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

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 $\text{opt}(I)$ (מסומן לעתים $\text{val}(I)$) 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-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-$[1,s]\in$ NPH-gap − MAX − 3SAT.

הערה הניסוח החדש מספיק כי ל-$[1,s]$ gap − MAX − 3SAT יש מוודא הסת' שעונה על הקריטריונים האמורים לעיל ולכן עם רדוקציה מכל $L\in$ NP נקבל את משפט ה-PCP המקורי.

המוודא 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, כלומר s הוא קבוע התקפות במקרה הזה.

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 P $\neq$ NP אז לא קיים אלג' α-מקרב פולינומי ל-MAX − 3SAT עבור $\alpha>s$ (כאשר s הקבוע ממשפט ה-PCP).

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

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

- אם $w\in L$ אז $b\ge\alpha\underbrace{\mathrm{val}\left(f\left(w\right)\right)}_{\ge1}\ge\alpha>s$.
- אם $w\notin L$ אז $b\le\mathrm{val}\left(f\left(w\right)\right)\le s$.

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 $\mathsf{P}=\mathsf{NP}$ סתירה. ■

מסקנה אם $\mathsf{gap}-\mathsf{MAX}-\mathsf{3SAT}\left[c,s\right]\in\mathsf{NPH}$ וגם $\mathsf{P}\neq\mathsf{NP}$ 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 ושחקן נוסף משתנה בפסוקית. הראשון מחזיר השמה למשתנים בפסוקית והאחרון השמה למשתנה.

הם מנצחים אם ההשמה של הראשון מספקת את הפסוקית ואם שני השחקנים מסכימים על הערך המושם במשתנה שניתן לאחרון מתוך הפסוקית.

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

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

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

$(*)$ מונוטוניות ההסת' : השחקנים אידאליים ולכן אם הפסוקית ניתנת להשמה תחת ההשמה (אסטרטגיה) שהוסכמה בהתחלה, שניהם ייתנו אותה. 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 ממנה הוא חושף 3 ערכים למוודא ושל 2 היא המוסכמת במקור ממנה הוא חושף ערך אחד למוודא). $s_1(c), s_2(c)$ הן וקטורים ב-$\{0,1\}^3$.

$(**)$ 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

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

■

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

- $P_1 = \langle Q_1, \Sigma_1\rangle, P_2 = \langle Q_2, \Sigma_2\rangle$ 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 $\text{val}(G) = \sup_{\text{strategies}} P(\text{success})$.

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

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

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

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 $\operatorname{val}\left(G\right)=\max_{\text{det}'\text{ strategies}}P\left(\text{success}\right)$ 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 $h\left(u,w\right)=P_{i\in[n]}\left(u_i\neq w_i\right)$ (שיעור הקוורדינטות עליהן הוקטורים מסכימים).
- R - הקצב (rate) שערכו $\frac{\log|C|}{\log|\Sigma^n|}$.
- q - גודל הא"ב, $q=|\Sigma|$.

הערה אם 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 הערך העליון בקצב, אם נסתכל בבסיס $|\Sigma|$ נותן לנו את מספר האותיות ב-Σ שנדרשות כדי לייצג את כל המילים ב-C (אם $\log_{|\Sigma|}|C|=17$ אז נוכל לקודד את כל המילים באורך 17). לכן היחס למעשה מגדיר את היעילות של 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 $1\geq R+\frac{d}{2}+o_{|\Sigma|}(1)$.

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. 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).

(ii) המילים ב-$B_0\left(\frac{d}{2}\right)$ הם המילים על לכל היותר $\frac{d}{2}$ אותיות שאינם 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).

(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 פרובולות, 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) איתם נעבוד להיות $d\leq n\leq q$ ונבחר $a_1,\ldots,a_n\in\mathbb{F}_q$. הקוד של ריד-סולומון הוא

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

הערה זהו קוד לינארי מסגירות הפולינומים מדרגה לכל היותר d לחיבור.

נחשב את הפרמטרים של הקוד.

- אורך הקוד הוא n.
- מרחק הקוד הוא $1-\frac{d}{n}$ כי שני פולינומים שונים הם לכל היותר שווים ב-d נקודות.
- קצב הקוד הוא $\frac{d+1}{n}$ כי $\dim C=d+1$ וזהו קוד לינארי.
- גודל הא"ב הוא $q=\left|\Sigma_q\right|$.

אם נבחר $d\leq\frac{n}{2}$ נקבל קצב ומרחק $\frac{1}{2}$ שזה מה שרצינו, וגודל א"ב בין n ל-$2n$ (שם בהכרח יש ראשוני).

כרגע יש לנו n^n מילים ב-$|\Sigma|^n$. נרצה משהו עם משמעותית פחות אותיות. אם נבחר קוד עם n מילים, נוכל לבחור כל מילה לייצג אות אחרת ב-Σ וכך לייצג קודים ב-C באמצעות מילים מהקוד הקטן יותר, ובתקווה עדיין לשמר את אותן התכונות.

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' כאשר $q_1\gg q_2$. נדרוש $\left|C_2\right|\geq q_1$ וקיום $E:\Sigma\overset{\text{חח"ע}}{\to}C_2$ (קידוד אותיות 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.
- קצב הקוד הוא $R_1\cdot R_2$ (עד כדי קבוע קטן) מהחישוב

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

כאשר באופן אופטימלי $|C_2|$ קרוב כמה שיותר (מלמעלה) ל-q_1.

הערה 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 ואורך מילה $\log\log\log n$.

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

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 $k = \log n$) לכן יש בו $k^{\frac{k}{2}} = |C_2| \geq n$.

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

נוכל להפעיל זאת שוב עם C_3 שלו פרמטרים $\left(\log\log n, \frac{1}{2}, \frac{1}{2}, \log\log n\right)$ ונקבל $C \circ C_3$ עם פרמטרים $\left(n \log n \log\log n, \frac{1}{8}, \frac{1}{8}, \log\log n\right)$.

בטווח הארוך אמנם, אנחנו מאבדים ביצועים ולא מתקרבים ל-$q = 2$. 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 אותו עם $C \circ C_3$ ולקבל קוד עם קצב, מרחק וגודל א"ב קבוע, ומספר 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 $\log n = 2^{2^{\log\log\log n}}$ כלומר נוכל בזמן פולי' לעשות ברוט פורס על כל הקבוצות עד שנגיע לאחת שהיא קוד עם פרמטרים מספקים. 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 $w_1 \in \{0,1\}^N$ ונשלול את כל מה שבכדור ברדיוס $\frac{1}{100}$ שלה. נבחר מילה נוספת זמינה ונשלול את מה שברדיוס שלה, וחוזר חלילה. מובטח לנו המרחק של לפחות $\frac{1}{100}$ בין כל שתי מילים. 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 של "נכונות הוכחה" כאשר הבדיקה במרכאות כי היא הסת' ונכונות ההוכחה במרכאות כי 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.

עם זאת השיטה שבה נשתמש שכן תעבוד תדחה בהסת' δ את $w\in\Sigma^n$ אם $\epsilon\le\Delta\left(w,C\right)$ כאשר ϵ,δ קבועים כלשהם, Δ פ' מרחק ו-$\Delta\left(w,C\right)=\min\limits_{c\in C}\Delta\left(w,c\right)$. כאן בגלל שקודים אמורים להיות רחוקים אחד מהשני וממילים מקריות שלא בקוד, הרי שמילים לא בקוד נדחה בסבירות גבוהה.

הגדרה יהי $n\in\mathbb{N}$ ו- $C\subseteq\Sigma^n$ קוד. T אלג' רנדומי הוא local − tester− $\left(\epsilon,\delta,h\right)$ 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-$\Delta\left(w,C\right)\ge\epsilon$ מתקיים $P\left(w\text{ דוחה את } T\right)\ge\delta$ (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, $h=2$ יש אלג' עם כמעט שלמות 1 ו-$h=3$ כבר יש שלמות 1.

local − tester עבור קוד ריד-סולומון

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

דוגמה קודים עם $d=2$ הם שערוך פרבולה ב-n-הנקודות. עם $q=4$ אפשר לדגום שלושה ערכים, הם מגדירים לנו את פרבולה (שהיא הפולינום של מילת הקוד אם זו אכן מילת קוד) 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 כזה ע"י דגימת $d+1$ נקודות שקובעות את הפולינום המשרה את המילה (לכאורה) ואז חיזוי האות ה-$d+1$ עם הפולינום ובדיקת שוויון עם מה שיש במילה באמת (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 $\{a_1, \ldots, a_n\} \supseteq b_1 \neq \ldots \neq b_{d+1}$. 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 $b_0 \neq \ldots \neq b_{d+1} \in \{a_1, \ldots a_n\}$ 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

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

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

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

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 מסכימים על לכל היותר d ערכים ממשפט שוורץ-זיפל והקוד לינארי ו-$\left\{ x^{\vec{i}} \right\}_{\vec{i}}$ הוא בסיס למרחב המולטינומים ויש $\binom{d+m+1}{d}$ 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 $H_m = \left\{ f : f(x) = \sum_{i=1}^{m} a_i x_i,\ a_i \in \mathbb{F}_q \right\}$.

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 שבקוד 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'), גם אם כשהמילה היא מילת קוד היא אכן מושרת מוקטור עם m ביטים ומספר מילות הקוד הוא m (אחת לכל וקטור ב-$M_{1\times m}\left(\mathbb{F}_2\right)$).

הפרמטרים של קוד האדמארד הם $(n,d,R,q)=\left(2^m,\frac{1}{2},\frac{m}{2^m},2\right)$ 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 לקודי ריד-סולומון עם כל המספרים ב-$\{a\}$ בלבד, כלומר $RS_{d,q}$ הוא למעשה $RS_{d,0,\ldots,q-1,q}$ כאשר q תמיד ראשוני.

הערה בהסתכלות על מילות קוד כפ' מתקיים

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

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).

ככלל אמנם נדמה שהקצב לעתים הוא גרוע (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 $m=d,q=2d$, נקבל קצב שהוא בקירוב (5 סתם לשם הדגמה) $\frac{\binom{2d}{d}}{q^d}\approx\frac{c^d}{(5c)^d}$ כאשר למעשה הקודים שאנחנו מייצגים מושרים מפולינומים שדורשים $n=c^d$ לייצוג, ומפיתוח קצר מקבלים שזה פולינומי קטן ב-n.

לעומת זאת קוד הדמארד נותן קצב $\frac{m}{2^m}$ שהוא אקספוננציאלי קטן ב-m שזה רע מאוד, כי קצב גבוה הוא טוב.

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 $f\left(x\right)=f\left(y\right)+f\left(x+y\right)$ (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 f נקראת random-self-reducable אם היא מקיימת שלכל x, בהסת' גבוהה מתקיים $f(x)=f(y)+f(x+y)$ 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 באקראיבאקראי $x,y\in\mathbb{F}_2^m$ 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 $P(f(y)=g(y))\geq1-\epsilon$ וכך גם עבור $x+y$ ולכן $P(f(x)=g(x))\geq1-2\epsilon$ 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-$P_{x,y}(B_f(x,y))\geq1-\epsilon$. 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

$$g(x)=\underset{y\in\mathbb{F}\mathbb{F}_2^m}{\mathrm{Maj}}(f(y)+f(x+y))$$

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) תיתן תוצאות מיטיבות ואכן כך. נוכיח כי $\mathrm{dist}(f,g)\leq2\epsilon$.

$$\begin{aligned}1-\epsilon&\leq P_{x,y}(f(x)=f(y)+f(x+y))\\&=E_x[P_y(B_f(x,y)\mid x)]\quad\text{התוחלת השלמה}\\&\overset{(*)}{\leq}P_x(M)\cdot1+(1-P_x(M))\frac{1}{2}\\&=\frac{1}{2}+\frac{1}{2}P_x(M)\end{aligned}$$

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

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

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

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

נרצה לחזק את המשוואה הנ"ל עד כדי הוכחת התכונה השלישית

נאמר כי $(x, y, x+y)$ חופשית אם $x, y \in_R \mathbb{F}_2^m$, מעוגנת אם x קבוע ו-$y \in_R \mathbb{F}_2^m$ וקבועה 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: מתקיים ש-y_1, y_2, y_1+y_2 היא חופשית, וכך גם $x+y_1, x+y_2, y_1+y_2$ ולכן מהתנאי שדרשנו לעצמנו בתחילת ההוכחה הכללית, ההסת' שכל אחת מהמשוואות הבאות לא מתקיימות הוא לכל היותר ϵ

$$f\left(y^1\right) = f\left(y^2\right) + f\left(y^1+y^2\right)$$
$$f\left(x+y^1\right) = f\left(x+y^2\right) + f\left(y^1+y^2\right)$$

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

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

■

טענת ביניים גדולה לכל x (לא רק $1-2\epsilon$ מתוך כולם), $P_y(g(x) = f(x+y) + f(y)) \geq 1-2\epsilon$ (כלומר יש רוב מוחץ של y-ים שנותנים ערך $f(x) = g(x)$).

הוכחה: יהי $x \in \mathbb{F}_2^m$. נסמן $p = P_y(f(y) + f(x+y)) = 0$ ולכן $g(x) = 0$ אם $p > \frac{1}{2}$ ואחרת $g(x) = 1$. לכן מתקיים

$$1 - 2\epsilon \leq (\star) = p^2 + (1-p)^2 = 1 - 2p(1-p)$$

כלומר $p(1-p) \leq \epsilon$. אם $p < \frac{1}{2}$ אז $\frac{1}{2}p < p(1-p)$ כלומר $p \leq 2\epsilon$ ואחרת $1-p \leq 2\epsilon$. זה אומר ש-$p \geq 1-2\epsilon$ או ש-$1-p \geq 1-2\epsilon$.

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. ■

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. ■

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, $g\left(x\right)=\underset{r\in_{R}\mathbb{F}_{q}}{\text{plur}}\sum a_{i}f\left(x+r\cdot i\right)$. 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.