

ה- i . אין מניעה, אגב, שנבחר בצלע כלשהי בשני הכיוונים. כלומר, יש התאמה חח"ע בין המחוברים בפיתוח והאוסף \mathcal{L} של התת-גרפים המכוונים הבאים של G : כל תת גרף ב \mathcal{L} הוא אוסף של מעגלים מכוונים, זרים בקדקדים הפוגשים את כל קדקדי הגרף (וכאמור גם $\{(j, i), (i, j)\}$ נחשב לצורך זה כמעגל באורך 2). נתבונן בתת גרף $H \in \mathcal{L}$, ונזכור שאנו מניחים כי אין ב G זיווג מושלם.

שימו לב שבמעגל זוגי יש זיווג מושלם. מכיוון ש H גרף פורש, אילו היו כל המעגלים ב H בעלי אורך זוגי היה ב G זיווג מושלם בניגוד להנחתנו. יוצא אם כן שבכל $H \in \mathcal{L}$ יש מעגלים אי זוגיים. מכאן נרצה להסיק שאכן $\det(A) = 0$ כפי שטענו. אנו נראה שבפיתוח של $\det(A)$ ניתן לסדר את האיברים זוגות זוגות כך שאם אחד מהם הוא u אז בן זוגו הוא $-u$ והטענה תנבע.

כאמור המחוברים ב $\det(A)$ הם בהתאמה חח"ע עם משפחת התת גרפים המכוונים \mathcal{L} . בכל $H \in \mathcal{L}$ נציין מעגל $C = C_H$ אי זוגי מסויים - נאמר את זה הכולל את הקדקד בעל האינדקס הנמוך ביותר הנמצא במעגל א"ז כלשהו ב H .

בן הזוג של H יהיה הגרף המכוון $H^* \in \mathcal{L}$ המתקבל ע"י היפוך כיווני הצלעות במעגל C_H . מכיוון שהמעגל C_H הוא מאורך אי זוגי, ומכיוון ש A אנטי סימטרית, יוצא שאם u הוא המחובר המתאים לגרף H אז ל H^* מתאים המחובר $-u$. נותר עוד לברר נקודה אחת. בנוסחת הדטרמיננט יש לכפול כל מחובר ב ± 1 לפי סימנה של התמורה המתאימה σ . התמורה σ מורכבת ממעגלים c_1, c_2, \dots, c_l , $\text{sgn}(\sigma) = \prod \text{sgn}(c_i)$, ואם c הוא המעגל שאת כיוונו הפכנו וקיבלנו את המעגל c^* , אז קל לוודא כי $\text{sgn}(c) = \text{sgn}(c^*)$, והסיבה היא שכתמורות c, c^* הן הופכיות, ולתמורות הופכיות יש אותו הסימן:

$$\text{sgn}(\pi) \cdot \text{sgn}(\pi^{-1}) = \text{sgn}(\pi \cdot \pi^{-1}) = \text{sgn}(id) = 1$$

יוצא שבמקרה זה $\det(A) \equiv 0$ כדרוש. התרגום של המשפט הנ"ל לאלגוריתם הסתברותי יעיל הוא די פשוט עתה, בהסתמך על הלמה האלגברית הבאה:

למה (Schwartz-Zippel): יהיה Q פולינום במשתנים x_1, x_2, \dots, x_n ממעלה כוללת d , מעל שדה F , ונניח כי Q איננו זהותית 0. תהיה $S \subset F$ קבוצה סופית. נציג למשתנים x_i ערכים אקראיים מתוך הקבוצה S . ההסתברות ש Q יתאפס בה-צבה כזו היא $\frac{d}{|S|} \geq$.

הוכחת הלמה: באינדוקציה על מספר המשתנים n . כאשר $n = 1$ הטענה היא בפשטות שלפולינום במשתנה יחיד ממעלה d יש $d \geq$ שורשים. צעד האינדוקציה: נציג

$$Q = Q_0(x_2, \dots, x_n) + x_1 Q_1(x_2, \dots, x_n) + \dots + x_1^k Q_k(x_2, \dots, x_n)$$

כש $k \leq d$ וכן $\text{total deg}(Q_i) \leq d - i$. את ההסתברות ש Q מתאפס בהצבה מקרית נעריך כך: אם $Q_k(r_2, \dots, r_n) = 0$ (כש $r_i \in S$ הוא הערך המקרי של x_i וזה קורה בהסתברות של $\frac{d-k}{|S|} \geq$ אפילו לא נבדוק אם Q אכן מתאפס, ואילו אם $Q_k(r_2, \dots, r_n) \neq 0$ אז $Q(x_1, r_2, \dots, r_n)$ הוא פולינום ממעלה k במשתנה היחיד x_1 , וההסתברות שיתאפס $\frac{k}{|S|} \geq$ יוצא

$$\Pr(Q(r_1, \dots, r_n) = 0) \leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}$$

כפי שטענו.

האלגוריתם: הצב ערכים מקריים ל x_{ij} שבמטריצת Tutte מן התחום $\{1, \dots, 2n\}$. אם למטריצה המתקבלת דטרמיננטה שונה מאפס הצהר "ב G יש זיווג מושלם" (בטענה

זו אף פעם אין טעות). אם הדטרמיננטה מתאפסת הצהר "כנראה אין ב G זיווג מושלם".
ההסתברות לכך שההצהרה נכונה היא $\leq 1/2$. על מנת לצמצם את ההסתברות השגיאה
ל $\epsilon \geq$ חוזרים על הנ"ל $\log 1/\epsilon$ פעמים.