראה שהאינטרפולציות עבור r_1,r_2 מקריים שוות בהסת' קרובה ל-1 (כלומר שוויון על סדרות חופשיות, זו טענת הביניים הקטנה). משם ניתן להוכיח שהשוויון בין g ו-f מתקיים לסדרות מעוגנות בהסת' $\approx 1-d^2\epsilon$ באמצעות טיעון מהסת' שלא קשור לקודים (החישוב עם p). לסיום אפשר להוכיח ש-f שווה ל-g עבור סדרות קבועות בהסת' קרובה ל-1. זה מוכיח ש-g מקיים את האינטרפולציות לכל סדרה חשבונית, ובתרגיל הוכחנו שתחת שדה ראשוני זה מספיק כדי להוכיח ש-g הוא פולינום.

שבוע $\mathbb{V}$ | הרחבה נמוכת-מימד

הגדרה יהי הטור $p(x_1,\ldots,x_m)=\sum_{\alpha\in\mathbb{N}_0^m}a_\alpha\prod_{i=1}^n x_i^{\alpha_i}$. אם המקדמים של p מתאפסים מחוץ לתחום חסום, נגדיר את המעלה הטוטאלית של p להיות $\deg p=\max_{\alpha:a_\alpha\neq 0}\sum_{i=1}^m\alpha_i$ ואת המעלה האינדיווידואלית להיות $\deg' p=\max_{\alpha:a_\alpha\neq 0}\|\alpha\|_\infty$.

דוגמה עבור $x_1x_2x_3+x_1x_2x_7^2$, הדרגה הטוטאלית היא 4 והאינדיבידואלית היא 2.

הגדרה נגדיר $RM'_{d,m,q}=\left\{f:\mathbb{F}_q^m\to\mathbb{F}_q:\deg' f\le d\right\}$.

הערה מתקיים $RM_{d,m,q}\subseteq RM'_{d,m,q}\subseteq RM_{dm,m,q}$.

נציג שתי דרכים לקידוד מילה כלשהי $(a_0,\ldots,a_d)$ באמצעות הקוד $RS_{d,q}$.

- נשתמש ב-$\{a_i\}$ כמקדמים של פולינום ואז נשערך ב-$0,\ldots,q-1$ וזו תהיה מילת הקוד שלנו (שמושרת ע"י הפולינום שיצרנו). הבעיה היא שאין לנו דרך לשחזר ממילת הקוד את המילה המקורית.

- נגדיר פולינום באמצעות אינטרפולציה ביחידות ע"י $f(i)=a_i$ לכל $i\in\{0,\ldots,d\}$ ונשתמש במילת הקוד המושרת ע"י פולינום זה (השערוך שלו ב-$\{0,\ldots,q-1\}$). שחזור ממילת הקוד הוא טריוויאלי - המילה היא רישת $d+1$ הערכים הראשונים של מילת הקוד.

ניתן להכליל זאת לפולינום בכמה משתנים; לדרגה טוטאלית d יש לנו $\binom{d+m}{m}$ מקדמים, לכן נצטרך לבחור קבוצה $S\subseteq\mathbb{F}_q^m$ בגודל $\binom{d+m}{d}$ שבה נשערך וזו תהיה מילת הקוד שלנו.

הגדרה S היא <u>קבוצת אינטרפולציה</u> לקוד C (שמכיל פ' מהצורה $\mathbb{F}_q^m\mapsto\mathbb{F}_q$) אם לכל פ' חלקית $f:S\to\mathbb{F}_q$ קיימת הרחבה יחידה $\hat{f}:\mathbb{F}_q^m\to\mathbb{F}_q$ שהיא פ' ב-C.

דוגמה עבור $m=1$, $S=\{0,\ldots,d\}$ היא קבוצת אינטרפולציה (ישיר ממשפט האינטרפולציה).

דוגמה למה לא כל קבוצה היא קבוצת אינטרפולציה? נביט ב-$C = RM_{d,m,q}$ עבור $m \gg 1$ ו-$d = 2$.

נבחר ישר בקובייה $\mathbb{F}_q^m$ ונגדיר f כך שיהיה 0 על כל הישר למעט נקודה אחת, בה נדרוש שיהיה 1. $m > 4$ ולכן יש לפחות 3 אפסים על הישר.

נזכור כי כל פולינום רב משתני ממעלה טוטאלית $\leq d$ הוא גם מדרגה $\leq d$ על כל ישר (אם נחליף את הפרמטרים ב-$u + tv$ אז נקבל פולינום במשתנה יחיד מדרגה לכל היותר d). לכן, כל הרחבה ל-f שתגיע מ-C (שהיא בהכרח פולי') היא בהכרח פולינום האפס ($d = 2 < 3$). עם זאת כמובן שיש לנו ערך שונה מאפס שדרשנו לכן לא נוכל להרחיב את f לפולינום בקוד.

Low-Degree Extension

נרצה לבצע קידוד אינטרפולציה ל-$RM'_{d,m,q}$.

טענה תהי $H \subseteq \mathbb{F}_q$ בגודל $d+1$ (לדוגמה $H = \{0, \ldots, 1, d\}$) ו-$S = H^m \subseteq \mathbb{F}_q^m$, אזי S היא קבוצת אינטרפולציה ל-$RM'_{d,m,q}$, כלומר לכל $f : S \to \mathbb{F}_q$ קיימת הרחבה יחידה $\hat{f} : \mathbb{F}_q^m \to \mathbb{F}_q$ שהיא מילת בקוד $RM'_{d,m,q}$.

הערה במקרה כזה נאמר כי $\hat{f}$ היא ה-low-degree extension של f.

הוכחה: יהי $x^0 \in S$. נסתכל על $\mathbb{1}_{x^0} : S \to \mathbb{F}_q$. עבור כל i נגדיר את $f_i : \mathbb{F}_q \to \mathbb{F}_q$ להיות הפולינום היחיד מדרגה $\leq d$ המקיים $f_i(y) = \mathbb{1}_{\{y = x_i^0\}}$ לכל $0 \leq y \leq d$.

עתה נגדיר $f(x) = \prod_{i=1}^{m} f_i(x_i)$, וזו ההרחבה ל-$\mathbb{1}_{x^0}$. לפולינום הזה יש דרגה אינדבידואלית d. כל פ' היא קומבינציה לינארית של פ' מהצורה $\mathbb{1}_x$ ולכן כל פ' ניתנת להרחבה.

יחידות מתקבלת כי אם $\hat{f}, \hat{f}'$ פולינומים שעונים על התנאים בטענה, אז הם מדרגה $\leq d$ בכל משתנה, ואם נקבע את כל המשתנים חוץ מ-x_i, נקבל שני פולינומים מדרגה $\leq d$ שמסכימים על $d+1$ נקודות ($\{0, \ldots, d\}$), ולכן הם שווים (הוכחנו טענה זו בשאלה $6\ (b)$ של התרגיל עבור $m = 2$). ■

בדיקת סכום ומכפלה עם אורקל פולינומי

נניח שיש לנו "קופסה פולינומית" שמציגה ממשק $f_{d,m,q}$ כאשר $f : \mathbb{F}_q^m \to \mathbb{F}_q$ פ' מדרגה טוטאלית לכל היותר d ונוכל להגיש שאילתות לחישוב ערכי f.

בהינתן קופסאות $f_{d,m,q}$ ו-$g_{d,m,q}$ ו-$h_{2d,m,q}$, נרצה לבדוק האם $f + g = h$ או $f \cdot g = h$. המבחן לבדיקת סכום פולינומי מגריל $x \in_R \mathbb{F}_q^m$ ומוודא כי $f(x) + g(x) = h(x)$.

השלמות היא 1 כי אם $f + g = h$ אז תמיד נקבל שוויון, והנאותות היא $\frac{dm}{q}$ (אם $(f+g) - h$ אינו פולינום האפס, הוא מתאפס בהסת' $\leq \frac{dm}{q}$ משווארץ-זיפל).

הערה אם זה היה דטרמיניסטי היינו צריכים להשוות d^m ערכים.

כדי לקבל נאותות 0 נצטרך להשוות את הערכים של הקופסאות על קבוצת אינטרפולציה, אז נטען של-$f+g$ ול-h ישנן הרחבות יחידות, שמושרות מאותה קבוצת אינטרפולציה ולכן הן שוות על כל הדומיין. השוואת שערוכים של נקודות מתוך קבוצה שאינה קבוצת אינטרפולציה לא תאפשר להכריע בהסת' 1 האם באמת מתקיים שוויון, מפני שיחידות ההרחבה נחוצה לטיעון השוויון על כל הדומיין.

הערה בדומה, מבחן בדיקת המכפלה פולינומית מגריל $x\in_R\mathbb{F}_q^m$ ומוודא כי $f(x)\cdot g(x)=h(x)$. השלמות היא שוב 1 והנאותות היא $\frac{2dm}{q}$.

תכונת הסכום

הגדרה נתונות קופסאות $f^0_{d,m,q},f^1_{d,m-1,q},\ldots,f^{m-1}_{d,1,q},f^m$ כאשר $f^m\in\mathbb{F}_q$. נאמר כי $\left(f^0,\ldots,f^m\right)$ מקיימת את <u>תכונת הסכום</u> אם

$$f^i\left(x_{i+1},\ldots,x_m\right)=\sum_{y=0}^{d}f^{i-1}\left(y,x_{i+1},\ldots,x_m\right)$$

לכל $i\in[m]$ ו-$(x_1,\ldots,x_m)\in\mathbb{F}_q^m$.

נרצה לחשב סכום של d^m ערכים ב-$\mathbb{F}_q$ בזמן תת-אקספ' (ב-m). נסדרם על קוביה m-ממדית, כלומר נתאים לכל אינדקס מהקבוצה $S=\{0,\ldots,d\}^m$ מספר מהערכים שלנו, ונסמן את ההעתקה הזו ב-$f:S\to\mathbb{F}_q$. נסמן $f^0=\hat{f}$, הרחבת ה-low-degree ל-$\mathbb{F}_q^m$.

נניח שבהינתן f^0, מוכיח חזק חישובית סיפק לנו קופסאות נוספות כך ש-$\left(f^0,\ldots,f^m\right)$ מקיימת את תכונת הסכום.

הערה בהמשך נסיר את האמון העיוור שלנו במוכיח ונוסיף מבחן שבודק (הסת') שהקופסאות אכן מקיימות את תכונת הסכום.

אינטואיטיבית, סדרת קופסאות שמקיימת את תכונת הסכום היא סדרת קוביות שערוכים ממימד יורד (ב-1) בכל פעם, שעבורן סכימת האיברים על ישר מיושר למימד הראשון שווה לשערוך אחד מתוך הקוביה הבאה. כלומר, הסכום של כל הערכים של f^0 בישר שהפרמטר שלו הוא ערך המימד הראשון, שווה לערך אחד של f^1 שהוא קוביה $m-1$ ממדית. כדי לסכום את כל הערכים בקוביה S (שהם ערכי הפולינום f^0 בכל נקודה), מספיק שנסכום רק את כל הערכים בקוביה ה-$m-1$ ממדית של ערכי f^1. באותו האופן, כל סכום ערכי ישר בקוביה של ערכי f^1 הוא ערך אחד בקוביה של f^2 וחוזר חלילה.

לכן, f^m (סקלר) יהיה סכום כל הערכים בקופסה שלנו.

מבחן ה-sum-check

נציע גרסה ראשונה למבחן הסת' לבדיקת תכונת הסכום, ה-sum-check; לכל i, נגריל $(x_i,\ldots,x_m)$ ונבדוק האם המשוואה בהגדרת תכונת הסכום מתקיימת עבור x ו-i (כלומר האם המעבר מ-f^{i-1} ל-f^i על הישר $(\cdot,x_i,\ldots,x_m)$ עובד).

כל בדיקה דורשת $d+2$ קריאות כלומר סה"כ $\approx dm$ קריאות. למבחן יש שלמות 1. בהנחה שמדובר בקופסאות פולי' אבל שלא בהכרח מקיימות את תכונת הסכום, ההסת' שיצלחו לעבוד עלינו במעבר בין f^{i-1} ל-f^i היא $\frac{d(m-(i-1))}{q}$ (מאותו נימוק שהצגנו במבחן בדיקת הסכום

הפולינומי). לכן הנאותות של המבחן היא $\frac{dm}{q}$ כי המקרה המאתגר ביותר הוא איתור שגיאה כשבדיוק מעבר אחד ב-m-יה שקרי, ובפרט בין f^0 ל-f^1.

שימוש ה-sum-check ב-PCP

נשתמש בבדיקת הסכום (ה-sum-check) שעתה הצגנו כדי לבדוק שמשוואה ב-n משתנים מדרגה טוטאלית ≥ 2, כלומר מהצורה $\sum_{i,j}^{n} a_i x_i x_j + \sum_{k}^{n} b_k x_k = c$, מתקיימת בלי לשערך את כל המשתנים שלה, אלא במספר קבוע או לפחות ב-$\log\log$ משתנים. נוכל לבחור $d = \log n$ ו-$m = \frac{\log n}{\log\log n}$ ולקבל $d^m = (\log n)^{\frac{\log n}{\log\log n}} = 2^{\log\log n \cdot \frac{\log n}{\log\log n}} = n$.

הגדרה יהי $n \in \mathbb{N}$ (מגולם בהגדרה). בעיית ההכרעה Quadratic Solvability בפרמטרים h, q, שנסמנה $QS_{h,q}$, מקבלת קלט של אוסף משוואות מדרגה טוטאלית 2 ב-n-משתנים מעל $\mathbb{F}_q$ ובכל משוואה $\geq h$ משתנים שונים, ומחלקת את אוסף מערכות המשוואות כנ"ל למערכות ניתנות לסיפוק ומערכות שלא ניתנות לסיפוק.

דוגמה עבור $q = 11$ מערכת המשוואות הבא היא קלט תקין לבעיה

$$\begin{cases} x_1x_2 + x_3^2 - 7 = 0 \\ x_7x_3 + x_2^2 - 1 = 0 \\ \vdots \end{cases}$$

עם בדיקת משוואות לוקאלית כנ"ל נוכל להוכיח רדוקציה מ-3SAT ל-$QS_{c,q}$ ומשם ל-$\text{gap}\left(1, \frac{1}{2}\right) - QS_{c,q}$ (עבור c, q קבועים) שעבורו נותר למצוא מוודא הסת' ולסיים את הוכחת ה-PCP בניסוח קשיות קירוב בעיות ב-NP. נעשה זאת ע"י החלפת כל משוואה ריבועית במשוואות ריבועיות קטנות יותר כך שהראשונה מתקיימת אם"ם כל האחרונות מתקיימות. כל אחת מהמשוואות החדשות תהיה שקולה (תתקיים אם"ם) לבדיקה אפשרית בתהליך הריקורסיבי הנ"ל שתיארנו. כלומר, לכל i ולכל $(x_i, \ldots, x_m)$ תהיה לנו משוואה שתבדוק האם תכונת הסכום מתקיימת עבור $(x_i, \ldots, x_m)$ במעבר בין f^{i-1} ל-f^i.

המוודא ל-gap-QS יבדוק רק משוואה קטנה אחת לכל i, עבור משוואה גדולה אחת (אקראית), כשבפועל זוהי הרצת למבחן בדיקת הסכום. אפע"פ הבדיקה היחסית לוקאלית של משוואות, הרדוקציה תחזיר לנו מספר משוואות קטנות לכל משוואה גדולה כמספר הבדיקות האפשריות (לכל הגרלה אפשרית של $(x_i, \ldots, x_m)$ לכל i). הגרלת x לכל שלב גוררת מספר בדיקות אפשריות מאוד גדול, $q^m \cdot q^{m-1} \cdot \ldots \cdot q^1 \approx q^{m^2}$, לכן נצטרך להקטין את ה-randomness, קרי מספר הביטים האקראיים שנדגום במהלך המבחן.

מבחן עם פחות בדיקות אפשריות יקבע $x \in_R \mathbb{F}_q^m$ בהתחלה ואז בכל שלב יבצע את הבדיקה על $(x_i, \ldots, x_m)$ (סה"כ q^m בדיקות שונות). למבחן זה יש שלמות 1, נאותות $\frac{dm}{q}$ ולוקאליות $m\,(d+2)$. זהו מבחן ה-sum-check.

משפט לכל ראשוני q, $QS_{4,q} \in \text{NPH}$.

הוכחה: נוכיח $\text{3SAT} \leq_p QS_{4,q}$. בהינתן הסגר $x_1 \vee x_2 \vee x_3$ נסתכל עליו כ-$x_1 + x_2 + x_3$. נרצה משוואה שתקבל 0 אם הסכום מקבל 0 ו-1 אם הוא מקבל $1, 2, 3$. מעקרון ההכלה וההדחה נקבל שהמשוואה היא

$$x_1 \vee x_2 \vee x_3 = x_1 + x_2 + x_3 - x_1x_2 - x_2x_3 - x_1x_3 + x_1x_2x_3 = 1$$

קל לקבל משוואה דומה להסגרים עם ליטרלים עם שלילה.

- כדי לאכוף ש-x_i מקבל 0 או 1, נוסיף משוואות $x_i^2 - x_i = 0$.
- כדי להוריד את הדרגה הטוטאלית של המשוואות המרכזיות ל-2, נגדיר לכל ij x_{ij} שיחליף מכפלה של המשתנים x_i ו-x_j, ונוסיף לכל ij את המשוואה $x_{ij} = x_i \cdot x_j$.

אכן יש לכל היותר 4 משתנים במשוואה כי יש רק מונום אחד עם דרגה 3 ואותו נוריד לדרגה 2 עם משתנה נוסף, כלומר 3 משתני הסגרים ומשתנה איחוי אחד. במשוואות האכיפה האחרות ברור שאנחנו מתחת ל-4.

נחזיר את מערכת המשוואות שכוללת את כל המשוואות משלושת הסוגים. ■

עתה נרצה להוכיח $QS_{n,q} - \text{gap}\left(1, \frac{1}{\sqrt{q}}\right) \leq_p QS_{4,q}$ כאשר $q = \log^2 n$. כלומר להעביר מערכת משוואות $\begin{pmatrix} p_1=0 \\ \vdots \\ p_k=0 \end{pmatrix}$ למערכת משוואות $\begin{pmatrix} r_1=0 \\ \vdots \\ r_{k^c}=0 \end{pmatrix}$ כך שאם אחת מהמשוואות p_i לא ספיקה, לפחות $\frac{1}{\sqrt{q}}$ מ-r_j לא יהיו ספיקות. נוכל להשיג זאת באמצעות הכפלה במטריצה יוצרת M של קוד וכך נקבל את התכונה הבאה: אם יש השמה מספקת למשוואות אז הכפלת M בשערוך תניב $M \cdot 0 = 0$. אם ההשמה לא מספקת, אז מילת הקוד (שערוך המשוואות תחת איזושהי השמה) אינה 0 ובגלל שזה קוד (אידאלית טוב), היא רחוקה מאוד ממילת הקוד 0 ולכן הרבה משוואות לא ישתערכו ל-0 כנדרש.

שבוע $\mathbb{VII}$ | בדיקת Low-Degree

נבחר $\mathbb{F} = \mathbb{F}_q$. בהינתן $f : \mathbb{F}^m \to \mathbb{F}$, נרצה לבדוק האם היא פולינום מדרגה נמוכה (LDE). נניח ש-f מיוצג לנו באמצעות טבלת ערכים B_0, וכן שיש לנו את B_1 ו-B_2 שהן טבלאות פולינומים (חד- ודו-משתניים בהתאמה) לכל ישר ומישור בהתאמה.

בדיקות דרגה-נמוכה

- Line Test: לבחור ישר מקרי ב-$\mathbb{F}^m$ (קוביה m-ממדית) ולבדוק שכל הישר מקבל את הערכים של פולינום האינטרפולציה שמשרות $d+1$ הנקודות הראשונות.
- Line v. Point Test: לבחור ישר מקרי ב-$\mathbb{F}^m$ ולבדוק ששערוך מתוך B_0 בנקודה מקרית על הישר מסכים עם הפולינום המתאים לישר ב-B_1.
- Plane v. Point Test: לבחור מישור מקרי ב-$\mathbb{F}^m$ ולבדוק ששערוך מתוך B_0 בנקודה מקרית במישור מסכימה עם הפולינום המתאים למישור ב-B_2.
- Plane v. Plane (Line) Test: לבחור שני מישורים מקריים ולבדוק האם הפולינומים המתאימים להם ב-B_2 מסכימים על הישר שהוא החיתוך שלהם.

הערה כל הטסטים האלה שקולים מבחינת החוזק שלהם, אבל את האחרון הכי קל להוכיח, ספציפית עבור $m = 3$ ומשם באינדוקציה.

משפט נבחר $m = 3$ ותהי $\delta > 0$. נניח שמתקיים

$$P_{p_1,p_2}\left(B_2\left[p_1\right]|_{p_1 \cap p_2} = B_2\left[p_2\right]|_{p_1 \cap p_2}\right) \geq \epsilon$$

כאשר p_1, p_2 מישורים (ולכן $p_1 \cap p_2$ ישר או $\varnothing$). אזי יש רשימה קצרה של פולינומים $f_1, \ldots, f_{\frac{1}{\delta}}$ (שתלויה לוגית רק בטבלאות) כך ש-$\deg f_i \leq d$ ו-

$$P\left(B_2\left[p_1\right]|_{p_1 \cap p_2} = B_2\left[p_2\right]|_{p_1 \cap p_2} \ \wedge \ \exists i : \left(B_2\left[p_1\right] = f_i|_{p_1} \wedge B_2\left[p_2\right] = f_i|_{p_2}\right)\right) \geq \epsilon - \delta - 2\sqrt{\frac{d+1}{q}}$$

הערה אין לנו בעיה ש-p_1, p_2 לא יסכימו, אבל נרצה שאם הם מסכימים אז זה יהיה בהכרח כי הם שווים לאחד מה-f_i-ים.

הערה במציאות נשתמש ב-$\delta = C \cdot \frac{d+1}{q}$, ב-$q$ גדול מחזקה קבועה של d ו-$m \approx \log n$ כך שסה"כ קיבלנו חסם פולילוגריתמי ב-n.

גרפים טרנזיטיביים

הגדרה יהי $G = \langle V, E \rangle$ גרף לא מכוון. נאמר כי G טרנזיטיבי אם לכל $(v,u), (u,w) \in E$ מתקיים $(v,w) \in E$. בנוסף נגדיר לכל $(v,w) \notin E$

$$\beta\left(v,w\right) = P_{u \in V}\left(\left(v,u\right) \in E \wedge \left(u,w\right) \in E\right)$$

ולגרף כולו נגדיר $\beta\left(G\right) = \max\limits_{(v,w) \notin E} \beta\left(v,w\right)$ (האי-צלע שבגללה כמה שיותר קודקודים לא מקיימים טרנזטיביות על שלושת הקודקודים).

טענה גרף טרנזטיבי הוא איחוד זר של קליקות (רכיבי הקישרות).

טענה יהי G גרף לא מכוון. אזי מספיק למחוק לכל היותר $2\sqrt{\beta\left(G\right)}\left|V\right|^2$ קשתות כדי להפכו לטרנזיטיבי.

הוכחה: נציג אלג' להפיכת G לגרף טרנזיטיבי ונוכיח שהורדנו את כמות הקשתות המותרת.

1. לכל $v \in V$ עם $d\left(v\right) \leq \sqrt{\beta}\left|V\right|$ (מספר השכנים שלו), נוריד את כל הקשתות שיוצאות ממנו.
2. לכל $v \in V$ שנשארו (עם שכנים), נמחק קשתות בין שכנים של v לאי-שכנים של v (אם $(v,u) \in E$ ו-$(v,w) \notin E$, נוריד את (u,w) אם היא ב-E).

נובע ישירות משלב 2 ש-G לאחר מחיקת הקשתות הוא טרנזטיבי.

נשים לב כי לכל v שעבורו נמחק צלעות בשלב השני, אוסף הצלעות שנמחקות (בריצת האלג', כלומר זה לא סטטי אלא תלוי בסדר הריצה על הקודקודים) הוא

$$E^v_{removed} = \left\{\left(u,w\right) \in E : w \in C\left(v\right) \setminus \left(N\left(v\right) \cup v\right) \wedge u \in N\left(v\right)\right\}$$

כלומר כל הצלעות (u,w) עבורן u שכן של v ו-w אי-שכן באותו רכיב קישרות.

בדומה נסמן את אוסף זוגות הקודקודים שאילו היו צלעות היו נמחקות בשלב 2 על v, כלומר שאנחנו "מסתכלים" עליהם לצורך מחיקה בשלב השני

$$E_{non}^{v}=\{(u,w):w\in C(v)\setminus(N(v)\cup v)\wedge u\in N(v)\}=(C(v)\setminus(N(v)\cup v))\times N(v)$$

מתקיים

$$|E_{removed}^{v}|\leq|C(v)\setminus(N(v)\cup v)|\cdot\beta\cdot|V|$$

כי ל-w יש $|C(v)\setminus(N(v)\cup v)|$ אפשרויות ולכל w יש לכל היותר $\beta|V|$ u-ים כך ש-$(v,u)\in E$ ו-$(u,w)\in E$ אבל כאמור $(v,w)\notin E$.

בנוסף מתקיים

$$|C(v)\setminus(N(v)\cup v)|\cdot\sqrt{\beta}\cdot|V|\leq|E_{non}^{v}|$$

כי לקודקודים שנותרו עם שכנים לאחר שלב הראשון יש לפחות $\sqrt{\beta}|V|$ שכנים (החישוב על בסיס עוצמה של מכפלה קרטזית).

לסיום

$$\sum_{v\in V}|E_{remove}^{v}|\leq\sum_{v\in V}\sqrt{\beta}|E_{non}^{v}|=\sqrt{\beta}\sum_{v\in V}|E_{non}^{v}|\overset{(*)}{\leq}\sqrt{\beta}|V|^{2}$$

$(*)$ נטען כי לכל $(u,w)\in E$ קיים לכל היותר v יחיד עבורו $(u,w)\in E_{non}^{v}$, כי אם $(u,w)\in E_{non}^{v_1}$ אז u שכן של v_1 ו-w לא (אבל כן באותו רכיב הקשירות), ולכן כל v_2 אחר ש-u שכן שלו, הוא ברכיב הקשירות של v_1 ולכן לא באותו רכיב קשירות כמו w כי הוצאנו את מרכיב הקישרות שלהם בהורדה כשראינו את v_1 לפני v_2. ■

גרף המישורים

הגדרה יהיו $m,q\in\mathbb{N}$ והטבלה B_2 ממבחן המישור-מול-מישור. <u>גרף המישורים</u> הוא $G_p=\langle V_p,E_p\rangle$ כאשר $V_p=\{\mathbb{F}^m$ מישורים ב- $\}$ ו-$(p_1,p_2)\in E_p$ אם"ם מתקיים $B_2[p_1]|_{p_1\cap p_2}=B_2[p_2]|_{p_1\cap p_2}$ (המאורע $\mathcal{S}$).

טענה $\beta(G_p)\leq\frac{d+1}{q}$.

הוכחה: תהי $(p_1,p_2)\notin E_p$. יהי p_3 מישור נוסף. בסיכוי נמוך מאוד, p_3 מקביל ל-$p_1\cap p_2$ (כלומר לאחד מ-p_1,p_2). הסיכוי הזה הוא $\frac{1}{q}$ כי אם המישור מוגדר ע"י $\{v:wv^T=a\}$ אז ישר u מקביל למישור אם $wu^T=0$ ובגלל שהכל מתפלג אחיד זה $\frac{1}{q}$. אחרת, $p_1\cap p_2$ נחתך עם p_3, הלא זו נקודת חיתוך של שלושת המישורים. הנקודה הזו מתפלגת אחיד על $p_1\cap p_2$.

אם f_1,f_2, הפולינומים המתאימים (מ-B_2) ל-p_1,p_2 לא מסכימים על הערכים המתקבלים בישר המשותף להם, אז הם מסכימים על לכל היותר $\frac{d+1}{q}$ נקודות (קונטרה-פוזיטיב לשוורץ-זיפל עבור $f_1-f_2\neq 0$). לכן, הסיכוי ש-p_3 כן מסכים עם p_1,p_2 בנקודת המפגש של השלושה

(שמתפלגת אחיד כאמור), היא לכל היותר $\frac{d+1}{q}$, כלומר $\beta\left(p_1,p_2\right)\leq\frac{d+1}{q}$. במונחי הגדרת הטרנזיטיביות מתקיים $\left(p_1,p_3\right),\left(p_3,p_2\right)\in E$ אבל $\left(p_1,p_2\right)\notin E$. ■

שבוע $\mathbb{VIII}$ | המשך בדיקת Low-Degree

משפט (המשפט המרכזי להרצאה זו) תהי $\delta>0$. אזי יש רשימה קצרה של פולינומים $f_1,\ldots,f_{\frac{1}{\delta}}$ (שתלויה לוגית רק בטבלאות) כך ש-$\deg f_i\leq d$ ו-

$$P_{p_1,p_2}\left(\underbrace{B_2\left[p_1\right]|_{p_1\cap p_2}=B_2\left[p_2\right]|_{p_1\cap p_2}}_{A}\ \wedge\ \underbrace{\nexists i:\left(B_2\left[p_1\right]=f_i|_{p_1}\wedge B_2\left[p_2\right]=f_i|_{p_2}\right)}_{\overline{B}}\right)\leq\delta+2\sqrt{\frac{d+1}{q}}$$

הערה זו גרסה חזקה יותר של המשפט שראינו בתחילת ההרצאה הקודמת (כך שמספיקה הוכחתו להסקת המשפט המקורי).

טענה תהי $\delta>0$. אזי יש רשימה קצרה של קליקות $K_1,\ldots,K_{\frac{1}{\delta}}$ ב-G_p כך ש-$\left|K_i\right|\leq\delta\left|V_p\right|$ ו-

$$P_{p_1,p_2}\left(\underbrace{B_2\left[p_1\right]|_{p_1\cap p_2}=B_2\left[p_2\right]|_{p_1\cap p_2}}_{A}\ \wedge\ \underbrace{\nexists i:\left(B_2\left[p_1\right]\in K_i\wedge B_2\left[p_2\right]\in K\right)}_{\overline{B}}\right)\leq\delta+2\sqrt{\frac{d+1}{q}}$$

הוכחה: יהיו p_1,p_2 מישורים ב-$\mathbb{F}_q^m$. נחלק את מרחב ההסת' לארבעה מאורעות זרים:

1. הם לא מסכימים ($\overline{A}$).
2. הם מסכימים אבל לא באותה קליקה ב-G_p - זה קורה בהסת' $\leq 2\sqrt{\frac{d+1}{q}}$ (נובע ממספר הצלעות שהאלג' שהופכך לגרפים לטרנזיטיביים מסיר).
3. הם מסכימים ובאותה קליקה ב-G_p בגודל $\leq\delta$ - נשים לב להבחנות הבאות:
   - יש לכל היותר $\frac{1}{\delta}$ קליקות בגודל $\leq\delta$ (מהקודקודים), כי אנחנו בגרף איחוד זר של קליקות.
   - הסיכוי ששני צמתים מקריים ב-G_p יהיו שייכים לאותה קליקה בגודל $\leq\delta$ הוא $\leq\delta$. **הוכחה:** נגריל את הצומת הראשון, הוא נמצא בקליקה כלשהי. עתה נגריל את הצומת השני, ובגלל שבקליקה המקורית יש δ מהקודקודים בגרף, בסיכוי $\leq\delta$ גם הצומת השני יהיה שם. ■
4. הם מסכימים ובאותה קליקה ב-G_p בגודל $\leq\delta$ ($A\wedge B$) - זה המקרה שבו נרצה שהפולינומים שלהם שמסכימים על החיתוך יהיו שווים לפולינום גלובלי מהרשימה הקצרה.

המאורע שבמשפט, $A\wedge\overline{B}$, שווה בדיוק לאיחוד הזר של המאורע השני והמאורע השלישי, הן מנימוק מהשלמה למרחב כולו יחד עם המאורע הראשון והרביעי והן מנימוק מהותי באשר לשוויון ההגדרות. לכן ההסת' שהוא יקרה חסומה מלמעלה ע"י סכום ההסת' של שני המאורעות, שהיא $\delta+2\sqrt{\frac{d+1}{q}}$. ■

טענה נבחר $\delta\geq\frac{d+1}{q}$. תהי K קליקה ב-G_p של לפחות δ מישורים מדרגה $\geq d$. אזי קיים $f:\mathbb{F}_q^3\to\mathbb{F}$ מדרגה $\geq d$ כך ש-$B_2\left[p\right]=f|_p$ לכל $p\in K$.

הוכחה: עבור ישר מקרי יש בתוחלת δ מישורים מאונכים לכיוון הזה כי

$$\delta\overset{(*)}{\leq}P_{\text{מישור } a\text{, כיוון } T}\left(P+D\in K\right)=E_{\text{כיוון } a}P_{\text{מישור } T}\left(\left\{\lambda\in\mathbb{F}_q:\lambda a+T\in K\right\}\right)$$

$(*)$ כיוון (הזזה אפינית) עם מישור (אפיני) נותנים מישור מקרי מתפלג אחיד. ההסת' שמישור מקרי יהיה בקליקה היא בדיוק הגודל היחסי של K מתוך V_p.

לכן מהמונוטוניות ההפוכה של התוחלת, קיים כיוון a ומישור T עבורם $\left|\underbrace{\left\{\lambda\in\mathbb{F}_q:\lambda a+T\in K\right\}}_{\Lambda}\right|\geq\delta\cdot q$. ולכן $\delta\cdot q\geq\frac{d+1}{q}q=d+1$. $|\Lambda|\geq d+1$. נבחר איזושהי תת קבוצה $\Lambda\supseteq\left\{\xi_1,\ldots,\xi_{d+1}\right\}$.

לכל $i\in\left[d+1\right]$, נסמן $f_i=B_2\left[P+\xi_iD\right]$. נגדיר $f\left(x,y,z\right)=\sum_{i=0}^{d}\varphi_i\left(x\right)f_i\left(y,z\right)$ כאשר φ_i פולינום אינטרפולציה מדרגה d שמקיים $\varphi_i\left(\xi_j\right)=\delta_{ij}$, לכל $j\in\left[d+1\right]$. בגלל ש-φ_i ו-f_i הם מדרגה לכל היותר d כל אחד, f מדרגה לכל היותר $2d$.

קיים כיוון a' (לא נוכיח למה) שאינו a ומישור T' שחותך את T בישר עבורם $\left|\underbrace{\left\{\lambda\in\mathbb{F}_q:\lambda a'+T'\in K\right\}}_{\Lambda'}\right|\geq2\left(d+1\right)$. כל מישור מ-$\Lambda'$ חותך כל מישור מ-Λ ב-$d+1$ נקודות במצטבר ולכן לכל מישור p המושרה מ-$\Lambda\cup\Lambda'$, $B_2\left[p\right]=f|_p$. נשים לב שהטיעון הנ"ל לא מחזיק מים אם מפעילים אותו על f כפולינום הגלובלי בכל משתניו, כי הוא מדרגה $2d$ ויש לנו הסכמה רק ב-$d+1$ חיתוכים. עם זאת, בכיוון a, הפולינום הגלובלי הוא רק מדרגה d (כשמסתכלים עליו כפולינום במשתנה אחד, λ). לכן נוכל להעביר ישר מכל נקודה p במישור מ-Λ' בכיוון a שיחתוך את $d+1$ המישורים מ-Λ. עתה, מאינטרפולציה על $d+1$ נקודות החיתוך נסיק ש-p חייבת לקבל את הערך של הפולינום הגלובלי כי דרגת הפולינום הגלובלי המצומצם לכיוון a ופולינום האינטרפולציה היא d ויש לנו $d+1$ הסכמות ביניהם.

בנוסף, מטיעון גאומטרי שלא נוכיח, כל מישור ב-$\mathbb{F}_q^3$ חותך את $3\left(d+1\right)$ המישורים בבדיוק $d+1$ נקודות ולכן כל ה-$3d+3$ מסכימים על הישרים שבחיתוכים שלהם. לכן כל המרחב מסכים על f.

נציג מבט על להוכחה ש-$\deg f\leq d$ (התכונה הזו נחוצה כדי שבאינדוקציה על m הדרגה לא תעלה אקספ'). נניח בשלילה כי $\deg f>d$. הפולינום הגלובלי שווה לפולינום מ-B_2 בכל מישור בנפרד, ולכן בהכרח התכונה הגלובלית של דרגה $>d$ מתקיימת עבור מישור כלשהו (זה גרעין ההוכחה, שלא נוכיח), ולכן אחת ההשמות מ-B_2 היא מדרגה $>d$ בסתירה לכך שכולן מדרגה $\geq d$ (מובטח לנו ש-B_2 מכילה רק פולינומים מדרגה $\geq d$). ■

מסקנה המשפט מתחילת ההרצאה מתקיים.

הוכחה: הראנו בטענה השנייה שכל קליקה גדולה מספיק ב-G_p מסכימה על פולינום גלובלי כלשהו, ולכן בהצבת ביטויי שוויון לפולינום הגלובלי במקום שייכות לקליקה, נקבל בדיוק את המשפט המרכזי. ■

שבוע $\mathbb{VIII}$ | כפליות ו-Long Code

בהאדמארד ראינו מבחן פשוט שמקבל פ' $f:\{0,1\}^n\to\{0,1\}$ ובודק האם מתקיים $f(x)+f(y)=f(x+y)$ עבור $x,y\in_R\{0,1\}^n$.

הערה נעבור מחיבור לכפל; נמפה $0\mapsto 1$, $1\mapsto -1$, ונקבל בדיוק את אותו המבחן עם שינוי שמות ("0" שהוא עכשיו "1" עדיין לא משפיע על החישוב, כ-0 בחיבור וכ-1 בכפל).

הגדרה נאמר כי $\chi:\{-1,1\}^n\to\{-1,1\}$ היא כפלית (multiplicative character) אם $\chi(x)\chi(y)=\chi(x\cdot y)$ לכל $x,y\in\{-1,1\}^n$ כאשר כפל הוא pair-wise.

הערה χ היא הומומורפיזם מ-$\{-1,1\}^n$ לחבורה הכפלית $\{-1,1\}$.

הגדרה נסמן $L_2\left(\{-1,1\}^n\right)=\mathbb{R}^{\{-1,1\}^n}$. לכל $f\in L_2\left(\{-1,1\}^n\right)$ נגדיר

$$\|f\|_2=\sqrt{\frac{1}{2^n}\sum_{x\in\{-1,1\}^n}f^2(x)}=\sqrt{E_{x\in_R\{-1,1\}^n}\left[f^2(x)\right]}$$

ו-$\langle f\mid g\rangle=E_x\left[f(x)\,g(x)\right]$.

הערה היתרון בשינוי השקוף בשמות הוא שההרחבה ל-$\mathbb{R}$ הוא הרבה יותר נוח (אחרת $1+1=2$ ב-$\mathbb{R}$ וכך איבדנו תכונות רצויות).

דוגמה עבור χ כפלית נקבל ש-$\|\chi\|_2=1$ כי זהו ממוצע הערכים של χ (בערך מוחלט), שהם הרי כולם 1.

$f\in\{0,1\}^n\to\{0,1\}$ היא פ' לינארית אם"ם $f(x)=\sum_{i=1}^n a_ix_i=\sum_{i\in S\subseteq[n]}x_i:=f_S(x)$ כאשר $S=\{i:a_i=1\}$. לכן אוסף הפ' הלינאריות $\{0,1\}^n\mapsto\{0,1\}$ הוא $\{f_S:S\subseteq[n]\}$. בדומה, אוסף כל הפ' הכפליות $\{\pm1\}^n\to\{\pm\}$ הוא $\{\chi_S\}_{S\subseteq[n]}$ $S\subseteq[n]$ כאשר $\chi_S(x)=\prod_{i\in S}x_i$.

טענה $\chi_S\cdot\chi_T=\chi_{S\triangle T}$. נשתמש בזה כדי להוכיח ש-3Lin2 הוא קשה ב-NP.

הוכחה:

$$\chi_S(x)\,\chi_T(x)=\prod_{i\in S}x_i\prod_{j\in T}x_j=\prod_{i\in S\triangle T}x_i\prod_{j\in S\cap T}x_j^2=\prod_{i\in S\triangle T}x_i=\chi_{S\triangle T}$$

■

מסקנה

$$\langle\chi_S\mid\chi_T\rangle=E_x\left[\chi_S(x)\,\chi_T(x)\right]=E_x\left[\chi_{S\triangle T}(x)\right]=\begin{cases}1 & S=T\\ 0 & S\neq T\end{cases}$$

הוכחה: אם $S=T$ אז $S\triangle T=\varnothing$ ואז כל המכפלות הן 1 ואחרת יש מספר שווה של n-יות שנותנות -1 ו-1 ולכן זה מצטמצם (לכל $n-1$-יה x', $\{\chi((x',-1)),\chi((x',1))\}=\{\pm1\}$ לכל χ כפלית). ■

מסקנה אוסף הפ' הכפליות הוא קבוצה אורתונ', ובפרט הוא בסיס אורתונ' של $\{f:\{\pm1\}^n\to\{\pm1\}\}$

הוכחה: לכל f, $f=\sum\limits_{f(y)=-1}\chi_{S_y}$ כאשר $S_y=\{i:y_i=-1\}$. ■

מסקנה לכל f מתקיים $f=\sum\limits_{S\subseteq[n]}\hat{f}(S)\chi_S$ כאשר $\hat{f}(S)=\langle f\mid\chi_S\rangle\in[-1,1]$ (תכונה של בסיסים אורתונ').

טענה ככל ש-f,g יותר קרובות, כך המכ"פ שלהן יותר קרוב ל-0.

הוכחה: מרחק מוגדר ע"י $\text{dist}(f,g)=P_x(f(x)\neq g(x))$. עבור $f,g:\{\pm1\}^n\to\{\pm1\}$ מתקיים

$$\begin{aligned}\langle f\mid g\rangle&=E[f(x)g(x)]=1\cdot P_x(f(x)=g(x))+(-1)P_x(f(x)\neq g(x))\\&=1-2\text{dist}(f,g)\end{aligned}$$

■

מסקנה אם $\langle f\mid\chi_S\rangle=\hat{f}(S)>1-\epsilon$ אז $\text{dist}(f,\chi_S)\leq\frac{1}{2}\epsilon$.

מסקנה לכל $f:\{\pm1\}^n\to\{\pm1\}$ ו-$S\subseteq[n]$, $f=\chi_S$ אמ"ם $\hat{f}(S)=1$.

הוכחה: $1=\|f\|_2^2=\sum\limits_{S'}\hat{f}^2(S')=\hat{f}^2(S)+\sum\limits_{S'\neq S}\hat{f}^2(S')$ ולכן $\hat{f}(S')=0$ לכל $S'\neq S$ אמ"ם $\hat{f}(S)=1$. ■

מבחן הכפליות

טענה אם $P_{x,y}(f(x)f(y)=f(x\cdot y))>1-\epsilon$ אז קיים S כך ש-$\hat{f}(S)>1-c\cdot\epsilon$ (ו-$\text{dist}(f,\chi_S)\leq\frac{c}{2}\cdot\epsilon$).

הערה הוכחנו את הטענה הזו במקרה של מבחן הלינאריות, עתה נוכיח אותה שוב עם כלים אחרים.

הוכחה: מההנחה, $f\left(x\right)\cdot f\left(y\right)\cdot f\left(x\cdot y\right)$ היא 1 בהסת' לפחות $1-\epsilon$ ו--1 בהסת' לכל היותר ϵ, לכן מתקיים

$$\begin{aligned}1-2\epsilon &< E_{x,y}\left[f\left(x\right)f\left(y\right)f\left(x\cdot y\right)\right]\\ &=E_{x,y}\left[\left(\sum_{S}\hat{f}\left(S\right)\chi_{S}\left(x\right)\right)\left(\sum_{T}\hat{f}\left(T\right)\chi_{T}\left(y\right)\right)\left(\sum_{R}\hat{f}\left(R\right)\chi_{R}\left(x\cdot y\right)\right)\right]\\ &=\sum_{S,R,T}\hat{f}\left(S\right)\hat{f}\left(R\right)\hat{f}\left(T\right)E_{x,y}\left[\chi_{S}\left(x\right)\chi_{T}\left(y\right)\chi_{R}\left(x\cdot y\right)\right]\\ &=\sum_{S,R,T}\hat{f}\left(S\right)\hat{f}\left(R\right)\hat{f}\left(T\right)E_{x,y}\left[\chi_{S}\left(x\right)\chi_{T}\left(y\right)\chi_{R}\left(x\right)\chi_{R}\left(y\right)\right]\\ &=\sum_{S,R,T}\hat{f}\left(S\right)\hat{f}\left(R\right)\hat{f}\left(T\right)E_{x}\left[\chi_{S}\left(x\right)\chi_{R}\left(x\right)\right]E_{y}\left[\chi_{T}\left(y\right)\chi_{R}\left(y\right)\right]\\ &=\sum_{S,R,T}\hat{f}\left(S\right)\hat{f}\left(R\right)\hat{f}\left(T\right)\delta_{S,R}\delta_{T,R}\\ &=\sum_{S}\hat{f}^{3}\left(S\right)\end{aligned}$$

כלומר

$$1-2\epsilon\leq\sum_{S}\hat{f}^{3}\left(S\right)\leq\max_{S}\left\{\hat{f}\left(S\right)\right\}\cdot\sum_{S}\hat{f}^{2}\left(S\right)\leq\max_{S}\left\{\hat{f}\left(S\right)\right\}$$

ולכן קיים S עבורו $1-2\epsilon\leq\hat{f}\left(S\right)$, ומכאן גם ש-$\mathrm{dist}\left(f,\chi_{S}\right)\leq\epsilon$. ■

מסקנה אם $P_{x,y}\left(f\left(x\right)\cdot f\left(y\right)=f\left(x\cdot y\right)\right)=\frac{1}{2}+\epsilon$ אז קיים S כך ש-$\mathrm{dist}\left(f,\chi_{S}\right)\leq\frac{1}{2}-\epsilon$. כלומר, גם אם הסיכוי לשוויון הוא ממש קצת מעל זה של פ' מקרית, f כבר הרבה יותר קרובה לפ' כפלית (ב"קוד") מאשר פ' מקרית.

הערה מספר ה-S-ים עבורם $\hat{f}\left(S\right)=\left\langle f\mid\chi_{S}\right\rangle\geq2\epsilon$ הוא לכל היותר $\frac{1}{4\epsilon^{2}}$ כי $\sum\hat{f}^{2}\left(S\right)=1$.

מבחן ה-Long Code

הגדרה יהיו $f,g:\left\{\pm1\right\}^{n}\rightarrow\left\{\pm1\right\}$. מבחן Long Code הוא מבחן שאם עוברים אותו בהסת' $>\frac{1}{2}+\delta$ אז בהכרח קיימת S עבורה

$$\hat{g}\left(S\right)>\varphi_{1}\left(\delta\right)\ \wedge\ \left|\hat{f}\left(S\right)\right|>\varphi_{2}\left(\delta\right)\ \wedge\ 0<\left|S\right|\leq\varphi_{3}\left(\delta\right)$$

כלומר ש-g תהיה קרובה לפ' הכפלית χ_{S}, f תהיה קרובה ל- χ_{S} או ל-$-\chi_{S}$, ו-S תהיה לא גדולה מדי.

הערה נשים לב כי $\chi_{\{i\}}\left(x\right)=x_{i}$, ולכן נוכל להשתמש ב-$\chi_{\{i\}}=\left(1,\ldots,1,-1,1,\ldots,1\right)$ כקידוד ל-i.

הגדרה הקוד $\left\{\chi_{\{i\}}\right\}_{i\in[n]}$ נקרא Long Code.

הערה הקצב של ה-Long Code הוא $\frac{1}{2^{n}}$.

נציע שני מבחנים שינסו לענות על הדרישות שהצבנו לעיל, כל אחד יקיים תכונה שהקודם לא מקיים, ומבחן שלישי שיקיים את כל הדרישות.

1. נבחר $x, y \in_R \{\pm 1\}^n$ ונבדוק $f(x) g(y) = f(x \cdot y)$.

   עבור f, g המתאימים ל-$\chi_{\varnothing}$, נקבל $1 \cdot 1 = 1$ כך שנעבור את המבחן בהסת' 1 בניגוד לכך שלא קיימת S שמקיימת את התנאים שנרצה שיתקיימו (בפרט עם $|S| > 0$).

2. נבחר $x, y \in_R \{\pm 1\}^n$ ו-$\mu \in_R \{\pm 1\}$ ונבדוק $\mu \cdot f(\mu \cdot x) g(y) = f(x \cdot y)$.

   עתה $\chi_{\varnothing}$ לא עובר את המבחן בהסת' 1 אלא בהסת' $\frac{1}{2}$, (רק עבור $\mu = 1$, כי עבור $\mu = -1$ נקבל $1 \neq -1 \cdot 1 \cdot 1$ לכל x, y). הבעיה היא f, g שמקיימות את שתי התכונה הראשונות אבל עם S גדולה יעברו את המבחן בהסת' גבוהה, לכן נוסיף רעש שיוריד את ההסת' הזו.

המבחן הסופי יבחר $x, y \in_R \{\pm 1\}^n$, $\mu \in_R \{\pm 1\}$ ו-$z \in \{\pm 1\}^n$ מתוך ההתפלגות

$$P(z_i = 1) = 1 - \epsilon,\ P(z_i = -1) = \epsilon$$

ואז יבדוק $\mu \cdot f(\mu \cdot x) g(y) = f(z \cdot x \cdot y)$.

הערה למבחן יש שלמות $1 - \epsilon$, כי מילת Long Code חוקית עוברת בהסת' $1 - \epsilon$ (ההסת' ש-z_i עבור i הקוורדינטה המקודדת היא 1, כי ב--1 המבחן נכשל).

טענה המבחן שהצגנו מקיים את תנאי מבחן ה-Long Code.

הוכחה: נניח כי

$$P(\mu \cdot f(\mu \cdot x) g(y) = f(z \cdot x \cdot y)) \geq \frac{1}{2} + \delta$$

לכן מכפלת האגפים תהיה 1 בהסת' לפחות $\frac{1}{2}+\delta$ ו--1 בהסת' לכל היותר $\frac{1}{2}-\delta$ ובמעבר לתוחלת נקבל

$$\begin{aligned}
2\delta &\le E\left[\mu\cdot f\left(\mu\cdot x\right)g\left(y\right)f\left(z\cdot x\cdot y\right)\right]\\
&= E\left[\mu\left(\sum_{S}\hat{f}\left(S\right)\chi_S\left(\mu\cdot x\right)\right)\left(\sum_{T}\hat{g}\left(T\right)\chi_T\left(y\right)\right)\left(\sum_{R}\hat{f}\left(R\right)\chi_R\left(z\cdot x\cdot y\right)\right)\right]\\
&= \sum_{S,T,R}\hat{f}\left(S\right)\hat{g}\left(T\right)\hat{f}\left(R\right)\cdot E\left[\mu\cdot\chi_S\left(\mu\cdot 1^n\right)\chi_S\left(x\right)\chi_T\left(y\right)\chi_R\left(z\right)\chi_R\left(x\right)\chi_R\left(y\right)\right]\\
&= \sum_{S,T,R}\hat{f}\left(S\right)\hat{g}\left(T\right)\hat{f}\left(R\right)\cdot E_\mu\left[\mu\cdot\chi_S\left(\mu\cdot 1^n\right)\right]\cdot E\left[\chi_S\left(x\right)\chi_R\left(x\right)\right]\cdot E_y\left[\chi_T\left(y\right)\chi_R\left(y\right)\right]E_z\left[\chi_R\left(z\right)\right]\\
&= \sum_{S,T,R}\hat{f}\left(S\right)\hat{g}\left(T\right)\hat{f}\left(R\right)\cdot E_\mu\left[\mu\cdot\chi_S\left(\mu\cdot 1^n\right)\right]\cdot\delta_{S,R}\cdot\delta_{T,R}\cdot E_z\left[\chi_R\left(z\right)\right]\\
&= \sum_{S}\hat{f}\left(S\right)^2\hat{g}\left(S\right)\cdot E_\mu\left[\mu\cdot\chi_S\left(\mu\cdot 1^n\right)\right]E\left[\chi_S\left(z\right)\right]\\
(*) &= \sum_{S:2\nmid|S|}\hat{f}\left(S\right)^2\hat{g}\left(S\right)\cdot E\left[\chi_S\left(z\right)\right]\\
(**) &= \sum_{S:2\nmid|S|}\hat{f}\left(S\right)^2\hat{g}\left(S\right)\cdot\prod_{i\in S}E\left[z_i\right]\\
&= \sum_{S:2\nmid|S|}\hat{f}\left(S\right)^2\hat{g}\left(S\right)\cdot\left(1-2\epsilon\right)^{|S|}
\end{aligned}$$

$(*)$ עבור $|S|$ זוגי מתקיים $E_\mu\left[\mu\cdot\chi_S\left(\mu\cdot 1^n\right)\right]=E_{\mu_R\in\{\pm1\}^n}\left[\mu^{|S|+1}\right]=0$.

$(**)$ z_i מוגרלים ב"ת ולכן כפליות התוחלת מתקיימת ובנוסף $\chi_S\left(z\right)=\prod_{i\in S}z_i$.

נגדיר $\varphi_3\left(\delta\right)=\log_{1-2\epsilon}\delta$ ולכן

$$\begin{aligned}
\sum_{S:2\nmid|S|}\hat{f}\left(S\right)^2\hat{g}\left(S\right)\cdot\left(1-2\epsilon\right)^{|S|} &= \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3}}\hat{f}\left(S\right)^2\cdot\hat{g}\left(S\right)\cdot\left(1-2\epsilon\right)^{|S|}+\sum_{\substack{S:2\nmid|S|\\|S|>\varphi_3}}\hat{f}\left(S\right)^2\cdot\underbrace{\hat{g}\left(S\right)}_{\le1}\cdot\underbrace{\left(1-2\epsilon\right)^{|S|}}_{<\delta\ (*)}\\
&\le \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3}}\hat{f}\left(S\right)^2\cdot\hat{g}\left(S\right)\cdot\left(1-2\epsilon\right)^{|S|}+\delta\underbrace{\sum_{S:2\nmid|S|}\hat{f}\left(S\right)^2}_{\le1}\\
&\le \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3}}\hat{f}\left(S\right)^2\cdot\underbrace{\hat{g}\left(S\right)}_{\in[-1,1]}\cdot\underbrace{\left(1-2\epsilon\right)^{|S|}}_{\le1}+\delta\\
&\le \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0}}\hat{f}\left(S\right)^2\cdot\underbrace{\hat{g}\left(S\right)}_{\ge0}\cdot\underbrace{\left(1-2\epsilon\right)^{|S|}}_{\le1}+\delta\\
&\le \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0}}\hat{f}\left(S\right)^2\cdot\hat{g}\left(S\right)+\delta
\end{aligned}$$

$(*)$ $(1-2\epsilon)^x$ היא פ' יורדת ב-x.

נגדיר $\varphi_1(\delta)=\frac{\delta}{2}$ ולכן

$$\begin{aligned}\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0}}\hat{f}(S)^2\cdot\hat{g}(S)+\delta &\le \sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)}}\hat{f}(S)^2\cdot\hat{g}(S)+\overbrace{\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1>\hat{g}(S)}}\hat{f}(S)^2}^{\le1}\cdot\underbrace{\hat{g}(S)}_{<\frac{\delta}{2}}+\delta\\&\le\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)}}\hat{f}(S)^2\cdot\hat{g}(S)+\delta+\frac{\delta}{2}\end{aligned}$$

מתקיים $\sum_{\hat{g}(S)>\varphi_1}\hat{g}(S)\le\varphi_1\sum_{\hat{g}(S)>\varphi_1}\hat{g}(S)^2\le1$. נגדיר $\varphi_2(\delta)=\sqrt{\varphi_1\cdot\frac{\delta}{4}}$ ולכן

$$\begin{aligned}\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)}}\hat{f}(S)^2\cdot\hat{g}(S)+\delta+\frac{\delta}{2}&\le\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|\ge\varphi_2}}\hat{f}(S)^2\cdot\hat{g}(S)+\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|<\varphi_2}}\hat{f}(S)^2\cdot\hat{g}(S)+\delta+\frac{\delta}{2}\\&\le\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|\ge\varphi_2}}\hat{f}(S)^2\cdot\hat{g}(S)+\frac{1}{\varphi_1}\overbrace{\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|<\varphi_2}}\hat{g}(S)\varphi_1}^{\le1}\cdot\underbrace{\hat{f}(S)^2}_{\le\varphi_1\cdot\frac{\delta}{4}}+\delta+\frac{\delta}{2}\\&\le\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|\ge\varphi_2}}\hat{f}(S)^2\cdot\hat{g}(S)+\delta+\frac{\delta}{2}+\frac{\delta}{4}\end{aligned}$$

ולכן $\sum_{\substack{S:2\nmid|S|\\|S|\le\varphi_3\wedge\hat{g}(S)\ge0\\\varphi_1\le\hat{g}(S)\wedge\left|\hat{f}(S)\right|\ge\varphi_2}}\hat{f}(S)^2\cdot\hat{g}(S)\ge\frac{\delta}{4}>0$ ובגלל שכל הנסכמים הם חיוביים, בהכרח שקיים S שמקיים את תנאי הסכום, כלומר $|S|\le\varphi_3,\ \varphi_2\le\left|\hat{f}(S)\right|,\ \varphi_1\le\hat{g}(S)$. ■

הערה אם למבחן הייתה שלמות של 1 היינו מקבלים שלפתור מערכת משוואות לינאריות זה קשה ב-NP שזה לא פשוט לא נכון (תהליך גאוס-ז'ורדן).

שבוע $\mathbb{IX}$ | UGC וקשיות 3Lin2

הגדרה תהי $h:\{\pm1\}^n\to\{\pm1\}$. נגדיר $L_{\eta,k}=\bigcup_{\substack{|S|\le k\\\left|\hat{h}(S)\right|\ge\eta}}S$, כלומר איחוד הקבוצות שאינן גדולות מדי (לא יותר מ-k) ומקדם הפורייה שלהן ביחס ל-h הוא לא קטן מדי (לא פחות מ-η).

הערה $|L_{\eta,k}(h)| \le \frac{k}{\eta^2}$ כי כל קבוצה היא בגודל לכל היותר k, ו-$1 \ge \sum_{|\hat{h}(S)|\ge\eta} \hat{h}(S)^2 \ge \left|\left\{S : \hat{h}(S) \ge \eta\right\}\right| \eta^2$.

טענה יהיו f, g פ' שעוברות את המבחן בהסת' $\frac{1}{2}+\delta \le$. נסמן $L(g) = L_{\frac{\delta}{4},\varphi_3}(g)$, $L(f) = L_{\frac{\delta}{4},\varphi_3}(f)$ ונבחר $j \in_R L(g)$, $i \in_R L(f)$. אזי $P(i=j) \ge \left(\frac{\delta^2}{\varphi_3(\delta)\cdot 16}\right)^2$.

הוכחה: $L(f) \cap L(g) \neq \varnothing$ כי הראנו בסוף ההרצאה הקודמת שקיימת S עם $\hat{g}(S)$, $\left|\hat{f}(S)\right|$ גדולים ככל שנרצה (כי f, g עוברות את המבחן בהסת' מספקת). נסמן $k \in L(f) \cap L(g)$ ולכן

$$P(i=j) \ge P(i=k=j) = \frac{1}{L(f)} \cdot \frac{1}{L(g)} \ge \left(\frac{1}{\frac{\varphi_3}{\left(\frac{\delta}{4}\right)^2}}\right)^2 > 0$$

■

מסקנה בהינתן פ' שעוברות את הבחינה, נוכל לבחור קוורדינטה מתוך f ו-g באופן ב"ת אחת מהשנייה, והסיכוי שהקוורדינטות הללו יהיו שוות חסומה מלמטה (עם חסם גדול מ-0), קטן כרצוננו כתלות ב-δ.

הערה נרצה בהינתן $\sigma \in S_n$, לבדוק האם יש $i \in L(f)$ ו-$j \in L(g)$ שעבורן $i = \sigma(j)$ (ולא סתם $i = j$). כדי לעשות את זה, במבחן ה-Long Code שהראנו, נסתכל על $g(\sigma(y))$ במקום $g(y)$ ("החלפת שמות").

הגדרה בעיית ה-Unique Label Cover מקבלת כקלט גרף מכוון (V, E) ואילוצים $\Sigma \xrightarrow{\text{חחע"ל}} \Sigma \ni c_e$ לכל $e \in E$. הבעיה מבקשת למצוא השמה $f : V \to \Sigma$ עם $P_{(u,v)\in E}\left(f(u) = c_{(u,v)}(f(v))\right)$.

הערה אינטואיטיבית, האילוצים מגדירים לכל צלע (מכוונת) אילו זוגות אותיות (צבעים) מותרים, או לחלופין לכל צלע ואות לקודקוד הראשון, איזה צבע חייב להיות לקודקוד השני כדי לקיים את האילוץ. לסיום אנחנו רוצים למצוא צביעה של הגרף שעבורו מספר הצלעות עם אילוצים מסופקים הוא מקסימלי.

השערה (UGC) לכל η קיים Σ בגודל קבוע כך ש-$(\eta, 1-\eta)-\mathrm{gap}-\mathrm{ULC} \in \mathsf{NPH}$.

טענה $\left(\frac{1}{2}+\delta, 1-\epsilon\right)-\mathrm{gap}-3\mathrm{Lin}2 \in \mathsf{NPH}$.

הערה נשתמש בהשערה להוכחת הטענה כדי להקל על עצמנו, אפע"פ שניתן להוכיח אותה גם בלי השערות.

הוכחה: נוכיח שקיימת רדוקציה $(\eta, 1-\eta)-\mathrm{gap}-\mathrm{ULC} \le_p \left(\frac{1}{2}+\delta, 1-\epsilon\right)-\mathrm{gap}-3\mathrm{Lin}2$.

יהי $(G, \{c_e\}) \in \mathrm{ULC}$. לכל $v \in V$, נגדיר ("ענן" של) $2^{|\Sigma|}$ משתנים חדשים (מקודדים ע"י $\{\pm1\}^{|\Sigma|}$) לאוסף המשוואות ב-3Lin2, ואת ההשמה לענן נסמן ב-$f_v : \{\pm1\}^{|\Sigma|} \to \{\pm1\}$. לכל $(u,v) \in E$, נתאים את המשוואות של מבחן ה-Long Code עבור f_u ו-f_v עם הפרמוטציה $c_{(u,v)}$, כלומר, כל האפשרויות למשוואה $\mu \cdot f(\mu \cdot x) g(y) = f(z \cdot x \cdot y)$ (בדומה לשימוש ב-sum-check ברדוקציה ל-QS), כאשר במקרה הזה בגלל שהגרלת z היא ממשוקלת, נגלם את העובדה שמערכת המשוואות שלנו היא למעשה ממושקלת (או לחלופין מכילה כפילויות כדי לממש משקול ללא פ' משקול).

נוכיח שהרדוקציה נכונה, כלומר, נראה שהרדוקציה מתאימה נכונה את $\mathcal{Y}, \mathcal{N}$ של בעיית ההבטחה הראשונה לשנייה.

ראשית נראה התאמה של $\mathcal{Y}$-ים; תהי $A:V\rightarrow\Sigma$ שמקיימת $P_{(u,v)\in E}\left(A\left(u\right)=c_{(u,v)}\left(A\left(v\right)\right)\right)\geq1-\eta$, כלומר צביעה שמספקת לפחות $1-\eta$ מאילוצי הצביעה על הצלעות. נוכיח שהפלט הרדוקציה הוא אוסף משוואות לינאריות שניתן לספק לפחות $1-\epsilon$ ממנו.

נגדיר השמה למערכת המשוואות באופן הבא: לכל $u\in V$ ו-$x\in\{\pm1\}^{n}$, נגדיר $f_{u}\left(x\right)=x_{A(u)}$ (מוגדר היטב כי $|\mathrm{Im}\,A|=|\Sigma|$ ולכן נוכל לסדר את Σ כך שכל צבע ייצג אינדקס ב-$\{0,\ldots,|\Sigma|-1\}$), כלומר הדיקטטורה המתאימה ל-$A\left(u\right)$. אינטואיטיבית משימים ב-x בענן של u את הערך "מהי הקוורדינטה של x באינדקס המתאים לצבע של u בצביעה A".

עבור u ו-v שמקיימים את אילוץ הצביעה, כלומר $A\left(u\right)=c_{(u,v)}\left(A\left(v\right)\right)$, קיים i כך ש-$f_{u}=f$ ו-$f_{v}=g$ הם הדיקטטורה המתאימה ל-i (עד כדי הפרמוטציה על אחד מהם) ולכן המבחן עובר אם"ם

$$x_{i}y_{i}=\mu\cdot\mu\cdot x_{i}y_{i}=\mu f\left(\mu x\right)g\left(y\right)=f\left(zxy\right)=z_{i}x_{i}y_{i}$$

אם"ם $z_{i}=1$ שזה קורה בהסת' $1-\epsilon'$. כלומר, לכל אילוץ c_{e} שמסתפק (יש $1-\eta$ כאלה), $1-\epsilon'$ מהמשוואות בענן שלו מסתפקות. לכן סה"כ לפחות $\left(1-\eta\right)\left(1-\epsilon'\right)\geq1-\eta-\epsilon'$ משוואות מסתפקות ולכן עבור $\epsilon=\eta+\epsilon'$ פלט הרדוקציה מקיים את תנאי השלמות (הוא ב-$\mathcal{Y}$).

עתה נראה התאמה של $\mathcal{N}$-ים בקונטרה-פוזיטיב; נניח שיש השמה שמספקת לפחות $\frac{1}{2}+\delta$ מהמשוואות ונראה השמה למערכת שמספקת לפחות η מהאילוצים (כלומר אם קלט אינו ב-$\mathcal{N}$ של הבעיה השנייה, הוא אינו ב-$\mathcal{N}$ של הראשונה). בגלל שאחוז המשוואות המסופקות הוא ממוצע המשוואות המסופקות בכל ענן (נוסף על אלגברה לא מעניינת), ההשמה הזו מספקת $\frac{1}{2}+\frac{\delta}{2}\leq$ משוואות בלפחות $\frac{\delta}{2}$ מ"ענני" המשוואות המושרים ע"י כל אילוץ (כלומר מבחן ה-Long Code עובר הסת' זו עבור האילוץ).

לכל קודקוד u, נבחר דיקטטורה המתאימה ל-$\xi_{u}\in_{R}L\left(f_{u}\right)=L_{\frac{\frac{\delta}{2}}{4},\varphi_{3}\left(\frac{\delta}{2}\right)}\left(f_{u}\right)$ כהשמה לאוסף משתנים המושרה מ-u. אם אילוץ $c_{(u,v)}$ צביעה שענן המשוואות שלו $\frac{1}{2}+\frac{\delta}{2}$ מסופק, מהמסקנה שהוכחנו למעלה $P\left(\xi_{u}=\xi_{v}\right)\geq\left(\frac{\delta^{2}}{\varphi_{3}\left(\frac{\delta}{2}\right)\cdot64}\right)^{2}$ ולכן תוחלת מספר האילוצים שמתקיימים הוא $\leq\frac{\delta}{2}\cdot\left(\frac{\delta^{2}}{\varphi_{3}\left(\frac{\delta}{2}\right)\cdot64}\right)^{2}$ שזה גדול מ-η כי אנחנו יכולים לבחור η קטן כרצוננו. ■

הערה בעיית ה-LC היא ULC אבל עם אילוצים שאינם בהכרח תמורות אלא סתם פ' $\Sigma\mapsto\Sigma$, כלומר לכל צלע וקודקוד ראשון אפשר לבחור אולי כמה צבעים לקודקוד השני שיספקו את האילוץ.

לא סיימנו את ההוכחה כי ה-UGC היא השערה. במבחן נוכיח $\left(1,1-\epsilon\right)-\mathrm{gap}-3\mathrm{SAT}\leq_{p}\mathrm{LC}$ באופן הבא; נבחר $\Sigma=\{\pm1\}^{3}\setminus\{(1,1,1)\}$ (1 מייצג F כך שאלו הן כל שלשות הליטרלים שמספקים פסוקית). נגדיר

$$V=\{x_{i}\}\cup\{\overline{x_{i}}\}\cup\{c_{j}\},\quad E=\{(c_{j},x_{i}):x_{i}\in c_{j}\}\cup\{(c_{j},\overline{x_{i}}):\overline{x_{i}}\in c_{j}\}$$

והאילוץ $c_{e}\left(c_{j}\right)=\left(x_{i},x_{i},x_{i}\right)$ לכל $e=\left(c_{j},x_{i}\right)$ (ואם זה ליטרל בשלילה אז כמובן עם שלילה). כך, הערך של x_{i} ב-c_{j} שווה לערך של x_{i} (כפי שהשניים מתבטאים מצביעת הקודקוד c_{j} ו-x_{i} בהתאמה) אם"ם האילוץ מתקיים.

לכן אם בקלט ה-3SAT יש השמה מספקת g, נבחר צביעה ל-$\left(V,E,\{c_{e}\}\right)$ באופן הבא: $f\left(x_{i}\right)=\left(g\left(x_{i}\right),g\left(x_{i}\right),g\left(x_{i}\right)\right)$ לכל קודקוד

x_i המייצג ליטרל (ובדומה עבור ליטרלי שלילה), ו-

$$f\left(c_j\right)=\left(g\left(\xi_{c_j,1}\right),g\left(\xi_{c_j,2}\right),g\left(\xi_{c_j,3}\right)\right)$$

כאשר $\xi_{c_j,i}$ הוא המשתנה ה-i בפסוקית ה-j. לפחות אילוץ אחד מכל שלשה שנוצרת מפסוקית חייב להסתפק, אחרת כל הליטרלים הם 1 (F) ונקבל פסוקית שלא סופקה, כלומר לא ב-3SAT. אם אי אפשר לספק יותר מ-$1-\epsilon$ מהמשוואות, נותר להוכיח איזה חסם עליון זה נותן מספר אילוצי הצביעה שניתנים לסיפוק.

ישנם שני רכיבים נוספים בהוכחה שנותרו לא פתורים:

1. כיצד נשתמש במבחן ה-Long Code בלי הנתון שהאילוצים הם תמורות.
2. השגת נאותות $1-\epsilon$, שהיא מהותית קרובה ל-1, לעומת הנאותות שראינו ב-ULC, η, שהיא מהותית קרובה ל-0. הפתרון לכך הוא באמצעות בדיקה של כמה זוגות פסוקיות-משתנים בכל פעם.

סוף.