הוכחות אוטומטיות של זהויות קומבינטוריות / אופיר גורודצקי, מרץ 2013

ההרצאה הזו מבוססת על הספר הנהדר A=B של Petkovšek, Wilf & Zeilberger משנת 1996[1]. הספר סוקר את הנושא בצורה מעולה, אבל אורכו 208 עמודים והוא באנגלית. סיכום זה בא לתקצר את הספר בשפת הקודש תוך העברת הרעיונות המרכזיים. אני חורג מהספר בכמה נקודות: סדר הצגת האלגוריתמים שונה, דוגמאות שאינן הופיעו בספר הוספו, וחלק מההוכחות הפכו לתרגילים (פתרונות לחלקם מופיעים בסוף הסיכום). בנוסף, אני מבהיר נקודות שלא בוהרו בספר המקורי. השמטתי כמה נושאים מתקדמים (כמו q־זהויות ואלגוריתם הייפר) וגם את נושא השימוש במחשב ־ כל האלגוריתמים ממומשים ב־Maple.

קריאה מהנה. אשמח לקבל כל הערה/הארה/תיקון/שיפור בנושא למייל הבא: bambaman1@gmail.com.

הקדמה

"המטרה הסופית של המתמטיקה היא לבטל כל צורך במחשבה תבונית" ־ מיוחס[2] לאלפרד וייטהד, מדען ופילוסוף בריטי

זהויות הן אובייקט נפוץ בכל ענף מתמטי כמעט:

גיאומטריה: $V-E+F=2$ (נוסחת אוילר), $A^2+B^2=C^2$ (משפט פיתגורס)

אלגברה: $\prod_{p \text{ is a prime}}(1-p^{-s})^{-1}=\sum_{n\geq1}n^{-s}$ (מכפלת אוילר), $\det(AB)=\det(A)\det(B)$ (כפליות הדטרמיננטה)

פיזיקה: $E=mc^2$ (שקילות מסה־אנרגיה), $\vec{F}=m\vec{a}$ (החוק השני של ניוטון)

לכן, כלי שמסוגל להוכיח זהויות, או אפילו להמציא אותן, יהיה בעל ערך גבוה. מהפכת המחשוב לא פסחה על המתמטיקה, ובהרצאה זו נדבר על הוכחות אוטומטיות וממוחשבות לזהויות מסוג מסויים, זהויות בינומיות. נדבר גם על יצירת זהויות חדשות מקיימות.

לפני שנפנה לכך, נדבר קצת על מה אי־אפשר לעשות עם מחשב.

המחשב אינו כל יכול

לא על כל שאלה במתמטיקה אפשר לענות. ב1900 הילברט פירסם 23 שאלות פתוחות ומהותיות בעיניו, וביניהן השאלה הבאה (שאלה מספר 10): מציאת אלגוריתם שמכריע האם למשוואה דיופנטית יש פיתרון?[3] משוואה דיופנטית היא משוואה מהצורה $P(x_1,\cdots,x_n)=0$ כאשר P פולינום עם מקדמים שלמים והמשתנים x_i יכולים לקבל רק ערכים שלמים. מטייסביץ' הראה ב־1970 שאין כזה אלגוריתם.[4]

<u>תרגיל 1:</u> הראו שאם היה אלגוריתם שמכריע האם קיים פיתרון, אפשר היה לבנות ממנו אלגוריתם שמכריע האם יש פיתרון במספרים טבעיים, ולהיפך.

[1] ניתן להורדה בחינם מהאתר http://www.math.upenn.edu/~wilf/Downld.html.

[2] ויקיפדיה מערערת על מקור הציטוט

[3] בויקיפדיה האנגלית מוצגת ההגדרה הבאה לאלגוריתם שהילברט ביקש: A process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

[4] עוד 2 בעיות של הילברט שקיבלו תשובה שלילית: (שאלה 1) הוכחת השערת הרצף, שגורסת שאין עוצמה בין $\aleph_0$ ל$2^{\aleph_0}$. גדל וכהן הראו שאי־אפשר להפריך או להוכיח את ההשערה מתוך האקסיומות הסטנדרטיות ZFC, כלומר ההשערה לא תלויה בZFC. (שאלה 2) הוכחת העקביות של אקסיומות האריתמטיקה (פיאנו). משפט אי־השלמות השני של גדל מראה שתורה עקבית שמקיימת את אקסיומות האריתמטיקה לא יכולה להוכיח את העקביות של עצמה.

עוד דוגמא שלילית, הפעם כזו שקשורה לזהויות: נסתכל על אוסף הפונקציות במשתנה x הנוצרות מכפל, חיבור והרכבה של הפונקציות $e^x, \sin x, |x|$ והפונקציות הקבועות $\mathbb{Q} \cup \{\ln 2, \pi\}$. ריצ'רדסון הוכיח ב־1968 שאין אלגוריתם שמכריע האם 2 פונקציות כאלו מסכימות לכל x ממשי, מה ששקול לאלגוריתם שבודק האם פונקציה כזו מתאפסת תמיד. ויקיפדיה האנגלית מלאה בעוד הרבה דוגמאות של בעיות לא כריעות[5].

המחשב יכול לעשות דברים מסויימים

המחשב אומנם לא יכול לפתור משוואה דיופנטית כללית, אבל יש משפחות שלמות של משוואות שהוא כן יודע לפתור, לדוגמא משוואות Pell: $x^2 - Dy^2 = 1$. בדומה, המחשב אינו יכול להוכיח כל זהות, אבל יש משפחות רחבות ומעניינות של זהויות שהוא כן יודע להוכיח. לרוב הדבר נעשה באמצעות הצגת 2 האגפים בצורה קנונית: כל איבר במשפחה אפשר לרוב להציג בהרבה דרכים (נגיד $\frac{1}{2}$ ו־$\frac{2}{4}$) אבל אם נמצא לכל איבר ייצוג ספציפי ("קנוני") חח"ע, ונבנה אלגוריתם שמחשב לכל איבר את הנציג הקנוני שלו, נוכל לוודא את הזהות $A = B$ באופן הבא: נבחר ל־A ול־B נציגים קנוניים ונשווה ביניהם. העיקרון מובן בצורה הכי טובה דרך דוגמאות:

- זהויות בין מספרים רציונליים: נניח שיש לנו 2 ביטויים שמורכבים מכפל, חלוקה וחיבור של מספרים שלמים. כדי לוודא שיוויון ביניהם, נעביר כל ביטוי כזה לצורה הקנונית הבאה: $\frac{a}{b}$ כאשר a, b שלמים זרים ו־$b > 0$. האלגוריתם שמעביר מספר לצורה קנונית (ובפרט מוכיח את קיומה) הוא אלגוריתם 'המכנה המשותף' מימי התיכון, ולאחר מכן צמצום בגורם המשותף המקסימלי של המונה והמכנה (באמצעות אלגוריתם אוקלידס). 2 נציגים קנוניים שווים אמ"מ המונה והמכנה שווים. דוגמא: $\frac{1}{101\cdot 33} + \frac{1}{101\cdot 11} = \frac{3}{50\cdot 50} + \frac{1}{33\cdot 25\cdot 100\cdot 101}$. הנציג הקנוני של 2 האגפים הוא $\frac{4}{3333}$.

- זהויות בין פולינומים: נניח שאנחנו רוצים להשוות פולינומים בשני משתנים, x, y. פולינומים אלו מהווים מרחב וקטורי, וצורה קנונית אפשרית היא הצגה בבסיס מסויים, לדוגמא: $\{x^i y^j\}_{i,j}$. עוד בסיס אפשרי - $\{\binom{x}{i}\binom{y}{j}\}_{i,j}$. בשביל לעבור לצורה הקנונית הראשונה, צריך רק לפתוח סוגריים. כך אפשר להוכיח זהויות נפלאות, ביניהן $(2ab)^2 + (a^2-b^2)^2 = (a^2+b^2)^2, (a+b)^2 = a^2 + 2ab + b^2$. זהויות יותר מתוחכמות, ב־4 משתנים:

  1. $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$ - תוצאה של זהות זו היא שמכפלת סכום שני ריבועים היא גם כן סכום שני ריבועים[6]. מסקנה נוספת היא הוכחה לאי־שיוויון קושי־שוורץ במקרה של שני משתנים ממשיים: $(a^2+b^2)(c^2+d^2) - (ac+bd)^2 = (ac-bd)^2$[7].
  2. $a^4+b^4+c^4+d^4-4abcd = (a^2-b^2)^2 + (c^2-d^2)^2 + 2(ab-cd)^2$ - אי־שיוויון הממוצעים עבור 4 משתנים. (אפשרי להכליל סוג זה של הוכחה לכל כמות משתנים!)

- זהויות טריגונומטריות: לדוגמא, $\sin 2x = 2\cos x \sin x$. נשתמש בזהויות $\sin x = \frac{e^{ix}-e^{-ix}}{2i}, \cos x = \frac{e^{ix}+e^{-ix}}{2}$[8] כדי להציג כל זהות טריגונומטרית כזהות של פונקציות רציונליות ב־$t = e^{ix}$ (שימו לב ש־$e^{-ix} = t^{-1}$, ולכן בין השאר $\cos(nx) = \frac{t^n+t^{-n}}{2}, \sin(nx) = \frac{t^n-t^{-n}}{2i}$), זהות כזו אפשר להפוך לזהות של פולינומים (באמצעות הכפלה במכנה משותף), וזו בעיה שאנחנו כבר יודעים לפתור. שימו לב: השתמשנו בכך שפולינום שמתאפס על מעגל היחידה המרוכב (תמונת t) הוא בהכרח פולינום האפס. טענה זו היא יחסית חלשה ונותנת השראה לעוד דרך להוכיח זהויות טריגונומטריות - הצבה! נעביר זהות טריגונומטרית מהצורה $f(\sin x, \cos x) = 0$ כאשר f פונקציה רציונלית ב־$\sin x, \cos x$ לזהות פולינומיאלית $g(t) = 0$, עבור $|t| = 1$. בגלל שזה שקול לכך שהפולינום g זהותית אפס, מספיק לוודא אותה עבור $\deg g + 1$[9] ערכים של $t = e^{ix}$,

[5] http://en.wikipedia.org/wiki/List_of_undecidable_problems

[6] הכללה של אוילר ל־4 ריבועים: $(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = (a_1b_1-a_2b_2-a_3b_3-a_4b_4)^2 + (a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2 + (a_1b_3-a_2b_4+a_3b_1+a_4b_2)^2 + (a_1b_4+a_2b_3-a_3b_2+a_4b_1)^2$. יש גם הכללה ל־8 ריבועים.

[7] ובמקרה הכללי: $(\sum a_i^2)(\sum b_j^2) - (\sum a_k b_k)^2 = \sum_{i<j}(a_ib_j - a_jb_i)^2$

[8] נובעות מהשוואת טורי טיילור או מנוסחת אוילר.

[9] g אמור להיות זהותית אפס, לכן אנחנו מצפים ש־$\deg g = 0$. לכן כשנכתוב $\deg g$ נתכוון ל**חסם עליון** על $\deg g$.

כלומר מספיק לוודא את הזהות המקורית עבור $\deg g + 1$ זוויות (כמובן שהן צריכות להיות שונות מודולו 2π). לדוגמא, כדי לוודא את $\sin 2x = 2\cos x \sin x$ מספיק להציב 7 ערכים, נגיד: 7 כפולות של $\frac{\pi}{4}$.
באופן כללי, עבור ביטוי טריגונומטרי ממעלה d, הצורה הבאה היא צורה קנונית: $(f(0), f(\frac{2\pi}{d+1}), f(2 \cdot \frac{2\pi}{d+1}), \cdots, f(d \cdot \frac{2\pi}{d+1}))$.

- זהויות פיבונאצ'י: תהי $\{F_n\}_{n\geq 0}$ סדרת מספרי פיבונאצ'י: $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. מספרים אלו מקיימים זהויות מגוונות, כמו למשל $F_{2n+1} = F_n^2 + F_{n+1}^2$. אם נגדיר $\phi = \frac{1+\sqrt{5}}{2}, \overline{\phi} = \frac{1-\sqrt{5}}{2}$ להיות שורשי המשוואה $x^2 = x + 1$, אז נקבל מהתורה של סדרות נסיגה את הנוסחה המפורשת $F_n = \frac{\phi^n - \overline{\phi}^n}{\phi - \overline{\phi}}$. אם מציבים $s = \phi^n, t = \overline{\phi}^n$ ומשתמשים בכך ש־ $F_{an+b} = \frac{\phi^{an+b} - \overline{\phi}^{an+b}}{\phi - \overline{\phi}} = \frac{\phi^b s^a - \overline{\phi}^b t^b}{\phi - \overline{\phi}}$ פולינום בs, t, מקבלים שכל זהות הופכת להיות מהצורה $F(x, y) = 0$ כאשר F פולינום ו־(x, y) מקבלים את הערכים $(\phi^n, \overline{\phi}^n)$. בגלל ש־$\phi\overline{\phi} = -1$, $F(x, x^{-1})$ פונקציה רציונלית שמתאפסת על $\{\phi^{2n}\}_{n\geq 1}$ מתקיים ש־$F(x, x^{-1})$ זהותית אפס. בדומה, $F(x, -x^{-1}) = 0$. לכן הוכחת זהויות פיבונאצ'י הופכת להיות שוב שקולה להוכחת (שתי) זהויות של פונקציות רציונליות במשתנה אחד. בדומה למקרה הטריגונומטרי, בעצם מספיק לוודא את הזהות ל$\deg p_1 + 1$ ערכים זוגיים ו$\deg p_2 + 1$ ערכים אי־זוגיים, כאשר p_1, p_2 הפולינומים במונים של $F(x, x^{-1}), F(x, -x^{-1})$. לדוגמא, כדי לוודא את $F_{2n+1} = F_n^2 + F_{n+1}^2$ מספיק להציב שבעה ערכים זוגיים ועוד שבעה אי־זוגיים.

<u>תרגיל 2:</u> חיקרו את האנלוגיה הבאה בין זהויות טריגונומטריות לזהויות פיבונאצ'י: נגדיר את סדרת לוקאס - $L_0 = 2, L_1 = 1, L_{n+2} = L_{n+1} + L_n$. הנוסחה המפורשת לה היא $L_n = \phi^n + \overline{\phi}^n$. הזוג (L_n, F_n) אנלוגי ל$(\cos x, \sin x)$, לדוגמא: $L_n^2 - 5F_n^2 = 4(-1)^n$ מול $\cos^2 x + \sin^2 x = 1$, ו־$F_{2n} = L_n F_n$ מול $\sin 2x = 2\cos x \sin x$.

<u>זהויות בינומיות</u>

זהויות בינומיות, או בשמן הרשמי "זהויות היפרגאומטריות", הן סוג מסויים של זהויות שמופיעות בין השאר בקומבינטוריקה, הסתברות ומדעי המחשב, ונחקרות כבר מאות שנים. לפני שנפנה להגדרה הפורמלית, אפשר להגיד שזהות היפרגיאומטרית מערבת עצרות ופולינומים. דוגמאות מוכרות:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n, \sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}, \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

דוגמאות פחות מוכרות:

$$\sum_{i+j+k=n} \binom{i+j}{i}\binom{j+k}{j}\binom{k+i}{k} = \sum_{0\leq j\leq n} \binom{2j}{j}, \text{ Dixon's Identity: } \sum_{s=0}^{2m} (-1)^s \binom{2m}{s}^3 = (-1)^m \binom{3m}{m,m,m}$$

ב־60 השנים האחרונות חלה אוטומציה מרשימה בהוכחות של זהויות היפרגיאומטריות. מעבר לכך שמחשבים יכולים להוכיח זהויות באופן מהיר, הם יכולים גם למצוא זהויות. מחשבים הפכו להיות כלי מרכזי בתחום.

לפני כן, הוכחות של זהויות היו מעין קסם - באמצעות פירוש קומבינטורי, אינדוקציה, פונקציות יוצרות, הצגה אינטגרלית או דרך אחרת.

דוגמא להוכחה עם פונקציות יוצרות: גיזרו את 2 אגפים הבינום של ניוטון - $(1+x)^n = \sum_{k=0}^{n} x^k \binom{n}{k}$, והציבו $x = 1$.

דוגמא להוכחה קומבינטורית: הגורם הk־י בסכום $f(k) = \sum_{k=0}^{n} k\binom{n}{k}$ שווה למספר הדרכים לבחור תת־קבוצה בגודל k מתוך קבוצה בגודל n, ומתוך תת־קבוצה זו לבחור נציג. אפשר לספור את הסכום הזה בצורה אחרת: לבחור בהתחלה את הנציג - יש לכך n אפשרויות - ואז לבחור את שאר איברי הקבוצה שלו - לכך יש 2^{n-1} אפשרויות, ומקבלים $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.

ישנן הוכחות קומבינטוריות ולא קומבינטוריות שהן גאוניות יותר וטריוויאליות פחות, ולכן נרצה אלגוריתם שיודע להתמודד עם זהויות כאלה באופן אחר.

אנחנו נציג אלגוריתמים שיודעים:

- למצוא רקורסיות לסכום היפרגיאומטרי $F(n) = \sum_k f(n,k)$ (לרוב הרקורסיות הללו ניתנות לפיתרון בידיים, אבל יש אלגוריתם שלא נציג שיודע לפתור רקורסיות כאלו)
- באמצעות האלגוריתם הנ"ל להוכיח זהויות היפרגיאומטריות מהצורה $F(n) = \sum_k f(n,k)$, כאשר F נתונה
- ליצור זהויות היפרגיאומטריות חדשות מתוך זהויות קיימות

<u>טורים היפרגיאומטריים</u>

ניזכר בכך שסדרה $\{t_k\}_{k\geq 0}$ תיקרא גיאומטרית אם t_{k+1}/t_k קבוע ולא תלוי ב־k. הטור המתאים $\sum t_k$ יקרא טור גיאומטרי.

באופן דומה, סדרה $\{t_k\}_{k\geq 0}$ תיקרא היפרגיאומטרית אם t_{k+1}/t_k הוא פונקציה רציונלית ב־k, ואז הטור $\sum_{k\geq 0} t_k$ יקרא טור היפרגיאומטרי. מותר ל־t_k להיות תלוי בפרמטרים, לדוגמא: $t_k = x^k, k!, \frac{(2k+7)!}{(k-3)!}$. בצורה הכי כללית, $\frac{t_{k+1}}{t_k} = \frac{\prod_{i=1}^{p}(k+a_i)}{\prod_{j=1}^{q}(k+b_j)}x$. הקונבנציה היא להוסיף את $k+1$ למכנה (כלומר להכפיל מונה ומכנה ב$k+1$), ומקבלים את הצורה הבאה: $\frac{t_{k+1}}{t_k} = \frac{\prod_{i=1}^{p}(k+a_i)}{\prod_{j=1}^{q}(k+b_j)(k+1)}x$ (כאשר x לא תלוי ב־k). בנוסף, מנרמלים כך ש$t_0 = 1$. בהינתן צורה זו, הטור $\sum_{k\geq 0} t_k x^k$ מסומן בתור ${}_pF_q\left[\begin{matrix} a_1 & \cdots & a_p \\ b_1 & \cdots & b_q \end{matrix} ; x\right]$, ובמפורש:

$$ {}_pF_q\left[\begin{matrix} a_1 & \cdots & a_p \\ b_1 & \cdots & b_q \end{matrix} ; x\right] = \sum_{k\geq 0} \frac{(a_1)_k \cdots (a_p)_k}{(b_1)_k \cdots (b_q)_k} \frac{x^k}{k!} = \sum_{k\geq 0} t_k, \text{ where } (a)_k = a(a+1)\cdots(a+k-1) $$

דוגמא:

$$ {}_2F_1\left[\begin{matrix} -n & , -n \\ 1 & \end{matrix} ; 1\right] = \sum_{k\geq 0} \frac{(-n)_k^2}{(1)_k} \frac{1}{k!} = \sum_{k=0}^{n} \frac{(n!/(n-k)!)^2}{k!^2} = \sum_{k=0}^{n} \binom{n}{k}^2 $$

ביטוי זה שווה ל$\binom{2n}{n}$, ויש תוכנות מתמטיקה שיודעות להציג זהויות בצורה כזו ולחפש האם הן מוכרות. שימו לב שכדי שהסכום יכיל מספר סופי של איברים נדרש שאחד מבין ה־a_i יהיה שלם שלילי.

מבחינה היסטורית, טורים היפרגיאומטריים, בעיקר עבור $p=2, q=1$, נחקרו ע"י גדולי המתמטיקאים, ביניהם: אוילר, גאוס ורימן. הם מופיעים בחקר משוואות דיפרנציאליות ופונקציות מרוכבות, והיה בהם עניין רב גם בלי הקשרים הקומבינטוריים שבהם הם מופיעים. עם זאת, נקודת המבט שלנו תהיה שונה ובין השאר הטורים שלנו יהיו כמעט תמיד **סכומים סופיים**.

ברוח ההגדרות האלו, פונקציה $f(n)$ תיקרא היפרגיאומטרית אם $f(n+1)/f(n)$ פונקציה רציונלית ב־n. בדומה, פונקציה $f(n,k)$ תיקרא היפרגיאומטרית אם $f(n+1,k)/f(n,k), f(n,k+1)/f(n,k)$ הן פונקציות רציונליות ב־n ו־k.

דוגמא: $(an+bk+c)!$, $\binom{n}{k}$. נשים לב שפונקציות היפרגיאומטריות סגורות לכפל וחילוק.

האלגוריתם הראשון ־ הנזירה מארי סלין

נתעסק בסכומים מהצורה $F(n) = \sum_k f(n,k)$ כאשר f היפרגיאומטרית, ולרוב גם F. הסכימה תהיה על כל המספרים השלמים, כאשר בדר"כ לf יהיה תומך קומפקטי, כלומר היא תתאפס על כמעט כל המספרים השלמים. הסכום F יקרא סכום היפרגיאומטרי. זהות היפרגיאומטרית היא הבעת F בצורה יפה, כמו פונקציה היפרגיאומטרית ב־n (כמו $\binom{2n}{n}$). נדגיש שהגדרה זו גמישה ויש זהויות שהן לא בדיוק כאלה.

נדגים את האלגוריתם של הנזירה סלין (Sister Mary Celine), משנת 1945, שהופיעה בעבודת הדוקטורט שלה, אותה כתבה בגיל 39. נפעיל אותו על הדוגמא הבאה:

$$F(n) = \sum_{k=0}^{n} k\binom{n}{k}$$

האלגוריתם מוצא רקורסיה ל$f(n,k)$ שתלויה רק בn. במקרה שלנו $f(n,k) = k\binom{n}{k}$, ונניח שקיימת רקורסיה מהצורה הבאה:

$$a(n)f(n,k) + b(n)f(n+1,k) + c(n)f(n,k+1) + d(n)f(n+1,k+1) = 0$$

כאשר a,b,c,d פונקציות רציונליות ב־n. כדי למצוא אותן נחלק ב$f(n,k)$. בגלל שf היפרגיאומטרית, המקדמים של המשתנים יהיו פונקציות רציונליות:

$$\frac{f(n+1,k)}{f(n,k)} = \frac{n+1}{n+1-k}, \frac{f(n,k+1)}{f(n,k)} = \frac{n-k}{k}, \frac{f(n+1,k+1)}{f(n,k)} = \frac{f(n+1,k+1)}{f(n+1,k)}\frac{f(n+1,k)}{f(n,k)} = \frac{n+1-k}{k}\frac{n+1}{n+1-k} = \frac{n+1}{k}$$

נכתוב את הרקורסיה שוב, אחרי שנכפיל במכנה המשותף $k(n+1-k)$:

$$a(n)k(n+1-k) + b(n)(n+1)k + c(n)(n-k)(n+1-k) + d(n)(n+1)(n+1-k) = 0$$

בגלל שa,b,c,d לא תלויים בk, אפשר לקבץ חזקות של k ולהשוות אגפים (פה אנחנו משתמשים בצורה קנונית לפולינום בk):

$$\begin{array}{rcl} (c(n)(n^2+n) + d(n)(n+1)^2) & k^0 & + \\ (a(n)(n+1) + b(n)(n+1) + c(n)(-2n-1) + d(n)(-n-1)) & k^1 & + \\ (c(n) - a(n)) & k^2 & = 0 \end{array}$$

ומקבלים 3 משוואות, המיוצגות ע"י המטריצה הבאה:

$$\begin{pmatrix} 0 & 0 & n(n+1) & (n+1)^2 \\ n+1 & n+1 & -2n-1 & -n-1 \\ -1 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \vec{0}$$

בגלל שיש יותר נעלמים ממשוואות, וזו מערכת הומוגנית, בהכרח יש פיתרון לא־טריוויאלי. למעשה, אפשר לחשב את הגרעין בשיטות סטנדרטיות של אלגברה לינארית ולקבל שמרחב הפתרונות נתון ע"י $d(-1-\frac{1}{n}, 0, -1-\frac{1}{n}, 1)$. נבחר את הפיתרון $a(n) = -1-\frac{1}{n}, b(n) = 0, c(n) = -1-\frac{1}{n}, d(n) = 1$, כלומר מתקיימת הרקורסיה הבאה:

$$-(1+\frac{1}{n})f(n,k)-(1+\frac{1}{n})f(n,k+1)+f(n+1,k+1)=0$$

בגלל שהמקדמים לא תלויים בn, אפשר לסכום על k. כשנסכום, נעשה זאת על כל המספרים השלמים עם הקונבנציה הבאה[10]: $\binom{n}{k}$ מתאפס כאשר k שלילי או $k>n\geq 0$. נקבל:

$$-(1+\frac{1}{n})F(n)-(1+\frac{1}{n})F(n)+F(n+1)=0$$

כלומר קיבלנו רקורסיה מעומק 1: $F(n+1)=2\frac{n+1}{n}F(n)$. חישוב סופי מראה ש$F(1)=1$ ושימוש ברקורסיה נותן $F(n)=2^{n-1}\frac{n!}{(n-1)!}F(1)=n2^{n-1}$. וזה הכל. ■

זו סיטואציה שכיחה ־ הרבה פעמים הרקורסיה תהיה מהצורה $a_0(n)F(n+1)+a_1(n)F(n)=0$ ולכן $F(n)=F(0)\prod_{j=0}^{n-1}(-a_0(j)/a_1(j))$. במקרה זה מקבלים יצוג מפורש ל־F כפונקציה היפרגיאומטרית.

סיטואציה נוספת היא שמקבלים רקורסיה עם מקדמים קבועים שאפשר לפתור בדרכים סטנדרטיות לאחר מציאת שורשי הפולינום האופייני המתאים.

<u>תרגיל 3 (חשוב):</u> הבינו למה סכימה על כל השלמים היא חוקית.

עוד 2 דוגמאות:

- $L_n(x)=\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{x^k}{k!}$, פולינומי Laguerre, מקיימים את הרקורסיה $nL_n(x)+(x+1-2n)L_{n-1}(x)+(n-1)L_{n-2}(x)=0$, אותה אפשר למצוא עם האלגוריתם של סלין ־ הפרמטר x לא מפריע. פולינומים אלו אורתוגונליים לפי המכפלה הפנימית $\langle f,g\rangle=\int_0^\infty fge^{-x}dx$.[11]
- Reed-Dawson: נגדיר $F(n)=\sum_k\binom{n}{k}\binom{2k}{k}(-2)^{n-k}$. מנחשים שיש רקורסיה מעומק 2 ופותרים אותה. מקבלים 7 מחוברים (לא 8 כי המקדם של $f(n,k)$ מתאפס), סוכמים ומקבלים $(n+2)F(n+2)-4(n+1)F(n)=0$, וחישוב קצר מראה ש $F(n)=\begin{cases}0 & 2\nmid n\\ \binom{n}{n/2} & 2|n\end{cases}$.

<u>תרגיל 4:</u> השלימו את הפרטים בהוכחה הקומבינטורית הבאה Reed-Dawson:

- למה: $\sum_{k\geq 0}\binom{n}{2k}\binom{2}{k}2^{n-2k}=\binom{2n}{n}$. הוכחה: שני האגפים סופרים מילים באורך n המורכבות מהאלף־בית $\{a,b,c,d\}$ ומספר ה־a־ים שווה למספר ה־b־ים.
- נסתכל על מילים באורך n שבנויות מהאלף־בית $\{a,b,c,d,C,D\}$ וכמות ה־a־ים בהן שווה לכמות ה־b־ים. נגדיר מילה להיות זוגית אם היא מכילה מספר זוגי של אותיות קטנות, ואחרת היא אי־זוגית. ההפרש, בערך מוחלט, בין כמות המילים הזוגיות לכמות המילים האי־זוגיות נספר על ידי שני האגפים של Reed-Dawson. בהוכחה צריכים להמציא אינבולוציה הופכת סימן (Sign Reversing Involution).

---

[10] היא לא שרירותית. באופן זה $\binom{n}{k}$ מקיימת את המשוואות הבאות **לכל** n,k שלמים:

$$\begin{aligned}(k+1)\binom{n}{k+1} &= (n-k)\binom{n}{k}\\ (n+1-k)\binom{n+1}{k} &= (n+1)\binom{n}{k}\end{aligned}$$

[11] כל סדרה של פולינומים אורתוגונלים על הישר הממשי, $\{P_n\}_{n\geq 0}$, כאשר $\deg P_n=n$, מקיימת רקורסיה מהצורה $P_n(x)=(A_nx+B_n)P_{n-1}(x)+C_nP_{n-2}(x)$.

המשפט הכללי, שלא נוכיח, הולך כך: נניח ש$f(n,k)$ היא מהצורה הבאה:

$$f(n,k) \quad = \quad p(n,k)\frac{\prod_{i=1}^{u}(a_i n+b_i k+c_i)!}{\prod_{i=1}^{v}(u_i n+v_i k+w_i)!}x^k$$

כאשר p פולינום. לדוגמא, $\frac{(n+3k)!}{(n+3k+1)!}=\frac{1}{n+3k+1}$. יש פונקציות היפרגיאומטריות שלא עונות על ההגדרה, כמו $\frac{1}{n^2+k^2+1}$. פונקציות שיענו על ההגדרה יקראו "היפרגיאומטריות ממש", והאלגוריתם יכול להיכשל עבור פונקציות אחרות.

במקרה זה, אם נבחר רקורסיה בעומק $J=\sum|b_j|+|v_j|, I=1+\deg p+J(\sum|a_j|+|u_j|-1)$, כלומר ננסה לפתור $\sum_{0\le i\le I,0\le j\le J} f(n+i,k+j)a_{i,j}(n)=0$, בהכרח נקבל יותר נעלמים ממשוואות ונמצא פיתרון.

לא נוכיח את המשפט, אבל נסתמך עליו. הוא נותן לנו את רוב הכלים שחיפשנו:

- למצוא רקורסיה לסכום היפרגיאומטרי $F(n)$.
- להוכיח זהות, באמצעות: מציאת רקורסיה ל$\sum_k f(n,k)$, וידוא שגם F מקיימת אותה, ולבדוק שהזהות נכונה עבור כמה ערכים ראשונים. וידוא זה הוא גם פשוט במקרה ש־F היפרגיאומטרית: $\sum_i a_i F(n+i)=0$ שקול ל$\sum_i a_i\frac{F(n+i)}{F(n)}=0$, זהות בפונקציות רציונליות.
- יש אלגוריתם שלא נזכיר שמאפשר לפתור רקורסיה כללית עם מקדמים פולינומיאלים (אם הפיתרון F הוא סכום של פונקציות היפרגיאומטריות), והוא למעשה סוגר את הפינה.

עם זאת, יש אלגוריתמים יעילים יותר ומגניבים יותר, עליהם נדבר בהמשך.

תופעת WZ

תופעת WZ היא התופעה הנפלאה הבאה: אם מנרמלים את הזהות שלנו, לרוב (במובן אמפירי ולא מתמטי...) תהיה לה הוכחה **מאוד** קצרה בהמצאות קיומה של פונקציה היפרגיאומטרית דואלית. ובצורה יותר ברורה, הסיפור הוא כזה: נניח שיש לנו זהות $F(n)=\sum_k f(n,k)$ כאשר f היפרגיאומטרית. אם $f(n)$ לא זהותית אפס, זהות זו שקולה לזהות $\sum_k f(n,k)/f(n)=1$. בשני המקרים, יש לנו זהות מהצורה $\sum_k f(n,k)=\text{const}$ (זו הכוונה ב"נרמול הזהות").

תופעת WZ היא העובדה שבהמון מקרים, קיימת $g(n,k)$ היפרגיאומטרית כך ש:

$$(*)f(n+1,k)-f(n,k) \quad = \quad g(n,k+1)-g(n,k)$$

סכימה על k, תחת ההנחה $\lim_{|x|\to\infty} g(n,x)=0$ (שגם כן מתקיימת לרוב. למעשה, g לרוב מתאפסת עבור k גדול מספיק. קחו כדוגמא את $\binom{n}{k}$) מראה ש־$F(n)=\sum_k f(n,k)$ לא תלוי בn! לכן מספיק לוודא את הזהות עבור $n=1$, או כל ערך אחר של n. בהמשך, נראה ש$R=\frac{g}{f}$ היא בהכרח פונקציה רציונלית בn,k. למעשה, כדי להוכיח זהות כל מה שאני צריך הוא את הפונקציה R, כי ממנה ניתן לשחזר את g ולוודא את השיוויון $(*)$.

אם קורה התופעה, לפונקציה g קוראים חברת־WZ של f, והזוג (f,g) נקרא זוג־WZ. לפונקציה הרציונלית R קוראים 'סרטיפיקט ההוכחה'. הערה: לפעמים נותנים את $R(n,k)=\frac{g(n,k)}{f(n,k-1)}$ בתור הסרטיפיקט, זה לא משנה.

דוגמא בסיסית: ניקח את הזהות הפשוטה $\sum_k \binom{n}{k} = 2^n$. ננרמל ונקבל $\sum_k \binom{n}{k} 2^{-n} = 1$. מתקיימת תופעת WZ, והפונקציה $g(n,k) = -\binom{n}{k-1} 2^{-n-1}$ היא חברת־WZ של $f(n,k)$, ואכן:

$$\binom{n+1}{k} 2^{-n-1} - \binom{n}{k} 2^{-n} \quad = \quad -\binom{n}{k} 2^{-n-1} + \binom{n}{k-1} 2^{-n-1}$$

(זהות זו שקולה לזהות פסקל $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.) היופי בתופעת־$WZ$ הוא שהיא מראה שיש סימטריה מסוימת בעולם הזהויות: באגפים השונים של $(*)$ התפקידים של n ו־k הם הפוכים. בהמשך נראה איך לנצל סימטריה זו בשביל לייצר זהויות נוספות.

דוגמא פחות בסיסית: $\sum_k (-1)^k \binom{n}{k} \binom{2k}{k} 4^{n-k} = \binom{2n}{n}$. מנרמלים: $\sum_k (-1)^k \binom{n}{k} \binom{2k}{k} 4^{n-k} / \binom{2n}{n} = 1$. עבור $n=1$ מקבלים $\frac{4-2}{2} = 1$. סרטיפיקט ההוכחה הוא $R(n,k) = \frac{-2k^2}{(2n+1)(n-k+1)}$. כדי לוודא את השיוויון המערב את f, g נחלק אותו ב־$f(n,k)$:

$$\begin{aligned}
\frac{f(n+1,k)}{f(n,k)} - 1 \quad &= \quad \frac{R(n,k+1)f(n,k+1)}{f(n,k)} - \frac{R(n,k)f(n,k)}{f(n,k)} \\
\Longrightarrow \frac{n+1}{n+1-k} 4 \frac{n+1}{2(2n+1)} - 1 \quad &= \quad -\frac{2(k+1)^2}{(2n+1)(n-k)} (-\frac{1}{4}) \frac{n-k}{k+1} \frac{2(2k+1)}{k+1} + \frac{2k^2}{(2n+1)(n-k+1)} \\
\Longrightarrow \frac{2(n+1)^2}{(n+1-k)(2n+1)} - 1 \quad &= \quad \frac{2k+1}{2n+1} + \frac{2k^2}{(2n+1)(n-k+1)}
\end{aligned}$$

מכפילים במכנה המשותף $(n+1-k)(2n+1)$ ומקבלים
$2(n+1)^2 - (n+1-k)(2n+1) = (2k+1)(n+1-k) + 2k^2$. פתיחת סוגריים משלימה את הוידוא.

נותר להסביר איך מוצאים את g. נגדיר את הפונקציה $h(k) = f(n+1,k) - f(n,k)$. בעיית מציאת פונקציה G כך ש־$h(k) = G(k+1) - G(k)$ שקולה למציאת צורה יפה לסכום $\sum_{k=0}^{K-1} h(k) = G(K)$ (עד כדי זה שבבעייה הראשונה יש דרגת חופש של קבוע או פונקציה שלא תלויה ב־k). G היא בעצם g, רק שלא כתבנו את הפרמטר n: $G(k) = g(n,k)$.

נשים לב ש־$h(k)$ היפרגיאומטרית:
$\frac{h(k+1)}{h(k)} = \frac{f(n+1,k+1) - f(n,k+1)}{f(n+1,k) - f(n,k)} = (\frac{f(n+1,k+1)}{f(n,k)} - \frac{f(n,k+1)}{f(n,k)}) \cdot (\frac{f(n+1,k)}{f(n,k)} - 1)^{-1}$. נציג עתה אלגוריתם שפותר את הבעיה הכללית של מציאת סכום היפרגיאומטרי $\sum_{k=0}^{K-1} h(k) = G(K)$, בהינתן ש־$h$ היפרגיאומטרית ו־G היפרגיאומטרית עד כדי קבוע.

<u>האלגוריתם של גוספר</u>

האלגוריתם של גוספר הומצא על ידו ב־1978. ראינו כבר איך הוא ישמש אותנו, אבל הוא פותר בעיה שימושית ובעלת מוטיבציה בפני עצמה.

האלגוריתם של גוספר פותר בעיה של אינטגרציה דיסקרטית: האם אפשר לפשט סכום מהצורה $s_n = \sum_{k=0}^{n-1} t_k$ כאשר t_k ביטוי היפרגיאומטרי? שאלה זו שקולה, עד כדי קבוע, למציאת ביטוי s_n המקיים $s_{n+1} - s_n = t_n$. האלגוריתם מוצא s_n אם הוא קיים והיפרגיאומטרי.

נתאר את האלגוריתם בשלבים. **שלב א':** רדוקציה למציאת פונקציה רציונלית שמקיימת רקורסיה מעומק 1.

1. נסמן $r(k)=\frac{t_{k+1}}{t_k}$, פונקציה רציונלית ב־k.
2. נניח שיש פיתרון היפרגיאומטרי למשוואה $s_{n+1}-s_n=t_n$. נשים לב שאם s_n היפרגיאומטרי, מתקיים:

$$\begin{aligned}\frac{s_n}{t_n} &= \frac{s_n}{s_{n+1}-s_n}\\ &= \frac{1}{\frac{s_{n+1}}{s_n}-1}\end{aligned}$$

כלומר המנה היא פונקציה רציונלית (כי s_n היפרגיאומטרית). נסמן אם כן $s_n=y(n)t_n$, כאשר y פונקציה רציונלית שאותה אנחנו מחפשים.

3. המשוואה הבסיסית $s_{n+1}-s_n=t_n$ הפכה ל־$y(n+1)t_{n+1}-y(n)t_n=t_n$, כלומר:

$$y(n+1)r(n)-y(n) \quad = \quad 1$$

כלומר, קיבלנו נוסחת נסיגה מעומק 1 שמפתרונה $y(n)$ אפשר לשחזר את s_n בקלות: $s_n=y(n)t_n$.

כמו שהזכרנו בהתחלה, יש אלגוריתם שפותר נוסחאות נסיגה כאלו (עם מקדמים רציונליים) אוטומטית, אבל במקרה של עומק 1 נוכל להסתדר גם בלי!

שלב ב': רדוקציה למציאת פולינום שמקיים רקורסיה מעומק 1. שלב זה יותר תיאורטי.

<u>למה 1:</u> כל פונקציה רציונלית $r(n)$ אפשר להציג בצורה $\frac{a(n)}{b(n)}\frac{c(n+1)}{c(n)}$, כך ש־$\gcd(a(n),b(n+h))=1 \implies h\in\mathbb{N}_0$.

למה זו היא תרגיל (שנפתר בסוף המסמך). בואו נראה מה היא נותנת לנו. נפעיל אותה על r שלנו: $r(n)=\frac{a(n)}{b(n)}\frac{c(n+1)}{c(n)}$, ונציב במשוואה:

$$y(n+1)\frac{a(n)}{b(n)}\frac{c(n+1)}{c(n)}-y(n)=1 \implies y(n+1)\frac{a(n)c(n+1)}{b(n)}-c(n)y(n)=c(n)$$

כדי לבטל חלק מהמקדמים, טבעי לעשות את שינוי המשתנים $y(n)=\frac{b(n-1)}{c(n)}x(n)$, שנותן:

$$(*)a(n)x(n+1)-b(n-1)x(n) \quad = \quad c(n)$$

במובן מסויים, לא השתנה כלום ־ שוב קיבלנו משוואה מעומק 1. עכשיו המקדמים הם פולינומים במקום פונקציות רציונליות, אבל גם קודם יכולנו להגיע למצב זה באמצעות הכפלה במכנה משותף. מה שהשתנה הוא הקסם הבא:

למה 2: פיתרון בדמות פונקציה רציונלית למשוואה $(*)$ הוא בהכרח פולינום ב־n.

מהלמה הזו, שגם היא תרגיל, ברור מה צריך לעשות: להציב $x(n)=\sum_{i=0}^{d} a_i n^i$ כאשר d מעלת הפיתרון, להשוות מקדמים של חזקות זהות של n ולקבל משוואות לינאריות על a_i עם מקדמים שהם פולינומים (מזכיר את האלגוריתם של הנזירה סלין).

מבחינה אלגוריתמית, חסרים לנו 2 מרכיבים: הוכחה אלגוריתמית ללמה 1, וחסם על המעלה d. בנוסף, למה 2 דורשת הוכחה. אל תמשיכו הלאה בלי שפתרתם את 3 התרגילים הבאים: (יש פתרונות בסוף המסמך)

תרגיל 5: הוכיחו את למה 1 באופן אלגוריתמי.

תרגיל 6: הוכיחו את למה 2.

תרגיל 7: מצאו חסם למעלה d של הפיתרון x כפונקציה של a,b,c.

לסיכום: מחשבים את $r(n)=t_{n+1}/t_n$ ומציגים אותה בצורה של למה 1. כך מקבלים את המשוואה $x(n+1)a(n)-b(n-1)x(n)=c(n)$ שפותרים בעזרת אלגברה לינארית סטנדרטית (השוואת מקדמים ופתרון משוואות). מתוך x משחזרים את s באופן הבא: $s_n=y(n)t_n=x(n)\frac{b(n-1)}{c(n)}t_n$.

דוגמאות שימוש:

1. $S_n=\sum_{k=0}^{n-1} k!$: במקרה זה, $t_n=n!, r(n)=n+1$. בגלל ש$\gcd(n+1,1)=1$, אפשר לבחור $a(n)=n+1, b(n)=c(n)=1$ ולקבל את הרקורסיה $(n+1)x(n+1)-x(n)=1$. לרקורסיה זו לא יכול להיות פיתרון פולינומיאלי, כי המעלה של $x(n)+1$ קטנה ממש מהמעלה של $(n+1)x(n+1)$. לכן אין הצגה היפרגיאומטרית לסכום.

2. $S_n=\sum_{k=0}^{n} k\cdot k!$: במקרה זה $r(n)=\frac{(n+1)^2}{n}$, $t_n=n\cdot n!$. הפעם $h=1$ בעייתי כי $\gcd((n+1)^2,n+h)=n+1$ עבורו. לכן נכתוב $\frac{(n+1)^2}{n}=\frac{n+1}{1}\frac{n+1}{n}$ ולכן $a(n)=n+1, b(n)=1, c(n)=n$. מקבלים את הרקורסיה $x(n+1)(n+1)-x(n)=n$. מהשוואת מעלות ברור שפיתרון פולינומיאלי יהיה קבוע, ואכן $x(n)=1$ הוא פיתרון סבבה שנותן $y(n)=\frac{b(n-1)}{c(n)}x(n)=\frac{1}{n}$, כלומר $s_n=y(n)t_n=n!$. אכן, $s_{n+1}-s_n=t_n$, ולכן $\sum_{k=0}^{n} k!=\sum_{k=0}^{n}(s_{k+1}-s_k)=s_{n+1}-s_0=(n+1)!-1$.

2 הדוגמאות האלה מזכירות את ההבדל בין $\int_0^t e^{x^2}dx$ (פונקציה לא אלמנטרית) ל$\int_0^t xe^{x^2}dx=\frac{1}{2}\int_0^t (e^{x^2})'dx=\frac{1}{2}(e^{t^2}-1)$ (פונקציה אלמנטרית).

תרגיל 8: הראו שכשגוספר מצליח על $f(n+1,k)-f(n,k)$ אז הוא מחזיר פונקציה מהצורה $R(n,k)f(n,k)$ כאשר R רציונלית בn,k.

נשתמש באלגוריתם של גוספר כדי למצוא את חברת־WZ של $f(n,k)=\binom{n}{k}2^{-n}$.

$$\begin{aligned}
h(k) &= \binom{n+1}{k}2^{-n-1} - \binom{n}{k}2^{-n} \\
r(k) &= \frac{h(k+1)}{h(k)} \\
&= \frac{\binom{n+1}{k+1} - 2\binom{n}{k+1}}{\binom{n+1}{k} - 2\binom{n}{k}} \\
&= \frac{\frac{n+1}{k+1} - 2\frac{n-k}{k+1}}{\frac{n+1}{n+1-k} - 2} \\
&= \frac{n+1-k}{k+1} \cdot \frac{2k-n+1}{2k-n-1}
\end{aligned}$$

וזו כבר הצגה בצורה של למה 1, כלומר $a(k) = n+1-k, b(k) = k+1, c(k) = 2k-n-1$. נרצה לפתור את המשוואה $(n+1-k)x(k+1) - kx(k) = 2k-n-1$. משיקולי מעלות, x צריך להיות קבוע, ואכן $x=-1$ הוא פיתרון מתאים. על כן,

$$\begin{aligned}
g(n,k) &= h(k)\frac{b(k-1)}{c(k)}x(k) \\
&= -(\frac{k}{2k-n-1})(\binom{n+1}{k}2^{-n-1} - \binom{n}{k}2^{-n})
\end{aligned}$$

עוד קצת עבודת פישוט מראה ש-$g(n,k) = -\binom{n}{k-1}2^{-n-1}$.

<u>האלגוריתם של ציילברגר</u>

ציינתי שתופעת WZ לא תמיד קורה. בשביל זה יש את האלגוריתם של ציילברגר, שעובד מתי שהאלגוריתם של סלין עובד, ולמעשה נותן לנו את אותו הדבר: רקורסיה עבור $F(n) = \sum_k f(n,k)$. עם זאת, הוא עושה זאת באופן שונה לחלוטין ומשמעותית מהר יותר. ממנו גילו את תופעת WZ.

הרעיון הוא זה: היינו רוצים למצוא g כך ש-$f(n,k) = g(n,k+1) - g(n,k)$, כי אז לחשב סכום על k של $f(n,k)$ ביו 0 ל-n לדוגמא הופכת להיות בעיה פשוטה, כי הסכום נהיה טלסקופי: $g(n,n+1) - g(n,0)$. כדי למצוא g כזו, מפעילים את גוספר על $t_k = f(n,k)$. הכל טוב ויפה, ומעבר לכך - נראה שאנחנו מקבלים הרבה יותר ממה שאנחנו צריכים: אנחנו יכולים לחשב את $\sum_{k=0}^{N_0} f(n,k)$ גם עבור N_0 שרירותי, ולא רק עבור $N_0 = n$. במקרה $f(n,k) = \binom{n}{k}$ אפשר להראות שאין g שמקיימת זו. מכך אנחנו מסיקים שהכיוון זה נכשל כי האלגוריתם של גוספר לא יחזיר לנו תוצאה כרצוננו. אבל אפשר להציל רעיון זה. לדוגמא, ראינו מתופעת WZ שלפעמים גוספר עובד על $f(n+1,k) - f(n,k)$.

השיפור הוא זה: לחפש מקדמים $\{a_j(n)\}_{j=0}^J$ כך שעל $\sum_{j=0}^J a_j(n)f(n+j,k)$ אפשר יהיה להפעיל את גוספר, כלומר למצוא g היפרגיאומטרית שתקיים $\sum_{j=0}^J a_j(n)f(n+j,k) = g(n,k+1) - g(n,k)$. כשיש לנו את הזהות הזו, אפשר לסכום על k ולקבל $\sum_j a_j(n)F(n+j) = g(n,\infty) - g(n,-\infty)$. תחת התנאי $\lim_{|x|\to\infty} g(n,x) = 0$ שלרוב יתקיים, קיבלנו רקורסיה הומוגונית על $F(n)$, כמו באלגוריתם של סלין.

בעזרת האלגוריתם של סלין אפשר להוכיח שבהכרח קיימים J ומקדמים a_j מתאימים. אנחנו נציג את ההוכחה כעת, אך אפשר לדלג עליה, כי לאחריה נציג דרך עדיפה למצוא את J ו־a_j (עם זאת בדרך העדיפה לא ברור אפריורי שהאלגוריתם עובד).

קיום: מהאלגוריתם של סלין, נקבל $\sum a_{i,j}(n)f(n+j,k+i)=0$ (הסכימה היא גם על i וגם על j, ואנחנו רוצים רק על j). נכפיל 2 האגפים במינוס 1, ונוסיף לשני האגפים $\sum_{i,j} a_{i,j}(n)f(n+j,k)$:

$$\begin{aligned}\sum a_{ij}(n)f(n+j,k) &= \sum_{i,j} a_{i,j}(n)(f(n+j,k)-f(n+j,k+i)) \\ \Longrightarrow \sum_j(\sum_i a_{ij}(n))f(n+j,k) &= \sum_j\sum_{i>0} a_{i,j}(n)(f(n+j,k)-f(n+j,k+i))\end{aligned}$$

אני טוען שסיימנו! אגף שמאל הוא כמו שרצינו (סוכמים רק על j), רק נותר להראות שאגף ימין הוא מהצורה $g(n,k+1)-g(n,k)$ כאשר $g(n,k)/f(n,k)$ פונקציה רציונלית. לשם כך, מספיק לקחת ביטוי בודד $a_{i,j}(n)(f(n+j,k)-f(n+j,k+i))$. המקדם $a_{i,j}(n)$ לא משנה, לכן יש לנו את $f(n+j,k)-f(n+j,k+i)$ עם $i>0$. בגלל שאפשר לכתוב אותו כסכום טלסקופי $\sum_{i'=0}^{i-1}(f(n+j,k+i')-f(n+j,k+i'+1))$, מספיק להוכיח את זה עבור $f(n+j,k+i')-f(n+j,k+i'+1)$, ואז ברור ש־$g(n,k)=-f(n+j,k+i')$ והרציונליות נובעת מההיפרגיאומטריות של $f(n,k)$. ■

עכשיו נראה איך מוצאים את המקדמים בפועל. נראה זאת על דוגמא שתכיל את כל המרכיבים של הבעיה. ננסה להוכיח את הזהות $\sum_{k=0}^n \binom{n}{k}^2=\binom{2n}{n}$ ־ בלי לדעת את אגף ימין מראש! נסמן $f(n,k)=\binom{n}{k}^2$. ננחש את J. נתחיל בקטן: $J=1$ (אם לא נצליח, נגדיל ונחזור על הכל. בכל אופן, האלגוריתם של סלין נותן חסם עליון שתקף גם כאן, לפי הוכחת הקיום). אנחנו רוצים להפעיל את גוספר על $t_k=a_0(n)f(n,k)+a_1(n)f(n+1,k)$, כאשר a_0,a_1 מקדמים שיבחרו כך שגוספר יצליח (אחרי זה ההמשך ברור ־ סוכמים על k כאמור, ומקבלים רקורסיה). נחשב את $r(k)$:

$$\begin{aligned}\frac{t_{k+1}}{t_k} &= \frac{a_0(n)f(n,k+1)+a_1(n)f(n+1,k+1)}{a_0(n)f(n,k)+a_1(n)f(n+1,k)} \\ &= \frac{a_0(n)\binom{n}{k+1}^2+a_1(n)\binom{n+1}{k+1}^2}{a_0(n)\binom{n}{k}^2+a_1(n)\binom{n+1}{k}^2}\end{aligned}$$

נשתמש בהיפרגיאומטריות כדי לפשט את הביטויים ולהישאר עם פונקציות רציונליות. ראשית נחלק ב־$\binom{n}{k}^2$:

$$= \frac{a_0(n)(\frac{n-k}{k+1})^2+a_1(n)(\frac{n+1}{k+1})^2}{a_0(n)+a_1(n)(\frac{n+1}{n+1-k})^2}$$

ועכשיו נחשב מכנה משותף כך שבמונה ובמכנה יהיו פולינומים:

$$= \frac{a_0(n)(n-k)^2 + a_1(n)(n+1)^2}{a_0(n)(n+1-k)^2 + a_1(n)(n+1)^2} \frac{(n+1-k)^2}{(k+1)^2}$$

נסמן $r(k) = (n+1-k)^2, s(k) = (k+1)^2$ ו־$p_0(k) = a_0(n)(n+1-k)^2 + a_1(n)(n+1)^2$. השיוויון הופך ל$\frac{t_{k+1}}{t_k} = \frac{p_0(k+1)}{p_0(k)} \frac{r(k)}{s(k)}$. כדי להפעיל את גוספר, צריך להציג את $\frac{t_{k+1}}{t_k}$ בצורה $\frac{p(k+1)}{p(k)} \frac{p_2(k)}{p_3(k)}$, כאשר $\gcd(p_2(k), p_3(k+h)) = 1$ לכל $h \geq 0$ שלם. החלק הראשון של $\frac{t_{k+1}}{t_k}$, $\frac{p_0(k+1)}{p_0(k)}$, כבר נמצא בצורה הזו (וזה יהיה נכון לכל דוגמא שנבחר, למען האמת) לכן צריך למצוא הצגה זו רק עבור $\frac{r(k)}{s(k)}$, כלומר להציג $\frac{r(k)}{s(k)} = \frac{p_1(k+1)}{p_1(k)} \frac{p_2(k)}{p_3(k)}$. במקרה שלנו לא צריך להתאמץ, כי ההצגה $p_1 = 1, p_2 = r, p_3 = s$ היא כבר הצגה טובה (כי $\gcd(n+1-k, k+1+h) = 1$ כפולינומים בk כאשר n משתנה וh מספר). לכן אפשר לבחור:

$$\begin{aligned}
p_2(k) &= (n+1-k)^2 \\
p_3(k) &= (k+1)^2 \\
p(k) &= p_0(k)p_1(k) \\
&= a_0(n+1-k)^2 + a_1(n+1)^2 \\
&= (a_0 f(n,k) + a_1 f(n+1,k)) \frac{(n+1-k)^2}{f(n,k)}
\end{aligned}$$

ועכשיו נותר לפתור את הרקורסיה מעומק 1 הבאה: $p_2(k)x(k+1) - p_3(k-1)x(k) = p(k)$. היופי הוא שרק אגף ימין תלוי במקדמים הלא ידועים $a_i(n)$, ותלות זו היא לינארית! (זה גם תמיד קורה) לכן אפשר לעשות כרגיל רדוקציה למשוואות לינאריות: אלגוריתם גוספר נותן לנו הערכה Δ למעלה של $x(k)$ בk. נציב $x(k) = \sum_{l \leq \Delta} \beta_l k^l$ ונשווה מקדמים של אותן חזקות k ־ אלו משוואות בנעלמים $\{\beta_l\} \cup \{a_i\}$ (סה"כ $J + \Delta + 2$ נעלמים). במקרה שלנו, גוספר נותן $\Delta = 1$ (בידקו!) ובחרנו $J = 1$, אז יש 4 נעלמים. אם לא נמצא פיתרון, נגדיל את J ונחזור על התהליך, אבל הנה אנחנו מצליחים: נציב $x(k) = \beta_0 + \beta_1 k$ ונפתור בעצמנו:

$$\begin{aligned}
(n+1-k)^2(\beta_0 + \beta_1 + \beta_1 k) - k^2(\beta_0 + \beta_1 k) &= a_0(n)(n+1-k)^2 + a_1(n)(n+1)^2 \implies \\
[k^3]\beta_1 - \beta_1 &= 0 \\
[k^2]\beta_0 + \beta_1 - 2(n+1)\beta_1 - \beta_0 &= a_0 \\
[k^1](n+1)^2\beta_1 - 2(n+1)(\beta_0 + \beta_1) &= -2a_0(n+1) \\
[k^0](n+1)^2(\beta_0 + \beta_1) &= (a_0 + a_1)(n+1)^2
\end{aligned}$$

עכשיו צריך למצוא איבר לא טריוויאלי בגרעין.

המשוואה הראשונה היא טאוטולוגיה. המשוואה השנייה נותנת $a_0 = -(2n+1)\beta_1$. המשוואה השלישית, לאחר צמצום ב$n+1$ והצבת a_0, נותנת $\beta_0 = -\frac{3}{2}(n+1)\beta_1$. המשוואה הרביעית נותנת $\beta_0 + \beta_1 = a_0 + a_1$. לכן הגרעין נפרש ע"י $(a_0, a_1, \beta_0, \beta_1) = \beta_1(-2n-1, \frac{n+1}{2}, -\frac{3}{2}(n+1), 1)$. נבחר $\beta_1 = 2$ ונקבל את הפיתרון $x(k) = -3(n+1) + 2k$, ו$t_k = -2(2n+1)\binom{n}{k}^2 + (n+1)\binom{n+1}{k}^2$ מקיים משוואה מהצורה:

$$(*) - 2(2n+1)\binom{n}{k}^2 + (n+1)\binom{n+1}{k}^2 \quad = \quad G(n+1,k) - G(n,k)$$

כאשר $G(n,k)$ נתונה ע"י:

$$\begin{aligned}
G(n,k) &= s_k \\
&= \frac{p_3(k-1)}{p(k)} x(k) t_k \\
&= p_3(k-1)x(k)\frac{t_k}{p(k)} \\
&= k^2(-3n-3+2k)\frac{a_0 f(n,k) + a_1 f(n+1,k)}{a_0(n+1-k)^2 + a_1(n+1)^2} \\
&= k^2(-3n-3+2k)\frac{a_0 f(n,k) + a_1 f(n+1,k)}{(a_0 f(n,k) + a_1 f(n+1,k))\frac{(n+1-k)^2}{f(n,k)}} \\
&= (-3n-3+2k)\frac{f(n,k)k^2}{(n+1-k)^2} \\
&= (-3n-3+2k)\frac{n!^2}{(k-1)!^2(n-k+1)!^2}
\end{aligned}$$

נסכום את $(*)$ ונקבל $-2(2n+1)F(n) + (n+1)F(n+1) = 0$, רקורסיה מעומק 1 שנפתרת בקלות: $F(n+1) = \frac{2(2n+1)}{n+1}F(n) = \frac{(2n+2)(2n+1)}{(n+1)^2}F(n) \implies F(n) = \binom{2n}{n}F(1) = \binom{2n}{n}$.

עוד דוגמא: $F(n) = \sum_{k\geq 0}(-1)^k \frac{\binom{n}{k}}{\binom{x+k}{k}}$. מקבלים $(n+x)f(n,k) - (n+1+x)f(n+1,k) = g(n,k+1) - g(n,k)$ עם $R = \frac{g}{f} = \frac{k(k+x)}{n+1-k}$ (בדומה לתופעת־WZ, עכשיו כשנתתי את R, אפשר לוודא את השיוויון הנ"ל המקשר בין f לgg.) סכימה על k נותנת $F(n+1)/F(n) = \frac{n+x}{n+x+1}$, כלומר $F(n) = \frac{x}{x+n}F(1) = \frac{x}{x+n}$.

<u>תרגיל 9:</u> הראו שאלגוריתם ציילברגר על $F(n) = \sum_k f(n,k)$ עובד עם $J = 1$ אמ"מ קורה תופעת־WZ עבור $f(n,k)/F(n)$.

חשוב להבין שאלגוריתם ציילברגר מוצלח בהרבה מהאלגוריתם של סלין מבחינת סיבוכיות ־ ה־J שלו לרוב קטן בהרבה מה־J של אלגוריתם סלין (ובכל מקרה חסום על־ידו), ויש כמות לינארית של משתנים במקום ריבועית ($J+\Delta+2$ במקום $I \cdot J$).

<u>דואליות</u>

כאשר תופעת WZ מתרחשת, מלבד הוכחה קצרה אפשר לקבל זהויות חדשות מהזוג (f,g). זה נובע מהסימטריה היפה של השיוויון הבסיסי

$$f(n+1,k) - f(n,k) \quad = \quad g(n,k+1) - g(n,k)$$

הזהות הנלוות (Companion): יהי (f,g) זוג־WZ. נניח 2 הנחות סבירות: ש־ $f_k=\lim_{n\to\infty} f(n,k)$ קיים וסופי, וש־$\lim_{L\to\infty}\sum_{n\geq 0} g(n,-L)=0$. זאת בנוסף להנחה הרגילה $\lim_{|k|\to\infty} g(n,k)=0$.

נתחיל במשוואה הבסיסית:

$$f(n+1,k)-f(n,k) \quad = \quad g(n,k+1)-g(n,k)$$

נסכום על $n=0,\cdots,N$:

$$f(N+1,k)-f(0,k) \quad = \quad \sum_{n=0}^{N} g(n,k+1)-\sum_{n=0}^{N} g(n,k)$$

נשאיף את N לאינסוף ונקבל:

$$f_k-f(0,k) \quad = \quad \sum_{n\geq 0} g(n,k+1)-\sum_{n\geq 0} g(n,k)$$

סכימה על k בין $-L$ ל־$K-1$ והשאפת L לאינסוף נותנת את הזהות הבאה:

$$\sum_{k\leq K-1}(f_k-f(0,k)) \quad = \quad \sum_{n\geq 0} g(n,K)$$

שנקראת הזהות הנלוות. דוגמה: $\sum_k \binom{n}{k}^2=\binom{2n}{n}$ הופך ל־$\sum_k \binom{n}{k}^2/\binom{2n}{n}=1$. הסכום הזה מקיים את התופעה, עם $R(n,k)=\frac{-k^2(3n-2k+3)}{2(2n+1)(n-k+1)^2}$, ו־$G(n,k)=\frac{-(3n-2k+3)k^2}{2(2n+1)(n-k+1)^2}F(n,k)$. בנוסף, הוא מקיים את התנאים לקיום זהות נלוות, ומקבלים $f_k=0, f(0,k)=\delta_{0,k}$. הזהות הנלוות יוצאת:

$$\sum_{n\geq 0}\frac{-(3n-2k+3)}{2(2n+1)}\frac{n!^2}{(k-1)!^2(n-k+1)!^2\binom{2n}{n}} \quad = \quad \begin{cases}0 & k=0\\ -1 & k>0\end{cases}$$

ניתן לפשט ולקבל (תרגיל):

$$\sum_{n\geq 0}\frac{(3n-2k+1)}{(2n+1)}\frac{\binom{n}{k}^2}{\binom{2n}{n}} \quad = \quad 2$$

וזו זהות חדשה ומגניבה.

הזהות הדואלית:

הזהות הנלוות היא לא אינבולוציה, אבל עכשיו נציג כמה טרנספורמציות על זוג־WZ, שנותנות זוג חדש ורובן אינבולוציות.

בתור חימום, וגם כי זה יהיה שימושי בהמשך, נציג כמה טרנספורמציות פשוטות שמשמרות את היותו של (F,G) זוג־WZ. כולן חוץ מהראשונה הן אינבולוציות, ואפשר להרכיב אותן:

- $(F(n+\alpha,k+\beta),G(n+\alpha,k+\beta))$ לכל 2 מספרים מרוכבים α,β
- $(F(-n,k),-G(-n-1,k))$
- $(F(n,-k),-G(-n,-k+1))$
- $(G(k,n),F(k,n))$

תרגיל 10: ודאו שהטרנס' הנ"ל מקיימות את התכונות שהבטחתי, והראו שהטרנספורמציה

$$(F(n,k),G(n,k))\rightarrow(G(-k-1,-n),F(-k,-n-1))$$

מתקבלת מהרכבת האינבולוציות הקודמות.

עוד משפחה של טרנספורמציות היא זו: אם $p(n,k)$ היא פונקציה ב2 משתנים מרוכבים כך שהיא מחזורית עם מחזור 1 בכל אחד מהם בנפרד, אז גם $(p(n,k)f(n,k),p(n,k)g(n,k))$ הוא זוג־WZ.

נסמן ב(F',G') זוג חדש שנוצר ע"י הפעלת טרנספורמציות. נתעניין רק במקרים בהם לפונקציה G' יהיה תומך קומפקטי, כלומר לכל n $G'(n,k)$ תתאפס עבור k גדול מספיק. זה יבטיח לנו ש$\lim_{|x|\rightarrow\infty}G'(n,x)=0$ ולכן נוכל לסכום על k בתחום סופי ולקבל הוכחה לזהות החדשה $\sum_k F'(n,k)=\mathrm{const}$.

בשביל הזהות הדואלית, נבחר p מאוד מסויימת. לשם כך נשתמש בפונקציית גמא, שמאפשרת להגדיר עצרת לערכים לא טבעיים. פונקציית גמא מוגדרת ע"י $\Gamma(z)=\int_0^\infty t^{z-1}e^{-t}dt$ עבור $\Re(z)>0$. היא ניתנת להמשכה אנליטית לכל המישור המרוכב (מלבד שלמים אי־שליליים) ע"י המשוואה $\Gamma(z+1)=z\Gamma(z)$. התכונה המוכרת שלה היא ש$\Gamma(n)=(n-1)!$ עבור $n\geq 1$. באמצעותה נוכל להסתכל על פונקציות היפר־גיאומטריות $F(n,k)$ כפונקציות במשתנים מרוכבים. נתעסק רק עם פונקציות מהצורה הבאה:

$$\begin{aligned} F(n,k) &= x^n y^k r(n,k)\frac{\prod_i(a_in+b_ik+c_i)!}{\prod_i(u_in+v_ik+w_i)!} \\ &= x^n y^k r(n,k)\frac{\prod_i\Gamma(a_in+b_ik+c_i+1)}{\prod_i\Gamma(u_in+v_ik+w_i+1)} \end{aligned}$$

כאשר r רציונלית. אם f לא מוגדרת ב(n,k) כי יש שם גמא של מספר שלם אי־שלילי, אבל הגבול $\lim_{x\to n}(\lim_{y\to k} f(x,y))$ קיים, אז נגדיר את $f(n,k)$ להיות הגבול הזה.

כאשר (f,g) יהיו זוג־WZ, כלומר יתקיים השיוויון עבור $f(n+1,k)-f(n,k)=g(n,k+1)-g(n,k)$ עבור מספרים שלמים n,k, נניח שהוא נכון גם לn,k מרוכבים עבורם ההפרש מוגדר. (הערה: אם יש לכם הוכחה כללית לכך, אשמח לראות. בספר מתקיימת ההנחה הזו ללא הוכחה)

תכונה פחות מוכרת של Γ, שלא נוכיח כאן, היא נוסחת השיקוף של אוילר: $\Gamma(1-z)\Gamma(z)=\frac{\pi}{\sin(\pi z)}$, כלומר $(-z)!(z-1)!=\frac{\pi}{\sin(\pi z)}$.

לכן אם ניקח פונקציה של זוג־(WZ) ונחליף בה גורם/גורמים מהצורה $(an+bk+c)!$ בגורם/גורמים $(-1)^{an+bk}/(-an-bk-c-1)!$ נקבל זוג־WZ חדש, כי מנוסחת השיקוף נובע שחילוף זה שקול להכפלה/חילוק ב־p־ים מהצורה $p(n,k)=\frac{(-1)^{an+bk}}{\pi}\sin(\pi(an+bk+c+1))$, והיא בעלת מחזור 1 ב־$n$ וב־k (ההנחה היא שa,b שלמים ו־c ממשי). זהות שתתקבל משימוש ב־p כאלו ובטרנספורמציות הפשוטות הקודמות תיקרא זהות דואלית.

<u>הערה טכנית:</u> אם c שלם, אז כביכול אנחנו עושים משהו "לא חוקי" (גם כי אנחנו מחלקים לפעמים בp שאמורה להתאפס וגם כי עצרת של מספר שלילי לא מוגדרת). עוקפים את זה ככה: אם c שלם, מוסיפים לו אפסילון (זה יוצר זוג־WZ חדש, לפי הטרנספורמציה הראשונה), עושים את הטרנספורמציות הרצויות, ואז משאיפים את c חזרה למספר השלם שהוא היה. מהרציפות מקבלים זוג־WZ שוב, אלא אם הגבול יוצא אינסוף.

הגיע זמן הדוגמאות. בתור דוגמא ראשונה, ניקח את הזוג המוכר $(\binom{n}{k}2^{-n},-\binom{n}{k-1}2^{-n-1})$. נחליף ב־$G$ את $n!$ ב־$\frac{(-1)^n}{(-n-1)!}$ ואת $\frac{1}{(k-1)!}$ ב־$(-1)^k(-k)!$ (העברנו ביטוי אחד מהמונה למכנה ולהיפך). אנחנו מקבלים את G החדשה הבאה: $G'(n,k)=-\frac{(-k)!}{(-n-1)!(n-k+1)!}(-1)^{n-k}2^{-n-1}=\binom{-k}{-n-1}(-1)^{n-k+1}2^{-n-1}$, ו־$F$ החדשה היא: $F'(n,k)=\frac{(-1)^{n+k}}{(-n-1)!}\frac{(-k)!}{k(n-k)!}2^{-n}$.

נשתמש בטרנספורמציה מהתרגיל: $(F(n,k),G(n,k))\to(G(-k-1,-n),F(-k,-n-1))$ כדי לקבל את $F''(n,k)=\binom{n}{k}(-1)^{n-k}2^k$ ואת $G''(n,k)=\binom{n}{k-1}2^k(-1)^{n-k}$. ל־$G''$ יש תומך קומפקטי כמו שרצינו, ולכן $\sum_k\binom{n}{k}(-1)^{n-k}2^k=\text{const}$. חישוב עבור $k=0$ מראה שהקבוע הוא 1.

דוגמא שנייה: נחזור ל־$F(n,k)=\binom{n}{k}^2/\binom{2n}{n}$. ראינו מקודם שיש ל־$F$ חברת־WZ: $G(n,k)=\frac{-(3n-2k+3)k^2}{2(2n+1)(n-k+1)^2}\frac{n!^2}{(k-1)!^2(n-k)!^2\binom{2n}{n}}$. נחליף ב־$F$ את כל הגורמים מלבד $(n-k)!^2$ בגורמים ההפוכים להם ונקבל:

$$\begin{aligned}F'(n,.k)&=\frac{(-2n-1)!(-k-1)!^2}{(-n-1)!^4(n-k)!^2}\\ G'(n,k)&=(3-2k+3n)\binom{-k}{-n-1}^2\binom{-2n-2}{-n-1}/2\end{aligned}$$

שוב נשתמש בטרנספורמציה מהתרגיל כדי לקבל את הזוג הבא:

$$\begin{aligned} F''(n,k) &= \frac{-3k+2n}{2}\binom{n}{k}^2\binom{2k}{k} \\ G''(n,k) &= \frac{k}{2}\binom{n}{k-1}^2\binom{2k}{k} \end{aligned}$$

זה זוג־WZ ול־G'' יש תומך קומפקטי! לכן הסכום $\sum_k F''(n,k)$ קבוע. מחשבים עבור $n=0$ ויוצא 0. לכן: $\sum_k (2n-3k)\binom{n}{k}^2\binom{2k}{k}=0$.

<u>שימושים נוספים</u>

תהי f פונקציה היפרגיאומטרית 'מנורמלת', כלומר $\sum_k f(n,k)=\text{const}$, ותהי g חברת־WZ של f.

נניח ואנחנו רוצים לסכום את $h(n)=\sum_{k=0}^n f(n,k)$ (שימו לב לגבולות הסכימה ־ הם סופיים!), לדוגמא: $f(n,k)=\binom{3n}{k}/8^n$. נסכום את הזהות שמקשרת בין f לg בין 0 לn:

$$\begin{aligned} \sum_{k=0}^{n} f(n+1,k)-\sum_{k=0}^{n} f(n,k) &= g(n,n+1)-g(n,0) \\ \implies h(n+1)-h(n) &= g(n,n+1)-g(n,0)+f(n+1,n+1) \end{aligned}$$

נסכום על n בין 0 ל$N-1$:

$$(*)h(N) = h(0)+\sum(_{n=0}^{N-1} g(n,n+1)-g(n,0)+f(n+1,n+1))$$

נוסחה זו מאפשרת לחשב N ערכים של h ב$O(N)$ הערכות פונקציה במקום $O(N^2)$.

<u>פתרונות לתרגילים חשובים</u>

<u>תרגיל 5 ־ הוכחת למה 1:</u> נציג את $r(n)$ כפונקציה רציונלית $\frac{p(n)}{q(n)}$ עם מונה ומכנה זרים. אם התנאי "$h\in\mathbb{N}_0 \implies \gcd(p(n),q(n+h))=1$" מתקיים, סיימנו: $a=p, b=q, c=1$. אחרת, צריך לתקן את זה. נאתחל את $c=1$.

אם h ספציפי מפר תנאי זה, והgcd יוצא $g(n)\neq 1$, נעשה את התהליך הפשוט הבא:

- נחלק את p ב$g(n)$ ואת q ב$g(n-h)$.
- החילוקים שלנו מכריחים אותנו למצוא יצוג מהצורה $\frac{d(n+1)}{d(n)}$ ל$\frac{g(n)}{g(n-h)}$. נכתוב:

$$\frac{g(n)}{g(n-h)} = \frac{g(n)}{g(n-1)} \cdot \frac{g(n-1)}{g(n-2)} \cdot \dots \cdot \frac{g(n-h+1)}{g(n-h)}$$

כלומר נבחר $d(n) = \prod_{j=1}^{h} g(n-j)$, ונכפיל את c הנוכחי ב-d. דוגמא: עבור $r(n) = \frac{n+2}{n^2}$ יש h בעייתי והוא 2. נכתוב: $r(n) = \frac{1}{n} \cdot \frac{n+2}{n}$. כעת נכתוב את $\frac{n+2}{n}$ בתור המכפלה הטלסקופית $\frac{n+2}{n+1}\frac{n+1}{n}$, כלומר $d(n) = n(n+1)$.

נחזור על התהליך לכל ה־h הרעים. יש מספר סופי שלהם, וכדי למצוא אותם נחשב רזולטנטה. רזולטנטה היא פונקציה פשוטה לחישוב, שמקבלת 2 פולינומים ומחזירה פולינום במקדמים שלהם שמתאפס אמ"מ יש להם גורם משותף. אם $R(f,g)$ היא רזולטנטה, אז האפסים השלמים האי־שליליים של הפולינום $e(\alpha) = R(p(n), q(n+\alpha))$ הם בדיוק הערכים עבורם $\gcd(p(n), q(n+h)) \neq 1$. העלנו עכשיו 2 שאלות:

1. איך מחשבים רזולטנטה? קודם כל, נראה דוגמא פשוטה: הרזולטנטה של $ax+b, cx+d$ היא $ad-bc$. באופן כללי, לא נוכיח את זה אבל הרזולטנטה שווה לדטרמיננטה של מטריצה מגודל $(\deg f + \deg g) \times (\deg f + \deg g)$ ש$\deg g$ השורות הראשונות שלה הן מקדמי f בהזזות שונות, ו$\deg f$ השורות האחרונות הן מקדמי g בהזזות שונות. מטריצה זו נקראת מטריצת סילבסטר והיא נראית כך:

$$\begin{pmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots \\ 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & \cdots \\ \cdots & & & & & & \cdots \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots \\ 0 & g_m & g_{m=1} & \cdots & g_1 & g_0 & 0 \\ \cdots \end{pmatrix}$$

הערה: יש דרך אלטרנטיבית, והיא לפרק את f,g לגורמים אי־פריקים ולראות אם יש 2 גורמים ששווים עד כדי הזזה בקבוע של המשתנה n.

הערה 2: הצורה של למה 1 היא יחידה, כלומר היא צורה קנונית! (תרגיל)

2. איך מוצאים שורשים שלמים של פולינום? אם לפולינום מקדמים רציונליים, כמו שלרוב יקרא בסיטואציות שלנו, אפשר להכפיל במכנה משותף ולקבל פולינום עם מקדמים שלמים $\sum_{i=0}^{n} a_i x^i$. כל שורש חייב לחלק את a_0 (נובע מכך שמודולו השורש, הפולינום שווה לa_0), ולכן צריך לעבור רק על מחלקי a_0. אם לפולינום מקדמים בהרחבה כלשהי של הרציונליים (גם טרנסצנדנטית), אפשר לעשות רדוקציה לחיתוך אוסף משוואות עם מקדמים רציונליים (תרגיל).

תרגיל 6 ־ הוכחת למה 2: נניח שיש פיתרון רציונלי $x(n) = \frac{f(n)}{g(n)}$ עם f,g זרים, ונראה שg קבועה. נבחר N שלם מקסימלי כך ש$\gcd(g(n), g(n+N)) \neq 1$. הוא אי־שלילי כי $N=0$ מועמד. הוא סופי כי הוא חסום ע"י המרחק בין 2 השורשים הכי גדולים של g.

נסמן ב$u(n) = \gcd(g(n), g(n+N))$. השיוויון $x(n+1)a(n) - b(n-1)x(n) = c(n)$ הופך ל$f(n+1)g(n)a(n) - b(n-1)f(n)g(n+1) = c(n)g(n)g(n+1)$.

ודאו ש$u(n-N)|b(n-1)g(n+1)$ (רמז: f,g זרים). מקסימליות N מראה ש$u(n-N)|b(n-1)$, כלומר $u(n)|b(n+N-1)$.

בדומה, $u(n+1)|a(n)$, כלומר $u(n)|a(n-1)$. אבל אז $a(n-1), b(n+N-1)$ לא זרים, סתירה לבנייה של למה 1.

<u>תרגיל 7 ־ חסם על מעלת d:</u> המשוואה שלנו היא $x(n+1)a(n)-b(n-1)x(n)=c(n)$.

אם x ממעלה d, מקבלים: $x(n+1)a(n)$ ממעלה $d+\deg a$, ו$b(n-1)x(n)$ ממעלה $d+\deg b$. יש כמה מקרים:

- אם $\deg b \neq \deg a$, מקבלים שאגף שמאל ממאלה $d+\max\{\deg a, \deg b\}$, בעוד אגף ימין ממעלה $\deg c$, ולכן $d=\max\{\deg a, \deg b\}-\deg c$.
- אם $\deg a=\deg b$ אבל המקדם המוביל של a ושל b שונה, עדיין מקבלים את אותה המסקנה כי חיסור 2 הפולינומים באגף שמאל לא מוריד את מעלתם.
- אם $\deg a=\deg b$ ולשניהם אותו מקדם מוביל, זה הזמן להסתכל על המקדם הבא. נסמן בλ את המקדם המוביל המשותף, בA את המקדם של $n^{\deg a-1}$ ב$a(n)$ ובB את המקדם של $n^{\deg b-1}$ ב$b(n-1)$. הוכיחו את הטענה הבאה, שנובעת משיקולים דומים לשיקולים הקודמים: $d=\max(\{\deg c-\deg a+1, \frac{B-A}{\lambda}\}\cap\mathbb{N}_0)$, ואם התוצאה שלילית, או שהקבוצה ריקה ־ אין פיתרון פולינומיאלי למשוואה. (הערה: יתכן שהקבוצה, לפני החיתוך עם $\mathbb{N}_0$, תכיל ביטויים שאינם סקלרים.)