חסמים תחתונים לסיבוכיות תקשורת הסתברותית

ולעומק מעגלים בוליאנים מונוטונים

חיבור לשם קבלת תואר דוקטור לפילוסופיה

מאת רן רז

הוגש לסינט האוניברסיטה העברית בשנת תשנ"ב (1992)

עבודה זו נעשתה בהדרכתם

של פרופסור מיכאל בן־אור ופרופסור אבי ויגדרזון

תוכן העניינים

פרק א: הקדמה.

"סיבוכיות תקשורת" היא תחום החוקר את כמות האנפורמציה שחייבים שני שחקנים להעביר ביניהם, על מנת לחשב פונקציה התלויה בשני קלטים, הנמצאים אצל השחקנים השונים, כאשר מראש לא יודע כל שחקן מהו ערך הקלט של השחקן השני. התחום יוסד על ידי Yao [Y] ומאז נחקר בעבודות רבות, כאשר נקודת הענין המרכזית היא קבלת חסמים תחתונים על סיבוכיות התקשורת במקרים שונים.

הסכמה הלוגית של "מעגלים בוליאנים" היא מודל חישוב הנחקר כבר עשרות שנים. במודל זה הקלט ניתן בצורת ביטים והחישוב מתבצע על ידי שערים לוגיים. הפלט ניתן גם הוא בצורת ביטים ובמקרים רבים מניחים שהפלט הוא ביט בודד. שני משתנים חשובים המאפיינים מעגל בוליאני הם: גודלו ועומקו. גודלו של המעגל מוגדר כ: מספר השערים הלוגיים מהם הוא מורכב. עומקו של המעגל הוא המרחק המקסימלי בין קלט ופלט בו. אחד מכיווני המחקר המרכזיים בתחום המעגלים הבוליאנים, הוא מתן חסמים תחתונים לגודלם ולעומקם של מעגלים המחשבים פונקציות מסוימות. חסמים כאלה נותנים באופן מיידי חסמים דומים לכל מודלי החישוב האחרים, ובפרט גם למודל של מכונת Turing. ההצלחות בתחום זה, עד כה, זעומות. השאלות המרכזיות בתחום נשארו פתוחות. בפרט, החסמים הטובים ביותר הידועים לגבי פונקציות מפורשות הם $\Omega(n)$ לגודל ו- $\Omega(\log n)$ לעומק וזה הרי שום דבר.

הצלחה רבה יותר הושגה במתן חסמים תחתונים במודלי־חישוב חלשים יותר, אחד המודלים האלה הוא מודל החישוב של "מעגלים בוליאנים מונוטונים". מעגל מונוטוני הוא מעגל המחשב פונקציה בוליאנית מונוטונית בעזרת השערים הלוגיים: OR, AND בלבד. התוצאות הראשונות שנתנו חסמים תחתונים למעגלים כאלה, הושגו על ידי: Razborov [R1][R2], שהוכיח חסמים סופר־פולינומיאלים על גודלם של מעגלים המחשבים פונקציות מסוימות. תוצאות אלה שופרו לחסמים אקספוננציאלים [AB]. חסמים אקספוננציאלים התקבלו גם על ידי Andreev [A] מייד

אחרי [R1].

בין התחומים של: "חסמים תחתונים לסיבוכיות תקשורת" ו: "חסמים תחתונים לעומק של מעגלים בוליאנים", קיים קשר מפתיע שהתגלה על ידי Karchmer ו Wigderson [KW]. ב [KW] מדובר בסיבוכיות תקשורת של יחסים, והכונה היא לבעיות סיבוכיות תקשורת בהן לא צריכים השחקנים לחשב עבור כל קלט נתון ערך מסוים, אלה לתת אחת ממספר תשובות אפשריות. הקשר בין התחומים ניתן על ידי רדוקציה המתאימה לכל פונקציה בוליאנית f בעיית סיבוכיות תקשורת R_f, ולכל פונקציה מונוטונית, בעית סיבוכיות תקשורת R_f^m. סיבוכיות התקשורת של הבעיה R_f שוה בדיוק לעומק המיזערי של מעגל בוליאני כלשהו המחשב את f.

סיבוכיות התקשורת של הבעיה R_f^m שוה לעומק המיזערי של מעגל מונוטוני המחשב את f. הקשר בין שני התחומים נוצל ב [KW] להוכחת חסם של $\Omega(\log^2 n)$ לעומק מעגל מונוטוני המחשב את פונקצית ה st־קשירות בגרפים. פונקציה זאת מקבלת כקלט גרף, ומכריעה האם קיימת מסילה בין שני קודקודים מסוימים בתוכו.

אחת השאלות שטבעי לשאול לגבי קשר בין שני תחומים, היא השאלה: האם הקשר הכרחי או רק מספיק? או במילים אחרות: האם הקשר נותן כלי חדש המאפשר הבנה שונה מהותית, או אולי הוא מהוה בסך הכל הצגה אחרת של הדברים. ואמנם החסם שניתן ב [KW] לעומק מעגלים, משתמש במונחים של סיבוכיות תקשורת אבל ניתן לתרגום מיידי למונחים של מעגלים.

הבעיות R_f ו R_f^m עליהן דובר הן בעיות דטרמיניסטיות, אולם בתחום של סיבוכיות תקשורת מתאימים לכל בעיה את המקבילה ההסתברותית שלה ועוסקים גם בה. שאלה טבעית נוספת לגבי הקשר בין התחומים האמורים היא: האם ניתן להפיק תועלת לגבי מעגלים מן השמוש בסיבוכיות תקשורת הסתברותית?

תחום המחיה של עבודה זאת הוא הגשר שבין מחקר סיבוכיות התקשורת לבין מחקר העומק של מעגלים בוליאנים. העבודה תנסה לענות בחיוב על שתי השאלות שהעלנו, תוך כדי קבלת

חסמים תחתונים בשני התחומים. עיקר המאמץ בתחום של "סיבוכיות תקשורת" מושקע בפתוח כלים. התוצאות חשובות פחות, החשיבות העיקרית היא בדרך ההוכחה. בתחום של "מעגלים בוליאנים" המצב הפוך, יש חשיבות רבה לתוצאות עצמן ומאבק מתמיד לקבלת חסמים יותר ויותר טובים. בשתי נקודות אלה תשתדל העבודה לתרום.

פרק א' של העבודה יהיה מעין מבוא שיתן רקע בסיסי והגדרות חיוניות. פרקים ב' ג' וד' יעסקו בפונקצית ה st־קשירות, אותה כבר הזכרנו ובבעיות סיבוכיות תקשורת הקשורות לפונקציה זאת.

פרק ג' יתבונן בבעית סיבוכיות התקשורת R_f^m המתאימה לפונקצית ה st־קשירות בגרפים, ויוכיח לבעיה זאת חסם תחתון של $\Omega(\log^2 n)$ במקרה ההסתברותי, שהוא הכללה של אותו החסם שהוכח ב [KW] עבור המקרה הדטרמיניסטי.

פרק ד' משתמש באותן שיטות (של פרק ג') לקבלת תוצאה נוספת, הנותנת חסם תחתון לעומק של חישוב פונקצית ה st־קשירות בעזרת מעגל בוליאני מונוטוני למחצה, כלומר מעגל בוליאני שבו מאפשרים שלילות על מספר מוגבל של משתני הקלט. בפרט יוכח שכל מעגל שעומקו לוגריתמי, המחשב פונקציה זאת, משתמש בשלילותיהם של לפחות אחוז קבוע ממשתני הקלט. כל מעגל שמשתמש בשלילותיהם של פחות מאחוז קבוע של המשתנים הוא בעל עומק על־לוגריתמי. פרקים ג' וד' ישתמשו שניהם בכלים דומים ויסתמכו על מספר משפטי עזר שהוכחותיהם תינתנה בפרק ב'. המשותף למשפטי עזר אלה, שחלקם מענינים גם בפני עצמם, הוא שכולם מדברים על צורות אחידות של התנהגות של קבוצות גדולות.

פרק ה' הוא פרק עצמאי שאינו מסתמך על קודמיו ובו יוכחו חסמים תחתונים ליניארים לעומק מעגלים מונוטונים המחשבים פונקציות מסוימות בגרפים. בין פונקציות אלו יהיו פונקצית הזווג (Matching) ופונקצית ה Clique. דרך ההוכחה תהיה מתן שורה של רדוקציות פשוטות שחיבורן יתן רדוקציה אל פונקציות אלה מהבעיה של זרות קבוצות (Disjointness) בסיבוכיות תקשורת הסתברותית. בעיה זאת היא בעיה קלאסית בסיבוכיות תקשורת ולה הוכח חסם

ליניארי במקרה ההסתברותי ב [KS]. חסמים תחתונים אלה נותנים חסם תחתון של $\Omega(n)$ במונחים של מספר הקודקודים בגרף, ומהוים שיפור לחסמים קודמים של $\Omega(\log^2 n)$ לפונקצית הזווג [R2], ושל $\Omega(n^{1/3})$ לפונקצית ה Clique [AB], הנגזרים מהחסמים המקבילים לגודל (החסם $\Omega(n^{1/3})$ לפונקצית ה Clique הוא גם החסם הטוב ביותר שהיה ידוע עד כה לפונקציה כלשהי). החסמים של $\Omega(n)$ שנקבל הם הדוקים. מחסמים תחתונים אלה נובעות מספר תוצאות נוספות. אחת התוצאות המתקבלות מהחסם עבור פונקצית הזווג היא קיום פער בין עומק חישוב מונוטוני לעומק חישוב לא מונוטוני. הפער המתקבל הוא אקספוננציאלי.

כל פרקי העבודה תורמים לחזוק והבנת הקשר שבין "סיבוכיות תקשורת" לבין "עומק מעגלים בוליאנים" ומצביעים על האפשרות לקבל חסמים תחתונים לעומק מעגלים בעזרת שיטות ותוצאות של סיבוכיות תקשורת הסתברותית.

א.1: סיבוכיות תקשורת ומעגלים בוליאנים.

בעבודה זאת יתיחס המושג של "סיבוכיות תקשורת" לא רק לסיבוכיות התקשורת הרגילה של חישוב פונקציות, אליה נוהגים להתיחס בדרך כלל, אלה גם לסיבוכיות תקשורת של יחסים, שהיא הכללה פשוטה שיוסדה ב [KW]:

יהיו X,Y,Z קבוצות סופיות ו $R\subset X*Y*Z$ יחס כלשהו. לכל $x\in X,y\in Y$ נסמן ב $Z(x,y)$ את הקבוצה: $Z(x,y)=\{z|(x,y,z)\in R\}$. הזוגות (x,y) עבורם $Z(x,y)\neq\emptyset$ יקראו צלעות היחס R ויסומנו ב $E(R)$. בבעית התקשורת המתאימה ל R, או לחלופין במשחק התקשורת המתאים ל R תפורש X כקבוצת הקלטים האפשריים של שחקן I, Y כקבוצת הקלטים האפשריים של שחקן II ו Z כטווח ההחלטה של שני השחקנים. במשחק זה לשחקן I קלט $x\in X$ ולשחקן II קלט $y\in Y$ כאשר מניחים $(x,y)\in E(R)$. מטרתם של שני השחקנים היא להסכים על ערך $z\in Z(x,y)$. מראש אין לאף אחד משני השחקנים מידע כלשהו על הקלט של האחר.

פרוטוקול דטרמיניסטי P לבעיה R הוא סכמת פעולה לכל אחד משני השחקנים, לפיו מחליפים השחקנים מידע בינהם. בכל שלב מעביר אחד מהשחקנים מידע כלשהו על הקלט שלו, המותנה בקלט עצמו ובמידע שכבר קיבל מהשחקן השני. בסיום הפרוטוקול מסכימים ביניהם השחקנים על ערך $P(x,y)\in Z$. הפרוטוקול נכון אם לכל $(x,y)\in E(R)$ מתקים $P(x,y)\in Z(x,y)$. סיבוכיות התקשורת $c(P)$ של פורטוקול P היא המספר המקסימלי של ביטי מידע שמעבירים שני השחקנים ביניהם (כאשר המקסימום הוא על קבוצת כל הקלטים האפשריים $E(R)$). סיבוכיות התקשורת של הבעיה R, שתסומן ב $C(R)$ היא סיבוכיות התקשורת המינימלית של פרוטוקול הפותר את R.

<u>הערה:</u>

אם עבור פונקציה $g:X*Y\to Z$ נגדיר יחס מתאים $R\subset X*Y*Z$ על ידי $Z(x,y)=\{g(x,y)\}$ נקבל את ההגדרה הרגילה לסיבוכיות התקשורת של חישוב פונקציות.

כפי שכבר אמרנו, הסיבה העיקרית להרחבת המושג של סיבוכיות תקשורת היא שבעזרתה ניתן לפרש בעיות מתחום המעגלים הבוליאנים, על ידי בעיות מקבילות מתחום סיבוכיות התקשורת:

תהי $f:\{0,1\}^n\to\{0,1\}$ פונקציה בוליאנית כלשהי, נגדיר את היחס $R_f\subset f^{-1}(1)*f^{-1}(0)*[n]$ על ידי $(x,y,i)\in R_f$ אמ"ם $x_i\neq y_i$, כלומר: שחקן I מקבל קלט x עבורו $f(x)=1$, שחקן II מקבל קלט y עבורו $f(y)=0$ ומטרתם של שני השחקנים היא למצוא קורדינטה שבה שני הקלטים שונים.

תהי $f:\{0,1\}^n\to\{0,1\}$ פונקציה מונוטונית כלשהי, נגדיר את היחס $R_f^m\subset f^{-1}(1)*f^{-1}(0)*[n]$ על ידי $(x,y,i)\in R_f^m$ אמ"ם $x_i=1,y_i=0$, כלומר: שחקן I מקבל קלט x עבורו $f(x)=1$, שחקן II מקבל קלט y עבורו $f(y)=0$ ומטרתם למצוא קורדינטה שבה ב x יש 1 וב y יש 0. נעיר שהבעיה R_f^m שקולה לבעיה בה לשחקן I קלט x שהוא minterm של f, לשחקן II קלט y שהוא maxterm של f ומטרתם למצוא קורדינטה בה $x_i=1,y_i=0$. בהמשך נשתמש בעיקר בהצגה זאת של הבעיה R_f^m. כדי למנוע בלבול, הקיים בדרך כלל, לגבי המושגים minterm ו maxterm, נאמר כבר עכשיו שאצלנו המושג minterm יתיחס לערך x מינימלי עבורו $f(x)=1$, ואילו המושג maxterm יתיחס לערך y מקסימלי עבורו $f(y)=0$ (כאשר "מינימום" ו"מקסימום" מתיחסים לסדר הרגיל על קובית היחידה).

בעבודה זאת המושג מעגל בוליאני מתיחס למעגל בוליאני מעל הבסיס $\{\wedge,\vee,\neg\}$ כאשר השערים $\{\wedge,\vee\}$ הם בעלי דרגת כניסה 2, ואילו שער השלילה $\neg$ מופעל על הקלטים בלבד. מעגל הוא מונוטוני אם אינו מכיל שלילות. עבור פונקציה בוליאנית כלשהי f, נסמן ב $d(f)$ את העומק המזערי של מעגל בוליאני המחשב את f. עבור פונקציה מונוטונית f נסמן ב $d^m(f)$ את העומק המזערי של מעגל בוליאני מונוטוני המחשב את f.

משפט 1.1 [KW]:

1. לכל פונקציה בוליאנית f, $d(f)=C(R_f)$

2. לכל פונקציה בוליאנית מונוטונית f, $d^m(f)=C(R_f^m)$

משפט זה נותן את הקשר שבין שני התחומים שלנו. פרושו של משפט זה הוא שעל מנת לחקור את העומק או העומק המונוטוני של מעגל בוליאני המחשב פונקציה כלשהי f, מספיק לחקור את סיבוכיות התקשורת של הבעיות R_f ו R_f^m (ראה גם ב [K]).

א.2: סיבוכיות תקשורת הסתברותית.

פרוטוקול הסתברותי P לבעית תקשורת R הוא סכמת פעולה לכל אחד משני השחקנים, לפיו מחליפים השחקנים מידע ביניהם, כאשר הפעם מאפשרים לסכמת הפעולה להיות הסתברותית. כלומר: המידע שמעביר שחקן בשלב מסוים אינו תלוי רק בקלט שלו ובמידע שכבר עבר, אלא גם בהטלות מטבע. סיבוכיות התקשורת של פרוטוקול הסתברותי P על קלט $(x,y)\in E(R)$ היא תוחלת מספר ביטי המידע שמעבירים שני השחקנים בינהם עבור קלט זה (התוחלת נלקחת על מרחב כל הטלות המטבע האפשריות), נסמן סיבוכיות זאת ב $C_p(x,y)$. הסיבוכיות של הפרוטוקול P, שתסומן ב $c(P)$, תוגדר על ידי $c(P)=\max C_p(x,y)$, כאשר המקסימום נלקח על קבוצת הקלטים $(x,y)\in E(R)$.

נבחין בין שני מודלים הסתברותיים: המודל הציבורי שבו לשני השחקנים ביטים אקראיים משותפים, כלומר, כל אחד מהם רואה את תוצאות הטלות המטבע של חברו. והמודל הפרטי שבו לכל אחד משני השחקנים ביטים אקראיים משלו. המודל הפרטי הוא בברור חלש יותר מהציבורי.

הפלט $P(x,y)$ של פרוטוקול הסתברותי P על קלט (x,y) הוא משתנה מקרי. אנו מעוניינים בהסתברות המאורע: $P(x,y)\in Z(x,y)$.

עבור $0\le\varepsilon<1/2$ נגדיר: $P_\varepsilon(R)=\{\text{ציבורי } P \mid \forall(x,y)\in E(R),\ \Pr[P(x,y)\notin Z(x,y)]\le\varepsilon\}$

$\tilde{P}_\varepsilon(R)=\{\text{פרטי } P \mid \forall(x,y)\in E(R),\ \Pr[P(x,y)\notin Z(x,y)]\le\varepsilon\}$

וכן $P(R)=\{\text{דטרמיניסטי } P \mid \forall(x,y)\in E(R),\ P(x,y)\in Z(x,y)\}$

נגדיר את סיבוכיות התקשורת של בעיה R לפי כל אחד מהמודלים על ידי:

$$C_\varepsilon(R)=\min_{P\in P_\varepsilon(R)} c(P)$$

$$\tilde{C}_\varepsilon(R)=\min_{P\in \tilde{P}_\varepsilon(R)} c(P)$$

נשים לב ש

$$C(R)=\min_{P\in P(R)} c(P)$$

שלש העובדות הבאות נובעות מיידית מההגדרות:

1. $\tilde{P}_\varepsilon(R)\subset P_\varepsilon(R)$ ולכן $C_\varepsilon(R)\le\tilde{C}_\varepsilon(R)$

2. עבור $\delta<\varepsilon$ $C_\varepsilon(R)\le C_\delta(R)$, $\tilde{C}_\varepsilon(R)\le\tilde{C}_\delta(R)$

3. $C_0(R)\le C(R)$ (מכיון שפרוטוקול ב $P_0(R)$ הוא למעשה קומבינציה קמורה של פרוטוקולים ב $P(R)$).

המשפט הבא, שהוא הבחנה פשוטה אך חשובה של Newman, אומר שהמודל הציבורי חזק מן הפרטי אך במעט (לכל היותר ב $O(\log n)$ ביטים) ולכן מספיק לעסוק במודל זה שהוא פשוט יותר.

משפט 1.2 [N]:

לכל $\delta>\varepsilon>0$ או $\delta=\varepsilon=0$ $\tilde{C}_\delta(R)\le C_\varepsilon(R)+O(\log n)$ כאשר $n=\log(|X|*|Y|)$.

סקירת הוכחה:

פרוטוקול ציבורי הוא למעשה דרך לבחירת פרוטוקול דטרמיניסטי מבין קבוצה G של פרוטוקולים. הבחירה נעשית על ידי שני השחקנים בעזרת הביטים האקראיים המשותפים שלהם, ולאחריה מפעילים השחקנים את הפרוטוקול הנבחר על הקלטים. לכל זוג קלטים, ההסתברות ב G לתשובה נכונה היא לפחות $1-\varepsilon$. לפי חסם Chernoff קיימת תת קבוצה $\tilde{G}\subset G$ שגודלה $O(\log(|X||Y|))$ כך שלכל זוג קלטים, ההסתברות ב $\tilde{G}$ לתשובה נכונה היא לפחות $1-\delta$. נגדיר פרוטוקול פרטי שקול בצורה הבאה: שחקן I יבחר בצורה מקרית פרוטוקול ב $\tilde{G}$ ויודיע לשחקן II על בחירתו ($\log|\tilde{G}|$ ביטי מידע), שני השחקנים יפעילו פרוטוקול זה על הקלטים ויקבלו תשובה שתהיה נכונה בהסתברות גבוהה מ $1-\delta$. בחירת $\tilde{G}$ יכולה להעשות בצורה שבה הסיבוכיות הממוצעת ב $\tilde{G}$ לא תהיה גדולה בהרבה מזו ב G, לכל זוג קלטים (x,y).

נחזור עתה ליחסים המיוחדים R_f, R_f^m שהוגדרו בסעיף הקודם. אחד הדברים המיחדים יחסים אלה הוא שאפשר לודא נכונות של תשובה בעלות של שני ביטי מידע בלבד. לכן נכונה הלמה הפשוטה הבאה:

<u>למה 1.1:</u>

עבור יחס R שהוא R_f או R_f^m של פונקציה כלשהי, מתקים:

$$C_0(R) \le (C_\varepsilon(R)+2)(\log_{1/\varepsilon} n+1) \qquad \tilde{C}_0(R) \le (\tilde{C}_\varepsilon(R)+2)(\log_{1/\varepsilon} n+1)$$

<u>סקירת הוכחה:</u>

השחקנים יחזרו $\log_{1/\varepsilon} n$ פעמים על פרוטוקול שנכשל בהסתברות ε, ובכל פעם יודאו את נכונות התשובה. אם כל הפרוטוקולים נכשלו (מאורע שהסתברותו $\le 1/n$) יעבירו השחקנים זה לזה את הקלטים שלהם.

א.3 : יחסים בוליאנים כוללים.

לקבוצת הבעיות $\{R_f\}$ נגדיר בעיה כוללת U, לקבוצת הבעיות $\{R_f^m\}$ נגדיר בעיה כוללת U^m.

U^m, U יקראו גם יחסים כוללים ויוגדרו על ידי: $U,U^m \subset \{0,1\}^n * \{0,1\}^n * [n]$

$(x,y,i) \in U$ אמ"ם $x_i \neq y_i$, $(x,y,i) \in U^m$ אמ"ם $x_i=1,\ y_i=0$.

פרוטוקול ליחס הכולל U נותן גם פרוטוקל לכל אחד מהיחסים R_f, ולמעשה אם הפרוטוקול דטרמיניסטי הוא נותן גם נוסחה כוללת לכל הפונקציות הבוליאניות בעלות n משתנים (ראה [W]). פרוטוקול ל U^m הוא גם פרוטוקול לכל R_f^m, ונותן, אם הוא דטרמיניסטי, נוסחה מונוטונית כוללת לכל הפונקציות הבוליאניות המונוטוניות בעלות n משתנים.

היחסים R_f, R_f^m, U, U^m יקראו מעתה יחסים בוליאנים. בבואנו לעסוק בהתנהגות ההסתברותית של יחסים בוליאנים כלשהם, טבעי לבדוק תחילה את היחסים הכוללים U^m, U. ראשית נעסוק ביחס הכולל U, המשפט הבא של Hastad מראה שסיבוכיות התקשורת ההסתברותית של U נמוכה (O(logn)). מכיון ש U יחס כולל נובע מכך שסיבוכיות התקשורת ההסתברותית של כל יחס בוליאני R_f נמוכה.

משפט 1.3 [H]:

$\tilde{C}_0(U),\ C_0(U)=O(\log n)$

לפי משפט 1.2 מספיק לתת הוכחה עבור המודל הציבורי. ניתן כאן סקירת הוכחה של Karchmer למשפט.

סקירת הוכחה [K1]:

נתאר פרוטוקול תקשורת הסתברותי ל U שסיבוכיותו (O(logn:

בהנתן זוג קלטים (x,y), $(x,y) \in E(U)$ ולכן $x \neq y$. נחלק את הפרוטוקול לשני שלבים: בשלב ראשון ימצאו השחקנים וקטור a בעל n רכיבים המקיים ש $\langle a,x\rangle \neq \langle a,y\rangle$ (כאשר הביטוי

$<\alpha,\beta>$ מסמן את המכפלה הסקלרית מודולו 2 של שני וקטורים). בשלב השני יעשה שימוש בוקטור זה על מנת למצוא קורדינטה i שבה $x_i \neq y_i$.

שלב א: כדי למצוא וקטור a המקיים $<a,x> \neq <a,y>$ ייצרו השחקנים logn וקטורים בעלי n רכיבים כל אחד שיהיו מועמדים לכך. יצור הוקטורים יעשה מהביטים האקראיים המשותפים לשני השחקנים ולכן לא יעלה בהעברת מידע. השחקנים יחליפו בינהם את המכפלות הסקלריות מודולו 2 עם כל אחד מהוקטורים המועמדים ((O(logn) ביטי מידע). בהסתברות 1/n לא ימצא אף וקטור שיקיים $<a,x> \neq <a,y>$ ואז יעבירו השחקנים בינהם את הקלטים. בהסתברות 1-1/n ימצא וקטור a כזה.

שלב ב: נסמן ב S את קבוצת כל המקומות i בהם $a_i=1$. נסמן ב $\tilde{x},\tilde{y}$ את צמצומי הוקטורים x,y לקבוצה S, אזי ל $\tilde{x}$ ול $\tilde{y}$ זוגיות שונה. כל שנותר הוא להפעיל פרוטוקול למציאת קורדינטה שונה בין שני וקטורים שזוגיותם שונה, ב (O(logn) ביטי מידע.

משפט זה נותן פער מעריכי בין סיבוכיות תקשורת הסתברותית לסיבוכיות תקשורת דטרמיניסטית של יחסים בוליאנים במקרה הלא מונוטוני. לכן מסתבר שסיבוכיות תקשורת הסתברותית אינה קשורה ישירות לשאלות לגבי עומקם של מעגלים בוליאנים לא מונוטונים לחישוב פונקציות (והרי עומקם הוא $\Omega(n)$ עבור רוב הפונקציות). בעבודה זאת נעסוק בעיקר במקרה המונוטוני.

נעבור עתה ליחס הכולל המונוטוני U^m. המשפט הבא מראה שסיבוכיות התקשורת ההסתברותית של U^m היא גבוהה ($\Omega(n)$), ולכן נותן פער מעריכי בין המקרה המונוטוני למקרה הלא מונוטוני.

<u>משפט 1.4:</u>

$$\tilde{C}_\varepsilon(U^m) \ , \ C_\varepsilon(U^m)=\Omega(n)$$

מאחר ש $\tilde{C}_\varepsilon(R)\geq C_\varepsilon(R)$ מספיק להוכיח ש $C_\varepsilon(U^m)=\Omega(n)$. על מנת להוכיח את המשפט נזדקק לתוצאה ידועה לגבי פונקצית "זרות הקבוצות" (Disjointness) שהיא אחת הפונקציות שסיבוכיות התקשורת ההסתברותית שלה נחקרה ביסודיות. פונקציה זאת מוצגת כמשחק תקשורת בצורה הבאה $D\subset 2^{[n]}*2^{[2]}*\{0,1\}$, $(S,T,0)\in D$ אמ"ם $S\cap T=\emptyset$ $(S,T,1)\in D$ אמ"ם $S\cap T\neq\emptyset$.

כלומר: לכל אחד משני השחקנים תת קבוצה של [n] ועליהם להכריע האם שתי הקבוצות שבידיהם נחתכות.

לגבי פונקציה זאת ידוע חסם הסתברותי, שבו עוד נשתמש בהמשך, לפיו: $C_\varepsilon(D)=\Omega(n)$. ההוכחה לכך ניתנה ב [KS] ופושטה ב [R3].

<u>סקירת הוכחת משפט 1.4:</u>

נשים לב שאם שחקן II מתבונן בוקטור $\bar{y}$ שהוא הוקטור המשלים לוקטור הקלט y, ואם שני השחקנים מפרשים את הוקטורים שבידיהם כקבוצות חלקיות של [n] (הקבוצה המתאימה לוקטור α תהיה קבוצת הקורדינטות i בהן $\alpha_i=1$), מתקבלת הצגה חדשה של היחס U^m לפיה: $U^m\subset 2^{[n]}*2^{[n]}*[n]$ ו $(S,T,z)\in U^m$ אמ"ם $z\in S\cap T$. נשים לב ש $(S,T)\in E(U^m)$ אמ"ם $S\cap T\neq\emptyset$.

כלומר: לכל אחד משני השחקנים תת קבוצה של [n], ידוע ששתי הקבוצות נחתכות ועל השחקנים למצוא נקודת חתוך מסוימת.

מכיון שאפשר לאמת בקלות תשובת פרוטוקול למשחק U^m (ע"י העברת ביט מידע בודד), קיימת רדוקציה פשוטה מ D ל U^m הנותנת: $C_\varepsilon(D)\leq O(C_\varepsilon(U^m))$. מכאן ומהחסם של [KS] מתקבלת טענת המשפט.

א.4: בעיות של קשירות גרפים.

בעבודה זאת נעסוק רבות בבעיות הקשורות בקשירות של גרפים.

פונקצית קשירות הקודקודים (st-connectivity) מקבלת גרף לא מכוון בעל שני קודקודים מיוחדים s ו t ומחליטה האם יש מסלול בין s ל t. כלומר, פונקציה זאת : $stc:\{0,1\}^{n'}\rightarrow\{0,1\}$ מפרשת את הקלטים כצלעות גרף G על קבוצת קודקודים V עבורה $s,t\in V$ ו $|V|=n$, כאשר $n'=\binom{n}{2}$, ומוציאה כפלט 1 אם יש מסלול בין s ל t ו 0 אחרת.

אותנו תעניין במיוחד בעיית־התקשורת המונוטונית המתאימה R^m_{stc}. בבעיה זאת לשחקן I יש מסלול בין שני קודקודים מיוחדים t, s בקבוצת קודקודים V (minterm של הפונקציה stc), ולשחקן II יש חתך של V המפריד בין s ל t (maxterm של הפונקציה stc). את החתך של שחקן II נוח לפרש כצביעה של V בשני צבעים: s ו t. במונחים אלה מטרתם של שני השחקנים היא למצוא צלע במסלול של שחקן I שהיא דו־צבועה לפי הצביעה של שחקן II, מכיוון ש s ו t צבועים s ו t בהתאמה הרי שקיימת לפחות צלע דו־צבועה אחת במסלול המקשר ביניהם.

את הבעיה $R^m_{stc(l)}$ נגדיר כצמצום הבעיה R^m_{stc} למקרה שבו אורך המסלול המקשר בין s ו t הוא l. פרוטוקול פשוט פותר בעיה זאת בסיבוכיות תקשורת של O(logn*logl):

בשלב ראשון מעביר שחקן I את הקודקוד שנמצא בדיוק באמצע המסלול שלו (logn' ביטי מידע). שחקן II מחזיר ביט מידע בודד האומר אם קודקוד זה צבוע s או t. שחקן I מתרכז בחצי המסלול שקצוותיו צבועים בצבעים שונים ונותר עם מסלול שאורכו l/2, וממשיך באותה צורה. אחרי log l שלבים יהיה אורכו של המסלול - 1 , כלומר צלע בודדת.

המשפט העיקרי שהוכח ב [KW] הוא שכשמדובר בסיבוכיות תקשורת דטרמיניסטית חסם עליון זה הוא הדוק.

<u>משפט 1.5 [KW]:</u>

עבור $l\le n^{1/10}$, $C(R^m_{stc(l)})=\Omega(\log n*\log l)$.

אם נקח $l=n^{1/10}$ ונשתמש במשפט 1.1 נקבל:

תוצאה 1.1:

$$d^m(stc)=C(R^m_{stc})=\Omega(\log^2 n)$$

בפרק ג' של העבודה נוכיח הכללה הסתברותית למשפט 1.5 ונקבל ש

עבור $l=n^{1/100}$ $\qquad C_\varepsilon(R^m_{stc(l)})=\Omega(\log n*\log l)$

(למעשה המשפט נכון גם עבור אורכי מסלול אחרים)

אחת הבעיות העיקריות בהוכחת חסם זה, תהיה העובדה שכדי להוכיחו נצטרך להתבונן בקבוצת קלטים אפשריים שאינה מכפלה קרטזית של קבוצות קלטים של השחקנים השונים.

א.5: בעיות הזווג (Matching) וה Clique בגרפים.

פונקצית ה Clique(k) מקבלת כקלט גרף לא מכוון ומכריעה האם קיים בו תת גרף מלא מגודל k. פונקציית ה Matching(k) מקבלת כקלט גרף לא מכוון ומכריעה האם קיימות בו k צלעות בלתי תלויות (k צלעות שאינן נחתכות). באופן היסטורי , החסמים התחתונים הראשונים שניתנו על גדלי מעגלים בוליאנים מונוטונים ניתנו עבור פונקציות אלה. עבור פונקצית ה Clique ניתן חסם ב [R1] ששופר ב [AB] לחסם מעריכי. עבור פונקצית ה Matching ניתן חסם ב [R2] לפיו גודל המעגל המונוטוני הוא $\Omega(n^{\log n})$. מכיון שפונקצית ה Matching נמצאת ב P מתקבל מכאן פער בין סיבוכיות חישוב לסיבוכיות חישוב מונוטונית. ב [T] הוכח שפער זה הוא מעריכי (עבור פונקציה אחרת ב P). החסמים התחתונים האלה עבור גודל החישוב נותנים באופן אוטומטי חסמים מקבלים לגבי עומק חישוב, וכך מתקבל:

$$d^m(\text{Clique})=\Omega(n^{1/3}) \qquad d^m(\text{Matching})=\Omega(\log^2 n)$$

נשאלות שתי שאלות:

1. האם חסמים אלה הדוקים?
2. האם קיים פער בין עומק חישוב לבין עומק חישוב מונוטוני?

מסתבר, כפי שיוכח בפרק ה, שמתקיים: $d^m(\text{Clique}),d^m(\text{Matching})=\Omega(n)$

ומכאן גם שקיים פער מעריכי בין עומק חישוב לבין עומק חישוב מונוטוני.

פרק ב: אחידות ההתנהגות של קבוצות גדולות של מסלולים וחתכים בגרף.

לשם הוכחת חסמים תחתונים לבעיות הקשורות בקשירות של גרפים נתבונן בקבוצות של מסלולים מחד ובקבוצות של חתכים בגרף מאידך. העניין העיקרי שלנו יהיה בזוגות קלטים (חתך, מסלול) בהם עובר המסלול מצד אחד של החתך לצדו השני פעם אחת בדיוק. זוגות אלה נחלק למחלקות לפי האינדקס במסלול שחוצה את החתך, (כל המסלולים יהיו באותו אורך). לכל מחלקה כזאת יש מבנה של גרף דו־צדדי. בצד אחד נמצאים המסלולים, בצד שני החתכים וביניהם קשתות המקשרות בין זוגות הנמצאים במחלקה.

הלמות שנוכיח בפרק זה הם למות קומבינטוריות שישמשו אותנו בפרקים הבאים.

בסימונים שיוגדרו להלן נשתמש בשלשת הפרקים הקרובים:

תהי N קבוצת קודקודים. נסמן $n=|N|$. יהיו s,t שני קודקודים מיוחדים ב N.

נגדיר:

$A_N=$ קבוצת כל המסלולים באורך l ב N , המתחילים ב s ונגמרים ב t.

(לשם נוחות לא מופיע הפרמטר l בסימון).

$B_N=$ קבוצת כל החתכים של N המפרידים בין s ל t.

(אל אברי B_N נתיחס גם כאל צביעות של N בצבעים s ו t).

עבור תת קבוצה $U\subset N$ נגדיר:

$A_U=$ קבוצת כל המסלולים באורך l ב $U\cup\{s,t\}$, המתחילים ב s ונגמרים ב t.

$B_U=$ קבוצת כל הצביעות של U בצבעים s,t (חתכים).

נגדיר: $O_N^i=\{(a,b) \mid a\in A_N, b\in B_N,$ { הצלע ה i ב a היא הצלע היחידה הדו־צבועה לפי b.

$O_N=\bigcup_i O_N^i$

עבור $A\subset A_N, B\subset B_N$ נגדיר:

$$O^i_{AB}=\{(a,b) \mid a\in A,\ b\in B,\ (a,b)\in O^i_N\}$$
$$O_{AB}=\bigcup_i O^i_{AB}=\{(a,b) \mid a\in A,\ b\in B,\ (a,b)\in O_N\}$$

עבור $a\in A_N, B\subset B_N$ נגדיר:

$$O^i_{aB}=\{(a,b) \mid b\in B,\ (a,b)\in O^i_N\}=O^i_{\{a\}B}$$
$$O_{aB}=\bigcup_i O^i_{aB}=\{(a,b) \mid b\in B,\ (a,b)\in O_N\}=O_{\{a\}B}$$

עבור $A\subset A_N, b\in B_N$ נגדיר:

$$O^i_{Ab}=\{(a,b) \mid a\in A,\ (a,b)\in O^i_N\}=O^i_{A\{b\}}$$
$$O_{Ab}=\bigcup_i O^i_{Ab}=\{(a,b) \mid a\in A,\ (a,b)\in O_N\}=O_{A\{b\}}$$

בין שני האיברים התחתונים בששת הסימונים האחרונים יופיע לפעמים פסיק (,) לשם ריווח.

באופן כללי נשתמש באות A לסימון קבוצה של מסלולים ובאות B לסימון קבוצת חתכים.

האותיות a,b יסמנו מסלול בודד או חתך בודד בהתאמה. הסימנים O^i_N, O_N מתיחסים לקבוצת הקשתות בגרף החתכים־מסלולים עליו דברנו. כל ההגדרות האחרונות:

$O^i_{AB}, O_{AB}, O^i_{aB}, O_{aB}, O^i_{Ab}, O_{Ab}$ הם למעשה קבוצות קשתות בצמצומי גרפים אלה ל A,B,a,b.

האות α תסמן אצלנו בדרך כלל את גודלה של קבוצת מסלולים ביחס לקבוצת כל המסלולים האפשריים. α תכונה גם "צפיפות המסלולים". באות β נסמן בדרך כלל את גודלה היחסי של קבוצת חתכים בגרף. β תכונה גם "צפיפות החתכים". האות γ תסמן בדרך כלל את גודלה היחסי (צפיפותה) של קבוצת זוגות (חתך, מסלול).

באות U נשתמש פעמים רבות לתאור קבוצה חלקית של N . בסימונים השונים שהגדרנו עבור N נשתמש גם עבור U : את הקבוצות A_U, B_U כבר הגדרנו. הקבוצות O^i_U, O_U יוגדרו כשם שהוגדרו עבור N. הסימונים $O^i_{AB}, O_{AB}, O^i_{aB}, O_{aB}, O^i_{Ab}, O_{Ab}$ יתיחסו לפעמים לקבוצות $B\subset B_U, A\subset A_U$

ולאיברים $a\in A_U$, $b\in B_U$ ויהיו אז תתי קבוצות של O_U^i, O_U. יש כאן כפילות שנעשתה לשם פשטות הסימונים.

P תשמש הרבה פעמים לתאור מדת הסתברות. עבור $P:S\rightarrow R$ מדת הסתברות על קבוצה סופית S , נסמן ב $H(P)$ את אי הודאות של הפוקציה P (entropy):

$$H(P)=-\sum_{s}P(s)\log_2 P(s)$$

נגדיר את $I(P)$ להיות האינפורמציה של מידת הסתברות P:

$$I(P)=\log_2|S|-H(P)$$

במהלך העבודה כולה נשתמש בסימונים אסימפטוטים. הטענות, המעברים וההוכחות יהיו נכונים עבור פרמטר n ופרמטרים אחרים גדולים מאוד. מכיון שהכונה היא לתת חסמים אסימפטוטים, ולא מדויקים, יופיעו בטענות ובהוכחות קבועים רבים חסרי משמעות.

ב.1: הסטיה מאחידות של מדת הסתברות בעלת אינפורמציה נמוכה.

הלמה הראשונה שנוכיח היא טענת עזר, שבה נשתמש בלמות ובמשפטים הבאים, הנותנת חסמים להסתברות של מאורע בעל תומך ידוע, כאשר מדת ההסתברות היא בעלת אי ודאות גדולה, (אנפורמציה נמוכה).

למה 2.1:

תהי $P:S\to R$ מדת הסתברות על קבוצה סופית S. נסמן $|S|=s$. יהי ω כלשהו $\omega\le 1/100$.

נניח שמתקיים $I(P)\le\theta$ כאשר $\sqrt{\frac{4\theta}{\omega}}<1/10$.

נגדיר:

כאשר הסכום נלקח על $s*\omega$ האיברים הגדולים ביותר, $\bar{a}=\Sigma P(x)$.

כאשר הסכום נלקח על $s*\omega$ האיברים הקטנים ביותר, $\underline{a}=\Sigma P(x)$.

אזי:

$$\bar{a}\le\omega\left(1+\sqrt{\frac{4\theta}{\omega}}\right),\ \underline{a}\ge\omega\left(1-\sqrt{\frac{4\theta}{\omega}}\right)$$

הוכחה:

נוכיח את החסם עבור $\bar{a}$, החסם על $\underline{a}$ מוכח באותה צורה.

את ההתפלגות $P(x)$ נחלק מחדש כך שתהיה קבועה על $s*\omega$ האיברים הגדולים ביותר, וקבועה על כל השאר. בכך לא שינינו את $\bar{a}$ ואילו את $I(P)$ הקטנו. לכן נניח ש:

$$P(x)=\begin{cases}\frac{1}{s}(1+\Delta) & \text{על } s*\omega \text{ האיברים הגדולים ביותר}\\ \frac{1}{s}\left(1-\frac{\Delta\omega}{1-\omega}\right) & \text{אחרת}\end{cases}$$

כאשר:

$$\theta\ge I(P)=-\omega\log(1+\Delta)-(1-\omega)\log\left(1-\frac{\Delta\omega}{1-\omega}\right)$$

נפתח את $\log(1+x)$ לטור טיילור ונקבל עבור קבועים קטנים c_1,c_2:

$$\theta \geq -\omega\Delta+\frac{\omega\Delta^2}{2}+\frac{c_1}{6}\omega\Delta^3+\omega\Delta+\frac{\Delta^2\omega^2}{2(1-\omega)}+\frac{c_2}{6}\omega^3\Delta^3$$

אם נניח ש $\Delta<1/10$ מתקיים $|c_1|,|c_2|<2$ ולכן $\theta\geq I(P)\geq\omega\Delta^2/4$, כלומר: $\Delta\leq\sqrt{\frac{4\theta}{\omega}}$

וזה חסם חזק יותר על Δ. עובדה זאת והעובדה שפונקצית האינפורמציה $I(P)$ מונוטונית ב Δ מעידות שההנחה $\Delta<1/10$ היתה נכונה. (במילים אחרות: אם Δ אינו בתחום שבין 1/10 לבין $\sqrt{\frac{4\theta}{\omega}}$ על אחת כמה וכמה אינו גדול מ 1/10, כי קבוצת ה Δים האפשריים היא בברור קטע שקצהו האחד ב 0).

סוף הוכחת למה 2.1

קיבלנו, אם כן, דרך להעריך, בדיוק טוב מאוד, את $a=\Sigma p(x)$ כאשר הסכום לקוח על $s*w$ איברים כלשהם. כל זאת עבור מדת הסתברות P בעלת אנפורמציה נמוכה.

<u>הערה:</u>

ההגבלה $\omega\leq1/100$ אינה מהותית ונעשתה רק לשם פשטות. אם המשפט נכון לגבי $\omega\leq1/100$ הוא בודאי נכון (עם קבועים שונים במקצת) לכל ω.

ב.2: מבנה גרף המסלולים־חתכים.

הלמה השניה שנוכיח מתיחסת לגרף הדו־צדדי O_N^i, ונותנת הערכה למספר הצלעות בכל תת גרף מספיק גדול שלו. במובן זה הגרף הוא אחיד למדי, לכל תת גרף מספיק גדול שלו יש בערך אותו מספר צלעות. בעתיד נתבונן במשחקי תקשורת בהם קבוצת הקלטים האפשריים תהיה O_N. השימוש שנעשה בלמה (המענינת גם בפני עצמה) יהיה כפול: מצד אחד נותנת הלמה שאם A ו B גדולות מספיק הרי שיש במערכת הרבה קלטים אפשריים. מצד שני נסיק שהקבוצות O_{AB}^i הן בעלות גדלים כמעט זהים, לכן בקבוצת הקלטים האפשריים (בהם צלע דו־צבועה יחידה בכל מסלול) יתפלג מיקומה של הצלע הדו־צבועה במסלול, באופן די אחיד על פני המסלול.

<u>למה 2.2:</u>

עבור $l \le n^{1/100}$

תהי $A \subset A_N$ עבורה $\alpha \equiv |A|/|A_N| \ge n^{-1/100}$ תהי $B \subset B_N$ עבורה $\beta \equiv |B|/|B_N| \ge 2^{-n^{1/100}}$

לכל i נגדיר:

$$\gamma^i = \frac{|O_{AB}^i|}{|O_N^i|}$$

אזי לכל i מתקיים:

$$\alpha\beta(1-O(n^{-1/10})) \le \gamma^i \le \alpha\beta(1+O(n^{-1/10}))$$

<u>הוכחה:</u>

רעיון ההוכחה הוא להתבונן ב"הטלות" של O_{AB}^i על תתי־קבוצות קטנות של N. עבור רוב תתי הקבוצות תתנהג ה"הטלה" בצורה יפה, ונוכל להשתמש בלמה 2.1 כדי לחסום את $|O_{AB}^i|$ על ידי מיצוע על כל ההטלות האלה.

נראה קודם מהי משמעותה של "הטלה". נתבונן בכל תתי הקבוצות $U \subset N$ עבורן $s,t \in U$

ו $|U|=n^{1/2-1/100}$. עבור קבוצת מסלולים $L\subseteq A_N$ נסמן $L_{/U}=L\cap A_U$, כלומר, קבוצת כל המסלולים ב L המוכלים בקבוצה U.

לכל i,U נגדיר:

$$\gamma_U^i=\frac{|O^i_{A_{/U},B}|}{|O^i_{A_U,B_N}|}$$

כלומר, בעוד γ^i היא צפיפות הזוגות במערכת, γ_U^i היא צפיפות הזוגות עבורם המסלול נמצא כולו בקבוצה U.

המכנה $|O^i_{A_U,B_N}|$ הוא קבוע לכל U (כי |U| קבוע). לכן הצפיפות הכוללת γ^i היא מיצוע γ_U^i על כל הקבוצות U:

$$\gamma^i=\overline{\gamma_U^i}$$

(קו עליון מסמן מיצוע, מכאן ועד לסוף ההוכחה הכונה היא למיצוע על הקבוצות האפשריות U).

על הקבוצה B נוח להסתכל כעל התפלגות של חתכים: עבור קבוצת חתכים $Q\subseteq B_N$ (אצלנו בדרך כלל Q=B או $Q=B_N$) נגדיר את P_Q להיות מדת הסתברות על B_N שהיא מפולגת אחיד על Q:

$$P_Q(b)=\begin{cases}1/|Q| & b\in Q\\ 0 & \text{אחרת}\end{cases}$$

נגדיר את $P_{Q/U}$ להיות מדת הסתברות על B_U (B_U היא קבוצת כל החתכים של U), שהיא הטלה של מידת ההסתברות P_Q: לכל חתך $b'\in B_U$ תוגדר $P_{Q/U}(b')$ להיות $\sum P_Q(b)$ כאשר הסכום נלקח על כל $b\in B_N$ המסכימה עם b' על U.

במונחים אלה נוכל לפרק את המונה והמכנה בהגדרת γ_U^i לסכום של תרומות הצביעות השונות ב B_U:

$$|O^i_{A_{/U},B}|=\sum_{b\in B}|O^i_{A_{/U},b}|=\sum_{b'\in B_U}|B|P_{B/U}(b')|O^i_{A_{/U},b'}|=|B|\sum_{b'\in B_U}P_{B/U}(b')|O^i_{A_{/U},b'}|$$

$$|O^i_{A_U,B_N}|=\sum_{b\in B_N}|O^i_{A_U,b}|=\sum_{b'\in B_U}|B_N|P_{B_N/U}(b')|O^i_{A_U,b'}|=|B_N|\sum_{b'\in B_U}P_{B_N/U}(b')|O^i_{A_U,b'}|$$

כל אחד משני הסכומים האחרונים נפרק לשני חלקים, חלק "נורמלי" וחלק "א־נורמלי".

החלקים ה "א־נורמלים" יתגלו כזניחים ולכן ב γ^i_U (וגם ב $\overline{\gamma^i_U}$) נוכל להתעלם מהם:

נסמן ב $h(b')$ את משקל hamming של החלוקה b'. נאמר ש b' נורמלית (usual) אם

$|U|/2-|U|^{3/4} \le h(b') \le |U|/2+|U|^{3/4}$ **ואחרת נאמר ש b' א־נורמלית (unusual) .**

נקבל:

$$2.1)\quad |O^i_{A_{/U},B}|=|B|\sum_{b'usual}P_{B/U}(b')|O^i_{A_{/U},b'}|+|B|\sum_{b'unusual}P_{B/U}(b')|O^i_{A_{/U},b'}|$$

$$2.2)\quad |O^i_{A_U,B_N}|=|B_N|\sum_{b'usual}P_{B_N/U}(b')|O^i_{A_U,b'}|+|B_N|\sum_{b'unusual}P_{B_N/U}(b')|O^i_{A_U,b'}|$$

<u>טענה 2.1:</u>

אפשר להניח שהחלק הא־נורמלי בשני השויונות הוא $o(n^{-1/10})$ של החלק הנורמלי, ולכן זניח בהוכחת הלמה.

<u>הוכחה:</u>

נראה תחילה את הזניחות בשויון השני.

מכיוון ש $P_{B_N/U}(b')=|B_U|^{-1}$ (לפי הגדרה) ו $|O^i_{A_U,b'}|<|U|^l$ (לפי הגדרה) מתקיים:

$$|B_N|\sum_{b'unusual}P_{B_N/U}(b')|O^i_{A_U,b'}|=\frac{|B_N|}{|B_U|}\sum_{b'unusual}|O^i_{A_U,b'}|<\frac{|B_N|}{|B_U|}\sum_{b'unusual}|U|^l=$$

$$\frac{|B_N||U|^l}{|B_U|}\sum_{b'unusual}1<\frac{|B_N||U|^{(l+1)}}{|B_U|}\left(\frac{|U|}{|U|/2}+|U|^{3/4}\right)$$

קרובים אלמנטרים נותנים:

$$\binom{s}{s/2+s^{3/4}} \approx 2^s \left(\frac{1}{e}\right)^{2s^{1/2}}$$

ולכן בהתחשב בגודלו של I החלק ה א־נורמלי קטן מ:

$$\frac{|B_N|}{|B_U|} 2^s 2^{-s^{1/2}}$$

כאשר $s=|U|$. החלק הנורמלי בשויון הראשון גדול בברור מ:

$$\frac{|B_N|}{|B_U|} 2^s$$

ולכן היחס בינהם קטן מ:

$$2^{-s^{1/2}} \approx 2^{-n^{1/4}}$$

מכיון שבלמה 2.2 עלינו להוכיח שבממוצע:

$$|O^i_{A_{/U},B}| = |O^i_{A_U,B_N}| \alpha\beta(1+O(n^{-1/10}))$$

ומכיון שהצד הימני בשויון זה קבוע לכל U מקבלים שאפשר להתעלם מהחלק ה א־נורמלי ב $|O^i_{A_U,B_N}|$.

הצד השמאלי של השויון האחרון אינו קבוע ב U , לכן כדי להראות שהאיבר הא־נורמלי בצד השמאלי הוא זניח, נראה שהוא זניח ביחס לצד הימני (והרי אנו מוכיחים שויון בין הצדדים).

ואמנם, החלק הא־נורמלי ב $|O^i_{A_{/U},B}|$ קטן לפי הגדרה מזה שב $|O^i_{A_U,B_N}|$ וזניח ביחס לצד הימני של השויון האחרון מכיוון שמתקיים:

$$\alpha\beta \geq n^{-1/100} 2^{-n^{1/100}} >> 2^{-n^{1/4}}$$

סוף הוכחת הטענה.

לאחר שהוכחנו שבנוסחאות 2.1,2.2 האיברים הימניים זניחים נעבור לטפל באיברים השמאליים.

הטענה הבאה קובעת שעבור b' נורמלי $|O^i_{A_U,b'}|$ כמעט בלתי תלוי ב b'.

טענה 2.2:

קיים קבוע K התלוי רק ב n,l עבורו לכל b' נורמלית $|O^i_{A_U,b'}|=K(1+o(n^{-1/10}))$

הוכחה:

לפי ההגדרה: $|O^i_{A_U,b'}|=\binom{h(b')}{l-i}\binom{|U|-h(b')}{i}(l-i)!i!$

ולכן $(h(b')-(l-i))^{l-i}(|U|-h(b')-i)^i < |O^i_{A_U,b'}| < h(b')^{l-i}(|U|-h(b'))^i$

b' נורמלי לכן יש $-1\le c\le 1$ עבורו: $h(b')=|U|/2+c|U|^{3/4}$

מהשיוון ומאי השיוון האחרונים ומידיעת l מתקבל שקימים קבועים $-2 < c',c''< 2$ עבורם:

$$|O^i_{A_U,b'}| = (|U|/2+c'|U|^{3/4})^{l-i}(|U|/2+c''|U|^{3/4})^i = (|U|/2)^l\left(1+\frac{2c'}{|U|^{1/4}}\right)^{l-i}\left(1+\frac{2c''}{|U|^{1/4}}\right)^i$$

נבחר $K=(|U|/2)^l$ ונקבל שהתלות ב b' היא בגורם:

$$I=\left(1+\frac{2c'}{|U|^{1/4}}\right)^{l-i}\left(1+\frac{2c''}{|U|^{1/4}}\right)^i$$

אבל מכיוון ש $|U|^{1/4}\approx n^{1/8}$ ו $l\le n^{1/100}$ נקבל ש $I=1+o(n^{-1/10})$

סוף הוכחת הטענה.

נשתמש בשתי הטענות האחרונות על מנת להמשיך לפתח את נוסחאות 2.1,2.2 שהיחס ביניהם הוא γ^i_U. מכאן ועד סוף ההוכחה ישמש הסימון $\approx$ לתאור של שויון עד כדי פקטור של $1+O(n^{-1/10})$.

אם נזכור ש $P_{B_N/U}(b')$ היא פונקצית התפלגות אחידה, ולכן החלק הא־נורמלי בה זניח. ונשתמש בטענה 2.2 נקבל כמסקנה ש:

$$\sum_{b'usual} P_{B_N/U}(b')|O^i_{A_U,b'}|\approx K$$

שמוש בטענה 2.1 לגבי נוסחאות 2.1,2.2 והצבת המסקנה האחרונה נותן:

$$2.3 \quad \gamma^i_U = \frac{|O^i_{A_{/U},B}|}{|O^i_{A_U,B_N}|} \approx \frac{|B|\sum_{b'usual} P_{B/U}(b')|O^i_{A_{/U},b'}|}{|B_N|\sum_{b'usual} P_{B_N/U}(b')|O^i_{A_U,b'}|} \approx \beta\left(\sum_{b'usual} P_{B/U}(b')\frac{|O^i_{A_{/U},b'}|}{K}\right)$$

נגדיר את α_U להיות צפיפות המסלולים ב U $\alpha_U=|A_{/U}|/|A_U|$

שימוש בהגדרות, בטענה 2.2 , בכך ש $|O^i_{a,B_U}|$ קבוע ב a ובכך שכמעט כל הצביעות b' המשתתפות ב O^i_{a,B_U} הן נורמליות, נותן:

$$\sum_{b'usual} \frac{|O^i_{A_{/U},b'}|}{K} \approx \frac{\alpha_U * |B_U| * K}{K} = |B_U| * \alpha_U$$

כלומר, אם נתבונן באגף ימין של נוסחה 2.3 נראה שהביטויים $P_{B/U}(b')$ ממושקלים בסכום, וסכום כל המשקולות $\approx |B_U|\alpha_U$. מכיון שכל המשקולות נמצאות בקטע $[0,\ 1+O(n^{-1/10})]$ הרי שמתקבל שעד כדי פקטור של $1+O(n^{-1/10})$ מתקיים:

$$2.4 \quad \beta\sum_{Y_1} P_{B/U}(b') \le \gamma^i_U \le \beta\sum_{Y_2} P_{B/U}(b')$$

כאשר Y_1 היא קבוצת $|B_U|\alpha_U$ הערכים הקטנים ביותר של $P_{B/U}(b')$ ואילו Y_2 היא קבוצת $|B_U|\alpha_U$ הערכים הגדולים ביותר של $P_{B/U}(b')$.

בשלב זה היינו רוצים להשתמש בלמה 2.1 כדי לקבל חסמים לשני צידי אי־השויון האחרון, אלה שלשם כך צריך לדעת שהאינפורמציה $I(P_{B/U})$ נמוכה. זה איננו נכון באופן כללי אלה רק בממוצע (עבור U מסוימת תתכן אנפורמציה גבוהה). לכן נרצה לחסום את $\overline{\gamma^i_U}$. לשם כך נגדיר מידת הסתברות חדשה p על קבוצת כל הזוגות $\{(b',U)\ /\ b'\in B_U\}$ ע"י: $p(b',U)=P_{B/U}(b')/N_U$

כאשר N_U מסמן את מספר האפשרויות לבחירת U. נקבל:

$$\overline{\gamma_U^i} \le \overline{\beta\sum P_{B/U}(b')} \le \beta\sum p(b',U)$$

כאשר הסכום הראשון לקוח על $|B_U|\alpha_U$ האיברים הגדולים ביותר לכל U והסכום השני לקוח על $\alpha|B_U|N_U$ האיברים הגדולים ביותר $p(b',U)$. אי השויון השמאלי הוא פשוט החלק הימני של אי השויון 2.4. אי השויון הימני נובע מכך ש $\overline{\alpha_U}=\alpha$ (לפי הגדרה) ומכך ש $p(b',U)$ כולל את כל ההתפלגויות $P_{B/U}$, ובעצם באגף ימין אנו מאפשרים לקחת את $\alpha|B_U|N_U$ האיברים הגדולים בכלל ואילו באגף שמאל אנו לוקחים מספר קבוע של איברים מכל התפלגות (ובסך הכל אותו מספר איברים). באותו אופן מקבלים חסם תחתון על $\overline{\gamma_U^i}$, כלומר:

$$\beta\sum p(b',U) \le \overline{\gamma_U^i} \le \beta\sum p(b',U) \qquad 2.5$$

כאשר הסכום הראשון לקוח על $\alpha|B_U|N_U$ האיברים הקטנים ביותר והשני על $\alpha|B_U|N_U$ האיברים הגדולים ביותר.

<u>טענה 2.3:</u>

$$I(p(b',U)) \le n^{-1/2}$$

<u>הוכחה:</u>

לפי הגדרה $I(p(b',U))=\overline{I(P_{B/U})}$

האנטרופיה $H(P_B)$ מקיימת: $H(P_B)=\log_2|B| \ge |B_N|-n^{-1/100} = n-n^{-1/100}$

אם נתיחס אל P_B כהתפלגות רב מימדית ש $P_{B/U}$ היא היטל שלה על $|U|$ מימדים, הרי שתורת האנפורמציה אומרת ש:

$$\overline{H(P_{B/U})} \ge \frac{H(P_B)|U|}{n}$$

לכן:

$$\overline{H(P_{B/U})} \ge |U| - \frac{|U|}{n^{99/100}}$$

כלומר: $\overline{I(P_{B/U})} \le |U| n^{-99/100} = n^{-1/2}$

סוף הוכחת הטענה.

טענה 2.3 מאפשרת להשתמש בלמה 2.1 לגבי אי שויון 2.5 ולקבל:

$$\alpha\beta(1-O(n^{-1/10})) \le \alpha\beta\left(1-\sqrt{\frac{4n^{-1/2}}{\alpha}}\right) \le \overline{\gamma_U^i} \le \alpha\beta\left(1+\sqrt{\frac{4n^{-1/2}}{\alpha}}\right) \le \alpha\beta(1+O(n^{-1/10}))$$

וזה מה שצריך להוכיח כי $\gamma^i = \overline{\gamma_U^i}$.

<u>הערה:</u>

ההגבלה $\alpha \le 1/100$ הנדרשת בלמה 2.1 אינה מהותית (כפי שהערנו בסוף סעיף ב.1). ברור שאם המשפט נכון ל $\alpha \le 1/100$ הוא נכון גם ל α ים גדולים יותר.

סוף הוכחת למה 2.2

המסקנה הבאה נובעת מיידית מכך ש $|O_N^i|$ קבועה לכל i.

<u>מסקנה 2.1:</u>

בתנאי למה 2.2, עד כדי פקטור של $1+O(n^{-1/10})$, $|O_{AB}^i|$ בלתי תלוי ב i.

ב.3: ההתנהגות של קבוצה גדולה של צביעות, תחת הטלה.

הלמה הבאה קובעת שאם מתחילים עם קבוצת צביעות B בעלת צפיפות גבוהה מספיק ב B_N, ובוחנים את תת הקבוצה של כל הצביעות ב B, שמסכימות עם צביעה מקרית I, על תת קבוצה קטנה U, מקבלים בהסתברות גבוהה שצפיפות תת קבוצה זאת ב B_{N-U} קרובה לזאת של B ב B_N. משמעות הלמה היא שאפשר להניח שקבוצה מקרית קטנה צבועה בצביעה מקרית, מבלי "לאבד" צפיפות. בלמה דומה לזאת נעשה שמוש ב [KW] על מנת להוכיח חסם דטרמיניסטי ל R^m_{stc}. שם נצבעה קבוצה מקרית בצביעה מקרית כחלק מטכניקת "קיצוץ המסלולים" והלמה נועדה להבטיח שצפיפות קבוצת החתכים אינה קטנה בהרבה. אצלנו, הלמה מהווה בעיקר הכנה לזאת שאחריה המכלילה אותה.

<u>למה 2.3:</u>

תהי $B\subset B_N$ עבורה $\beta\equiv|B|/|B_N|\geq 2^{-n^{1/10}}$ נבחר אקראית בהתפלגות אחידה $U\subset N-\{s,t\}$ כאשר $|U|=n^{1/2}$. נצבע את U בצביעה מקרית I שתבחר בהתפלגות אחידה. נסמן ב $B_{/I}$ את קבוצת כל הצביעות ב B המסכימות עם I על U . אזי בהסתברות של לפחות $1-O(n^{-1/10})$ מתקיים:

$$\beta|B_{N-U}|(1-n^{-1/10})\leq|B_{/I}|\leq\beta|B_{N-U}|(1+n^{-1/10})$$

<u>הוכחה:</u>

כפי שהגדרנו במדויק בלמה 2.2 (ע"מ 23) נגדיר גם כאן את P_B להיות מדת הסתברות על B_N המפולגת אחיד על B, ואת $P_{B/U}$ להיות מדת הסתברות על B_U שהיא הטלה של P_B. כמו בלמה 2.2 נסמן גם כאן ב N_U את מספר האפשרויות לבחירת U ונגדיר מדת הסתברות p על מרחב ההסתברות $\{(b,U)\ /\ b\in B_U\}$ ע"י:

$$p(b,U)=\frac{P_{B/U}(b)}{N_U}$$

טענה 2.3 קבעה שהאנפורמציה של מדת הסתברות זאת נמוכה. כאן הגדלים של B ו U שונים

במעט אבל בדיוק אותה הוכחה נותנת: $I(p(b,U)) = \overline{I(P_{B/U})} \le n^{1/2-9/10} = n^{-4/10} \overset{def}{=} \theta$

עובדה שנזדקק לה לשם הפעלת למה 2.1. (גם כאן מסמן הקו העליון מיצוע)

צביעה I לא תקיים את תנאי הלמה שלנו אם מתקיים אחד משני התנאים הבאים:

1. $p(I,U) \ge \frac{1}{N_U|B_U|}(1+n^{-1/10})$
2. $p(I,U) \le \frac{1}{N_U|B_U|}(1-n^{-1/10})$

נסמן ב ω_1 את ההסתברות לקיום תנאי 1 וב ω_2 את ההסתברות לקיום תנאי 2.

יש $\omega_1 N_U|B_U|$ איברים $p(I,U)$ המקיימים את תנאי 1. לפי שכולם מקימים את תנאי 1 סכומם

גדול שווה מ $\omega_1(1+n^{-1/10})$, אבל לפי למה 2.1 סכומם קטן שווה מ:

$$\omega_1\left(1+\sqrt{\frac{4\theta}{\omega_1}}\right)$$

(על השמוש בלמה 2.1 ראה הערה בסוף ההוכחה).

לכן מתקבל: $n^{-1/10} \le \sqrt{\frac{4\theta}{\omega_1}}$

ובצורה דומה: $n^{-1/10} \le \sqrt{\frac{4\theta}{\omega_2}}$

לכן: $\omega_1+\omega_2 \le 8\theta * n^{2/10} < n^{-1/10}$

סוף הוכחת למה 2.3

<u>הערה:</u>

לפי תנאי למה 2.1 השימוש בה בלתי אפשרי אם $\sqrt{\frac{4\theta}{\omega}} \ge 1/10$ אבל אז מתקיים החסם

$\omega_1+\omega_2<n^{-1/10}$ בצורה טריויאלית. השמוש בלמה בלתי אפשרי גם אם $\omega_1>1/100$ או

$\omega_2>1/100$ אבל במקרה כזה (ב.ה.כ. $\omega_1>1/100$) נקטין את ω_1 מלאכותית ל $1/100$, ע"י התבוננות בתת קבוצה כלשהי של המאורעות (I,U) המקימים את תנאי 1. ונקבל עבור קבוצה זאת סתירה ללמה 2.1.

ב.4: עוד על התנהגות קבוצות גדולות של צביעות.

הלמה הבאה היא הכללה של הלמה הקודמת. גם למה זאת קובעת שבמקרים מסוימים אפשר להניח שתת־קבוצה קטנה U צבועה בצביעה מקרית I, מבלי "לאבד" צפיפות. אלה שבלמה זאת נתונה במקום קבוצת צביעות B (כפי שהיה בלמה הקודמת), משפחה של קבוצות צביעות $\{B_e\}$, שבה קבוצת צביעות B_e לכל עצם $e\in E$. העצמים שבטענת הלמה יהיו תתי־קבוצות קטנות. הלמה אומרת שתחת תנאים מסוימים על הגדלים, יהיה בהסתברות לא קטנה עצם $e\in E$ שכולו נמצא ב U וצבוע בצבע מסוים תחת I, ובנוסף לכך אם נבחן את קבוצת כל הצביעות ב B_e המסכימות עם I על U נקבל שצפיפות קבוצה זאת קרובה לצפיפותה המקורית של B_e. בשמושים שנעשה בלמה תהיה קבוצת העצמים אותה נבחן קבוצה של מסלולים, לכל מסלול תתאים קבוצה שונה של צביעות (בנגוד למצב ב [KW] ובלמה 2.3), ונרצה שבהסתברות לא קטנה יהיה מסלול מסוים שכולו צבוע בצבע מסוים, ובנוסף לכך הקבוצה B_e לא "תאבד" צפיפות, תחת ההנחה ש U צבועה ב I.

בסימונים בהם נשתמש תקרא קבוצת הקודקודים שלנו M (לשם הכלליות, ולשם מניעת בלבול סימונים בהמשך). ב E_M נסמן את קבוצת כל תתי הקבוצות של M שגודלן q, כאשר q קבוע כלשהו המקיים $q<m^{1/100}$ כאשר $m=|M|$.

<u>למה 2.4:</u>

תהי $E\subset E_M$ שצפיפותה ב E_M מקיימת: $\delta\equiv|E|/|E_M| > m^{-1/100}$

לכל $e\in E$ תהי $B_e\subset B_{M-e}$ קבוצת דו־צביעות של M-e שצפיפותה מקימת:

$$\beta_e\equiv|B_e|/|B_{M-e}| > 2^{-m^{1/10}}$$

נבחר אקראית בהתפלגות אחידה קבוצה $U\subset M$ שגודלה $|U|=m^{1/2}$ וצביעה I שלה. נסמן ב U_s,U_t את החלקים ב U שצבועים s ו t בהתאמה. נסמן לכל e ב $B_{e/I}$ את קבוצת הצביעות ב B_e המסכימות עם I על U-e.

אזי בהסתברות של לפחות 1/4 יש $e\in E$ המקיים:

1. $e\subset U_t$
2. $\beta_e|B_{M-U}|(1-m^{-1/10}) \le |B_{e/I}| \le \beta_e|B_{M-U}|(1+m^{-1/10})$

הוכחה:

הלמה נראית קלה להוכחה מכיון שדי פשוט להראות שבהסתברות גבוהה מאוד קיים e המקיים את תנאי 1, ואילו תנאי 2 מתקיים בהסתברות גבוהה לכל e (למה 2.3). טיעון זה אינו מספיק. הבעיה היא בתלות שבין בחירת e לבין קיום תנאי 2. כדי להפעיל את הטיעון בצורה מדויקת היינו צריכים לאמר בדיוק כיצד נבחר e מסוים המקיים את תנאי 1, ואז יתכן שעצם העובדה שבחרנו e זה מורידה בהרבה את ההסתברות לקיום תנאי 2. ואכן, אפשר לבנות דוגמאות בהן הטיעון נכשל.

כדי להוכיח את הלמה ניתן אלגוריתם הסתברותי לבחירת e מסוים המקיים את תנאי 1, עבורו תהיה ההסתברות לקיום תנאי 2 גבוהה. כדי להפעיל אלגוריתם זה נזדקק לעידון של מרחב ההסתברות שלנו:

ההסתברות לכך ש $|U_s|<|U|/4$ או $|U_t|<|U|/4$ קטנה אקספוננציאלית, לכן נוכל להתעלם מאפשרות זאת. נבחר את U,I בצורה הבאה:

ראשית נבחר את $|U_s|,|U_t|$, אחר כך נבחר את U_t כקבוצה מסודרת (עם חזרות) ולבסוף את U_s כקבוצה ללא מסודרת. נחלק את $\sqrt{m}/4$ האיברים הראשונים ב U_t ל k קבוצות של q איברים, לפי הסדר, (כאשר $k=\sqrt{m}/4q$). נקרא לקבוצות אלה $V_1,\dots,V_k$.

מידיעת δ ו k רואים שבהסתברות גבוהה אקספוננציאלית קיים i עבורו $V_i\in E$ לכן נניח שקיים i כזה. נסמן את ה i הראשון המקיים $V_i\in E$ ב i_0, ונקבע $e=V_{i_0}$. i_0 הוא משתנה מקרי. נסמן ב i' את האינדקס הראשון עבורו $Pr(i_0\le i') > 1/2$. נסמן ב f את הסדר על הקבוצה U_t. לכל שלשה (U_s,U_t,f) התאמנו זוג (e,i_0). לכל זוג (e,i_0) נסמן ב $T(e,i_0)$ את התמונה

ההפוכה שלו (קבוצת כל השלשות המתאימות לו). אם בחרנו זוג (e,i) הרי שמתקיים תנאי 1.

נראה שבהסתברות גבוהה מתקיים גם תנאי 2.

טענה 2.4:

אם בחרנו זוג (e,i) המקיים $i \le i'$ אזי $B_{e/I}$ מקיים את תנאי 2 בהסתברות גבוהה מ $1/2$.

הוכחה:

ההוכחה תשתמש בלמה 2.3 ותסתמך על כך ש $T(e,i)$ היא קבוצה גדולה. נבדוק ראשית מה גודלה של $T(e,i)$, כאשר המונח גודל מתייחס למידת ההסתברות תחת הבחירה שתארנו על מרחב השלשות $\{(U_s,U_t,f)\}$.

$T(e,i)$ מכילה את כל השלשות (U_s,U_t,f) עבורן מתקיים:

1. $e=V_i$

2. $V_j \in E$ עבורו $j<i$ אין

ההסתברות על $\{(U_s,U_t,f)\}$ לאי קיום תנאי 2 היא:

$$Pr(\exists j<i,\ V_j \in E) = Pr(i_0<i) \le Pr(i_0<i') \le 1/2$$

לכן מידת $T(e,i)$ היא לפחות חצי ממידת השלשות (U_s,U_t,f) עבורן $e=V_i$ (כי מאורעות 1 ו 2 בלתי תלוים). לכל שלשה מתאים גם הזוג הנוצר (U,I). עבור e מסוים נתבונן בכל הזוגות (U,I) עבורם $e \subset U_t$. נקרא לזוג כזה "טוב" אם מתקיים תנאי 2 (של הלמה):

$$\beta_e|B_{M-U}|(1-m^{-1/10}) \le |B_{e/I}| \le \beta_e|B_{M-U}|(1+m^{-1/10})$$ ואחרת יקרא הזוג "רע".

לפי למה 2.3 אחוז הזוגות הרעים $< O(m^{-1/10})$. מכיון שלכל זוג עבורו $e \subset U_t$ מתאימה קבוצת שלשות, (עבורה $e=V_i$), בעלת מידה קבועה, הרי שמתקבל שמידת השלשות ה"רעות" (שלשות להן מתאים זוג רע) מבין כל השלשות, עבורן $e=V_i$, קטנה מ $O(m^{-1/10})$. מכיון ש $T(e,i)$ כוללת לפחות חצי ממידת השלשות, עבורן $e=V_i$, הרי שגם אם כל השלשות הרעות נמצאות ב

$T(e,i)$, ההסתברות לשלשה ב $T(e,i)$ להיות רעה קטנה מ $2*O(m^{-1/10})$, וזה קטן מ $1/2$. לכן ההסתברות לקיום תנאי 2 של הלמה גדולה מ $1/2$.

סוף הוכחת הטענה.

למה 2.4 נובעת מטענה 2.4 ומכך שהזוג (e,i_0) מקיים $i_0 \le i'$ בהסתברות גדולה מ $1/2$ (לפי הגדרת i'). בסך הכל מתקבל שתנאי 1 מתקיים תמיד ותנאי 2 בהסתברות גבוה מ $1/2*1/2=1/4$.

סוף הוכחת למה 2.4

<u>הערה:</u>

פעמיים במהלך ההוכחה הזנחנו הסתברויות קטנות אקספוננציאלית, אבל הלמה נכונה כלשונה כי בטענה 2.4 קבלנו למעשה יותר ממה שדרשנו.

<u>הערה:</u>

את למה 2.3 הוכחנו עבור קבוצות U שגודלן $\sqrt{n}$, לשם הפשטות. למעשה נכונה הלמה באותו אופן לתחום רחב של גדלי U אפשרים. בשימוש שעשינו כאן בלמה, גודלה של U אינו במדויק $\sqrt{n}$, אבל הוא מקיים $|U|/\sqrt{n}=1+o(1)$. גם את למה 2.4 הוכחנו עבור $|U|=\sqrt{m}$, לשם הפשטות. בעתיד נשתמש בשתי הלמות עבור קבוצות U שגודלן קרוב ל $\sqrt{n}$ או $\sqrt{m}$ עד כדי כך, שמעט מאוד אנשים יכעסו על השמוש הלא מדויק.

פרק ג: סיבוכיות התקשורת ההסתברותית של היחס הבוליאני המונוטוני R^m_{stc}.

נחזור כעת לעסוק במודל ההסתברותי של סיבוכיות תקשורת, וביחסים בוליאנים, (שהם הבעיות המקשרות אותנו לשאלות לגבי עומק מעגלים). בסעיף א.4 הצגנו את הפונקציה הבוליאנית stc, ואת בעיות התקשורת המונוטוניות R^m_{stc} ו $R^m_{stc(l)}$. הזכרנו שעבור בעיות אלה קיים חסם תחתון הדוק במודל הדטרמיניסטי (משפט 1.5 [KW]). באופן הסטורי הוכחה זאת היא הראשונה שעשתה שימוש בסיבוכיות תקשורת לשם קבלת תוצאות לגבי עומק של מעגלים בוליאנים (במשפט 1.1), והראשונה שנתנה פער בין מחלקות החישוב המונוטוני NC^m_1 ו P^m. נוסיף לכך את פשטותה וחשיבותה של הפונקציה stc ונקבל את המוטיבציה לנתח את התנהגותם ההסתברותית של R^m_{stc} ו $R^m_{stc(l)}$. בפרק זה נוכיח הכללה הסתברותית של משפט 1.5 ונקבל ש:

1) $C_\varepsilon(R^m_{stc(l)})=\Omega(\log n*\log l)$ עבור $l=n^{1/100}$

2) $C_\varepsilon(R^m_{stc})=\Omega(\log^2 n)$ ולכן

נעיר עוד שמשפט זה מהווה דוגמא ראשונה לפער קיים בין סיבוכיות תקשורת הסתברותית, לבין סיבוכיות תקשורת לא דטרמיניסטית. לגבי פונקציות עדיין לא ידוע פער דומה.

אך כי ההוכחה שניתן כאן לחסם ההסתברתי מסובכת בהרבה, נקודת המוצא של הוכחה זאת היא הוכחת החסם הדטרמיניסטי שניתנה ב [KW]. בקווים כללים יש דמיון בין מבנה ההוכחה לבין מבנה הוכחת החסם הדטרמיניסטי, לכן נאמר כאן מספר מילים על הוכחה זאת:

אנו מעונינים בפרוטוקולי תקשורת דטרמיניסטים הפותרים את הבעיה R^m_{stc} במלואה, אולם נתבונן גם בפרוטוקולי תקשורת הפותרים צמצומים של הבעיה כולה. הבעיה $R^m_{stc(l)}$ היא צמצום

מסוג אחד של הבעיה הכללית, אנחנו נתעניין בפרוטוקולים הפותרים את $R^m_{stc(l)}$ על תתי קבוצות $A\subset A_N$ ו $B\subset B_N$. נאמר שפרוטוקול P פותר בעית R^m_{stc} עם פרמטים (n,l,α,β), אם עבור אורך מסלול l וגודל קבוצת קודקודים n, קיימת קבוצה $A\subset A_N$ עבורה $|A|=\alpha|A_N|$ וקבוצה $B\subset B_N$ עבורה $|B|=\beta|B_N|$, כך שאם שחקן I מקבל קלט $a\in A$ ושחקן II מקבל קלט $b\in B$ הפרוטוקול P נותן תשובה $P(a,b)$ שהיא פתרון נכון של R^m_{stc} עבור זוג קלטים זה.

במאמר מוסגר נאמר, שהסיבה להתבוננות בצמצומים כאלה הוא שכל פרוטוקול תקשורת אפשר לתאר כעץ שבשורשו "יושבת" בעית התקשורת המתאימה ובכל קודקוד שלו "יושבת" בעיה שהיא צמצום של הבעיה כולה. לפרוטוקול דטרמיניסטי הפותר את $R^m_{stc(l)}$ מתאים עץ צימצומים שבשורשו הפרמטרים $(n,l,1,1)$ ובקודקודיו האחרים פרמטרים (n,l,α,β) כאשר $\alpha,\beta\le 1$.

נסמן ב $C(n,l,\alpha,\beta)$ את סיבוכיות התקשורת המינימלית של פרוטוקול P הפותר בעית R^m_{stc} עם פרמטרים (n,l,α,β). משפט 1.5 נובע מ 3 טענות בסיסיות:

1. לכל $\beta>0$, $l<n^{1/10}$ וקבוע $\varepsilon<1$ $\quad C(n,l,n^{-\varepsilon},\beta)>0$

2. לכל n,l,α,β $\quad C(n,l,\alpha,\beta)\ge C(n,l,\alpha/2,\beta/2)+1 \Leftarrow C(n,l,\alpha,\beta)>0$

3. יש קבוע ε עבורו אם $l\le n^{\varepsilon}$, $\alpha\ge n^{-\varepsilon}$, $\beta\ge 2^{-n^{\varepsilon}}$ מתקיים:

$$C(n,l,\alpha,\beta)\ge C(n-\sqrt{n},l/2,\sqrt{\alpha}/4,\beta/2)$$

הטענה הראשונה אומרת שאם α גדול מספיק סיבוכיות התקשורת אינה 0. הטענה השניה מראה שכאשר α קטן פי 2 סיבוכיות התקשורת קטנה ב־1 לפחות. הטענה השלישית מאפשרת "להגדיל" את α.

שתי הטענות הראשונות פשוטות ביותר: טענה 1 נובעת מכך שאם נניח בשלילה שסיבוכיות התקשורת היא 0 הרי שהתשובה כבר ידועה לכל זוג קלטים a,b ב A,B. מכיון שהתשובה חייבת להיות צלע במסלול הרי שלכל המסלולים ב A צלע משותפת ולכן A אינה יכולה להיות

גדולה מידי. טענה 2 נובעת מהתבוננות בצעד הראשון של פרוטוקול הפותר את R^m_{stc} עם פרמטרים (n,l,α,β). אם בצעד זה מעביר שחקן I ביט מידע לשחקן II , הרי שהוא מחלק את קבוצת הקלטים שלו לשתי קבוצות ואומר באיזו מהן נמצא הקלט a (ביט מידע). המשך הפרוטוקול בענף המתאים לגדולה שבין שתי קבוצות אלה פותר את R^m_{stc} עם פרמטרים $(n,l,\alpha/2,\beta)$ ולכן גם עם פרמטרים $(n,l,\alpha/2,\beta/2)$. במקרה שבצעד הראשון משחק שחקן II נקבל אותה תוצאה בצורה דומה.

הפעלה חוזרת של טענה 2 $O(\log n)$ פעמים תוך שמוש בטענה 1 נותנת את החסם הטריואלי:

$$c(n,l,1,1) \geq c(n,l,n^{-\varepsilon},n^{-\varepsilon})+O(\log n) \geq O(\log n)$$

כלומר, בכל שלב α,β קטנים בפקטור 2 עד אשר $\alpha<n^{-\varepsilon}$.

טענה 3, שהיא הלמה המרכזית בהוכחת משפט 1.5, מאפשרת להגיע לחסם של $\Omega(\log^2 n)$ על ידי "הגדלת" ערכו של α בכל פעם שהוא מתקרב ל $n^{-\varepsilon}$, במחיר של הקטנה פי 2 של אורך המסלול l. בין כל שתי "הפעלות" של טענה 3 עוברים $O(\log n)$ צעדי פרוטוקול. בסך הכל אפשר להפעיל טענה זאת $O(\log n)$ פעמים עד שאורך המסלול הוא צלע בודדת, ומכאן החסם $\Omega(\log^2 n)$.

ניתן כאן קווים עקריים להוכחת הלמה המרכזית:

בהוכחת הלמה המרכזית (טענה 3) לוקחים פרוטוקול לבעית R^m_{stc} עם פרמטרים (n,l,α,β) וממנו יוצרים פרוטוקול עם פרמטרים $(n-\sqrt{n},l/2,\sqrt{\alpha}/4,\beta/2)$. דרך ההוכחה היא לבחור מקרית קבוצה $U\subset N$, עם $|U|=\sqrt{n}$, וצביעה שלה I, (כלומר, מחליטים על הצביעה של $\sqrt{n}$ קודקודים). עכשיו ניתן להגדיר שני פרוטוקולים חדשים, פרוטוקול ימני ופרוטוקול שמאלי, שכל אחד מהם הוא למעשה הפרוטוקול המקורי המופעל על תתי קבוצות של קבוצות הקלטים המקוריות A,B.

וכך יוגדרו הפרוטוקולים: כל מסלול נחצה לשניים, בדיוק באמצעו. הפרוטוקול השמאלי יקבל קבוצות קלטים A_L,B_L כאשר B_L היא קבוצת כל הצביעות ב B המסכימות עם I על U , ואילו A_L היא קבוצת כל המסלולים ב A שחציים הימני צבוע כולו, על ידי I, בצבע t, ושבחצים השמאלי

אך קודקוד אינו צבוע (אינו ב U). עבור זוג קלטים a,b $b\in B_L$ $a\in A_L$, חייב הפרוטוקול לתת תשובה שהיא בחצי השמאלי ולכן קל לייצר ממנו פרוטוקול הפועל למסלולים בגודל $l/2$. באותה צורה מוגדר הפרוטוקול הימני ומסתבר, שבהסתברות גבוהה מ 0, לפחות עבור אחד משני הפרוטוקולים קבוצות הקלטים גדולות מספיק והוא מהוה פתרון ל R^m_{stc} עם פרמטרים $(n-\sqrt{n},l/2,\sqrt{\alpha}/4,\beta/2)$, כמובטח.

נעבור עתה לעסוק במקרה ההסתברותי. מקרה זה מתבטא גם בכך שהפרוטוקול הוא הסתברותי וגם בכך שמאפשרים בו טעויות. פרוטוקול הסתברותי שטועה בהסתברות ε אפשר לראות כקומבינציה קמורה של k פרוטוקולים דטרמיניסטים, כך שעבור כל זוג קלטים (a,b), לפחות $(1-\varepsilon)k$ מבין פרוטוקולים אלה נותנים תשובה נכונה. מכאן ברור שאם נתבונן בקבוצה חלקית כלשהי של קלטים $W\subset A_N*B_N$, ימצא בין הפרוטוקולים לפחות אחד שנותן תשובה נכונה עבור לפחות $(1-\varepsilon)|W|$ קלטים ב W. אנחנו נעסוק בפרוטרקול דטרמיניסטי זה ונוכיח חסם תחתון עבורו. רק בסיום ההוכחה כולה נראה כיצד לעבור במדויק מחסם זה לחסם עבור פרוטוקול הסתברותי.

חסר טעם יהיה לקחת קבוצת קלטים $W=A_N*B_N$ מכיון שקל מאוד לתת פרוטוקול דטרמיניסטי מהיר מאוד שצודק על אחוז גבוה מתוך קבוצה זאת (כל צלע במסלול היא דו־צבועה עבור חצי מהצביעות, לכן אפילו פרוטוקול שתשובתו היא תמיד הצלע הראשונה במסלול, צודק על חצי מבין הקלטים A_N*B_N). באופן אינטואיטיבי ברור שקשה יהיה למצוא צלע דו־צבועה אם יש מעט צלעות כאלה, לכן נבחר את קבוצת הקלטים האפשריים שלנו כקבוצת הקלטים בהם יש צלע דו־צבועה יחידה. כלומר $W=O_N$.

ברצוננו, אם כן, לתת חסם תחתון לפרוטוקול דטרמיניסטי, הפותר בעית $R^m_{stc(l)}$ על אחוז גבוה של זוגות קלטים, מתוך הקבוצה O_N. לכן נגדיר סוג חדש של צמצומים לבעיה R^m_{stc}, שיתיחס

לפרמטר חדש γ, שהוא אחוז הזוגות האלה:

נאמר שפרוטוקול P פותר בעיית R^m_{stc} עם פרמטרים $(n,l,\alpha,\beta,\gamma)$, אם עבור אורך מסלול l וגודל קבוצת קודקודים n קימת קבוצה $A\subset A_N$ עבורה $|A|=\alpha|A_N|$, וקבוצה $B\subset B_N$ עבורה $|B|=\beta|B_N|$, כך שקימים $\gamma|O_{AB}|$ זוגות קלטים $(a,b)\in O_{AB}$ עבורם נותן הפרוטוקול P תשובה $P(a,b)$ שהיא פתרון נכון של R^m_{stc}.

נסמן ב $C(n,l,\alpha,\beta,\gamma)$ את סיבוכיות התקשורת המינימלית של פרוטוקול P הפותר בעית R^m_{stc} עם פרמטרים $(n,l,\alpha,\beta,\gamma)$.

בהוכחת משפט 1.5 הפרמטרים החשובים, שעל גודלם משתדלים לשמור, הם α ו l. הלמה המרכזית טוענת שאפשר להגדיל את α לכמעט $\sqrt{\alpha}$ במחיר של הקטנת l בפקטור 2. הפרמטרים החשובים בהוכחה שלנו, שעל גודלם נשתדל לשמוור, יהיו α ו $\gamma^{100}*l$. הלמה שתחליף את הלמה המרכזית תטען שאפשר להגדיל את α לכמעט $\sqrt{\alpha}$ במחיר של הקטנת $\gamma^{100}*l$ בפקטור מסוים. הסיבה להחזקה דוקא של $\gamma^{100}*l$ תתבהר בהמשך. במספר מקומות במהלך הוכחה נחזיק גם את גודלו של הפרמטר $\alpha*\gamma$, אבל לא מכיוון שפרמטר זה יהיה חשוב בפני עצמו, אלה מכיון ששמירה עליו תשמור על ערכו של α וזאת משום שערכו של γ יהיה בדרך כלל קרוב בהרבה ל 1 מאשר ערכו של α.

זוהי, אם כן, הלמה המרכזית בהוכחה. אולם למה זאת תושג רק בעזרת למה מכינה, שבה תעשה עיקר העבודה. הלמה המכינה תטען (תחת מספר תנאי גודל) שבהנתן פרוטוקול P עם פרמטרים $(n,l,\alpha,\beta,\gamma)$ מתקימת אחת מבין שתי האפשרויות הבאות:

אפשרות א: אפשר ליצור מ P פרוטוקול אחר שבו α גדל ל $O(\sqrt{\alpha})$, במחיר של הקטנת הפרמטרים β ו $\gamma^{100}*l$ בפקטור קבוע.

אפשרות ב: אפשר ליצור מ P פרוטוקול אחר שבו $\gamma^{100}*l$ גדל בפקטור מסוים, במחיר של

הקטנת הפרמטר $\alpha*\gamma$ בפקטור קבוע והפרמטר β אך במעט.

אפשר להבחין שאפשרות א נותנת למעשה את הלמה המרכזית, אבל יתכן שדוקא אפשרות ב מתקיימת. הלמה המרכזית תנבע מהפעלה חוזרת של אפשרות ב שוב ושוב, עד שהפרמטר γ גדול מאוד, ואז חייבת להתקיים אפשרות א. אפשרות א היא, אגב, הפשוטה יותר להוכחה מבין השתיים.

לאחר שנוכיח את הלמה המרכזית נוכיח שתי למות נוספות, שיחליפו את שתי הטענות הראשונות, מהן נובע משפט 1.5, ויתפקדו בצורה דומה. מכיון שכאן משתתף הפרמטר הנוסף γ לא יהיו ההוכחות כה פשוטות.

מבנה ההוכחה יהיה כדלהלן: ראשית נוכיח את הלמה המכינה, אחר כך נוכיח את הלמה המרכזית, בהמשך נראה כיצד מקבלים מהלמה המרכזית חסם על $c(n,l,1,1,1/4)$ ולבסוף נקבל מחסם זה חסם על סיבוכיותו של פרוטוקול הסתברותי לפתרון $R^m_{stc(l)}$.

כל הסימונים אותם הגדרנו בתחילת פרק ב יהיו בתוקף גם בפרק זה. סימון נוסף, שבו כבר השתמשנו בפרק ב, ובו נשתמש גם כאן יהיה הסימון $B_{/I}$: בהנתן קבוצת צביעות $B\subset B_N$, קבוצה חלקית $U\subset N$ וצביעה שלה I, תוגדר $B_{/I}$ להיות קבוצת כל הצביעות ב B המסכימות עם I על U.

בהנתן פרוטוקול P, הפותר צמצום של R^m_{stc}, ופועל על קבוצות קלטים $A\subset A_N, B\subset B_N$, נגדיר את קבוצת ההצלחה של הפרוטוקול ב O_{AB} להיות:

$T=\{(a,b) / (a,b)\in O_{AB}$, (a,b) והפרוטוקול נותן תשובה נכונה על $\}$

האותיות A,B לא יופיעו בסימון T לשם הפשטות.

הפרמטר γ מודד למעשה את "צפיפות ההצלחה": $\gamma=|T|/|O_{AB}|$. ברוח הסימונים מתחילת פרק ב, נגדיר כאן מספר קבוצות הצלחה חלקיות, וצפיפויות הצלחה חלקיות:

לכל i נגדיר:

$$T^i=T\cap O^i_{AB} \quad , \quad \gamma^i=|T^i|/|O^i_{AB}|$$

עבור קבוצות חלקיות $A'\subset A, B'\subset B$ נגדיר:

$$T^i_{A'B'}=T^i\cap O^i_{A'B'} \quad , \quad \gamma^i_{A'B'}=|T^i_{A'B'}|/|O^i_{A'B'}|$$

$$T_{A'B'}=T\cap O_{A'B'} \quad , \quad \gamma_{A'B'}=|T_{A'B'}|/|O_{A'B'}|$$

עבור $B'\subset B$ ו $a\in A$ נגדיר:

$$T^i_{aB'}=T^i\cap O^i_{aB'} \quad , \quad \gamma^i_{aB'}=|T^i_{aB'}|/|O^i_{aB'}|$$

$$T_{aB'}=T\cap O_{aB'} \quad , \quad \gamma_{aB'}=|T_{aB'}|/|O_{aB'}|$$

כמו גם בפרקים האחרים של העבודה, גם כאן יהיו ההוכחות נכונות רק אסימפטוטית, כלומר יתיחסו לפרמטר n גדול מאוד. במהלך הפרק יופיעו קבועים רבים, הן בטענות והן בהוכחותיהן, כמעט אף פעם לא תהיה לקבועים אלה משמעות מיוחדת. מטרת ההוכחות לתת חסמים אסימפטוטים ולא להגיע לקבועים "טובים" ככל האפשר.

ג.1: למה מכינה

לאחר ההקדמה המעט מיגעת, נעבור לחלק המייגע באמת, שהוא הוכחת הלמה המקדימה.

<u>למה 3.1 (למה מקדימה):</u>

יהי P פרוטוקול הפותר בעיית R^m_{stc} עם פרמטרים $(n,l,\alpha,\beta,\gamma)$ המקימים:

$$n^{1/200}<l<n^{1/100}\ ,\ \alpha>n^{-1/1000}\ ,\ \beta>2^{-n^{1/1000}}\ ,\ \gamma^{100}>n^{-\varepsilon}$$

כאשר ε קבוע קטן מאוד (הרבה יותר מהקבועים האחרים כאן). אנחנו נניח $\varepsilon=10^{-6}$.

יהיו $A\subset A_N, B\subset B_N$ קבוצות קלטים המעידות על כך ותהי $T\subset O_{AB}$ קבוצת ההצלחה של הפרוטוקול.

אזי מתקיימת לפחות אחת מבין שתי האפשרויות הבאות:

אפשרות א:

מ P אפשר לייצר פרוטוקול $\tilde{P}$ (בעל סיבוכיות תקשורת קטנה או שוה לזאת של P), הפותר בעיית R^m_{stc} עם פרמטרים $(\tilde{n},\tilde{l},\tilde{\alpha},\tilde{\beta},\tilde{\gamma})$ המקימים: $\tilde{n}=n-\sqrt{n}\ ,\ \tilde{l}\le l\ ,\ \tilde{\alpha}>k_\alpha\sqrt{\alpha}\ ,\ \tilde{\beta}>k_\beta\beta\ ,\tilde{\gamma}^{100}\tilde{l}>k_\gamma\gamma^{100}l$

כאשר $k_\alpha,k_\beta,k_\gamma$ קבועים קטנים גלובלים (לא תלויים בפרמטרים)

(אצלנו נקבל: $k_\alpha=1/25,\ k_\beta=1/2,\ k_\gamma=\frac{1}{3*40^{100}}$).

אפשרות ב:

מ P אפשר לייצר פרוטוקול $\tilde{P}$ (בעל סיבוכיות תקשורת קטנה או שוה לזאת של P), הפותר בעיית R^m_{stc} עם פרמטרים $(\tilde{n},\tilde{l},\tilde{\alpha},\tilde{\beta},\tilde{\gamma})$ המקימים:

$$\tilde{n}=n-\sqrt{n}\ ,\ \tilde{l}\le l\ ,\ \tilde{\alpha}\tilde{\gamma}>k_\alpha'\alpha\gamma\ ,\ \tilde{\beta}>\beta(1-n^{-1/10})\ ,\ \tilde{\gamma}^{100}\tilde{l}>4\gamma^{100}l$$

כאשר k_α' קבוע קטן גלובלי. (אצלנו נקבל $k_\alpha'=1/200$).

יש בחירה של l_L,l_R עבורה:

1. $\gamma_L,\gamma_R \geq \gamma/2$

2. $\gamma_L^{100}l_L,\gamma_R^{100}l_R \geq (1/2-o(1))\gamma^{100}l$

<u>הוכחה:</u>

סעיף 1 בטענה נובע מסעיף 2 ומכך ש $l_L,l_R<l$. נוכיח את סעיף 2:

ממסקנה 2.1 והגדרות $\gamma,\gamma_L,\gamma_R,\gamma^i$ נובע:

$$\gamma=\left(\sum_{i=1}^{l}\gamma^i/l\right)(1+O(n^{-1/10}))$$

$$\gamma_L=\left(\sum_{i=1}^{l_L}\gamma^i/l_L\right)(1+O(n^{-1/10}))$$

$$\gamma_R=\left(\sum_{i=l_L+1}^{l}\gamma^i/l_R\right)(1+O(n^{-1/10}))$$

ולכן:

$$(1+O(n^{-1/10}))\gamma l=\gamma_L l_L+\gamma_R l_R$$

לכן מכך ש $l=l_L+l_R$ ומכך שהפונקציה $f(x)=x^{100}$ קמורה נובע שעד כדי פקטור של $1+O(n^{-1/10})$ מתקיים:

$$\gamma^{100}l \leq \gamma_L^{100}l_L+\gamma_R^{100}l_R$$

מכיון שאם $l_L=0$ $\gamma^{100}l=\gamma_R^{100}l_R$, ואם $l_R=0$ $\gamma^{100}l=\gamma_L^{100}l_L$, הרי שהבעיה היחידה שנותרה היא הבדידות שבחציה ל l_L,l_R. בהסתמך על כך שלפי תנאי הלמה $\gamma^{100}>n^{-1/10^6}$ ו $l>n^{1/200}$ ולכן $\gamma^{100}*l>n^{1/1000}$ ועל כך ש $\gamma^i\leq 1$ לכל i, חישוב אלמנטרי מראה שהיחס $\gamma_L^{100}l_L/\gamma^{100}l$ גדל ב $o(1)$ כאשר מגדילים את l_L ב 1. מכיון שיחס זה, כפי שראינו, מתחיל ב 0 (כש $l_L=0$) וגומר ב 1 (כש $l_L=l$) הרי שבשלב מסוים הוא קרוב ל 1/2 עד כדי $o(1)$.

סוף הוכחת הטענה

מנקודה זאת נקבע את l_L,l_R להיות כאלה המקימים את טענה 3.1.

נגדיר את C_N כקבוצת כל המסלולים באורך l_L על הקבוצה N, המתחילים בקודקוד המיוחד s.

נגדיר את D_N כקבוצת כל המסלולים באורך l_R על הקבוצה N, המסתיימים בקודקוד המיוחד t.

כל מסלול $a\in A_N$ מתפרק לחלק שמאלי $c\in C_N$ ולחלק ימני $d\in D_N$. לציון חיבור מסלולים נשתמש בסימון c*d (כלומר כאן a=c*d).

הגדלים הבאים ילוו אותנו לאורך ההוכחה כולה, ויכונו "האיכות השמאלית" ו "האיכות הימנית" של מסלול $a\in A$:

$$f_L(a)=|\bigcup_{i=1}^{l_L} T^i_{aB}|/|\bigcup_{i=1}^{l_L} O^i_{aB_N}|$$

$$f_R(a)=|\bigcup_{i=l_L+1}^{l} T^i_{aB}|/|\bigcup_{i=l_L+1}^{l} O^i_{aB_N}|$$

מכיון ש $|O^i_{aB_N}|$ בלתי תלויה ב a הרי שהגדלים $f_L(a),f_R(a)$ מודדים את מספרם של "בני הזוג המוצלחים" של המסלול a.

עבור קבוצת מסלולים $\hat{A}\subset A$ נסמן ב $f_L(\hat{A}),f_R(\hat{A})$ את הממוצעים של $f_L(a),f_R(a)$, בהתאמה, על הקבוצה $\hat{A}$. כדי להבהיר את משמעותם של גדלים אלה נתבונן באיכות הכללית של מסלול $a\in A$:

$$f(a)=|\bigcup_{i=1}^{l} T^i_{aB}|/|\bigcup_{i=1}^{l} O^i_{aB_N}|$$

ובאיכות הכללית $f(\hat{A})$ של קבוצה $\hat{A}\subset A$, שהיא מצוע $f(a)$ על קבוצה זאת.

מכיון ש $|O^i_{aB_N}|$ קבועה ב a הרי ש:

$$f(\hat{A})=\sum_{a\in\hat{A}}|\bigcup_{i=1}^{l} T^i_{aB}|/(|\bigcup_{i=1}^{l} O^i_{aB_N}|*|\hat{A}|) = |\bigcup_{i=1}^{l} T^i_{\hat{A}B}|/|\bigcup_{i=1}^{l} O^i_{\hat{A}B_N}| = (|\bigcup_{i=1}^{l} T^i_{\hat{A}B}|/|\bigcup_{i=1}^{l} O^i_{\hat{A}B}|)*(|\bigcup_{i=1}^{l} O^i_{\hat{A}B}|/|\bigcup_{i=1}^{l} O^i_{\hat{A}B_N}|)$$

הגורם הראשון במכפלה $\gamma_{\hat{A}B}\approx$ לפי הגדרה. אם $\hat{A},B$ קבוצות גדולות מספיק, מתקבל לפי למה

2.2 שהגורם השני במכפלה ≈ β כאשר הסימן (≈) מסמן שויון עד כדי פקטור של $(1+O(n^{-1/10}))$. לכן אם $\hat{A},B$ מקיימות תנאי למה 2.2 הרי שמתקיים: 3.1 $f(\hat{A}) \approx \gamma_{\hat{A}B}*\beta$

(<u>הערה:</u> אם $\hat{A}$ אינו עומד בתנאי למה 2.2, נגדיל אותו שרירותית, אבל רק במונה של הגורם השני במכפלה (המקום היחיד שבו משתמשים בלמה) ונקבל באותו אופן שעד כדי פקטור של $(1+O(n^{-1/10}))$:

3.1' $$f(\hat{A}) < \gamma_{\hat{A}B}*\beta*n^{-1/100}*\frac{|A_N|}{|\hat{A}|}$$

גם באי השויון הזה נשתמש בהמשך.)

כלומר, הגודל $f(\hat{A})$ מתנהג כמו צפיפות ההצלחה כפול צפיפות החתכים. $f_L(\hat{A}), f_R(\hat{A})$ מתנהגים באותה צורה, כאשר הפעם מדובר בצפיפות ההצלחה בחלק השמאלי או הימני, בהתאמה. למשל מתקיים באותה צורה, לפי ההגדרות: 3.1a $f_L(A) \approx \gamma_L*\beta$

3.1b $f_R(A) \approx \gamma_R*\beta$

(אם A,B קבוצות גדולות מספיק)

מכיון ש β ישאר קבוע הרי שבאופן כללי $f\sim\gamma$.

אנחנו איננו מעוניינים במסלולים שאיכותם נמוכה, לכן נגדיר את קבוצות המסלולים האיכותיים, בצד הימני ובצד השמאלי: $A_L=\{a\in A \mid f_L(a)>\gamma_L*\beta/10\}$

$A_R=\{a\in A \mid f_R(a)>\gamma_R*\beta/10\}$

קבוצת המסלולים האיכותיים בשני הצדדים היא: $A'=A_L\cap A_R$

וכאן אנו מגיעים לתנאי הבורר בין שתי האפשרויות שלנו. היינו רוצים שלהרבה מסלולים תהיה איכות גבוהה בשני הצדדים , כלומר ש A' תהיה קבוצה די גדולה. במקרה זה נוכל ליצור הן "פרוטוקול ימני" והן "פרוטוקול שמאלי" מהקבוצה A', בדומה לנעשה ב [KW] (כמתואר בע"מ 39). מכיון שב A' האיכות (f) גבוהה גם מצד ימין וגם מצד שמאל נקבל צפיפות הצלחה (γ)

סבירה עבור כל אחד משני פרוטוקולים אלה. מכיון ש A' די גדולה נקבל בדומה ל [KW] שצפיפות המסלולים באחד משני הפרוטוקולים גדלה בצורה ניכרת. זאת תהיה אפשרות א שלנו.

האפשרות השניה היא ש A' קטנה למדי. במקרה זה אם ננסה לעבוד כמו באפשרות א עם הקבוצה A', לא נקבל הגדלה משמעותית של צפיפות המסלולים. אבל אם A' קטנה הרי שאחת הקבוצות A_L או A_R אינה גדולה בהרבה מ $|A|/2$. ב.ה.כ. תהיה זאת A_L ופרושו של דבר הוא שמסלולים רבים ב A הם בעלי איכות שמאלית נמוכה. לכן האיכות השמאלית של הקבוצה A_L תהיה גדולה באופן משמעותי מזאת של A וזה יאפשר לנו להגדיר על A_L פרוטוקול שמאלי שבו צפיפות ההצלחה תהיה גדולה יותר מצפיפות ההצלחה של הפרוטוקול המקורי, וכך נקבל הגדלה משמעותית של הגודל $\gamma^{100}*1$.

נפרק, אם כן, את המשך ההוכחה לשתי אפשרויות.

<u>אפשרות א:</u> $|A'|>|A|/10$

זוהי כאמור האפשרות הפשוטה יותר. במקרה זה נתבונן בקבוצה A' וממנה נמשיך בצורה דומה לנעשה ב [KW]. ההבדל העיקרי נובע מכך שכאן עלינו להתיחס לפרמטר הנוסף γ, ושקבוצת הקלטים האפשריים אינה מכפלה קרטזית. הבדל זה מתבטא בכך שיש צורך להשתמש בלמה 2.4 במקום בלמה 2.3, בה נעשה שמוש בהוכחת משפט 1.5. נסמן את צפיפות המסלולים ב A' ב $\alpha'=|A'|/|A_N|$. ראשית נגדיר את קבוצת החלקים השמאליים שלהם השלמות ימניות רבות, ואת קבוצת החלקים הימניים שלהם השלמות שמאליות רבות למסלול ב A':

$$C=\{c\in C_N \mid |\{d\in D_N \mid c*d\in A'\}| > |D_N|*\alpha'/4\}$$

$$D=\{d\in D_N \mid |\{c\in C_N \mid c*d\in A'\}| > |C_N|*\alpha'/4\}$$

נסמן $\alpha_C=|C| / |C_N| \quad \alpha_D=|D| / |D_N|$

לפי הגדרת C, מספר המסלולים ב A' שחלקם השמאלי אינו ב C קטן מ $|C_N|*|D_N|*\alpha'/4$. לפי

הגדרת D, מספר המסלולים ב A' שחלקם הימני אינו ב D קטן גם הוא מ $|C_N|*|D_N|*\alpha'/4$.

מכיון ש $|A_N|=|C_N|*|D_N|$ (לפי ההגדרות) הרי שמספר המסלולים ב A' שחלקם השמאלי ב C וחלקם הימני ב D גדול מ $|C_N|*|D_N|*\alpha'/2$, אבל מספר זה קטן מ $|C|*|D|$, לכן $|C|*|D|>|C_N|*|D_N|*\alpha'/2$ ומכאן ברור שאו $\alpha_C>\sqrt{\alpha'/2}$ או $\alpha_D>\sqrt{\alpha'/2}$.

נניח ב.ה.כ ש $\alpha_C>\sqrt{\alpha'/2}>\sqrt{\alpha/20}$. (נעיר כבר עתה שאי שויון זה הוא שיבטיח את "הגדלת" צפיפות המסלולים, בפרוטוקול החדש שנגדיר להלן.)

כפי שהסברנו בהקדמה לפרק (ע"מ 39), ניצור מהפרוטוקול P "פרוטוקול שמאלי" וממנו פרוטוקול חדש $\tilde{P}$ שיפעל על מסלולים באורך $\tilde{l}=l_L$:

נבחר מקרית בהתפלגות אחידה תת קבוצה $U\subset N$ שעוצמתה $|U|=\sqrt{n}$, וצביעה I שלה (בצבעים s ו t). הפרוטוקול $\tilde{P}$ יפעל על הקבוצה $\tilde{N}=N-U$ שעוצמתה $\tilde{n}=n-\sqrt{n}$. קבוצת הצביעות $\tilde{B}$ עליה יפעל $\tilde{P}$ תהיה $\tilde{B}=B_{/I}$, כאשר הכונה היא שכל צביעה $\tilde{b}\in\tilde{B}$ היא צמצום לקבוצה $\tilde{N}$ של צביעה $b\in B_{/I}$ (והרי $\tilde{B}\subset B_{\tilde{N}}$ ואילו $B_{/I}\subset B_N$). כלומר, $\tilde{B}$ היא קבוצת כל הצביעות ב $B_{\tilde{N}}$ שמושלמות על ידי I לצביעה ב B.

קבוצת המסלולים $\tilde{A}$ עליה יפעל $\tilde{P}$ תהיה:

$$\tilde{A}=C(U,I)=\left\{ c\in C \;\middle|\; \begin{array}{l} 1)\ c \text{ זר ל } U \\ 2)\ \exists d\in D_N \text{ שמולו מוכל ב } U \text{ וצבוע } t \text{ ע"י } I \\ \quad \text{והמסלול } a=c*d \text{ מקיים } a\in A' \\ \text{ו} \quad \left|\bigcup_{i=1}^{l_L} T^i_{aB_{/I}}\right| / \left|\bigcup_{i=1}^{l_L} O^i_{aB_{N-U}}\right| > \beta\gamma_L/20 \end{array} \right\}$$

(כאשר הכונה היא שלכל מסלול $c\in C$ הנמצא ב $\tilde{A}$ מוסף בקצהו הימני הקודקוד t, כי הרי $\tilde{A}$ היא קבוצת מסלולים מ s ל t)

כלומר, $\tilde{A}$ היא קבוצת כל המסלולים $c\in C$ להם השלמה d למסלול $a=c*d\in A'$ כך ש c לא

נצבעה בשום צבע (ע"י I), d נצבעה כולה בצבע t, ומתקיים תנאי נוסף. משמעות התנאי הנוסף תובן בהמשך, אולם נעיר כבר עתה שתנאי זה נועד להבטיח שבפרוטוקול החדש שנגדיר תהיה לכל מסלול איכות $\tilde{f}$ גבוהה, ולכן לפרוטוקול כולו צפיפות הצלחה $\tilde{\gamma}$ גבוהה.

לכל $c\in\tilde{A}$ נסמן ב d_c את אחת ההשלמות הימניות שלו המקימות את תנאי 2.

הפרוטוקול $\tilde{P}$ יוגדר בצורה הבאה:

בהנתן $\tilde{b}\in\tilde{B}$ שהיא צביעה של $\tilde{N}$, ו $c\in\tilde{A}$ שהוא מסלול בין s ל t ב $\tilde{N}$ (ממנו נקטום את הקודקוד t המופיע בקצהו הימני), ישלים שחקן II את $\tilde{b}$ לצביעה $b\in B$ ע"י צביעת U ב I, ואילו שחקן I ישלים את c למסלול $a=c*d_c\in A'$. על זוג הקלטים a,b יפעילו שני השחקנים את הפרוטוקול המקורי P ויקבלו תשובה (לא בהכרח נכונה). התשובה שיתן $\tilde{P}$ תהיה אותה התשובה שנתן P. אם התשובה שנתן P נכונה הרי שהיא נמצאת בחלק השמאלי c (כי d_c צבועה כולה בצבע t תחת I ולכן גם תחת b), ולכן היא מהוה תשובה נכונה גם לפרוטוקול $\tilde{P}$. ברור גם ש $\tilde{P}$ פועל בסבוכיות של תת פרוטוקול של P ולכן סבוכיות התתקשורת של $\tilde{P}$ קטנה או שוה לזאת של P.

לכל בחירה של U,I קיבלנו, אם כן, פרוטוקול $\tilde{P}$. כדי לסיים את הוכחת אפשרות א' נצטרך לתת חסמים על הפרמטרים $\tilde{\alpha},\tilde{\beta},\tilde{\gamma}$ של פרוטוקול זה. פרמטרים אלה אינם בהכרח גדולים, אנו נראה שהם גדולים מספיק עבור בחירות מסוימות של U,I, וזה מספיק מכיון שהמטרה היא להראות קיום של פרוטוקול $\tilde{P}$ אחד, הפועל עם פרמטרים מתאימים.

<u>טענה 3.2:</u>

יש זוגות U,I עבורם $\tilde{\alpha}>\alpha_C/5$ ו $2\beta>\tilde{\beta}>\beta/2$

<u>הוכחה:</u>

נאמר שזוג U,I הוא "נאות" אם מתקימת הדרישה הבאה (המבטיחה חסם על $\tilde{\beta}$):

$2\beta|B_{N-U}| > |B_{/I}| > \beta|B_{N-U}|/2$

נאמר שזוג U,I הוא נאות עבור מסלול $c\in C$, אם U,I נאות וגם $c\in C(U,I)$.

נראה להלן שלכל $c\in C$, ההסתברות לכך שהזוג U,I נאות עבור c גדולה מ $1/5$:

(U,I) אינו נאות עבור c אם מתקיים אחד משלושת המאורעות הבאים:

1. **(U,I) אינו נאות. מאורע שהסתברותו p_1 מקימת $p_1<O(n^{-1/10})$, כי B גדולה מספיק כדי לקיים את תנאי למה 2.3.**
2. **c אינו זר ל U. מאורע שהסתברותו p_2 מקימת $p_2=o(1)$, וזאת על פי חשובים אלמנטרים המשתמשים בכך ש $|U|*l_L<n^{3/4}$.**
3. **אין ל c השלמה d_c המקימת את תנאי 2 בהגדרת $C(U,I)$. מאורע שהסתברותו p_3 מקימת $p_3<3/4$, לפי למה 2.4, שהשימוש בה יוסבר להלן.**

וכך יעשה השמוש בלמה 2.4 לשם חסימת p_3:

קבוצת הקודקודים תהיה $M=N$. ולכן $m=n$. E_M תהיה קבוצת כל תתי הקבוצות של M שגודלן $q=l_R<m^{1/100}$ (כנדרש בתנאי הלמה). קבוצת העצמים E תהיה קבוצת ההשלמות האפשריות ל c ב A'

$$E=\{V_d \mid d\in D_N,\ c*d\in A'\}$$

כאשר V_d היא קבוצת הקודקודים בהם עובר המסלול d. כל קבוצה $e\in E$ נזהה לחלוטין עם המסלול $d\in D_N$ עבורו $e=V_d$. אם יש מספר מסלולים כאלה נבחר שרירותית אחד מהם, ומכאן ואילך נתיחס אל e גם כאל מסלול. לפי הגדרת C

$$|E|/|E_M| > \alpha'/4 > \alpha/40 > m^{-1/100}$$

כנדרש בתנאי הלמה.

לכל $e\in E$ נגדיר את B_e להיות קבוצת האיברים הימניים (הצביעות) בקבוצת זוגות הקלטים $\bigcup_{i=1}^{l_L} T^i_{c*e,B}$ לאחר צמצום כל צביעה ל $M-e$ (כדי שיתקים $B_e\subset B_{M-e}$ כנדרש בלמה). כלומר, B_e

(לפני הצמצום) היא קבוצת כל הצביעות $b\in B$ שלפיהן במסלול $c*e$ צלע דו־צבועה יחידה שהיא ב c, ושעבורן $P(c*e,b)$ הוא פתרון נכון לבעיה R^m_{stc}. באופן אינטואיטיבי B_e היא קבוצת בני הזוג המוצלחים מצד שמאל של המסלול $c*e$. כל שנותר כדי להראות את קיום התנאים ללמה 2.4 הוא להראות את החסם הדרוש על β_e.

לפי הגדרות B_e, f_L:

$$3.2 \qquad |B_e|=f_L(c*e)*|\bigcup_{i=1}^{l_L} O^i_{c*e,B_M}|$$

לכל מסלול a מתקיים לפי הגדרה: $|O^i_{a,B_N}|=|B_{N-V_a}|$ (כאשר V_a היא קבוצת הקודקודים עליה נשען a). לכן:

$$\beta_e\equiv|B_e| / |B_{M-e}|=f_L(c*e)*l_L*|B_{M-e-v_c}| / |B_{M-e}| = f_L(c*e)*l_L*2^{-l_L}$$

נזכור ש $c*e\in A'\subset A_L$ ולכן לפי הגדרת A_L: $\quad 3.3 \quad f_L(c*e)>\gamma_L*\beta/10$

נזכור גם ש $\gamma_L>\gamma/2$ $\quad l_L>1$ $\quad$ ו $\quad 2^{-l_L}>2^{-l}$ ונקבל:

$$\beta_e > \gamma_L*\beta*l_L*2^{-l_L}/10 > \gamma*\beta*2^{-l}/20 > 2^{-m^{1/10}}$$

כאשר אי השויון האחרון נובע מהחסמים על γ,β,l, ונותן את החסם הנדרש בלמה 2.4.

(<u>הערה:</u> לכאורה נדמה שיש כאן תנאי, שהיה מהוה מגבלה, אם היינו רוצים להפעיל את הלמה לגבי מסלולים ארוכים יותר. למעשה ניתן להיפתר ממגבלה זאת על ידי הפעלת הלמה עם קבוצת קודקודים $M=N-V_c$, במחיר של סיבוך הסימונים.)

לכן מתקימת למה 2.4 ובהסתברות של לפחות $1/4$ $\exists e\in E$ שכולו מוכל ב U וצבוע t תחת I, ו

$|B_{e/I}|\geq\beta_e|B_{M-U}|/2$. נציב $\quad |B_{e/I}|=|\bigcup_{i=1}^{l_L} T^i_{c*e,B_I}|$ (לפי הגדרה)

ו: $\beta_e = |B_e| / |B_{M-e}| = f_L(c*e)*|\bigcup_{i=1}^{l_L} O^i_{c*e,B_M}|/|B_{M-e}|$ (לפי נוסחה 3.2)

ונקבל: $|\bigcup_{i=1}^{l_L} T^i_{c*e,B_M}|/|\bigcup_{i=1}^{l_L} O^i_{c*e,B_{N-U}}| \geq f_L(c*e)/2 \geq \gamma_L*\beta/20$ (לפי אי שויון 3.3)

כאשר השתמשנו גם בהצבת הגדלים הקבועים של קבוצות ה B וה O המתאימות.

קבלנו, אם כן שבהסתברות של לפחות 1/4 יש ל c השלמה d_c המקימת את תנאי 2 בהגדרת C(U,I). לכן הסתברות המאורע המשלים היא $p_3<3/4$.

מכיון שקבלנו $p_1+p_2+p_3<3/4+o(1)$ הרי שההסתברות לכך שהזוג U,I נאות עבור c גדולה מ 1/5. פרושו של דבר שיש זוג U,I שהוא נאות עבור 1/5 מהמסלולים $c\in C$. לכן:

$|C(U,I)|/|C| > 1/5$ כלומר $\tilde{\alpha}>\alpha_C/5$.

מכיון ש U,I הוא נאות הרי שגם $2\beta>\tilde{\beta}>\beta/2$

סוף הוכחת הטענה.

קיבלנו אם כן עבור בחירה מסוימת של U,I: $2\beta>\tilde{\beta}>\beta/2$

ו $\tilde{\alpha} > \alpha_C/5 > \sqrt{\alpha'/50} > \sqrt{\alpha/500} > \sqrt{\alpha}/25$

כדי לקבל חסם על $\tilde{\gamma}^{100}\tilde{l}$ נשים לב שתנאי 2 בהגדרת C(U,I) מבטיח שבפרוטוקול החדש $\tilde{P}$ האיכות הכללית $\tilde{f}$ של כל מסלול $\tilde{a}$ מקימת $\tilde{f}(\tilde{a})>\beta\gamma_L/20$. לפי נוסחה 3.1, מכאן נובע שעד כדי פקטור של $1+O(n^{-1/10})$ מתקיים: $\tilde{\gamma}\tilde{\beta}>\beta\gamma_L/20$ (נוסחה 3.1 נכונה עבור $\tilde{f},\tilde{\beta},\tilde{\gamma}$ כשם שהיא נכונה עבור f,β,γ. כאן נעשה השמוש עבור הקבוצות $\tilde{A},\tilde{B}$. קבוצות אלה עומדות בתנאי למה 2.2 לפי החסמים שהוכחנו על $\tilde{\alpha},\tilde{\beta}$)

לכן לפי $\tilde{\beta}<2\beta$ מתקבל $\tilde{\gamma}>\gamma_L/40$ ומכאן

$\tilde{\gamma}^{100}\tilde{l} > \gamma_L^{100} * l_L / 40^{100} > \gamma^{100} * 1 / 3 * 40^{100}$ (לפי טענה 3.1)

סוף אפשרות א'.

<u>אפשרות ב:</u> $|A'| \le |A|/10$

לכן או $|A_L| \le |A|*11/20$ **או** $|A_R| \le |A|*11/20$ **(או שניהם). ב.ה.כ. נניח** $|A_L| \le |A|*11/20$ **ונסמן** $\alpha_L = |A_L|/|A_N|$**. כל מסלול מחוץ ל** A_L **הוא בעל איכות שמאלית נמוכה, ולכן באפשרות זאת האיכות השמאלית "מתרכזת" על קבוצה קטנה יחסית. אם ל** A_L **היתה <u>איכות־כללית</u> גבוהה היינו יכולים להחליף את** A **ב** A_L **ולקבל הגדלה של** γ **בלי לפגוע בהרבה בגודל** $\alpha*\gamma$**. אולם מדובר כאן באיכות־שמאלית ולא באיכות־כללית ולכן אנו חייבים להגדיר "פרוטוקול שמאלי" (כמו באפשרות א') ולקבל ממנו פרוטוקול חדש** $\tilde{P}$ **שבו תהיה הגדלה של** $\tilde{\gamma}$ **תוך שמירה על ערך** $\tilde{\alpha}*\tilde{\gamma}$**.**

הבעיה העיקרית כאן תהיה חוסר האחידות. אם באפשרות א' היתה קבוצה C **של מסלולים שהיתה גדולה מספיק ולכל מסלול** c **בה היו השלמות רבות** d **למסלול** $c*d$**, עם איכות שמאלית מספיק גבוהה, הרי שהמצב ב** A_L **הוא מאוד לא אחיד מבחינת האיכויות השמאליות של המסלולים השונים, ומבחינת מספר ההשלמות שיש לכל מסלול שמאלי. אנו יודעים <u>שבממוצע</u> המצב טוב, אבל אם ננסה להתבונן בפרוטוקול שמאלי המתבסס על** A_L **עצמה, אנו עלולים לקבל איכויות מאוד נמוכות הנובעות דוקא מהמסלולים הגרועים. לכן כדי להבטיח הצלחה נצטרך לפני ביצוע "קיצוץ המסלולים" להביא את המצב ליתר אחידות.**

מטרתנו הסופית יכולה להיות להגיע לקבוצת מסלולים שמאליים C_5**, כך שלכל מסלול** $c \in C_5$ **יש קבוצת השלמות ימניות** $D_5(c)$ **ומתקימות 4 דרישות:**

א) לכל $c \in C_5$ $|D_5(c)|$ **גדולה למדי. דרישה זאת נועדה להבטיח את התנאים ללמה 2.4, שהשימוש בה יהיה דומה לזה שנעשה באפשרות א'.**

ב) לכל $c\in C_5$ יתקים שלכל $d\in D_5(c)$ יהיה ערכו של $f_L(c*d)$ לא קטן בהרבה מהממוצע של $f_L(c*d)$ על $D_5(c)$. דרישה זאת נועדה להבטיח שההשלמה הימנית הספציפית שתבחר למסלול השמאלי c לא תיצור מסלול c*d שאיכותו נמוכה יחסית, (כלומר, איכות c*d תהיה קרובה ל"איכותו" של c).

ג) אם נגדיר את איכותו של מסלול $c\in C_5$ כמיצוע האיכויות השמאליות $f_L(c*d)$ על הקבוצה $D_5(c)$, נקבל שהאיכות הממוצעת של הקבוצה C_5 גדולה מהאיכות השמאלית הממוצעת של הקבוצה A בפרוטוקול המקורי. דרישה זאת נועדה להבטיח את הגדלת $\tilde{\gamma}$ ביחס ל γ_L ולכן את הגדלת $\tilde{\gamma}^{100}\tilde{l}$ ביחס ל $\gamma^{100}l$.

ד) הגודל $\alpha*f_L(A)$ בפרוטוקול המקורי לא יהיה גדול בהרבה מהגודל המתאים עבור הקבוצה C_5 (גודל זה הוא גודלה של C_5 כפול האיכות הממוצעת בה). דרישה זאת נועדה להבטיח שגודלו של $\tilde{\alpha}*\tilde{\gamma}$ לא יקטן בהרבה. הסיבה להתבוננות ב $\alpha*\gamma$ ולא ב α עצמו תוסבר להלן. כפי שנראה בהמשך, בפועל נוח יותר יהיה להגיע לדרישות מאוד דומות אך שונות במעט מדרישות אלה.

לאחר שנגיע לקבוצה C_5 המקימת את הדרישות ניצור פרוטוקול שמאלי וממנו פרוטוקול חדש $\tilde{P}$, בצורה די דומה לאפשרות א'. ההבדל העיקרי יהיה שכאן נצטרך לשמור על <u>איכותה הממוצעת</u> של C_5, החסם שיהיה לנו על איכותו של כל מסלול ב C_5 לא יספיק. על מנת להגיע לקבוצה המיוחלת C_5 נתחיל מהקבוצה A_L שתכונה אצלנו A_1 ונעבור בשלבים לקבוצות A_2,A_3,A_4,A_5. בכל שלב נדרוש את קיומו של תנאי נוסף, ונעבור לתת קבוצה של הקבוצה שבחנו בשלב הקודם. כך שמתקים $A_L=A_1\supset A_2\supset A_3\supset A_4\supset A_5$.

לכל קבוצה A_i נגדיר:

"צפיפות הקבוצה" או "צפיפות המסלולים": $\alpha_i=|A_i|/|A_N|$

האיכות השמאלית הממוצעת: $f_i=f_L(A_i)$

לכל מסלול $c\in C_N$ **ולכל** i **נגדיר:**

קבוצת ההשלמות הימניות: $D_i(c)=\{d\in D_N \mid c*d\in A_i\}$

וצפיפותה: $\mu_i(c)=|D_i(c)| / |D_N|$

הקבוצה C_i **תהיה קבוצת כל החלקים השמאליים האפשריים ב** A_i**. כלומר:**

$$C_i=\{c\in C_N \mid \mu_i(c)>0\}$$

איכות המסלול $c\in C_i$ **תוגדר כמיצוע האיכות השמאלית** $f_L(c*d)$ **על הקבוצה** $D_i(c)$**:**

$$f_i(c)=\sum_{d\in D_i(c)} f_L(c*d) / |D_i(c)| = \sum_{d\in D_i(c)} f_L(c*d) / (\mu_i(c)*|D_N|)$$

ב $f_i(C_i)$ **נסמן את איכות הקבוצה** C_i**, שהיא האיכות הממוצעת** $f_i(c)$ **על** C_i**.**

צפיפות הקבוצה C_i **תהיה:** $\alpha_{C_i}=|C_i|/|C_N|$

במונחים אלה מקבלות הדרישות שלנו את הצורה הבאה:

א) לכל $c\in C_5$ $D_5(c)$ **גדולה.**

ב) לכל $c\in C_5$ **ו** $d\in D_5(c)$ **יהיה** $f_L(c*d)$ **קרוב ל** $f_5(c)$**.**

ג) $f_5(C_5)$ **גדלה פי פקטור מסוים מ** $f_L(A)$**.**

ד) $\alpha*f_L(A)$ **אינו גדול בהרבה מ** $\alpha_{C_5}*f_5(C_5)$**.**

כדי לפשט את ההוכחה נגדיר מערכת דרישות חדשה שתהיה מאוד דומה לקודמת ותתפקד בצורה זהה. במערכת זאת תחליף הפונקציה $f_4(c)$ **את תפקידה של** $f_5(c)$ **. הגודל** $f_4(C_5)$ **יוגדר כמיצוע** $f_4(c)$ **על** C_5**:**

א) לכל $c\in C_5$ $D_5(c)$ **גדולה.**

ב) לכל $c\in C_5$ **ו** $d\in D_5(c)$ **יהיה** $f_L(c*d)$ **קרוב ל** $f_4(c)$ **.**

ג) $f_4(C_5)$ גדולה פי פקטור מסוים מ $f_L(A)$.

ד) $\alpha^* f_L(A)$ אינו גדול בהרבה מ $\alpha_{C_5}^* f_4(C_5)$.

בסימן = נסמן מכאן ועד לסוף הוכחת אפשרות ב, שויון עד כדי פקטור של $1+o(1)$.

אין בידנו חסם תחתון סביר על גודלה של A_L. לכן α_1 עלול להיות קטן מאוד, אולם יש איזון בין α_1 ל γ_L המתבטא בחסם על $\alpha_1^* f_1$. זוהי גם הסיבה לכך שלכל אורך ההוכחה נתבונן במכפלת האיכות בצפיפות המסלולים, ולא בצפיפות המסלולים עצמה. מהחסם על $\alpha_1^* f_1$ מתקבל גם חסם עבור f_1, לכן יוצא שדרישות ג, ד "מתקימות" עבור הקבוצה A_1.

בשלבים השונים נוסיף תנאים שיבטיחו את קיום דרישות א ו ב ומעבר לקיום דרישות ג, ד ע"י הקבוצה C_i במקום A_i. בכל שלב נראה שלמרות התנאים שהוספנו, עדין מתקימים חסמים נאותים על האיכות הממוצעת (f_i או $f_i(C_i)$) ועל מכפלת האיכות הממוצעת בצפיפות המסלולים ($\alpha_i^* f_i$ או $\alpha_{C_i}^* f_i(C_i)$).

אפשר להבחין ש A_i נוצרת מ $C_i,\{D_i(c)\}$ ולהפך. יהיו שלבים בהם נגדיר את A_i וממנה נקבל את $C_i,\{D_i(c)\}$, ויהיו שלבים בהם נעבוד בצורה הפוכה.

אולם לפני שנתחיל במלאכה נראה מהם החסמים על $\alpha_1^* f_1$ ועל f_1.

<u>טענה 3.3:</u>

$$\sum_{a\in A_1} f_L(a) > 0.9\beta\gamma_L|A|^*(1-o(1)) \qquad (1$$

$$\alpha_1 f_1 > 0.9\alpha\beta\gamma_L(1-o(1)) \qquad (2$$

$$f_1 > 1.5\beta\gamma_L \qquad (3$$

<u>הוכחה:</u>

לפי נוסחה 3.1a $f_L(A)\approx\beta\gamma_L$ ולכן:

$$\sum_{a\in A} f_L(a) \approx \beta\gamma_L |A|$$

לפי הגדרת A_L ברור ש:

$$\sum_{a\in A-A_L} f_L(a) \le \beta\gamma_L |A|/10$$

ומכאן נובע סעיף 1 לפי

$$\sum_{a\in A} f_L(a) = \sum_{a\in A-A_1} f_L(a) + \sum_{a\in A_1} f_L(a)$$

(נזכור ש $A_1=A_L$)

סעיף 2 הוא למעשה כתיבה מחדש של סעיף 1 תוך כדי הצבה $|A|=\alpha*|A_N|$

ו

$$\sum_{a\in A_1} f_L(a) = \alpha_1 * f_1 * |A_N|$$

סעיף 3 נובע מסעיף 2 ומאי השויון: $\alpha_1 \le \alpha*11/20$ השקול לתנאי: $|A_L| \le |A|*11/20$

המתקים באפשרות ב ב.ה.כ. (כפי שראינו)

סוף הוכחת הטענה

סעיפים 2,3 נותנים חסמים חשובים להמשך ההוכחה, אולם כפי שראינו נבעו חסמים אלה מהחסם בסעיף 1. בשלבים הבאים נשמור תמיד על חסם מקביל לחסם זה, ונזכור שאפשר ממנו להגיע לחסמים על $\alpha_i * f_i$ ועל f_i.

נעבור כעת לתאור השלבים השונים:

שלב א:

בשלב זה נזרוק את כל המסלולים להם איכות שמאלית $(f_L(a))$ גבוהה מאוד. הסיבה למעשה מוזר זה היא שבהמשך יהיה קל יותר לבצע חישובים.

נגדיר: $A_2=\{a\in A_1 \mid f_L(a) < 2\beta\}$

<u>טענה 3.4:</u>

$$\sum_{a\in A_2} f_L(a) > 0.9\beta\gamma_L|A|*(1-o(1))$$

<u>הוכחה:</u>

נגדיר $Z=A_1-A_2=\{a\in A_1 \mid f_L(a) \geq 2\beta\}$. **לכל** $a\in Z$ $f_L(a)\geq 2\beta$ **ולכן** $f_L(Z)\geq 2\beta$ **וזאת סתירה לנוסחה 3.1a (נוסחה 3.1a נכונה עבור הקבוצה Z כשם שהיא נכונה עבור הקבוצה A , אלה שאז** γ_L **מוחלף באיכות השמאלית של הקבוצה Z לבדה. הסתירה מתקבלת מכך שאיכות שמאלית זאת קטנה או שוה ל 1 מעצם הגדרתה). לכן מסתבר ש Z קטנה מכדי לקיים נוסחה זאת, כלומר אינה עומדת בתנאי למה 2.2. לכן** $|Z| < n^{-1/100}|A_N|$. **יתרה מזאת, Z מקימת:**

$$\sum_{a\in Z} f_L(a) < 2\beta n^{-1/100}|A_N|$$

כי אחרת נגדיל שרירותית את Z לקבוצה $\hat{Z}$ **שגודלה** $n^{-1/100}|A_N|$, **ונקבל עבור קבוצה זאת סתירה לנוסחה 3.1a וללמה 2.2.**

מהחסמים על α,γ **שדרשנו בתנאי למה 3.1, ומסעיף 1 בטענה 3.1 נובע ש**

$$n^{-1/100}|A_N| / \gamma_L|A|=o(1)$$

$$\sum_{a\in Z} f_L(a) = \beta\gamma_L|A|*o(1)$$

הצבה באי השויון האחרון נותנת:

מכאן ומסעיף 1 בטענה 3.3 נובעת טענה 3.4 כי $A_2=A_1-Z$.

סוף הוכחת הטענה

שלב ב:

בשלב זה נזרוק את כל המסלולים השמאליים שלהם מעט השלמות ימניות ב A_2 **, על מנת להבטיח את קיומה של דרישה א. ניצור את** $A_3,C_3,\{D_3(c)\}$ **בצורה המוכה: קודם ניצור את** C_3 **ואת** $\{D_3(c)\}$ **ומהם ניצור את** A_3**. נגדיר:**

$$C_3=\{c\in C_2 \mid \mu_2(c) > n^{-1/200}\}$$

ולכל $c\in C_3$

$$D_3(c)=D_2(c)$$

ומהם ניצור

$$A_3=\{(c*d) \mid c\in C_3 ,\ d\in D_3(c)\}$$

(הקבוע $1/200$ **נקבע לפי** $1/1000<1/200<1/100$**)**

<u>טענה 3.5:</u>

$$\sum_{a\in A_3} f_L(a) > 0.9\beta\gamma_L|A|*(1-o(1))$$

<u>הוכחה:</u>

נגדיר $Z=A_2-A_3$ **. לפי הגדרות** Z, $C_3,\{D_3(c)\}$, **לכל מסלול שמאלי** $c\in C_N$, **יש לכל היותר** $n^{-1/200}*|D_N|$ **השלמות ימניות ב** Z**. לכן** $|Z| \le n^{-1/200}*|A_N|$**.**

מכיוון ש $Z\subset A_2$, **לכל** $a\in Z$ $f_L(a)<2\beta$**. (לפי הגדרת** A_2**). לכן:**

$$\sum_{a\in Z} f_L(a) < 2\beta*n^{-1/200}*|A_N|$$

מהחסמים על α,γ **שדרשנו בתנאי למה 3.1 ומסעיף 1 בטענה 3.1 נובע ש:**

$$n^{-1/200}|A_N| / \gamma_L*|A|=o(1)$$

לכן:

$$\sum_{a\in Z} f_L(a) = \beta\gamma_L|A|*o(1)$$

מכאן ומטענה 3.4 נובעת טענה 3.5 כי $A_3=A_2-Z$.

סוף הוכחת הטענה.

שלב ג:

טענה 3.5 נותנת חסם על סכום האיכויות בקבוצה A_3. כפי שראינו בשלב א, חסם זה בצרוף חסם עליון על α_3 נותנים חסמים על $\alpha_3 f_3$ ועל f_3. בשלב זה נתמקד בקבוצה C_4, שהיא קבוצת המסלולים האיכותיים ביותר ב C_3. על סכום האיכויות בקבוצה C_4 נוכיח חסם מקביל לטענות 3.5, 3.4, 3.3. וממנו נקבל חסמים על $\alpha_{C_4} f_4(C_4)$ ועל $f_4(C_4)$. חסמים אלה יבטיחו את קיומן של דרישות ג ו ד.

נגדיר את C_4 להיות קבוצת $\alpha_3*|C_N|$ המסלולים האיכותיים ביותר ב C_3 (המסלולים בעלי $f_3(C)$ הגבוה ביותר). זה אפשרי כי $|C_3| = \alpha_{C_3}*|C_N| \geq \alpha_3|C_N|$. לפי ההגדרה מתקיים $\alpha_{C_4}=\alpha_3$.

לכל $c\in C_4$ נגדיר $D_4(c)=D_3(c)$. ומהם ניצור את $A_4=\{c*d \mid c\in C_4 \ , \ d\in D_4(c)\}$.

<u>טענה 3.6:</u>

$$\sum_{c\in C_4} f_4(c) > 0.9\beta\gamma_L*(|A| / |D_N|)*(1-o(1)) \qquad (1$$

$$\alpha_{C_4}*f_4(C_4) > 0.9\alpha\beta\gamma_L*(1-o(1)) \qquad (2$$

$$f_4(C_4) > 1.5\beta\gamma_L \qquad (3$$

<u>הוכחה:</u>

את סכום האיכויות על A_3 נציג כסכום ממושקל של האיכויות ב C_3:

$$\sum_{a\in A_3} f_L(a)=\sum_{c\in C_3} \mu_3(c)*|D_N|*f_3(c)$$

(הנוסחה נובעת מכך ש $f_3(c)$ הוא מיצוע $f_L(a)$ על $D_3(c)$).

הביטוים $|D_N|*f_3(c)$ בצד הימני של הנוסחה ממושקלים ע"י המשקולות $\mu_3(c)$. סכום המשקולות מקיים:

$$\sum_{c\in C} \mu_3(c) = |A_3| / |D_N| = \alpha_3*|C_N|$$

(כי $|A_N| = |C_N|*|D_N|$)

לכל c $\mu_3(c)\le 1$ ואם נחלק מחדש את מסת המשקולות כך שתתרכז כולה על $\alpha_3*|C_N|$ הערכים הגדולים ביותר של $f_3(c)$ רק נגדיל את הסכום. לכן:

$$\sum_{c\in C_4} f_3(c)*|D_N| \ge \sum_{a\in A_3} f_L(a)$$

$D_4(c)=D_3(c)$ ולכן לכל c $f_4(c)=f_3(c)$ לכן:

$$|D_N|*\sum_{c\in C_4} f_4(c) \ge \sum_{a\in A_3} f_L(a)$$

סעיף 1 של הטענה נובע מאי שויון זה ומטענה 3.5.

סעיף 2 הוא כתיבה מחדש של סעיף 1 תוך כדי הצבת:

$$\sum_{c\in C_4} f_4(c) = \alpha_{C_4}*f_4(C_4)*|C_N| \qquad \text{ו} \qquad |A| = \alpha*|A_N| = \alpha|C_N|*|D_N|$$

סעיף 3 נובע מיידית מסעיף 2 ומאי השויון $\alpha_{C_4}\le\alpha*11/20$ הנובע מכך שלפי השלבים השונים $\alpha_{C_4} = \alpha_3 \le \alpha_2 \le \alpha_1 \le \alpha*11/20$

סוף הוכחת הטענה.

שלב ד:

כדי להבטיח את קיומה של דרישה ב נשמיט מכל קבוצה $D_4(c)$ **את ההשלמות** $d\in D_4(c)$ **עבורן** $f_L(c*d)$ **אינו קרוב מאוד לערכו של** $f_4(c)$**. כדי להבטיח שדרישה א עדיין נשמרת (**$D_5(c)$**) אינה קטנה מידי) נצטרך לדרוש גם חסם תחתון על** $f_4(c)$ **ולזרוק מסלולים שמאליים שאינם עומדים בו. בסיום שלב זה נשאר עם קבוצה** C_5 **המקימת את כל ארבע הדרישות.**

נגדיר אם כן: $C_5=\{c\in C_4 \mid f_4(c) \geq n^{-1/500}\beta\gamma_L\}$

ולכל $c\in C_5$ $D_5(c)=\{d\in D_4(c) \mid f_L(c*d) \geq 0.9f_4(c)\}$

מהם נגדיר כרגיל את $A_5=\{c*d \mid c\in C_5 \ , \ d\in D_5(c)\}$

<u>טענה 3.7:</u>

1) $$\sum_{c\in C_5} f_4(c) > 0.9\beta\gamma_L*(|A| / |D_N|)*(1-o(1))$$

2) $$\alpha_{C_5}*f_4(C_5) > 0.9\alpha\beta\gamma_L*(1-o(1))$$

3) $$f_4(C_5)>1.5\beta\gamma_L$$

<u>הוכחה:</u>

נגדיר: $Z=C_4-C_5=\{c\in C_4 \mid f_4(c) < n^{-1/500}\beta\gamma_L\}$

לכן $$\sum_{c\in Z} f_4(c) < n^{-1/500}\beta\gamma_L*|C_N|=n^{-1/500}\beta\gamma_L(|A_N|/|D_N|)$$

לפי החסם על α **שדרשנו בתנאי למה 3.1:** $n^{-1/500}*|A_N| / |A|=o(1)$

לכן $$\sum_{c\in Z} f_4(c) = \beta\gamma_L*(|A|/|D_N|)*o(1)$$

מכאן ומסעיף 1 בטענה 3.6 נובע סעיף 1. סעיף 2 הוא כתיבה מחדש של סעיף 1 תוך כדי הצבת:

$$\sum_{c\in C_5} f_4(c) = \alpha_{C_5} * f_4(C_5) * |C_N| \quad \text{ו} \quad |A| = \alpha |A_N| = \alpha |C_N| * |D_N|$$

סעיף 3 נובע מיידית מסעיף 2 ומכך ש $\alpha_{C_5} \le \alpha_{C_4} \le \alpha * 11/20$ **. (כפי שראינו בטענה 3.6)**

סוף הוכחת הטענה.

כדי להראות שבשלב ד לא "הרסנו" את דרישה א, נוכיח:

<u>טענה 3.8:</u>

לכל $c\in C_5$ $\mu_5(c)>n^{-1/100}$

<u>הוכחה:</u>

עבור $c\in C_5$ **נגדיר** $Z=D_4(c)-D_5(c)$ **ונקבל:**

$$\sum_{d\in D_5(C)} f_L(c*d) = \sum_{d\in D_4(C)} f_L(c*d) - \sum_{d\in Z} f_L(c*d)$$

לפי הדרישה משלב א לכל $c*d\in A_5\subset A_2$ **מתקיים** $f_L(c*d)<2\beta$ **לכן אגף שמאל קטן מ** $\mu_5(c)*|D_N|*2\beta$**. האיבר הראשון באגף ימין שוה לפי ההגדרות ל** $\mu_4(c)*|D_N|*f_4(c)$**. לפי הגדרות** $D_5(c)$ **ו** Z **לכל** $d\in Z$ $f_L(c*d)<0.9f_4(c)$**, לכן האיבר הימני קטן שוה מ** $|Z|*0.9f_4(c)$ **וזה קטן שוה מ** $0.9\mu_4(c)*|D_N|*f_4(c)$ **(כי** $Z\subset D_4(c)$**). נציב כל זאת ונקבל:**

$$\mu_5(c)*|D_N|*2\beta > \mu_4(c)*|D_N|*f_4(c) - 0.9\mu_4(c)*|D_N|*f_4(c)$$

$$\mu_5(c)*\beta > 0.05*\ \mu_4(c)*f_4(c)$$

באי שויון זה נציב $f_4(c)\ge n^{-1/500}\beta\gamma_L$ **(נובע מהגדרת** C_5**).**

ו $\mu_4(c)>n^{-1/200}$ **(נובע מהגדרת** C_3 **בשלב ב ומכך ש** $C_5\subset C_3$ **ו** $(\mu_4(c)=\mu_3(c)=\mu_2(c)$

ונקבל $\mu_5(c) > 0.05*n^{-1/500}*n^{-1/200}*\gamma_L > n^{-1/100}$

(נובע מהחסם שדרשנו על γ בתנאי למה 3.1 ומסעיף 1 בטענה 3.1 לפיו $\gamma_L \geq \gamma/2$)

סוף הוכחת הטענה.

קיבלנו אם כן מערכת המקימת את כל ארבע הדרישות:

א) לכל $c \in C_5$	$\lvert D_5(c)\rvert > n^{-1/100}*\lvert D_N\rvert$	(טענה 3.8)	3.4
ב) לכל $c \in C_5$ ו $d \in D_5(c)$	$f_L(c*d) \geq 0.9 f_4(c)$	(הגדרת $D_5(c)$)	3.5
ג)	$f_4(C_5) > 1.5\beta\gamma_L$	(טענה 3.7)	3.6
ד)	$\alpha_{C_5} f_4(C_5) > 0.9\alpha\beta\gamma_L(1-o(1))$	(טענה 3.7)	3.7

ממערכת זאת ניצור, בצורה דומה למקרה א, "פרוטוקול שמאלי", וממנו פרוטוקול חדש $\tilde{P}$ שיפעל על מסלולים באורך l_L. כמו באפשרות א, נבחר מקרית בהתפלגות אחידה תת קבוצה $U \subset N$ וצביעה I שלה (בצבעים s ו t). הפרוטוקול $\tilde{P}$ יפעל על הקבוצה $\tilde{N}=N-U$ שעוצמתה $\tilde{n}=n-\sqrt{n}$. קבוצת הצביעות $\tilde{B}$ שעליה יפעל $\tilde{P}$ תהיה $\tilde{B}=B_{/I}$. (כאשר גם כאן הכונה היא שכל צביעה $\tilde{b} \in \tilde{B}$ היא צמצום לקבוצה $\tilde{N}$ של צביעה $b \in B_{/I}$). נגדיר את קבוצת המסלולים $C(U,I)$ להיות:

$$C(U,I)=\left\{ c\in C_5 \;\middle|\; \begin{array}{l} 1)\ c \text{ זר ל } U \\ 2)\ \exists d\in D_N \text{ שכולו מוכל ב } U \text{ וצבוע } t \text{ ע"י } I \\ \quad \text{והמסלול } a=c*d \text{ מקיים } a\in A_5 \\ \text{ו } \left|\bigcup_{i=1}^{l_L} T^i_{aB_{/I}}\right| / \left|\bigcup_{i=1}^{l_L} O^i_{aB_{N-U}}\right| > 0.9 f_L(a) \end{array} \right\}$$

(כאשר גם כאן הכונה היא שלכל מסלול $c \in C_5$ הנמצא ב $C(U,I)$ מוסף בקצהו הימני הקודקוד t)

הקבוצה $\tilde{A}$ עליה יפעל $\tilde{P}$ תוגדר מ $C(U,I)$ בהמשך.

לכל $c\in C(U,I)$ נסמן ב d_c את אחת מההשלמות הימניות שלו המקימת את תנאי 2 בהגדרת $C(U,I)$.

הפרוטוקול $\tilde{P}$ יוגדר על $c\in C(U,I), \tilde{b}\in \tilde{B}$ בצורה זהה לזאת בה הוגדר באפשרות א (שחקן I משלים את c ל $a=c*d_c$, שחקן II משלים את $\tilde{b}$ ל b ע"י צביעת U ב I, ושני השחקנים מפעילים את P על a,b). גם כאן יפעל $\tilde{P}$ בסיבוכיות קטנה או שוה לסיבוכיות P ויתן תשובה נכונה בכל פעם ש P נותן תשובה נכונה.

לכל בחירה של U,I קיבלנו פרוטוקול $\tilde{P}$. כמו באפשרות א, נצטרך להראות שיש בחירות מסוימות של U,I שייתנו את החסמים הנדרשים על $\tilde{\alpha}*\tilde{\gamma},\tilde{\beta}$ ו $\tilde{\gamma}^{100}\tilde{I}$. לשם כך נצטרך להגדיר את $\tilde{A}$ בצורה שונה במעט מאשר באפשרות א, הסיבה לכך היא ששם היה לנו חסם על איכותו של כל אחד מהמסלולים המשתתפים בתהליך. כאן יש חסם רק על הממוצע $f_4(C_5)$ (נוסחה 3.6). אם נגדיר $\tilde{A}=C(U,I)$ (כמו באפשרות א) לא נוכל להבטיח את איכות הפרוטוקול $\tilde{P}$, כי ייתכן שדוקא המסלולים $c\in C_5$ שאיכותם נמוכה מופיעים בהרבה מהקבוצות $C(U,I)$, ולכן איכות $\tilde{P}$ מושפעת בעיקר ממסלולים אלה. כדי שנוסחה 3.6 תתן חסם על איכות $\tilde{P}$ צריך להבטיח שכל $c\in C_5$ יופיע ב $\tilde{A}$ בהסתברות שוה.

זוג U,I יקרא "נאות" אם מתקיימת הדרישה הבאה (המבטיחה חסם על $\tilde{\beta}$):

$$\beta|B_{N-U}|(1-n^{-1/10}) < |B_{/I}| < \beta|B_{N-U}|(1+n^{-1/10})$$

זוג U,I יקרא נאות עבור מסלול $c\in C_5$, אם U,I נאות וגם $c\in C(U,I)$.

טענה כמעט זהה לטענה הבאה הוכחה במהלך הוכחת טענה 3.2, נחזור כאן על ההוכחה בקוים כלליים בלבד.

טענה 3.9:

לכל $c\in C_5$, $Pr(c$ נאות עבור $(U,I)) > 1/5$

הוכחה:

(U,I) אינו נאות עבור c אם מתקיים אחד משלושת המאורעות הבאים:

1) (U,I) אינו נאות. מאורע שהסתברותו $p_1<O(n^{-1/10})$ לפי למה 2.3.

2) c אינו זר ל U. מאורע שהסתברותו $p_2=o(1)$, לפי ש $|U|*l_L<n^{3/4}$.

3) אין ל c השלמה d_c המקימת את תנאי 2 בהגדרת $C(U,I)$. מאורע שהסתברותו $p_3<3/4$ לפי למה 2.4.

השימוש בלמה 2.4 זהה לשימוש שנעשה בה בהוכחת טענה 3.2, כאשר הפעם:

$E=\{V_d \mid d\in D_5(c)\}$ והחסם על $|E|$ ניתן לפי אי שויון 3.4. החסם על β_e ניתן כמו קודם, לפי נוסחה 3.2 ממנה מגיעים לזהות $\beta_e=f_L(c*e)*l_L*2^{-l_L}$ כאשר הפעם מחליף את אי השויון 3.3, החסם: $f_L(c*e)> 0.9*n^{-1/500}\beta\gamma_L$ הנובע מהחסם $f_4(c) \geq n^{-1/500}\beta\gamma_L$ המופיע בהגדרת C_5 ומאי שויון 3.5. (החסם על $f_4(c)$ לא נכלל בארבעת התנאים שדרשנו, למרות שנעשה בו שימוש, מכיון שתרומתו להבנה האינטואיטיבית של ההוכחה אינה מהותית)

כמו קודם נובעת מלמה 2.4, קיומה בהסתברות 1/4, של השלמה d_c המקיימת את תנאי 2 בהגדרת $C(U,I)$. (כאשר הפעם הוחלף הפקטור $(1-m^{-1/10})$ מלמה 2.4 בפקטור 0.9, במקום ב 0.5 במקרה א)

קיבלנו $p_1+p_2+p_3 < 3/4+o(1)$ ולכן בהסתברות של לפחות 1/5 (U,I) נאות עבור c

סוף הוכחת הטענה

המסקנה מטענה 3.9 היא שגם אם נאפס את הקבוצות $C(U,I)$ עבור זוגות U,I שאינם

נאותים, עדיין יופיע כל מסלול $c\in C_5$ בלפחות 1/5 מהקבוצות $C(U,I)$. נזרוק כל מסלול $c\in C_5$ שרירותית מחלק מהקבוצות $C(U,I)$ בהן הוא מופיע כך שיופיע בדיוק ב 1/5 מהקבוצות, ונקבל קבוצות חדשות $\tilde{C}(U,I)\subset C(U,I)$ המקיימות:

אם (U,I) אינו נאות $\tilde{C}(U,I)=\emptyset$

ולכל $c\in C_5$ $\qquad \Pr(c\in \tilde{C}(U,I))=1/5 \qquad$ 3.8

הקבוצה $\tilde{A}$ תוגדר כ $\tilde{A}=\tilde{C}(U,I)$ עבור הזוג U,I המתאים.

טענה 3.2, הוכיחה באמצעות א את קיומם של זוגות U,I עבורם $\tilde{\alpha}$ ו $\tilde{\beta}$ גדולים מספיק. החסם על $\tilde{\gamma}$ התקבל מיידית מכך שאיכותו של כל מסלול היתה גבוהה. כאן אין חסם סביר על איכותו של כל מסלול לכן נזדקק לטענה מורכבת מעט יותר הנותנת גם חסם על $\tilde{\gamma}$. באופן אינטואיטיבי $\tilde{\alpha}$ מודד את גודלה של $\tilde{A}$ ו $\tilde{\gamma}$ מתנהג כמו האיכות הממוצעת בה. נגדיר את הצפיפות $\alpha(U,I)$ להיות:

$$\alpha(U,I)=|\tilde{C}(U,I)| / |C_N|$$

ואת האיכות $f(U,I)$ להיות מיצוע $f_4(c)$ על $\tilde{C}(U,I)$:

$$f(U,I)=\sum_{c\in \tilde{C}(U,I)} f_4(c) / |\tilde{C}(U,I)|$$

כדי להבטיח את קיום החסמים הנדרשים נצטרך להראות קיום זוג U,I עבורו גם $f(U,I)$ וגם $\alpha(U,I)*f(U,I)$ גבוהים.

<u>טענה 3.10:</u>

יש (U,I) עבורו

1) $\alpha(U,I)*f(U,I) > \alpha_{C_5} f_4(C_5)/50$

2) $f(U,I) \geq 0.9 f_4(C_5)$

הוכחה:

נסמן ב V **את קבוצת כל הזוגות האפשריים** (U,I)**, וב** χ **את מספרם** $(\chi=|V|)$.

נסמן ב W **את קבוצת השלשות:** $W=\{(c,U,I) \mid (U,I)\in V\ ,\ c\in \tilde{C}(U,I)\}$

לפי נוסחה 3.8 $|W|=|V|*|C_5|*1/5$

ו

$$\sum_W f_4(c)=|V|*|C_5|*1/5*f_4(C_5)$$

(כי כל $c\in C_5$ **מופיע בדיוק ב** $1/5$ **מהקבוצות** $\tilde{C}(U,I)$**)**

נציב בשוויונות האחרונים: $|V|=\chi$ **ו** $|C_5|=\alpha_{C_5}*|C_N|$ **ונקבל:** $|W|=\chi\alpha_{C_5}*|C_N|/5$

ו

$$\sum_W f_4(c)=\chi\alpha_{C_5}f_4(C_5)*|C_N|/5$$

נסמן ב V' **את קבוצת כל הזוגות** $(U,I)\in V$ **המקיימים את תנאי 1 של הטענה. נסמן ב** W' **את קבוצת כל השלשות המתאימים:** $W'=\{(c,U,I)\in W \mid (U,I)\in V'\}$

לפי הגדרות W' **ו** $\alpha(U,I),f(U,I)$ **מתקיים:**

$$\sum_{W-W'} f_4(c)=\sum_{(U,I)\in V-V'}\ \sum_{c\in\tilde{C}(U,I)} f_4(c)=\sum_{(U,I)\in V-V'} f(U,I)*|\tilde{C}(U,I)|=\sum_{(U,I)\in V-V'} f(U,I)*\alpha(U,I)*|C_N|$$

נשתמש באי קיום תנאי 1 עבור $(U,I)\in V-V'$ **ובכך ש** $|V-V'|\le|V|=\chi$ **ונקבל:**

$$\sum_{W-W'} f_4(c)\le\chi\alpha_{C_5}f_4(C_5)*|C_N|/50$$

לכן

$$\sum_{W'} f_4(c)=\sum_W f_4(c)-\sum_{W-W'} f_4(c)\ge(1/5-1/50)\chi\alpha_{C_5}f_4(C_5)*|C_N|$$

אבל $|W'|\le|W|=\chi\alpha_{C_5}*|C_N|/5$

לכן מתקבל שמיצוע $f_4(c)$ **על** W' **הוא לפחות** $0.9f_4(C_5)$**. מכיון שמיצוע זה הוא גם מיצוע**

ממושקל של $f(U,I)$ עבור זוגות $(U,I)\in V'$, הרי שקיים זוג $(U,I)\in V'$ עבורו

$f(U,I) \geq 0.9f_4(C_5)$

סוף הוכחת הטענה.

נקבע את (U,I) להיות זוג המקיים את טענה 3.10 ונראה שהפרוטוקול הנוצר $\tilde{P}$ מקיים את כל התנאים שנדרשו באמפשרות ב (כל שנותר הוא מתן חסמים על $\tilde{\beta}$, $\tilde{\alpha}\tilde{\gamma}$, $\tilde{\gamma}^{100}\tilde{I}$):

החסם על $\tilde{\beta}$, שהוא הפשוט ביותר נובע מכך שזוג (U,I) המקיים את טענה 3.10 הוא בהכרח נאות (אחרת $\tilde{C}(U,I)=\emptyset$). לפי הגדרת זוג נאות מתקיים ש: $\beta(1-n^{-1/10}) < \tilde{\beta} < \beta(1+n^{-1/10})$

כדי להגיע לחסמים על $\tilde{\alpha}\tilde{\gamma}$ ועל $\tilde{\gamma}^{100}\tilde{I}$ נצטרך לנתח את התנהגות פונקצית האיכות $\tilde{f}$ בפרוטוקול החדש: כל מסלול $\tilde{a}\in\tilde{A}$ הוא למעשה מסלול שמאלי $c\in\tilde{C}(U,I)\subset C(U,I)$. לכל מסלול כזה מתאימה השלמה d_c למסלול $c*d_c\in A_5$. אם נזכר בהגדרת הפרוטוקול $\tilde{p}$ ובהגדרת פונקצית האיכות f, נקבל שתנאי 2 בהגדרת $C(U,I)$ פרושו למעשה ש $\tilde{f}(\tilde{a}) > 0.9f_L(c*d_c)$.

שימוש באי שויון 3.5 יתן $\tilde{f}(\tilde{a}) > 0.81f_4(c)$. מיצוע על $\tilde{A}$ באגף שמאל, ועל $\tilde{C}(U,I)$ באגף ימין (נזכור ש $\tilde{A}=\tilde{C}(U,I)$) יתן:

$$\tilde{f}(\tilde{A}) > 0.81f(U,I) \qquad 3.9$$

נשתמש בסעיף 2 של טענה 3.10 ונקבל:

$$\tilde{f}(\tilde{A}) > 0.72f_4(C_5)$$

ולפי אי שויון 3.6 מתקבל:

$$\tilde{f}(\tilde{A}) > 1.08\beta\gamma_L$$

ולפי נוסחה 3.1 מכאן נובע

$$\tilde{\gamma}\tilde{\beta} > 1.07\beta\gamma_L$$

(נוסחה 3.1 נכונה עבור $\tilde{f},\tilde{\beta},\tilde{\gamma}$ כשם שהיא נכונה עבור f,β,γ. כאן נעשה השימוש בנוסחה עבור הקבוצות $\tilde{A},\tilde{B}$. החסם שהוכח על $\tilde{\beta}$ מראה ש $\tilde{B}$ עומדת בתנאי למה 2.2. הסיבה לכך ש

$\tilde{A}$ עומדת בתנאי הלמה תוסבר בהערה בהמשך)

לפי $\tilde{\beta} < \beta(1+n^{-1/10})$ $\tilde{\gamma} > 1.06\gamma_L$

לכן $\tilde{\gamma}^{100}\tilde{l} > 50\gamma_L^{100}l_L$

ולפי טענה 3.1 $\tilde{\gamma}^{100}\tilde{l} > (50/3)\gamma^{100}l > 4\gamma^{100}l$

אם באי שיויון 3.9 נכפיל אגף שמאל ב $\tilde{\alpha}$ ואגף ימין ב $\alpha(U,I)$ (שזה אותו דבר) נקבל:

$$\tilde{\alpha}\tilde{f}(\tilde{A}) > 0.81\alpha(U,I)f(U,I)$$

ולפי טענה 3.10 (סעיף 1): $\tilde{\alpha}\tilde{f}(\tilde{A}) > (0.81/50)\alpha_{C_5}f_4(C_5)$

לפי אי שויון 3.7 מתקבל: $\tilde{\alpha}\tilde{f}(\tilde{A}) > 0.014\alpha\beta\gamma_L$

לפי נוסחה 3.1 מכאן נובע: $\tilde{\alpha}\tilde{\beta}\tilde{\gamma} > 0.013\alpha\beta\gamma_L$

ולפי $\tilde{\beta} < \beta(1+n^{-1/10})$ $\tilde{\alpha}\tilde{\gamma} > 0.012\alpha\gamma_L$

לכן לפי טענה 3.1 $\tilde{\alpha}\tilde{\gamma} > 0.005\alpha\gamma=(1/200)\alpha\gamma$

<u>הערה:</u>

השתמשנו בנוסחה 3.1, מבלי להוכיח ש $\tilde{A}$ עומדת בתנאי למה 2.2. זה נכון כי אחרת בנוסחה $\tilde{\alpha}\tilde{f}(\tilde{A}) > 0.014\alpha\beta\gamma_L$ נציב את אי שויון 3.1' ונקבל: $\tilde{\alpha}\tilde{\beta}\tilde{\gamma}*\tilde{n}^{-1/100}/\tilde{\alpha} > 0.014\alpha\beta\gamma_L$ נציב $\tilde{\beta}<2\beta$ ו $\tilde{\gamma}\leq 1$ ונקבל: $2*\tilde{n}^{-1/100} > 0.014\alpha\gamma_L > 0.007\alpha\gamma$ בסתירה לחסמים שנדרשו על α ועל γ בתנאי המשפט.

קבלנו אם כן את החסמים הנדרשים על $\tilde{\beta}$ ועל $\tilde{\gamma}^{100}\tilde{l}$ ו $\tilde{\alpha}\tilde{\gamma}$.

סוף אפשרות ב'.

ג.2: למה מרכזית.

למה 3.1 היותה רק הכנה ללמה הבאה שממלאת תפקיד מקביל ללמה המרכזית בהוכחת החסם הדטרמיניסטי של [KW] (טענה 3 עליה סיפרנו בהקדמה לפרק).

<u>למה 3.2 (למה מרכזית):</u>

יהי P פרוטוקול הפותר בעית R^m_{stc} עם פרמטרים $(n,l,\alpha,\beta,\gamma)$ המקימים:

$\gamma^{100}>n^{-\varepsilon}$, $\beta>2*2^{-n^{1/1000}}$, $\alpha>n^{-0.9/1000}$, $n^{1.1/200}<l<n^{1/100}$ **(כאשר $\varepsilon=10^{-6}$ כפי שהנחנו בלמה 3.1). אזי מ P אפשר לייצר פרוטוקול $\tilde{P}$ (בעל סיבוכיות תקשורת קטנה או שוה לזאת של P), הפותר בעיית R^m_{stc} עם פרמטרים $(\tilde{n},\tilde{l},\tilde{\alpha},\tilde{\beta},\tilde{\gamma})$ המקימים:**

$$\tilde{n}>n-\sqrt{n}*\log n \quad , \quad \tilde{l}\le l \quad , \quad \tilde{\alpha}>n^{-1/10000}\sqrt{\alpha} \quad , \quad \tilde{\beta}>\beta/4 \quad , \quad \tilde{\gamma}^{100}\tilde{l}>k_\gamma\gamma^{100}l$$

כאשר k_γ הוא הקבוע הקטן הגלובלי מלמה 3.1 $\left(k_\gamma=\frac{1}{3*40^{100}}\right)$

(<u>הערה:</u> החסמים התחתונים על α,β,l בלמה זאת נקבעו להיות גדולים במעט מאלה בלמה 3.1, כדי לאפשר הפעלה חוזרת של למה 3.1.)

<u>הוכחה:</u>

נשתמש בלמה 3.1. ננסה להפעיל את אפשרות א של הלמה. אם אפשרות ב היא זאת שמתקימת נחזור ונפעיל אפשרות זאת שוב ושוב, עד שמתקיים התנאי של אפשרות א. בכל פעם שמופעלת אפשרות ב גדל $\gamma^{100}*l$ בפקטור 4, מכיוון ש l אינו גדל הרי ש γ^{100} גדל בפקטור של 4 לפחות. בתחילה $\gamma^{100}>n^{-\varepsilon}$ ובסיום $\gamma^{100}\le 1$ (מעצם הגדרתו) לכן לא יתכן שאפשרות ב הופעלה יותר מ $\varepsilon\log n$ פעמים. יוצא, אם כן, שאנו מפעילים את אפשרות ב מס' פעמים קטן מ $\varepsilon\log n$ ואחרכן פעם אחת את אפשרות א. הפרוטוקול הסופי $\tilde{P}$ שמתקבל הוא המבוקש. נבדוק מה קרה לפרמטרים השונים:

מס' הקודקודים: $\tilde{n} \geq n-\sqrt{n}*\varepsilon\log n-\sqrt{n} > n-\sqrt{n}*\log n$

אורך המסלול: $\tilde{l} \leq l$

נסמן ב $\hat{n},\hat{l},\hat{\alpha},\hat{\beta},\hat{\gamma}$ את הפרמטרים המתקבלים לפני הפעלת אפשרות א. נקבל:

צפיפות המסלולים: $\hat{\alpha}\hat{\gamma} \geq \left(\frac{1}{200}\right)^{\varepsilon\log n}\alpha\gamma$

לכן: $\hat{\alpha} \geq \left(\frac{1}{200}\right)^{\varepsilon\log n}(\gamma/\hat{\gamma})*\alpha$

ואילו: $\tilde{\alpha}>\sqrt{\hat{\alpha}}/25$

נציב $\varepsilon=10^{-6}$, $\gamma>n^{-\varepsilon/100}$ ו $\hat{\gamma}\leq 1$ ונקבל: $\tilde{\alpha} >n^{-1/10000}\sqrt{\alpha}$

צפיפות הרחבים: $\hat{\beta} \geq (1-n^{-1/10})^{\varepsilon\log n}*\beta = (1-o(1))*\beta$

לכן: $\tilde{\beta} > \hat{\beta}/2 > \beta/4$

ואילו: $\tilde{\gamma}^{100}\tilde{l} > k_\gamma\hat{\gamma}^{100}\hat{l} \geq k_\gamma\gamma^{100}l$

קיבלנו את החסמים שדרשנו על $\tilde{\alpha},\tilde{\beta},\tilde{\gamma}^{100}\tilde{l}$. נראה עכשיו שאומנם אפשר להשתמש שוב ושוב בלמה 3.1. לשם כך צריך להראות שהפרמטרים השונים עומדים בתנאי למה 3.1 לאורך כל הדרך: החסמים שקבלנו על $\hat{\alpha}$ ו $\hat{\beta}$ תקפים לאורך כל הדרך ומקימים תנאי למה 3.1 (לשם כך הגדלנו מעט את החסמים התחתונים על α ו β בתנאי למה 3.2). החסם $\gamma^{100}>n^{-\varepsilon}$ תקף לאורך כל הדרך מכיון שצפיפות ההצלחה רק גדלה כאשר מופעלת אפשרות ב של למה 3.1.

כל שנותר הוא להוכיח את החסם המתאים עבור אורך המסלול. מכיון שאורך המסלול רק קטן, מספיק להוכיח את החסם עבור $\hat{l}$. נזכור ש $\hat{\gamma}^{100}*\hat{l} \geq \gamma^{100}*l$ לכן $\hat{l} \geq (\gamma^{100}/\hat{\gamma}^{100})*l$

נציב $\gamma^{100}>n^{-\varepsilon}$ ו $\hat{\gamma}^{100}\leq 1$ ונקבל: $\hat{l} > n^{-\varepsilon}*l > n^{1/200}$

(לשם כך הוגדל החסם שנדרש על l).

סוף הוכחת למה 3.2

ג.3: חסם תחתון לפרוטוקול דטרמיניסטי עם טעויות.

בהקדמה לפרק ראינו שמשפט 1.5 (חסם דטרמיניסטי ל R^m_{stc}) נבע מ 3 טענות. למה 3.2 מתפקדת בצורה דומה לטענה השלישית, שהיתה הטענה המרכזית שם, ומצביעה על האפשרות "להגדיל" את α בכל פעם שערכו קטן מערך מסוים. נוכיח עתה שתי למות נוספות שיתפקדו בצורה דומה לשתי הטענות האחרות.

למה 3.3, שהיא המקבילה לטענה הראשונה שם, מהוה למעשה את המקרה הבסיסי בהוכחה האינדוקטיבית, ומראה שאם α,β,γ גדולים מספיק סיבוכיות התקשורת גדולה מ 0.

<u>למה 3.3:</u>

עבור $n^{1/200}\le l\le n^{1/100}$, $\alpha\ge n^{-1/100}$, $\beta\ge 2^{-n^{1/100}}$, $\gamma\ge n^{-1/1000}$ מתקיים $C(n,l,\alpha,\beta,\gamma)>0$

<u>הוכחה:</u>

נניח בשלילה $C(n,l,\alpha,\beta,\gamma)=0$ אזי יש קבוצות A,B המעידות על כך. מכיון שסיבוכיות תקשורת 0 פרושה שהתשובה כבר ידועה, הרי שיש תשובה i שנכונה עבור $\gamma*|O_{AB}|$ זוגות $(a,b)\in O_{AB}$. מכיון שהתשובה i נכונה רק בקבוצה O^i_{AB} מתקבל מכאן ש:

$$|O^i_{AB}|\ge\gamma*|O_{AB}|=\gamma*l*\left(\sum_{j=1}^{l}|O^j_{AB}|/l\right)$$

וזאת בסתירה למסקנה 2.1, כי $\gamma*l>2$ (ותנאי למה 2.2 מתקיימים)

סוף הוכחת למה 3.3.

למה 3.4, שהיא המקבילה לטענה השניה, בודקת מה קורה ל α,β,γ כאשר "יורדים" בעץ הפרוטוקול, כלומר, לאחר שהשחקנים החליפו ביניהם מספר ביטים של מידע. בגלל הצורך לחסום בצורה מספקת גם את הקטנת α וגם את הקטנת γ, נוח להתבונן בפרוטוקול הנוצר לאחר העברת $O(\log n)$ ביטי מידע, ולא ביט מידע בודד.

למה 3.4:

עבור $\alpha \geq n^{-1/2000}$, $\beta \geq 2^{-n^{1/2000}}$, $\gamma \geq n^{-1/100000}$ ו $n^{1/200} \leq l \leq n^{1/100}$

מתקיים $C(n,l,\alpha,\beta,\gamma) \geq C(n,l,\tilde{\alpha},\tilde{\beta},\tilde{\gamma}) + k*\log_2 n$

כאשר $\tilde{\alpha} \geq n^{-1/10000}*\alpha$, $\tilde{\beta} \geq n^{-1/10000}*\beta$, $\tilde{\gamma} \geq \gamma/2$ ו k קבוע קטן. אצלנו נניח $k=10^{-6}$.

הוכחה:

יהי P פרוטוקול לפתרון R^m_{stc} עם פרמטרים $(n,l,\alpha,\beta,\gamma)$ הפועל בסיבוכיות $C(n,l,\alpha,\beta,\gamma)$, ויהיו A,B קבוצות הקלטים עליהן פועל P. נתבונן ב $k\log_2 n$ הצעדים הראשונים של הפרוטוקול: בכל צעד מחלק אחד השחקנים את קבוצת הקלטים האפשריים שלו לשניים, ואומר באיזה משני החלקים נמצא הקלט שלו. לכן $k\log_2 n$ הצעדים הראשונים מהוים עץ שבו m עלים, כאשר $m \leq n^k$. על כל עלה i $(1 \leq i \leq m)$ "יושבות" קבוצות קלטים A_i, B_i. המכפלות $\{A_i * B_i\}_{i=1}^m$ מהוות חלוקה של A*B. המשך הפרוטוקול על כל עלה מהוה פרוטוקול חדש P_i לפתרון R^m_{stc} עם פרמטרים $(n,l,\alpha_i,\beta_i,\gamma_i)$ מסוימים. נראה שאחד מהפרוטוקולים האלה הוא פרוטוקול עם פרמטרים $(n,l,\tilde{\alpha},\tilde{\beta},\tilde{\gamma})$ אשר מעיד על נכונות הלמה.

מכיון שהפרוטוקול P מורכב מהפרוטוקולים $\{P_i\}_1^m$ הפועלים על העלים השונים, מתקיים:

$$\bigcup_{i=1}^{m} T_{A_iB_i} = T_{AB}$$

ולכן:

$$\sum_{i=1}^{m} \gamma_i * |O_{A_iB_i}| = \gamma * |O_{AB}|$$

ברצוננו למצוא אינדקס i עבורו $\alpha_i, \beta_i, \gamma_i$ גדולים שלושתם מהחסמים על $\tilde{\alpha},\tilde{\beta},\tilde{\gamma}$ (בהתאמה).

לכן נפרק את הסכום השמאלי לארבעה סכומים. נגדיר:

$V_\alpha = \{i \mid 1 \le i \le m \qquad \alpha_i \le n^{-1/10000}\alpha\}$

$V_\beta = \{i \mid 1 \le i \le m \qquad \beta_i \le n^{-1/10000}\beta\}$

$V_\gamma = \{i \mid 1 \le i \le m \qquad \gamma_i \le \gamma/2\}$

$V = \{i \mid 1 \le i \le m \qquad i \notin V_\alpha \cup V_\beta \cup V_\gamma\}$ ו

ונקבל

$$\gamma * |O_{AB}| \le \sum_{V_\alpha} \gamma_i * |O_{A_iB_i}| + \sum_{V_\beta} \gamma_i * |O_{A_iB_i}| + \sum_{V_\gamma} \gamma_i * |O_{A_iB_i}| + \sum_{V} \gamma_i * |O_{A_iB_i}| \qquad 3.10$$

נראה שכל אחד משלושת הסכומים הראשונים קטן למדי:

לפי למה 2.2 לכל $i \in V_\alpha$ $\qquad |O_{A_iB_i}| \le 2 * n^{-1/10000} * \alpha * \beta * |O_N|$

(זה נכון כי $\alpha_i \le n^{-1/10000} * \alpha$ ו $\beta_i \le \beta$. גם אם α_i או β_i אינם עומדים בתנאי למה 2.2 נוכל להוסיף שרירותית ל A_i או ל B_i, איברים, עד שיהיו גדולות מספיק ויעמדו בתנאי הלמה).

נזכור ש $\gamma_i \le 1$ ונקבל:

$$\sum_{V_\alpha} \gamma_i * |O_{A_iB_i}| \le 2 * n^k * n^{-1/10000} \alpha\beta |O_N|$$

$$\sum_{V_\beta} \gamma_i * |O_{A_iB_i}| \le 2 * n^k * n^{-1/10000} \alpha\beta |O_N|$$

באותה צורה מתקבל:

לפי ש $\{A_i * B_i\}_{i=1}^m$ חלוקה של $A*B$ ושלכל $i \in V_\gamma$ $\gamma_i \le \gamma/2$. מתקבל:

$$\sum_{V_\gamma} \gamma_i * |O_{A_iB_i}| \le \gamma/2 \sum_{V_\gamma} |O_{A_iB_i}| \le \gamma |O_{AB}|/2$$

נציב כל זאת באי שויון 3.10, ונזכור שלפי למה 2.2 $\qquad |O_{AB}| = (1+O(n^{-1/10}))\alpha * \beta * |O_N|$

ונקבל:

$$\sum_{V}\gamma_i*|O_{A_iB_i}| \geq \alpha\beta\gamma|O_N|*(0.9*0.5-4*n^k*n^{-1/10000}/\gamma) > 0$$

לכן V אינה ריקה , לכן יש $i\in V$. נסמן $\tilde{\alpha}=\alpha_i, \tilde{\beta}=\beta_i, \tilde{\gamma}=\gamma_i$ ונקבל ש $\tilde{\alpha},\tilde{\beta},\tilde{\gamma}$ עומדים בתנאי

הלמה. הפרוטוקול P_i פותר בעית R^m_{stc} עם פרמטרים $(n,l,\tilde{\alpha},\tilde{\beta},\tilde{\gamma})$.

מאחר שפרמטרים אלה עומדים בתנאי למה 3.3 ברור שסיבוכיות P_i אינה 0 ולכן העלה ה i חייב

להיות ברמה ה $k*\log_2 n$ של עץ הפרוטוקול P שפיתחנו (אחרת היינו ממשיכים לפתחו). לכן P_i

התקבל מ P אחרי העברת $k*\log_2 n$ ביטי מידע ולכן הסיבוכיות שלו קטנה לפחות ב $k*\log_2 n$.

לכן P_i מעיד על כך ש: $C(n,l,\alpha,\beta,\gamma) \geq C(n,l,\tilde{\alpha},\tilde{\beta},\tilde{\gamma})+k*\log_2 n$

סוף הוכחת למה 3.4

נראה עתה כיצד להשתמש בלמות 3.2 ו 3.4 על מנת לקבל חסם תחתון לפרוטוקול הפותר בעיית

R^m_{stc} עם פרמטרים. ההוכחה תתקבל ע"י הפעלה אינדוקטיבית של שתי הלמות, לסרוגין.

השמוש בלמה 3.3, המהוה את בסיס האינדוקציה, כבר הוכנס בהוכחת למה 3.4.

<u>משפט 3.1:</u>

עבור $l=n^{1/100}$ $\quad C(n,l,1,1,1/4)=\Omega(\log n*\log l)$

(<u>הערה:</u> המשפט נכון גם עבור אורכים אחרים של המסלול, וכן כם לפרמטרים α,β,γ אחרים.)

<u>הוכחה:</u>

על פרמטרים $(n,l,\alpha,\beta,\gamma)$, העומדים בתנאי למות 3.2 ו 3.4, נפעיל קודם את למה 3.4 ואחר כך

את למה 3.2 ונקבל: $C(n,l,\alpha,\beta,\gamma) \geq C(\tilde{n},\tilde{l},\tilde{\alpha},\tilde{\beta},\tilde{\gamma})+k\log_2 n$

כאשר k קבוע כלשהו, ו: $\tilde{n} > n-\sqrt{n}*\log n \quad , \quad \tilde{l} \leq l \quad , \quad \tilde{\alpha} > n^{-1/10000}*n^{-1/20000}*\sqrt{\alpha}$

$\tilde{\beta} > 1/4*n^{-1/10000}\beta \quad , \quad \tilde{\gamma}^{100}\tilde{l} > k_\gamma*(1/2)^{100}\gamma^{100}*l$.

אם נניח $\alpha \geq n^{-1/2000}$ נקבל גם $\tilde{\alpha} > \tilde{n}^{-1/2000}$.

לכן נוכל להתחיל עם פרמטרים $(n,l,1,1,1/4)$ ולהפעיל שוב ושוב את התהליך, $O(\log n)$ פעמים

עד אשר $\tilde{\gamma}^{100}\tilde{l} \leq \tilde{n}^{-\varepsilon}*l$.

בכל שלב לפני השלב הסופי מתקיים: $\tilde{\alpha} > n^{-1/2000}$ $\quad \tilde{l} \leq l \quad \tilde{n} > n/2$

$$\tilde{\beta} > (1/4*n^{-1/10000})^{O(\log n)} > 2^{-\tilde{n}^{1/2000}}$$

ו: $\tilde{\gamma}^{100}\tilde{l} > \tilde{n}^{-\varepsilon}*l$

מאי שויון זה נובע גם ש: $\tilde{\gamma}^{100} > \tilde{n}^{-\varepsilon}$

וגם ש: $\tilde{l} > \tilde{n}^{-\varepsilon}*l > n^{1/150}$

כך שתנאי למות 3.2 ו 3.4 אכן מתקימים לאורך כל הדרך.

בסה"כ קיבלנו: $c(n,l,1,1,1/4) \geq k*\log_2 n*O(\log n) = O(\log^2 n)$

סוף הוכחת משפט 3.1

ג.4: חסם תחתון לפרוטוקול הסתברותי.

כל שנותר, כדי להוכיח את ההכללה ההסתברותית למשפט 1.5, הוא להראות כיצד עוברים מחסם לפרוטוקול דטרמיניסטי עם שגיאות, לחסם על פרוטוקול הסתברותי.

משפט 3.2:

עבור $l=n^{1/100}$ $\quad C_{1/2}(R^m_{stc(l)})=\Omega(\log^2 n)$

הוכחה:

יהי P פרוטוקול הסתברותי לפתרון $R^m_{stc(l)}$ הטועה בהסתברות 1/2. P הוא קומבינציה קמורה של k פרוטוקולים דטרמיניסטים כך שלכל $(a,b)\in O_N$ לפחות k/2 מביניהם נותנים תשובה נכונה. לפחות k/6 מבין הפרוטוקולים נותנים תשובות נכונות על לפחות $|O_N|/3$ זוגות (כי $5/6*1/3+1/6<1/2$).

כל פרוטוקול כזה הוא פרוטוקול דטרמיניסטי ל R^m_{stc} עם פרמטרים $(n,l,1,1,1/3)$ ולכן מקיים את משפט 3.1. גם אם נסיר מפרוטוקול כזה את $|O_N|/12$ זוגות הקלטים שלהם הסיבוכיות הגבוהה ביותר (ע"י עצירה אחרי מס' צעדים מסוים), ונניח שעבורם התשובה מוטעית, עדיין יתקימו, עבור פרוטוקול כזה, תנאי משפט 3.1 (כי $\gamma\geq 1/3-1/12=1/4$). לכן כל פרוטוקול כזה נותן סיבוכיות $\Omega(\log^2 n)$ עבור לפחות 1/12 מזוגות הקלטים. מכיון ש 1/6 מהפרוטוקולים הם כאלה, ברור מכאן שסיבוכיות P היא $\Omega(\log^2 n)$.

סוף הוכחת המשפט.

פרק ד: עוד על קשירות st- בגרפים.

בפרק זה נמשיך לעסוק בבעיות של קשירות בגרפים, ונוכיח תוצאה לגבי מעגלים בוליאנים. התוצאה תעסוק בחישוב "מונוטוני־למחצה" של פונקצית ה קשירות-st.

ד.1: חסם תחתון לחישוב מונוטוני־למחצה של קשירות -st.

נתבונן במעגלים בוליאנים לחישוב הפונקציה stc, בהם מופעלות שלילות רק על מישתני הקלט עצמם, (כל מעגל אפשר להעביר לצורה כזאת מבלי לשנות את עומקו). מכיון ש stc היא פונקציה מונוטונית חייב כל משתנה קלט להופיע בחיוב (ללא הפעלה של שלילה עליו). אם אף משתנה קלט אינו מופיע בשלילה המעגל הוא מונוטוני, משפט 1.5 תקף, ולכן עומק המעגל הוא $\Omega(\log^2 n)$. אם מאפשרים שלילה על כל משתני הקלט המעגל הוא מעגל לא מונוטוני כללי, ועל עומקו לא ידוע חסם לא טריויאלי. נשאלת השאלה: מה קורה אם מאפשרים שלילות על קבוצה מוגבלת של משתני קלט? או באופן הפוך: מה אפשר לאמר על מספר משתני הקלט המופיעים בשלילה, כפונקציה של עומק המעגל?

ננסה לנתח את הבעיה מנקודת מבט של סיבוכיות־תקשורת: תהי $f:\{0,1\}^n\to\{0,1\}$ פונקציה בוליאנית מונוטונית, ותהי $E\subset[n]$ קבוצת אינדקסים. נאמר שמעגל בוליאני הוא מונוטוני מחוץ ל E אם משתני הקלט היחידים עליהם מופעלת שלילה הם אלה המתאימים לקבוצת האינדקסים E. נסמן ב $d^E(f)$ את העומק המיזערי של מעגל בוליאני, מונוטוני מחוץ ל E, המחשב את f. אם $E=[n]$ המעגל הוא כללי ו $d^E(f)=C(R_f)$. אם $E=\emptyset$ המעגל הוא מונוטוני ו $d^E(f)=C(R_f^m)$. נגדיר לכל E משחק תקשורת חדש:

$R_f^E\subset f^{-1}(1)*f^{-1}(0)*[n]$ ע"י $(x,y,i)\in R_f^E$ אמ"ם $x_i=1,y_i=0$ או $x_i=0,y_i=1$ ו $i\in E$.

כלומר: שחקן I מקבל קלט x עבורו $f(x)=1$, שחקן II מקבל קלט y עבורו $f(y)=0$, ומטרתם של השחקנים היא למצוא קורדינטה מחוץ ל E שבה ב x יש 1 וב y 0, או קורדינטה בתוך E שבה שני הקלטים שונים.

כאשר $E=[n]$ $R_f^E=R_f$, כאשר $E=\emptyset$ $R_f^E=R_f^m$.

המשפט הבא מכליל את משפט 1.1. ההוכחה זהה לחלוטין להוכחת משפט 1.1, שהיא הוכחה אינדוקטיבית פשוטה שנתנה ב [KW]. לא נכלול הוכחה זאת כאן.

משפט 4.1:

לכל פונקציה בוליאנית מונוטונית f, וקבוצת אינדקסים E מתקיים $d^E(f)=C(R_f^E)$.

הערה:

אם נתיר סיבוכיות אין־סופיות יהיה המשפט נכון באותן הגדרות גם לפונקציות שאינן מונוטוניות.

נחזור כעת לעסוק בפונקציה $f=stc$. משפט 4.2 יתן חסם תחתון ל $C(R_{stc}^E)$ ולכן גם ל $d^E(stc)$, חסם זה יהיה גבוה יותר ככל שהקבוצה E קטנה יותר. הוכחת המשפט אינה יחודית לפונקציה stc ויכולה להעשות גם לפונקציות אחרות.

האינטואיציה למשפט 4.2 באה מהחסם ההסתברותי של משפט 3.2. כדי לקבל תוצאה חזקה יותר נשתמש בגירסה של משפט 1.5 (שגם לה מובן הסתברותי) הטוענת את הטענה הבאה:

משפט 1.5 [KW]:

עבור $l\le n^{1/10}$ כל פרוטוקול תקשורת דטרמיניסטי לפתרון $R_{stc(l)}^m$, הנותן תשובה נכונה לכל זוג $(a,b)\in A*B$ כאשר $B=B_N$ ו $A\subset A_N$ בעלת עוצמה $|A|\ge|A_N|/2$, הוא בעל סיבוכיות של $\Omega(\log n*\log l)$.

(הערה: המשפט נכון גם לקבוצות קלטים A,B קטנות יותר.)

משפט 4.2:

לכל $l<n^{1/100}$ וקבוצת אינדקסים E שעוצמתה $|E|<(n/l)^2/100$ מתקיים

$C(R^E_{stc}) = \Omega(\log n * \log l)$.

הוכחה:

באופן אינטואיטיבי יהיה המשפט נכון, אם ההסתברות לכך שמסלול באורך l חותך את הקבוצה E קטנה. במקרה כזה פרוטוקול לפתרון $R^E_{stc(l)}$ נותן פעמים רבות יחסית תשובה i שאינה ב E. תשובה כזאת מהוה גם תשובה ל $R^m_{stc(l)}$ ולכן יש רדוקציה הסתברותית מהבעיה $R^m_{stc(l)}$ ל $R^E_{stc(l)}$. מכיון שהחסם ל $C(R^m_{stc(l)})$ נכון הסתברותית, נקבל מכאן חסם ל $C(R^E_{stc(l)})$.

למעשה כדי שההסתברות לחיתוך בין מסלול באורך l לקבוצה E תהיה נמוכה, צריך לדרוש דרישה נוספת על E (למשל נוכל לדרוש שדרגת E כגרף תהיה נמוכה). כדי לחסוך תנאי נוסף כזה, ההוכחה שניתן תעבור דרך פונקציה מעט שונה שתקרא פונקצית הקשירות ST- (STc):

פונקצית הקשירות ST- מקבלת כקלט גרף לא מכוון בעל קבוצת קודקודים N שעוצמתה 3n. ב N מוכלות שתי קבוצות קודקודים זרות S ו T שעוצמתן n. פלט הפונקציה הוא 1 אם יש מסלול בין S ל T ו 0 אחרת.

לפיכך minterm של הפונקציה הוא מסלול בין S ל T העובר רק דרך קודקודים ב $N-(S\cup T)$, maxterm של הפונקציה הוא חתך המפריד בין S ל T (שמפורש גם כצביעה בצבעים s ו t). כמו בעבר תהיה המטרה בבעיה R^m_{STc}, מציאת קשת במסלול שהיא דו־צבועה לפי הצביעה . הבעיה $R^m_{STc(l)}$ תוגדר להיות צמצום בעיה זאת למקרה שבו אורך המסלול הוא l.

בין פונקצית הקשירות st- לפונקצית הקשירות ST- קיימות שתי רדוקציות פשוטות , המראות שמבחינת סיבוכיות שתי הפונקציות כמעט זהות. רדוקציות אלה יאפשרו לנו להוכיח את שתי הטענות הבאות: טענה 4.1 תאמר שאותו החסם ממשפט 1.5 נכון גם עבור הפונקציה STc. טענה 4.2 תראה שמספיק להוכיח את משפט 4.2 עבור הפונקציה STc.

טענה 4.1:

עבור $l \le n^{1/10}$ כל פרוטוקול תקשורת דטרמיניסטי לפתרון $R^m_{STc(l)}$ הנותן תשובה נכונה לכל זוג $(a,b) \in A*B$, כאשר B היא קבוצת כל הצביעות האפשריות (maxterms) ו A מכילה לפחות חצי מהמסלולים האפשריים (minterms), הוא בעל סיבוכיות של $\Omega(\log n * \log l)$.

הוכחה:

נפרק את קבוצת המסלולים A ל n^2 קבוצות, לפי קודקוד ההתחלה של המסלול $(s \in S)$, וקודקוד הסיום $(t \in T)$. לפחות אחת מהקבוצות האלה $A(s,t)$ מכילה לפחות חצי מהמסלולים האפשריים בין s ל t. צמצום פרוטוקול התקשורת לקבוצה זאת, נותן פרוטוקול לפתרון $R^m_{stc(l)}$ העומד בתנאי משפט 1.5 (בניסוחו האחרון). לכן הפרוטוקול המצומצם והפרוטוקול כולו הם בעלי סיבוכיות של $\Omega(\log n * \log l)$.

סוף הוכחת הטענה.

טענה 4.2:

כדי להוכיח את משפט 4.2 מספיק להוכיח שלכל $l < n^{1/10}$ וקבוצת אינדקסים E שעוצמתה $|E| < (n/l)^2/10$ מתקיים $C(R^E_{STc}) = \Omega(\log n * \log l)$.

הוכחה:

נזכור שלפי משפט 4.1 $C(R^E_{STc}) = d^E(STc)$, $C(R^E_{stc}) = d^E(stc)$.

הטענה נובעת באופן מיידי מכך שכל מעגל לפתרון stc עם m קודקודים, מהוה גם מעגל לפתרון STc עם 3n קודקודים , כאשר $3n=m-2$. זה נכון כי מתוך m-2 הקודקודים הלא מיוחדים במקור, נבחר שתי קבוצות זרות שגודלן n (S ו T). את הקבוצה S נחבר לקודקוד s ואת T נחבר ל t. כעת יש מסלול בין S ל T אמ"ם יש מסלול בין s ל t. מכיון ש

$$(m/l)^2/100 = ((3n+2)/l)^2/100 < (n/l)^2/10$$

ומכיון ש $m^{1/100} = (3n+2)^{1/100} < n^{1/10}$

הרי שמעגל הסותר את משפט 4.2 סותר גם את התנאי המספיק בטענה 4.2.

סוף הוכחת הטענה.

כל שנותר על מנת להוכיח את משפט 4.2, הוא לחזור במדויק על הטיעון האינטואיטיבי מתחילת ההוכחה, עבור הפונקציה STc:

עבור $l<n^{1/10}$ וקבוצת אינדקסים E המקיימת $|E|<(n/l)^2/10$ יהי P פרוטוקול לפתרון R^E_{STc}.

נראה כיצד לקבל מ P פרוטוקול חדש לפתרון $R^m_{STc(l)}$:

בבעיה $R^m_{STc(l)}$ לשחקן I מסלול a באורך l שהוא minterm של STc, עליו נסתכל כגרף G_a $(STc(G_a)=1)$. לשחקן II חתך b המפריד בין S ל T שהוא maxterm של STc, עליו נסתכל כגרף G_b $(STc(G_b)=0)$. שחקן II יסיר מ G_b את כל הצלעות הנמצאות בקבוצה E, ויקבל גרף חדש G_b' שגם עליו $STc(G_b')=0$.

על הזוג (G_a, G_b') יפעילו שני השחקנים את הפרוטוקול P ויקבלו תשובה i. מכיוון ש G_b' מאופס על הקבוצה E הרי שהתשובה i היא צלע ב $G_a - G_b'$. כלומר i היא צלע במסלול a שחוצה את החתך b, או צלע במסלול a הנמצאת בקבוצה E. אם המסלול a אינו חותך את הקבוצה E הרי שהאפשרות הראשונה היא שמתקיימת, ולכן התשובה i שקיבלנו מהוה פתרון נכון ל $R^m_{STc(l)}$.

קיבלנו אם כן פרוטוקול ל $R^m_{STc(l)}$ שנותן תשובה נכונה בכל מקרה שבו המסלול a זר ל E.

ההסתברות לכך שהצלע ה i במסלול מקרי באורך l בין S ל T, נמצאת ב E, מקיימת: $Pr(a_i \in E) \le (n/l)^2/(10*n(n-1)) < 1/(5l^2)$ לכן ההסתברות לכך שמסלול מקרי באורך l בין S ל T אינו חותך את E מקיימת: $Pr(a \cap E=\emptyset) \ge 1-l*1/(5l^2) > 1/2$

לכן הפרוטוקול החדש שקיבלנו עומד בתנאי טענה 4.1 ולכן הוא בעל סיבוכיות של $\Omega(\log n*\log l)$.

מכיוון שסיבוכיות הפרוטוקול החדש אינה גבוהה מזאת של המקורי הרי ש P הוא בעל סיבוכיות של $\Omega(\log n*\log l)$. לכן מתקיים התנאי המספיק מטענה 4.2 ולפי טענה זאת מכאן נובע משפט 4.2.

סוף הוכחת משפט 4.2.

<u>מסקנה 4.1:</u>

בכל מעגל NC_1 לפתרון הפונקציה stc מופעלות שלילות על $\Omega(n^2)$ משתני קלט.

פרק ה: עומק החישוב המונוטוני של פונקציות ה־ Clique וה־ Matching.

אחת הפונקציות שסיבוכיות התקשורת שלה נחקרה ביסודיות, היא פונקצית "זרות הקבוצות" (Disjointness) , אותה הכרנו בסעיף א.3, ושתכונה להלן DISJ. עבור סיבוכיות התקשורת של פונקציה זאת ידוע חסם תחתון ליניארי, גם במקרה ההסתברותי:

משפט 5.1 [KS]:

$$C_{1/3}(DISJ) = \Omega(n)$$

בפרק זה נראה כיצד חסם זה, המענין גם לכשעצמו, מהוה כלי עזר חזק להוכחת חסמים תחתונים לעומק של מעגלים מונוטונים המחשבים פונקציות מסוימות.

בסעיף א.5 הכרנו את פונקצית הזווג בגרפים. הזכרנו שלעומק החישוב המונוטוני של פונקציה זאת ידוע חסם תחתון של $\Omega(\log^2 n)$ [R2]. בפרק זה נראה, בעזרת שורה של רדוקציות פשוטות, כיצד אפשר ל"תרגם" כל מעגל מונוטוני לחישוב פונקצית הזווג בגרף, לפרוטוקול תקשורת הסתברותי לפתרון בעיית זרות־הקבוצות. רדוקציה זאת מראה שעומק מעגל מונוטוני לחישוב פונקצית הזווג הוא ליניארי. בהמשך הפרק נראה כיצד אותה הוכחה נותנת חסמים גם עבור מספר פונקציות נוספות, ונקבל כמסקנה קיומו של פער אקספוננציאלי בין עומק חישוב מונוטוני לבין עומק חישוב כללי.

ת.1: חסם תחתון לפונקצית הזווג בגרף.

תהי N קבוצת קודקודים שעוצמתה $|N|=3n$. תהי MATCH הפונקציה המונוטונית המקבלת כקלט גרף G על קבוצת הקודקודים N, ונותנת כפלט $MATCH(G)=1$ אמ"ם בגרף G יש זווג בגודל n (n צלעות שאינן נחתכות), אחרת $MATCH(G)=0$. נוכיח:

משפט 5.2:

$$d^m(MATCH)=\Omega(n)$$

סימונים:

נסמן ב P_N את קבוצת כל הזווגים בגודל n על N (כלומר, כל איבר ב P_N הוא קבוצה של n צלעות שאינן נחתכות). נסמן ב Q_N את קבוצת כל תתי הקבוצות בגודל n של N. נסמן ב $\hat{Q}_N$ את קבוצת כל תתי הקבוצות בגודל n-1 של N.

משפט 5.2 יוכח בעזרת משפט 5.1 ע"י מספר רדוקציות פשוטות. הרדוקציה הראשונה תעבור לבעית סיבוכיות תקשורת מתאימה:

היחס $\hat{M}\subset P_N*\hat{Q}_N*\left[\binom{N}{2}\right]$ יוגדר ע"י: $(p,\hat{q},e)\in\hat{M}$ אמ"ם $e\in p$ ו $e\cap\hat{q}=\varnothing$.

כלומר, במשחק התקשורת $\hat{M}$ שחקן I מקבל n צלעות שאינן נחתכות (p), שחקן II מקבל קבוצת קודקודים חלקית בגודל n-1 $(\hat{q})$, ומטרתם למצוא צלע ב p שאינה נשענת על קודקוד ב $\hat{q}$ (יש לפחות אחת כזאת כי $|p|>|\hat{q}|$).

טענה 5.1:

$$C(\hat{M})\le d^m(MATCH)$$

הוכחה:

P_N היא קבוצת ה minterms של הפונקציה MATCH. לכל $\hat{q}\in\hat{Q}_N$ נתאים גרף הכולל את כל

הצלעות הנשענות על קודקוד אחד לפחות מ $\hat{q}$, ונקבל maxterm של הפונקציה MATCH. תחת פירוש זה $\hat{Q}_N$ היא קבוצה של maxterms של הפונקציה MATCH, ומתקבל ש $\hat{M}$ היא תת-בעיה של הבעיה R^m_{MATCH}. כלומר, כל פרוטוקול ל R^m_{MATCH} נותן גם פרוטוקול למשחק $\hat{M}$ לכן $C(\hat{M})\le C(R^m_{MATCH})$, מכאן וממשפט 1.1 מתקבלת הטענה.

סוף הוכחת הטענה.

השלב הבא יהיה לעבור מבעית התקשורת $\hat{M}$, לבעית תקשורת חדשה M שתהיה בעית הכרעה (כלומר M היא פונקציה ולא יחס, ראה הערה בסעיף א.1). הפונקציה $M:P_N*Q_N\rightarrow\{0,1\}$ תוגדר ע"י $M(p,q)=1$ אמ"ם יש צלע $e\in p$ שאינה נשענת על קודקוד ב q. (במשחק התקשורת M, שחקן I מקבל $p\in P_N$, שחקן II מקבל $q\in Q_N$ ומטרתם לאמר האם יש צלע ב p שאינה נשענת על קודקוד ב q).

נרצה להראות, שבמובן הסתברותי מסוים, סיבוכיות התקשורת של M חסומה מלעיל ע"י סיבוכיות התקשורת של $\hat{M}$. לשם כך נגדיר מספר הגדרות נוספות:

לכל זוג $(p,q)\in P_N*Q_N$ נסמן:

מס' הצלעות ב p שאינן נשענות על נקודה ב q. $= n_0(p,q)$

מס' הצלעות ב p הנשענות על נקודה אחת ב q. $= n_1(p,q)$

מס' הצלעות ב p הנשענות על שתי נקודות ב q. $= n_2(p,q)$

לכל $0\le i\le n$ נסמן: $W_i=\{(p,q)\in P_N*Q_N \mid n_0(p,q)=i,\ n_1(p,q)=n-i,\ n_2(p,q)=0\}$

הקבוצות W_i הן תתי-קבוצות זרות של זוגות קלטים ל M.

במונחים אלה הפונקציה M מוגדרת ע"י: $M(p,q)=1$ אמ"ם $(p,q)\in W_0$.

נאמר שפרוטוקול הסתברותי, B , לפתרון בעית התקשורת M, הוא טוב בממוצע, אם הוא מקיים את שתי התכונות הבאות:

1. $Pr_{W_0}[B(p,q) = M(p,q) = 1] = 1$

2. לכל $1 \le i \le n$ $\quad Pr_{W_i}[B(p,q) = M(p,q) = 0] \ge 1/2$

כאשר Pr_{W_i} מתיחס למרחב הסתברות הבוחן את פעולת הפרוטוקול B על קלט מיקרי מהקבוצה W_i (כלומר מרחב מכפלה של התפלגות אחידה על W_i ושל מרחב הטלות המטבע של הפרוטוקול). שתי התכונות אומרות למעשה, ש B צודק תמיד על W_0, וצודק בהסתברות ממוצעת של 1/2 לפחות, על כל קבוצות ה W_i האחרות.

נסמן ב $\tilde{C}(M)$ את סיבוכיות התקשורת המינימלית של פרוטוקול הסתברותי B שהוא טוב בממוצע עבור הבעיה M.

<u>טענה 5.2:</u>

$$\tilde{C}(M) \le C(\hat{M}) + 1$$

<u>הוכחה:</u>

יהי A פרוטוקול דטרמיניסטי אופטימלי לפתרון הבעיה $\hat{M}$. מ A ניצור פרוטוקול הסתברותי B לפתרון הבעיה M:

בהינתן זוג $(p,q) \in P_N * Q_N$, שהוא קלט ל M, על השחקנים לאמר האם $(p,q) \in W_0$. שחקן II יסיר מהקבוצה q שברשותו קודקוד יחיד v (שהוגרל בהתפלגות אחידה) ויקבל קבוצה חדשה $\hat{q} \in \hat{Q}_N$. על הזוג $(p,\hat{q})$ יפעילו שני השחקנים את הפרוטוקול A, ויקבלו תשובה $e=A(p,\hat{q})$ שהיא צלע ב p שאינה נשענת על $\hat{q}$. אם $v \in e$ (הקודקוד המוסר נמצא על הצלע שהתקבלה) יתנו השחקנים את התשובה $B(p,q)=1$. אחרת תנתן התשובה $B(p,q)=0$.

אם $(p,q)\in W_0$ הרי שעל כל צלע ב p יש בדיוק נקודה אחת מ q. לכן אם נסיר מ q נקודה בודדת v, תוותר ב p צלע בודדת שאינה נשענת על $\hat{q}$. צלע זאת היא הצלע עליה נמצא v. מכיון שצלע זאת היא היחידה שאינה נשענת על $\hat{q}$ הרי שהיא תתקבל כתשובה בפרוטוקול A לכן נקבל $B(p,q)=1$, וזוהי תשובה נכונה. כלומר, B תמיד צודק על הקבוצה W_0.

אם $(p,q)\in W_1$ יש ב p צלע יחידה, e_0, שאינה נשענת על q, וב q נקודה יחידה, v_0, שאינה נמצאת על צלע ב p. אם שחקן II מגריל את הנקודה היחידה הזאת, תתקבל בהכרח התשובה $A(p,\hat{q})=e_0$ ולכן $B(p,q)=0$ שהיא תשובה נכונה. בכל מקרה אחר יוסר קודקוד $v_1\in q$ הנמצא על צלע $e_1\in p$. בזוג $(p,\hat{q})$ יש עתה שתי צלעות שהן תשובות אפשריות של הפרוטוקול A, הצלע e_0 והצלע e_1. אחת מהצלעות האלה מוחזרת באופן עיקבי כתשובה e עבור $(p,\hat{q})$ (כי A דטרמיניסטי). אבל לזוג $(p,\hat{q})$ יש ארבעה מקורות (p,q) אפשרים, כי הקודקוד שהוסר (v_1) יכול היה להיות על כל אחד משני הקצוות של כל אחת משתי הצלעות e_0,e_1. במיצוע על W_1, לכל אחד מארבעת המקורות האפשריים (p,q) הסתברות שוה (בהנתן שהגענו לזוג $(p,\hat{q})$). עבור שניים ממקורות אלה יתקיים $v_1\in e$ ולכן $B(p,q)=1$, ואילו עבור השניים האחרים יתקיים $v_1\notin e$ ולכן $B(p,q)=0$. לכן במיצוע על W_1 התשובה תהיה נכונה בהסתברות שהיא גדולה במעט מ 1/2.

קיבלנו לכן:

$$Pr_{W_0}[B(p,q) = M(p,q) = 1] = 1$$

ו

$$Pr_{W_1}[B(p,q) = M(p,q) = 0] > 1/2$$

ההוכחה עבור W_i ל $1<i$ זהה להוכחה עבור W_1 ומתקבל שלכל $1\le i$:

$$Pr_{W_i}[B(p,q) = M(p,q) = 0] > \frac{i}{(i+1)} \ge 1/2$$

לכן הפרוטוקול B הוא פרוטוקול טוב בממוצע לפתרון בעית התקשורת M, ומעיד על נכונות הטענה.

סוף הוכחת הטענה.

בעית התקשורת הבאה אליה נעבור, שכבר מזכירה במשהו את בעית זרות הקבוצות, תכונה אצלנו בעיית הפרדת האותיות (3-letters Distinctness) ותסומן ב DIST. בבעיה זאת לכל אחד משני השחקנים וקטור של אותיות (כשלכל אות יש שלוש אפשרויות), ומטרתם להכריע האם יש קורדינטה שבה שני הקלטים זהים.

באופן פורמלי: נסמן $V=\{a,b,c\}^n$ ונגדיר $DIST:V*V\rightarrow\{0,1\}$ ע"י $DIST(u,v)=1$ אמ"ם $\forall_i\ u_i\neq v_i$.

טענה 5.3:

$$C_{1/3}(DIST)\leq\tilde{C}(M)$$

הוכחה:

לכל $0\leq i\leq n$ נסמן: $Z_i=\{(u,v)\in V*V \mid$ יש בדיוק i קורדינטות בהן u,v מסכימים$\}$

הקבוצות Z_i מהוות חלוקה של מרחב הקלטים $V*V$ ומתקיים: $DIST(u,v)=1$ אמ"ם $(u,v)\in Z_0$.

יהי B פרוטוקול אופטימלי, שהוא טוב בממוצע, עבור הבעיה M. נראה כיצד ליצור מ B פרוטוקול הסתברותי C לפתרון הבעיה DIST:

בהינתן זוג קלטים $(u,v)\in V*V$, לבעיה DIST, יצרו שני השחקנים מ (u,v) זוג קלטים $(p,q)\in P_N*Q_N$, לבעיה M בצורה הבאה:

שני השחקנים יגרילו יחדיו (המודל הוא המודל הציבורי) חלוקה S, שהיא חלוקה של 3n הקודקודים ב N ל n שלשות $(S_1\ldots S_n)$ $(\forall_i\ |S_i|=3)$.

לכל i יגרילו השחקנים (יחדיו) העתקה חד חד ערכית $\rho_i: \{a, b, c\} \rightarrow S_i$. ההעתקה ρ_i מסמנת באות כל אחד משלושת הקודקודים ב S_i. בין שלשת הקודקודים ב S_i יש שלוש צלעות, נסמן ב E_i את קבוצת הצלעות האלה. ההעתקה המשלימה ל ρ_i תהיה ההעתקה $\bar{\rho}_i : \{a, b, c\} \rightarrow E_i$ ותסמן כל צלע באות שבה סומן הקודקוד הנגדי לה. באופן פורמלי:

עבור $\gamma \in \{a, b, c\}$ $\bar{\rho}_i(\gamma)=S_i-\{\rho_i(\gamma)\}$.

שחקן I ייצר מ $u \in V$ זווג $p \in P_N$ ע"י $P=\{\bar{\rho}_1(u_1),\ldots,\bar{\rho}_n(u_n)\}$, (כלומר, כל קורדינטה מתורגמת לצלע המתאימה בשלשה המתאימה). שחקן II ייצר מ $v \in V$ קבוצה $q \in Q_N$ ע"י $q=\{\rho_1(v_1),\ldots,\rho_n(v_n)\}$. (כלומר, כל קורדינטה מתורגמת לקדקד המתאים בשלשה המתאימה).

על הזוג (p,q) יפעילו שני השחקנים את הפרוטוקול B, ויקבלו תשובה $B(p,q)$. נניח שהחלוקה S וההעתקות ρ_i הוגרלו לפי התפלגות אחידה על כל האפשרויות, במקרה זה מתקיים שאם $(u,v) \in Z_i$ אזי (p,q) הוא משתנה מיקרי המפולג אחיד על W_i (לפי צורת הבניה). מאחר ש B טוב בממוצע הרי שאם $(u,v) \in Z_0$ $B(p,q)=1$, ואילו אם $(u,v) \in Z_i$ עבור $0<i$ אזי $B(p,q)=0$ בהסתברות של לפחות 1/2.

הפרוטוקול C יוגדר בצורה הבאה:

שני השחקנים יקבלו זוג (u,v) ייצרו ממנו זוג (p,q) עליו יפעילו את הפרוטוקול B. בהסתברות של 1/3 התשובה שתינתן תהיה $C(u,v)=0$ ובהסתברות של 2/3 יתנו השחקנים את התשובה $C(u,v)=B(p,q)$ (כאשר הבחירה בין המקרים תעשה ע"י הטלת מטבע המתפלג (1/3,2/3)).

עבור $(u,v) \in Z_0$ נקבל: $\Pr[C(u,v)=DIST(u,v)=1] = 1/3*0+2/3*1 = 2/3$

ואילו עבור $(u,v) \in Z_i$ ל $0<i$ $\Pr[C(u,v)=DIST(u,v)=0] \geq 1/3*1+2/3*1/2 = 2/3$

לכן לכל (u,v) B צודק בהסתברות של לפחות 2/3. לכן $B\in P_{1/3}(DIST)$ ומעיד על נכונות הטענה

סוף הוכחת הטענה.

טענו שהבעיה DIST מזכירה את הבעיה DISJ שהיא היעד הסופי שלנו. למעשה בין שתי בעיות אלה קיימות רדוקציות זולות. הטענה הבאה תהיה הצעד האחרון בהוכחת משפט 5.2.

טענה 5.4:

$$C_{1/3}(DISJ)\le C_{1/3}(DIST)$$

הוכחה:

בעיית התקשורת DISJ מוצגת באופן שקול בצורה הבאה: לכל אחד משני השחקנים וקטור ב $\{0,1\}^n$, ומטרתם לאמר האם יש קורדינטה i שבה בשני הוקטורים יש 1 ($x_i=y_i=1$). בהנתן זוג קלטים (x,y) לבעיה DISJ יתרגם שחקן I 0 ל a ו 1 ל c ויקבל מהוקטור x, וקטור חדש $u\in V$. שחקן II יתרגם 0 ל b ו 1 ל c ויקבל מהוקטור y וקטור חדש $v\in V$.

$$x_i=1,\ y_i=1 \quad\Leftrightarrow\quad u_i=c,\ v_i=c \quad\Leftrightarrow\quad u_i=v_i$$

לכן $DISJ(x,y)=DIST(u,v)$ ומכאן ברור שכל פרוטוקול ל DIST מגדיר גם פרוטוקול מקביל ל DISJ המעיד על נכונות הטענה.

סוף הוכחת הטענה.

משפט 5.2 נובע מיידית ממשפט 5.1 ומטענות 5.4, 5.3, 5.2, 5.1.

ה.2: מסקנות נוספות.

ההוכחה המפורטת, שניתנה בסעיף קודם, נתנה חסם תחתון לעומקו של מעגל בוליאני מונוטוני, המחשב את פונקצית הזווג בגרפים. הוכחה זאת מובילה באופן אוטומטי לחסמים תחתונים דומים עבור מספר פוקציות נוספות:

את פונקצית ה Clique(k) בגרפים הכרנו בסעיף א.5. פונקציה זאת תסומן להלן ב CL_k.

מסקנה 5.1:

עבור k-ים מסוימים מתקיים: $d^m(CL_k) = \Omega(n)$

הוכחה:

ההוכחה נובעת מכך שבעית התקשורת $\hat{M}$, שהוצגה בסעיף הקודם, היא תת-בעיה של בעית התקשורת $R^m_{CL_k}$. זה נכון כי את הקבוצה $\hat{Q}_N$ אפשר להציג כקבוצת כל ה Cliques בגודל $k=2n+1$ (ע"י זיהוי כל קבוצה $q\in \hat{Q}_N$ עם הגרף המלא הנוצר על ידי הקבוצה המשלימה). תחת זהוי זה $\hat{Q}_N$ היא קבוצת ה minterms של CL_k. אם לכל גרף $p\in P_N$ נתאים את הגרף המשלים (גרף שצלעותיה הן כל הצלעות שאינן ב p), נקבל שהגרף המשלים הוא תמיד maxterm של CL_k, ולכן P_N מוצגת תחת זהוי זה כקבוצה של maxterms של CL_k. לכן $C(\hat{M})\le d^m(CL_k)$ ומכאן המסקנה.

מסקנה 5.2:

$\forall k \;\; d^m(CL_k) = \Omega(k)$

הוכחה:

מיידית ממסקנה 5.1.

פונקצית הזווג המושלם (perfect-matching), שתכונה להלן PM, מקבלת כקלט גרף G ונותנת כפלט PM(G)=1 אמ"ם בגרף G יש זווג מושלם (זווג הכולל את כל הקודקודים).

מסקנה 5.3:

$d^m(PM)=\Omega(n)$

הוכחה:

מיידית ממשפט 5.2 ומרדוקציה סטנדרטית של בעיית הזווג לבעיית הזווג המושלם.

פונקצית הזווג הדו-צדדי (bipartite - matching), שתכונה להלן BM_k מקבלת כקלט גרף G דו-צדדי ונותנת כפלט $BM_k(G)=1$ אמ"ם בגרף G יש זווג בגודל k. פונקצית הזווג כוללת בתוכה את פונקצית הזווג הדו-צדדי. לא ידועה רדוקצה הפוכה, ובכל זאת נכונה המסקנה הבאה:

מסקנה 5.4:

עבור k-ים מסוימים מתקיים: $d^m(BM_k)=\Omega(n)$

הוכחה:

ההוכחה נובעת מרדוקציה פשוטה של בעית התקשורת $\hat{M}$, שהוצגה בסעיף הקודם, לבעית התקשורת $R^m_{BM_k}$ המתאימה לפונקציה BM_k המוגדרת עבור k=2n על קבוצת הקודקודים $N\cup\bar{N}$. הרדוקציה כוללת שכפול כל קודקוד i ל $i,\bar{i}$ ובהצגה הגרפית של $p\in P_N$ ו $q\in\hat{Q}_N$, שכפול כל צלע (i,j) ל $(i,\bar{j})$ ו $(\bar{i},j)$. מכאן מתקבל $C(\hat{M})\le d^m(BM_k)$.

פונקצית הזווג המלא הדו-צדדי (bipartite - perfect - matching), שתכונה להלן BPM, מקבלת כקלט גרף G דו-צדדי ונותנת כפלט BPM(G)=1 אמ"ם ב G יש זווג מושלם.

מסקנה 5.5:

$d^m(BPM)=\Omega(n)$

הוכחה:

נובעת מרדוקציה סטנדרטית של בעיית הזווג הדו-צדדי לבעיית הזווג הדו-צדדי המושלם.

יש לציין שכל החסמים התחתונים שניתנו בפרק זה הם הדוקים.

Von Zur Gathen, Borodin ו Hopcroft [BGH] **הראו שאלגוריתים הסתברותי לפונקצית הזווג, שהוצע ע"י** Lovasz [L] **ניתן למימוש במעגל שעומקו** $O(\log^2 n)$.

לכן $d(MATCH)=O(\log^2 n)$ **בעוד** $d^m(MATCH)=\Omega(n)$, **ומכאן נובע שקיים פער אקספוננציאלי בין עומק חישוב כללי לעומק חישוב מונוטוני.**

References

[A] A. E. Andreev, "On a Method for Obtaining Lower Bounds on the Complexity of Individual Monotone Functions", *Dokl. Ak. Nauk. SSSR*, Vol 282, pp. 1033-1037, 1985 (in Russian). English translation in: *Sov. Math. Dokl.*, Vol 31, pp. 530-534, 1985.

[AB] N. Alon and R. Boppana, "The Monotone Circuit Complexity of Boolean Functions", *Combinatorica*, Vol 7, No. 1 pp. 1-22,1987.

[BGH] A. Borodin, J. von zur Gathen and J. Hopcroft, "Fast parallel Matrix and GCD Computations", *Proceedings of the 23rd STOC*, pp.65-71, 1982.

[H] J. Hastad, Private Communication.

[K] M. Karchmer, "The Complexity of computation and restricted Machines", *Ph.D Thesis, The Hebrew University*, 1988.

[K1] M. Karchmer, Private Communication.

[KS] B. Kalyanasundaram and G. Snitger, "The Probabilistic Communication Complexity of Set Intersection", *Proceedings Structure in Complexity Theory* pp. 41-49, 1987.

[KW] M. Karchmer and A. Wigderson, "Monotone Circuits for Connectivity Require Super-logarithmic Depth", *Proceeding of the 20th STOC*, pp. 539-550,1988.

[L] L. Lovasz, "Determinants, Matchings and Random Algorithms", *Proceedings of FCT '89*, (ed. L. Budach), Akademie-Verlag, pp. 565-574, 1979.

[N] I. Newman, Private Commnication.

[R1] A. A. Razborov, "Lower Bounds for the Monotone Complexity of some Boolean Functions", *Dokl. Ak. Nauk. SSSR*, Vol 281, pp. 798-801, 1985 (in Russian). English translation in *Sov. Math. Dokl.* Vol 31, pp. 354-357, 1985.

[R2] A. A. Razborov, "Lower Bounds on the Monotone Network Complexity of the Logical Permanent", *Mat. Zametki*, Vol 37, pp. 887-900, 1985 (in Russian). English translation in: *Math. Notes of the Academy of Sciences of USSR*, Vol 37, pp. 485-493, 1985.

[R3] A. A. Razborov, "On the Distributional Complexity of Disjointness", ICALP 1990.

[T] E. Tardos, "The Gap between Monotone and Non-monoton Circuit Complexity is Exponential", *Combiatorica*, Vol 8, pp. 141-142, 1988.

[W] I. Wegner,"The Complexity of Boolean Functions" John Wiley, 1988.

[Y] A. C.-C. Yao, "Some Complexity Questions Related to Distributive Computing", *Proceedings of 11th STOC*, pp. 209-213 (1979).