התחפושות הרבות של אינדוקציה

מוטי בן־ארי

המחלקה להוראת המדעים

מכון ויצמן למדע

http://www.weizmann.ac.il/sci-tea/benari/

גרסה 1.6.3

תוכן עניינים

פרק 1
מבוא

אינדוקציה היא אחת משיטות ההוכחה השכיחות ביותר במתמטיקה, עד כדי כך שמשתמשים בה בצורה שיגרתית ואף בצורה לא־מפורשת. תופעת לוואי של השימוש השיגרתי היא שאינדוקציה נלמדת כמתכון של צעדים לביצוע ולא כמושג יסודי. מסמך זה מביא קורס קצר על אינדוקציה, המראה את העושר של המושג והדרכים השונות שמשתמשים בה במתמטיקה ובמדעי המחשב.

ההצגה היא רחבה במקום עמוקה: המטרה היא להציג אינדוקציה בכמה שיותר צורות, ולכן כל נושא יוצג על ידי דוגמה אחת ותרגיל אחד או שניים, שלא כמו בספר לימוד עם דוגמאות רבות ושפע תרגילים. המסמך כתוב ברמות שונות: חלקו מתאים לתלמידי תיכון מתקדמים וחלקו לסטודנטים ולמורים למתמטיקה ומדעי המחשב. אפשר לדלג על נושאים לא מוכרים.

פרקים 2-5 אמורים להיות נגישים לתלמידי תיכון. פרק 2 מכיל דיון די ארוך שמטרתו לנמק את הצורך באינדוקציה מתמטית ולהציג אותה כאקסיומה. פרק 3 מציג אינדוקציה המתמטית בצורתה הקלסית מעל למספרים השלמים, תוך דיון בצורות שונות של יישום האקסיומה. פרק 4 חשוב במיוחד כי הוא מראה שאינדוקציה היא שיטת הוכחה הפועלת על מבנים מתמטיים בנוסף למספרים השלמים. פרק 5 מזהיר ממוקשים: אינדוקציה היא לא שיטת ההוכחה היחידה והיא לא בהכרח השיטה המתאימה ביותר לכל משפט.

פרקים 6-8 מציגים את השימוש באינדוקציה במתמטיקה ברמת האוניברסיטה ובמדעי המחשב. פרק 6 דן באינדוקציה מעל נוסחאות של לוגיקה מתמטית ופרק 7 מדגים את השימוש באינדוקציה בהקשר של אוטומטים ושפות פורמליות. פרק 8 מדגים את השימוש באינדוקציה בהוכחת נכונות של תכניות מחשב.

פרקים 9-10 דנים בהיבטים פילוסופיים ותיאורטיים של אינדוקציה. פרק 9 מסביר איך המשמעות של המונח אינדוקציה במתמטיקה מתנגשת עם משמעותו במדע. פרק 10 מראה כיצד ניתן להוכיח את כלל ההיסק של אינדוקציה מתמטית, אם מניחים את עיקרון הסדר הטוב כאקסיומה. פרק 11 מסכם את הקורס.

נספח א' מציג תרגילים מאתגרים שאינם מחייבים ידע מתקדם במתמטיקה.

התשובות לכל התרגילים במסמך נמצאות בפרק ב'.

סקירה רחבה **מאוד** על אינדוקציה ניתן למצוא ב:

David S. Gunderson. *Handbook of Mathematical Induction: Theory and Applications*, Mathematical Association of America, 2010.

הבעת תודה אני מודה למיכל ארמוני וליוני עמיר על הערותיהן המועילות.

פרק 2

אינדוקציה מתמטית: אקסיומה נחוצה

מטרת פרק זה היא לנמק את הצורך באינדוקציה מתמטית, לתת הגדרה פורמלית עבורה ולהציג את אופיה כאקסיומה.

2.1 למה נחוצה אינדוקציה?

נקפוץ ישר להוכחת מספר משפטים:

משפט 1 כל מספר שלם אי־זוגי $n \geq 3$ הוא מספר ראשוני.

הוכחה המספרים $3, 5, 7$ הם מספרים ראשוניים. לכן, כל מספר אי־זוגי $n \geq 3$ הוא ראשוני. ∎

משפט 2 עבור כל מספר ראשוני p, $2^p - 1$ הוא מספר ראשוני.

הוכחה ברור שהמשפט נכון:

p	2	3	5	7
$2^p - 1$	3	7	31	127

∎

משפט 3 עבור כל מספר שלם $n \geq 0$, $2^{2^n} + 1$ הוא מספר ראשוני.
מספרים אלה נקראים מספרי *Fermat*.

הוכחה ברור שהמשפט נכון:

n	0	1	2	3	4
$2^{2^n} + 1$	3	5	17	257	65537

∎

$2^{11} - 1 = 2047 = 23 \times 89$ הוא לא מספר ראשוני כך שמשפט 1 אינו נכון. ניתן להראות ש־9, לכן גם משפט 2 לא נכון. המתמטיקאי Pierre de Fermat טען במאה ה־17 שמשפט 3 נכון, ועברו כמעט מאה שנים עד ש Leonhard Euler הראה שהמשפט לא נכון כי:

$$2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417\,.$$

מספרי Fermat גדלים מאוד ככל ש־n גדל. ידוע שהם אינם ראשוניים עבור $5 \leq n \leq 32$, אבל הפירוק לגורמים של חלק מהמספרים האלה עדיין לא ידוע.
מה לא נכון ב־"הוכחות" שלנו?
המשפטים האלה מביעים תכונות של **קבוצה אינסופית** של מספרים (לכל מספר אי־זוגי $n \geq 3$, לכל מספר ראשוני p, לכל מספר שלם $n \geq 0$) אבל בדקנו את התכונות רק עבור מספרים ספורים. אנו זקוקים לשיטת הוכחה שתאפשר לנו להוכיח שתכונה מתקיימת **לכל** האיברים בקבוצה אינסופית של מספרים, למרות שברור שההוכחה עצמה צריכה להיות סופית אם ברצוננו לסיים לכתוב אותה לפני קץ הימים.

2.2 מאיפה מגיעה אינדוקציה?

אינדוקציה מתמטית היא שיטה להוכחת תכונות של קבוצות אינסופיות.
לפני שננסח את כלל ההיסק של אינדוקציה נתחיל עם דוגמה:

$$1+2+3+4+5 \stackrel{?}{=} \frac{5 \cdot 6}{2}\,.$$

ברור ששני צדי המשוואה שווים ל־15. מה עם:

$$1+2+3+4+5+6+7+8+9+10 \stackrel{?}{=} \frac{10 \cdot 11}{2}\,.$$

במעט יותר מאמץ נמצא ששני הצדדים שווים ל־55.
כעת נניח שהתבקשת לחשב את הסכום:

$$1+2+3+\cdots+1528+1529\,.$$

סביר שאתה עצל מדי לחשב את הסכום אפילו עם מחשבון. מפתה להכליל את הדוגמאות הקודמות ולטעון ש:

$$1+2+3+\cdots+1528+1529 = \frac{1529 \cdot 1530}{2}\,.$$

רק כמה שניות דרושות כדי לחשב במחשבון את הצד הימני ולקבל את התוצאה 1169685. בכל זאת, כפי שראינו בסעיף 2.1, מאוד מסוכן לטעון לנכונות של טענה על קבוצה אינסופית של מספרים לאחר בדיקת מספרים ספורים בלבד.
אפילו אם היתה לנו הוכחה ש:

$$1+2+3+\cdots+1528+1529 = \frac{1529 \cdot 1530}{2}\,,$$

ההוכחה תקפה רק עבור אותה סדרה ולא עבור סדרות אחרות כגון:

$$1+2+3+\cdots+2997+2998\,.$$

אנו זקוקים להוכחה שעבור **כל** המספרים השלמים $n \geq 1$:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\,. \tag{2.1}$$

איך בכלל אפשר להוכיח שהמשוואה נכונה עבור כל אינסוף המספרים החיוביים? ברור שאין אפשרות להוכיח מספר אינסופי של משוואות, אבל נוכל לעשות משהו דומה. נניח שאליס טוענת שהיא יכולה להוכיח את המשוואה 2.1 **לכל מספר שלם חיובי שרירותי** גדול ככל שיהיה. אם הטענה של אליס נכונה, מתקבל על הדעת שהמשוואה 2.1 נכונה עבור **כל** $n \geq 1$. כמובן שלא מקובל המתמטיקה להסתמך על "מקבל על הדעת". עלינו למצוא ניסוח פורמלי של הטיעון.

2.3 אינדוקציה כשיטת הוכחה

נראה איך אליס יכולה להוכיח את משוואה 2.1 עבור כל מספר שלם שרירותי $n \geq 1$.

חברה בוב שואל אותה שאלה קלה: האם המשוואה נכונה עבור $n = 1$? אליס משיבה שלא צריך להיות גאון כדי להסכים לטענה כי:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}\,. \tag{2.2}$$

בוב מציג שאלה קשה יותר. האם המשוואה נכונה עבור $n = 2$? אליס יכולה להוכיח את הטענה בצורה ישירה:

$$\sum_{i=1}^{2} i = 1 + 2 = 3 = \frac{2(2+1)}{2} = 3\,,$$

אבל ככל מתמטיקאי טוב, היא עצלנית מאוד ומעדיפה להשתמש במשפטים שהיא הוכיחה כבר במקום להתחיל מאפס. אליס שמה לב ש:

$$\sum_{i=1}^{2} i = \sum_{i=1}^{1} i + 2\,,$$

ובנוסף ש:

$$\sum_{i=1}^{1} i$$

הוא הצד השמאלי של המשוואה 2.2. אליס מציבה במקום $\sum_{i=1}^{1} i$ את הצד הימני של משוואה 2.2 ומקבלת:

$$\sum_{i=1}^{2} i = \sum_{i=1}^{1} i + 2 = \frac{1(1+1)}{2} + 2 = \frac{2+4}{2} = \frac{2(2+1)}{2}\,.$$

אליס מסיקה שמשוואה 2.1 נכונה עבור $n = 2$.

מה עם $n = 3$? אליס משתמשת באותה שיטה כדי להוכיח את המשוואה עבור $n = 3$:

$$\sum_{i=1}^{3} i = \sum_{i=1}^{2} i + 3 = \frac{2(2+1)}{2} + 3 = \frac{6+6}{2} = \frac{3(3+1)}{2}\,.$$

תרגיל 1 עזור לאליס להוכיח את המשוואה 2.1 עבור $n = 4$.

האם אליס יכולה להוכיח את המשוואה 2.1 עבור $n = 1529$? בוודאי. כל שעליה לעשות הוא לכתוב 1528 הוכחות ולהשתמש בשיטה זו כדי להוכיח את הנוסחה עבור 1529. ברור שאליס עצלנית מדי. במקום זה היא טוענת שאין צורך ממש לכתוב את כל ההוכחות האלו, כי "ברור מאליו" שהשיטה עובדת עבור **כל** n. בניסוח פורמלי, אליס מציעה להשתמש בעיקרון של אינדוקציה מתמטית.

2.4 האקסיומה של אינדוקציה מתמטית

אקסיומה 1 (אינדוקציה מתמטית) תהי $P(n)$ תכונה (כגון משוואה, נוסחה או משפט), כאשר n מספר שלם חיובי. נניח שניתן:

- **טענת בסיס**: להוכיח ש־$P(1)$ נכונה.
- **צעד אינדוקטיבי**: עבור m שרירותי, להוכיח ש־$P(m+1)$ נכונה, בהנחה ש־$P(m)$ נכונה.

אזי $P(n)$ נכונה עבור כל $n \geq 1$.
ההנחה ש־$P(m)$ נכונה עבור m נקראת **הנחת האינדוקציה**.

נוכיח עכשו את המשוואה 2.1 תוך שימוש באינדוקציה מתמטית.

משפט 4 עבור $n \geq 1$:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\,.$$

הוכחה הוכחת טענת הבסיס פשוטה:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}\,.$$

הנחת האינדוקציה היא שהמשוואה נכונה עבור m:

$$\sum_{i=1}^{m} i = \frac{m(m+1)}{2}\,.$$

הצעד האינדוקטיבי הוא להוכיח את המשוואה עבור $m+1$:

$$\begin{aligned}
\sum_{i=1}^{m+1} i &= \sum_{i=1}^{m} i + (m+1) && (2.3)\\
&\overset{\bullet}{=} \frac{m(m+1)}{2} + (m+1) && (2.4)\\
&= \frac{m(m+1) + 2(m+1)}{2} && (2.5)\\
&= \frac{(m+1)(m+2)}{2}\,. && (2.6)
\end{aligned}$$

לפי האקסיומה של אינדוקציה מתמטית (אקסיומה 1):

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

נכונה עבור כל $n \geq 1$. ∎

נמקם כעת את השלבים של הצעד האינדוקטיבי. ב־(2.3) הסכום הוא של שני גורמים: הראשון הוא סכום המספרים מ־1 ל־m והשני הוא המספר $(m+1)$. ב (2.4), הסימן $\stackrel{\bullet}{=}$ מציין שאנו משתמשים **בהנחת האינדוקציה** כדי להציב $\frac{m(m+1)}{2}$ עבור $\sum_{i=1}^{m} i$. שאר ההוכחה (2.5-2.6) משתמש באלגברה פשוטה.

תרגיל 2 הוכח:

$$\sum_{i=1}^{n} i^2 = \frac{n}{6}(n+1)(2n+1).$$

כאשר משתמשים באינדוקציה מתמטית, כדאי תמיד לכתוב באופן מפורש את טענת הבסיס והנחת האינדוקציה.

השימוש בהנחת האינדוקציה יכול לבלבל, כי נראה שאנחנו מניחים את מה שאנחנו מנסים להוכיח. אבל ההוכחה היא לא מעגלית משום שאנחנו מניחים את התכונה עבור משהו קטן ומשתמשים בהנחה כדי להוכיח משהו גדול ממנו.

2.5 לבני דומינו נופלות

אינדוקציה מתמטית דומה לשורה של לבני דומינו הנופלות כולן כאשר מפילים את הלבנה הראשונה. הנפילה של הלבנה הראשונה מפילה את הלבנה השנייה, המפילה את הלבנה השלישית, וכו'. אינדוקציה מתמטית היא הטענה ש: (1) אם מפילים את הלבנה הראשונה, ו־(2) אם כל לבנה נופלת גורמת ללבנה השכנה ליפול, אזי כל הלבנים ייפלו, ללא תלות בכמות הלבנים. אם קשה לכם להאמין, חפשו ביוטיוב קטעי ווידיאו המציגים עשרות ואפילו מאות אלפי לבנים נופלות כאשר מפילים את הראשונה! מומלץ במיוחד היצירות של תלמידה בתיכון Lily Hevesh (`http://www.hevesh5.com/`).

2.6 אינדוקציה היא אקסיומה

היסק לוגי במתמטיקה מבוסס על המושג **מערכת אקסיומטית**: מתחילים עם מושגים בסיסיים שאינם מוגדרים. ניתנת רשימת אקסיומות וכללי ההיסק מפרטים איך לבנות הוכחה. המערכת האקסיומתית של Euclid לגיאומטריה במישור מוכרת היטב. היא כוללת מושגים בסיסיים כגון נקודה וקו, ואקסיומות כגון:

- בין שתי נקודות ניתן למתוח קו אחד.

- בהינתן קו ונקודה שלא נמצאת על הקו, קיים קו אחד שעובר דרך הנקודה והוא מקביל לקו הנתון.

כללי היסק לוגיים משמשים להוכחת משפטים. כלל ההיסק השכיח שביותר הוא *modus ponens* *(MP)*:

- אם הטענה P גוררת את הטענה Q.
- אם הטענה P נכונה.
- אזי הטענה Q נכונה.

בהוכחה שלהלן MP מצדיק את ההיסק מהטענות בשורות 2 ו־3 למסקנה בשורה 4:

1. לכל a, b, c, אם $a > b$ ו־$c > 0$ אזי $ac > bc$
2. אם $3 > 9$ ו־$5 > 0$ אזי $9 \cdot 5 > 3 \cdot 5$
3. $9 > 3$ ו־$5 > 0$
4. $9 \cdot 5 > 3 \cdot 5$
5. $45 > 15$

במסגרת החקירה והלמידה של לוגיקה מתמטית, כללי ההיסק מוצגים בצורה פורמלית. בעיסוק היומיומי במתמטיקה, משתמשים בכללים בצורה לא פורמלית, כי הם מוכרים ומקובלים. אקסיומות אמורות להיות טענות שנכונותן ברורה, אבל האמיתות של האקסיומות **אינה** רלוונטית לתקפות של הוכחה! חשוב רק שהמערכת הדדוקטיבית תהיה **נאותה**, שמשמעותה היא:

אם האקסיומות נכונות, **אז** המשפטים המוכחים מהאקסיומות גם הם נכונים.

ההוכחה הבאה היא נאותה למרות שהמסקנה אינה נכונה, כי הטענה בשורה 3 אינה נכונה:

1. לכל a, b, c, אם $a > b$ ו־$c > 0$ אזי $ac > bc$
2. אם $3 > 9$ ו־$-5 > 0$ אזי $9 \cdot -5 > 3 \cdot 5$
3. $3 > 9$ ו־$-5 > 0$
4. $9 \cdot -5 > 3 \cdot -5$
5. $-45 > -15$

במאה ה־19 מתמטיקאים התחילו לחקור מה יקרה אם במערכת האקסיומות של Euclid יחליפו את אקסיומת הקווים המקבילים באחת מהאקסיומות הבאות:

- בהינתן קו ונקודה שלא נמצאת על הקו, לא קיים קו שעובר דרך הנקודה והוא מקביל לקו הנתון.

- בהינתן קו ונקודה שלא נמצאת על הקו, קיימים אינסוף קווים שעוברים דרך הנקודה והוא מקביל לקו הנתון.

החלפת האקסיומה יצרה גיאומטריות אחרות, השונות מגיאומטריית המישור המוכרת. עם זאת, התיאוריות הגיאומטריות החדשות הן **עקביות**, שמשמעותה שלא תיווצר סתירה בפיתוח התיאוריות. הגיאומטריות החדשות התגלו כשימושיות, למשל, בתיאוריית היחסות של איינשטיין.

מערכת אקסיומטית עובר המספרים הטבעים לא פותח עד תחילת המאה ה־20. היא כוללת אקסיומות ברורות מאליהן כגון:

- $x + 0 = x$.
- $x_1 = x_2$ ו־$x_1 = x_3$ גוררות $x_2 = x_3$.

אינדוקציה מתמטית היא כלל היסק במערכות, לכן אין כלל שאלה האם אפשר **להוכיח** שהיא נכונה. עליך לקבל אותה כמו שאתה מקבל כל אנקסיומה אחרת, כמו $x + 0 = x$. כמובן שאתה רשאי לדחות את האקסיומה של אינדוקציה מתמטית, אבל אז עליך לדחות כמעט את כל המתמטיקה המודרנית.

אפשר להחליף את אקסיומת האינדוקציה באקסיומה אחרת הנקראת **עיקרון הסדר הטוב**. שתי האקסיומות שקולות במובן שכל אחת נובעת מהשנייה. עיקרון הסדר הטוב הוא יותר אינטואיטיבי מאינדוקציה, אך קל יותר להשתמש באינדוקציה. פרק 10 מביא את עיקרון הסדר הטוב והוכחה ששתי האקסיומות שקולות.

כמובן שאינדוקציה אינה השיטה היחידה להוכחת משפטים במתמטיקה. אולם, כמעט תמיד משתמשים באינדוקציה להוכחת משפטים על תכונות של קבוצות אינסופיות כגון כל המספרים השלמים או כל הפוליגונים. אינדוקציה מתאימה כאשר מבנה בנוי ממבנים קטנים יותר עד לרמה שהוכחה עבור המבנה הקטן ביותר היא ממש פשוטה. נתחיל עם משפטים על המספרים החיוביים או לא־שליליים, כאשר המספר הקטן ביותר הוא 1 או 0, והמספרים הגדולים יותר בנויים, למשל, מחיבור של מספרים קטנים. בהמשך נכליל את שיטת האינדוקציה למבנים אחרים.

פרק 3

אינדוקציה מעל המספרים השלמים

הפרק זה מציג דוגמאות לתכונות של מספרים שלמים הניתנות להוכחה באמצעות אינדוקציה מתמטית.

3.1 לא רק שוויונות

התכונה הראשונה שהוכחנו באמצעות אינדוקציה היתה השוויון:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} .$$

ניתן גם להוכיח אי־שוויונות באמצעות אינדוקציה:

משפט 5 עבור כל $n \geq 1$, $2^n \geq n+1$.

הוכחה טענת הבסיס פשוטה מאוד להוכחה: $2^1 = 2 \geq 1+1 = 2$. הנחת האינדוקציה היא $2^n \geq n+1$.[1] הצעד האינדוקטיבי הוא להוכיח ש־$2^{n+1} \geq (n+1)+1$:

$$2^{n+1} = 2^n \cdot 2 \overset{\bullet}{\geq} (n+1) \cdot 2 = 2n+2 \geq n+2 = (n+1)+1 .$$

ההנחה ש־ n חיובי מצדיקה את המסקנה ש־$2n+2 \geq n+2$. על פי אקסיומת האינדוקציה, האי־שיוון $2^n \geq n+1$ מתקיים לכל $n \geq 1$. ∎

תרגיל 3 לכל $n \geq 1$, $2n! \geq 2^n$.

3.2 לא רק משוואות

משפט 6 עבור כל $n \geq 1$, $n(n+1)$ מתחלק ב־2.

[1] בהצגה של האקסיומה בסעיף 2.4, השתמשנו בשמות שונים עבור המשתנה בהנחת האינדוקציה m והמשתנה בצעד האינדוקטיבי n. מכאן והלאה, נשתמש בשם n גם בהנחה וגם בצעד. זה לא אמור לבלבל.

הוכחה טענת הבסיס פשוטה מאוד להוכחה: $1 \cdot (1+1) = 2$ מתחלק ב־2. הנחת האינדוקציה היא ש־$n(n+1)$ מתחלק ב־2, והצעד האינדוקטיבי הוא להוכיח ש־

$$(n+1)((n+1)+1) = (n+1)(n+2)$$

מתחלק ב־2. לפי ההנחה, $n(n+1)$ מתחלק ב־2, כך שיש שתי אפשרויות:
אפשרות 1: $n+1$ מתחלק ב־2. אם כן, ברור ש־$(n+1)(n+2)$ גם מתחלק ב־2.
אפשרות 2: n מתחלק ב־2. אם כך, קיים $k \geq 1$ כך ש־$n = 2k$. אבל:

$$n+2 = 2k+2 = 2(k+1)\,,$$

ולכן $n+2$ וגם $(n+1)(n+2)$ מתחלקים ב־2. ∎

תרגיל 4 עבור כל $n \geq 1$, $n(n+1)(n+2)$ מתחלק ב־3.

תרגיל 5 עבור כל $n \geq 1$, $n^3 - n$ מתחלק ב־6.

תרגיל 6 עיקרון שובך היונים: אי־אפשר להניח $n+1$ יונים ב־n תאים כך שיש לכל היותר יונה אחת בכל תא.[2]

3.3 לא רק טענת בסיס מ־1

משפט 7 עבור כל $n \geq 1$, $n^2 \geq 2n+1$.

הוכחה טענת הבסיס קלה להוכחה:

$$1^2 = 1 \overset{?}{\geq} 2 \cdot 1 + 1 = 3\,.$$

משהו לא בסדר! נבדוק אם המשפט נכון עבור $n = 2$:

$$2^2 = 4 \overset{?}{\geq} 2 \cdot 2 + 1 = 5\,.$$

עדיין לא נכון. נבדוק $n = 3$:

$$3^2 = 9 \overset{?}{\geq} 2 \cdot 3 + 1 = 7\,.$$

נראה בסדר. האם אפשר להוכיח את צעד האינדוקציה? הנחת האינדוקציה היא $n^2 \geq 2n+1$. לכן, עבור כל $n+1$:

$$(n+1)^2 = n^2 + 2n + 1 \overset{\bullet}{\geq} (2n+1) + (2n+1) = 2(n+1) + 2n \geq 2(n+1) + 1\,,$$

כי n חיובי. מכאן שלכל $n \geq 3$, $n^2 \geq 2n+1$. ∎
המשפט כפי שניסחנו לא נכון, אבל אם נשנה את המשפט כך שלא נטען שהוא נכון עבור $1, 2$, המשפט נכון וניתן להוכיח אותו.
נניח שיש לנו שורה של לבני דומינו ונסלק את שני הראשונים: עדיין שאר הלבנים תיפולנה כאשר נפיל את הלבנה השלישית. העיקרון של אינדוקציה מתמטית הוא ללא שינוי: טענת הבסיס יכולה לטעון עבור מספר כלשהו והתכונה נכונה עבור כל מספר גדול או שווה לו.

תרגיל 7 עבור איזה מספרים מתקיים $2^n \geq n^2$? הוכח באינדוקציה.

[2] זה אולי נשמע כבדיחה אבל עיקרון שובך היונים הוא שימושי מאוד בהוכחות שונות במתמטיקה.

3.4 לא רק צעד אינדוקטיבי של $n+1$

משפט 8 הסכום של n המספרים האי־זוגיים הראשונים הוא n^2:

$$\overbrace{1+3+\cdots+(2n-1)}^{n} = n^2 .$$

הוכחה ההוכחה של טענת הבסיס פשוטה: $2\cdot 1-1=1=1^2$. הנחת האינדוקציה היא:

$$\overbrace{1+3+\cdots+(2n-1)}^{n} = n^2 .$$

הצעד האינדוקטיבי הוא:

$$\begin{aligned}\overbrace{1+3+\cdots+(2n-1)+(2n+1)}^{n+1} &= \overbrace{1+3+\cdots+(2n-1)}^{n}+(2n+1)\\ &\overset{\bullet}{=} n^2+(2n+1)\\ &= (n+1)^2 .\end{aligned}$$

∎

כל צעד באינדוקציה מוסיף 2 לאיבר בסכום מ־$2n-1$ ל־$2n+1$, שלא כמו בדוגמאות הקודמות בהן הצעד היה 1. אולם, עם סימון טוב יותר, ניתן לכתוב את הצעד האינדוקטיבי כך שהצעד הוא מ־n ל־$n+1$.

משפט 9 הסכום של n המספרים האי־זוגיים הוא n^2:

$$\sum_{i=1}^{n}(2i-1) = n^2 .$$

הוכחה הוכחת טענת הבסיס פשוטה ביותר: $2\cdot 1-1=1=1^2$. הנחת האינדוקציה היא $\sum_{i=1}^{n}(2i-1)=n^2$ והצעד האינדוקטיבי הוא:

$$\sum_{i=1}^{n+1}(2i-1) \overset{\bullet}{=} n^2+(2(n+1)-1) = n^2+2n+1 = (n+1)^2 .$$

∎

תרגיל 8 הסכום של n המספרים הזוגיים הוא $n(n+1)$.

3.5 לא רק טענת בסיס אחת

משפט 10 לכל $n\geq 1$, כל מספר עם $3n$ ספרות זהות מתחלק ב־3.

הוכחה טענת הבסיס: כל מספר עם 3 ספרות זהות מתחלק ב־3. קיימות עשר (!) טענות בסיס, ואין לנו ברירה אלא להוכיח כל אחת בנפרד:

$$\begin{array}{lllll} 000=3\cdot 0 & 111=3\cdot 37 & 222=3\cdot 74 & 333=3\cdot 111 & 444=3\cdot 148\\ 555=3\cdot 185 & 666=3\cdot 222 & 777=3\cdot 259 & 888=3\cdot 296 & 999=3\cdot 333. \end{array}$$

הצעד האינדוקטיבי פשוט יחסית. לפי הנחת האינדוקציה, מספר עם $3n$ ספרות זהות k מתחלק ב־3. לכן:

$$\overbrace{kkk}^{n+1} = \overbrace{kkk}^{n} \cdot 1000 + kkk \stackrel{\bullet}{=} 3i \cdot 1000 + kkk.$$

ברור שהגורם הראשון מתחלק ב־3 וניתן להראות שהגורם השני מתחלק ב־3 לפי החישובים של טענות הבסיס. ∎

משפט זה הוא מקרה קיצוני של עשר טענות בסיס, אבל לא נדיר להיתקל בהוכחות המחייבות יותר מטענת בסיס אחת.

סטודנט העיר לי שניתן להוכיח את כל טענות הבסיס ביחד. יהי n מספר תלת־ספרתי עם ספרות זהות. אז:

$$\begin{aligned} n &= 100k + 10k + k \\ &= (99+1)k + (9+1)k + k \\ &= (99+9)k + 3k\,, \end{aligned}$$

וברור ש־n מתחלק ב־3.

תרגיל 9 לכל $n \geq 1$, כל מספר עם 3^n ספרות זהות מתחלק ב־3^n.

רמז לכל $k \geq 1$, מה השארית של 10^k לאחר חלוקה ב־3?

3.6 לא רק הנחת אינדוקציה אחת

משפט 11 יהי $n > 1$. אזי ניתן לפרק את n למכפלה של מספרים ראשוניים.

הוכחה טענת הבסיס היא עבור מספר ראשוני n ואין מה להוכיח. אם n אינו ראשוני, $n = n_1 n_2$ עבור $2 < n_1, n_2 < n$. הנחת האינדוקציה היא ש־**כל** מספר $1 < m < n$ ניתן לפרק למכפלה של מספרים ראשוניים. הצעד האינדוקטיבי: לפי הנחת האינדוקציה, $n_1 = p'_1 \cdots p'_{k_1}$ ו־ $n_2 = p''_1 \cdots p''_{k_2}$ ולכן:

$$n = n_1 n_2 = p'_1 \cdots p'_{k_1} p''_1 \cdots p''_{k_2},$$

שהוא פירוק של n למכפלה של מספרים ראשוניים. ∎

אינדוקציה זו שונה ממקרים קודמים כי הצעד לא מוכיח $P(n+1)$ מ־$P(n)$. כאן מוכיחים את $P(n)$ מ־$P(n_1)$ ו־$P(n_2)$, כאשר n_1, n_2 שניהם קטנים מ־n ואפילו קטנים מאוד. למשל, $n = 945$ מתפרק לשני גורמים 21 ו־45. לפי הנחת האינדוקציה, m מתפרק לגורמים ראשוניים עבור כל $m < 945$, כאן, $21 = 3 \cdot 7$ ו־$45 = 3 \cdot 3 \cdot 5$, כך ש־$945 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7$.

אקסיומה 2 (אינדוקציה מתמטית שלמה) תהי $P(n)$ תכונה כאשר n הוא מספר שלם. נניח שניתן:

- **טענת בסיס**: להוכיח ש־$P(n_0)$ נכונה עבור מספר כלשהו n_0.[3]
- **צעד אינדוקטיבי**: עבור מספר שרירותי m, להוכיח ש־$P(m+1)$ נכונה בהנחה ש־$P(k)$ נכונה **לכל** $n_0 \leq k \leq m$.

אזי $P(n)$ נכונה לכל $n \geq n_0$.

אינדוקציה שלמה דומה למקרה שבו לבנת דומינו נופלת רק אם היא מקבלת מכה מיותר מאשר לבנה אחת.
אינדוקציה שלמה היא לא ממש הרחבה של המושג אינדוקציה. באינדוקציה מתמטית רגילה, כדי להוכיח $P(n+1)$ השתמשנו בעובדה שניתן להוכיח $P(n)$ וכדי להוכיח $P(n)$ השתמשנו בעובדה שניתן להוכיח $P(n-1)$, ..., עד $P(1)$. אם כן, למה לא להניח בצורה מפורשת את כל הטענות $P(1), \ldots, P(n)$? למעשה, ניתן לקבוע אינדוקציה שלמה כאקסיומה כי שתי הצורות ניתנות להוכחה אחת מהשנייה.

תרגיל 10 יהי $a_1 = 5, a_2 = 7, a_n = 3a_{n-1} - 2a_{n-2}$. אזי $a_n = 3 + 2^n$.

3.7 אינדוקציה לא־מפורשת

משפט 12 יהי $n > 1$. אזי ניתן לפרק את n כמכפלה של מספרים ראשוניים בדרך אחת בלבד. (שינוי סדר המספרים לא נחשב כפירוק שונה.)

במשפט 11 הראינו שקיים פירוק של כל מספר שלם לגורמים ראשוניים. בהוכחה שקיים פירוק יחיד, נגלה שלושה מקרים נוספים של שימוש באינדוקציה, לפעמים בצורה לא מפורשת.
ההוכחה משתמשת בשתי למות. נשאיר את ההוכחות שלהן כתרגילים.

למה 13 (הלמה של Euclid) יהיו n_1, n_2 מספרים שלמים ו־p מספר ראשוני. אם $p \mid n_1 n_2$, אזי $p \mid n_1$ או $p \mid n_2$. משמעות הסימן $\mid$ היא "מחלק".

למה 14 (הזהות של Bezout) יהי n_1, n_2 מספרים שלמים שלפחות אחד מהם לא אפס. אזי קיימים מספרים שלמים a, b כך ש־$\gcd(n_1, n_2) = an_1 + bn_2$. $\gcd(a, b)$ הוא המחלק המשותף הגודל ביותר של a ו־b.

משתמשים בזהות של Bezout כדי להוכיח את הלמה של Euclid. מוכיחים את הזהות של Bezout על ידי הגדרת קבוצה של מספרים חיוביים וטיעון שלקבוצה מוכרח להיות איבר קטן ביותר. מעט ספרי לימוד יטרחו להוכיח את הטיעון שהוא כל כך ברור באמצעות עיקרון הסדר הטוב השקול לאינדוקציה (פרק 10). קיים כאן שימוש באינדוקציה אבל הוא לא מפורש.
הלמה של Euclid טוענת טענה על מכפלה של שני מספרים, אבל אנו זקוקים לטענה על מכפלה כללית.

[3] אנו כבר לא מגבילים את עצמנו לטענת בסיס עבור $n = 1$.

למה 15 (הלמה הכללית של Euclid) יהי $n_1, \ldots, n_k$ מספרים שלמים ו־p מספר ראשוני. אם $p \mid n_1 \cdots n_k$, אזי $p \mid n_i$ עבור $1 \leq i \leq k$.

את הלמה ניתן להוכיח באינדוקציה.

קיים שימוש שלישי של אינדוקציה בהוכחה אבל הוא מוסתר עמוק יותר. ההוכחה שקיים פירוק יחיד מתחילה כך:

ננית שקיימים שני פירוקים למספרים ראשוניים:

$$n = p_1 \cdots p_k = q_1 \cdots q_m \,.$$

ברור ש־$p_1 \mid p_1 \cdots p_k$ ולכן גם $p_1 \mid q_1 \cdots q_m$. לפי הלמה הכללית של Euclid, $p_1 \mid q_i$, עבור $1 \leq i \leq m$, ו־**ללא הגבלת הכלליות**, $q_1 \mid p_1$. מה המשמעות של ביטוי זה השגור בהוכחות מתמטיות? המשמעות היא שלכל i, ניתן להחליף את המיקום במכפלה של q_1 ו־q_i:

$$q_1 \cdots q_i \cdots q_m = q_i \cdots q_1 \cdots q_m.$$

זה ברור לגמרי, אבל זהו טיעון שחייבים להוכיח אותו וההוכחה היא על ידי אינדוקציה על i תוך שימוש בכללי הקומטטיביות והאסוציאטיביות של מספרים שלמים.

הוכחת משפט הפירוק למכפלה של מספרים ראשוניים, **המשפט היסודי של האריתמטיקה**, מדגימה שאינדוקציה נמצאת בכל מקום, גם אם בצורה לא מפורשת.

תרגיל 11 (מאתגר) הוכח את הזהות של *Bezout*.

רמז תהי $S = \{x = an_1 + bn_2 : x > 0\}$. כדי לפשט את ההוכחה, נניח ש־$n_1, n_2 > 0$, כך ש־S היא קבוצה לא־ריקה המכילה $1 \cdot n_1 + 1 \cdot n_2$. לפי עיקרון הסדר הטוב (סעיף 10), קיים איבר קטן ביותר $d \in S$. השתמש באלגוריתם לחילוק מספרים שלמים והעובדה ש־d הוא האיבר הקטן ביותר ב־S כדי להראות ש־$d \mid n_1$, ש־$d \mid n_2$, ו־$d = \gcd(n_1, n_2)$.

תרגיל 12 הוכח את הלמה של *Euclid*.

רמז אם $p \mid n_1 n_2$ ו־p לא מחלק את n_1, אז $\gcd(p, n_1) = 1$. עכשיו ניתן להשתמש בזהות של Bezout.

הוכחה אנידוקטיבית של המספט היסודי של האריתמטיקה

ההוכחה שנתנו למספט היסודי של האריתמטיקה מופיעה ברוב ספרי הלימוד, אבל היא מסובכת שלא לצורך ומשתמשת בזהות של Bezout המוכחת בדרך כלל תוך שימוש בעיקרון הסדר הטוב. הוכחה אינדוקטיבית ישרה המיוחסת ל־Ernst Zermelo הרבה יותר פשוטה.[4] אין שניוי בהוכחת הקיום של פירוק למספרים רשאוניים ונשאר רק להוכיח שיש רק פירוק אחד.

טענת בסיס: ל־$n = 2$ פירוק יחיד למספרים ראשוניים, $n = 2$.

הנחת האינדוקציה: לכל $k < n$ קיים פירוק יחיד למספרים ראשוניים.

[4] https://planetmath.org/FundamentalTheoremOfArithmetic.

צעד האינדוקציה: אם n מספר ראשוני, ברור שקיים פירוק יחיד. נניח ש־n אינו ראשוני $n = pa$, כאשר p הוא **המספר הראשוני הקטן ביותר** המחלק את n. n אינו ראשוני, לכן $1 < a < n$. לפי הנחת האידוקציה, ל־a פירוק יחיד למספרים ראשוניים, לכן $n = pa$ הוא הפירוק היחיד למספרים ראשוניים **המכיל את** p. (זכור שסדר המספרים הראשוניים לא חשוב.) נניח שקיים פירוק שונה למספרים ראשוניים **שאינו מכיל את** p. n אינו ראשוני ולכן $n = qb$, כאשר $q \neq p$ הוא המספר הראשוני הקטן ביותר בפירוק זה. למעשה, $p < q$ כי הנחנו ש־p הוא המספר ראשוני הקטן ביות המחלק את n. כעת:

$$n - pb = qb - pb = b(q - p)\,.$$

אבל $p \mid (n - pb)$ ולכן $p \mid b(q - p)$. n אינו ראשוני, ולכן $1 < b < n$. לפי הנחת האינדוקציה, ל־b פירוק יחיד למספרים ראשוניים, ולפי ההנחה הפירוק של n ולכן של b לא מכיל את p. (אנחנו לא משתמשים בלמה של אוקלידיס, כי אנחנו רק שואלים אם p הוא אחד המספרים בפירוק למספרים ראשוניים.) לכן, $p \mid (q - p)$ כך ש־$p \mid q$. גם p וגם q הם מספרים ראשוניים, ולכן $p = q$, סתירה להנחה ש־$q \neq p$. ∎

3.8 הגדרה רקורסיבית

רקורסיה היא מושג מרכזי במתמטיקה ומדעי המחשב הקשור קשר הדוק עם אינדוקציה. בהוכחות באמצעות אינדוקציה, אנו מוכיחים טענת בסיס על מבנה קטן ומרחיבים את ההוכחה למבנים גדולים יותר. ברקורסיה, אנו מגדירים מבנה כמורכב ממבנים קטנים יותר עד שמגיעים למבנה בסיס הקטן ביותר.

דוגמה להגדרה רקוסיבית

הנה דוגמה פשוטה של רקורסיה:

$$\begin{aligned} a_1 &= 2 \\ a_{n+1} &= a_n + 2, \quad \text{for } n \geq 1\,. \end{aligned}$$

מה הערך של a_5? ובכן:

$$\begin{aligned} a_5 &= a_4 + 2 \\ &= a_3 + 2 + 2 \\ &= a_2 + 2 + 2 + 2 \\ &= a_1 + 2 + 2 + 2 + 2 \\ &= 2 + 2 + 2 + 2 + 2 \\ &= 10\,. \end{aligned}$$

בגלל הקשר בין רקורסיה לאינדוקציה, לא מפתיע שתכונות של מבנים המוגדרים על ידי רקורסיה ניתנות להוכחה באמצעות אינדוקציה. המשפט הבא פשוט מאוד אבל מדגים את השיטה.

משפט 16 לכל $n \geq 1$, $a_n = 2n$.

הוכחה הוכחת טענת הבסיס פשוטה מאוד: $a_1 = 2 = 2 \cdot 1$. הנחת האינדוקציה היא $a_n = 2n$. הצעד האינדוקטיבי הוא: $a_{n+1} = a_n + 2 \overset{\bullet}{=} 2n + 2 = 2(n+1)$. ∎

תרגיל 13 לכל $n \geq 1$, $\sum_{i=1}^{n} a_i = n(n+1)$.

מספרי פיבונצ'י

מספרי פיבונצ'י מהווים דוגמה קלסית להגדרה רקורסיבית:

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_n &= f_{n-1} + f_{n-2}, \quad n \geq 3 \end{aligned}$$ עבור .

שנים עשר מספרי פיבונצ'י הראשונים הם:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144\,.$$

משפט 17 כל מספר פיבונצ'י רביעי מתחלק ב־3.

דוגמאות $f_4 = 3 = 3 \cdot 1,\ f_8 = 21 = 3 \cdot 7,\ f_{12} = 144 = 3 \cdot 48$.
הוכחה טענת הבסיס מתקבלת באופן מיידי כי $f_4 = 3$ מתחלק ב־3. הנחת האינדוקציה היא ש־f_{4n} מתחלק ב־3. הצעד האינדוקטיבי הוא:

$$\begin{aligned} f_{4(n+1)} &= f_{4n+4} \\ &= f_{4n+3} + f_{4n+2} \\ &= (f_{4n+2} + f_{4n+1}) + f_{4n+2} \\ &= ((f_{4n+1} + f_{4n}) + f_{4n+1}) + f_{4n+2} \\ &= ((f_{4n+1} + f_{4n}) + f_{4n+1}) + (f_{4n+1} + f_{4n}) \\ &= 3f_{4n+1} + 2f_{4n}\,. \end{aligned}$$

ברור ש־$3f_{4n+1}$ מתחלק ב־3 ולפי הנחת האינדוקציה f_{4n} מתחלק ב־3, ולכן, $f_{4(n+1)}$ מתחלק ב־3. ∎

תרגיל 14 כל מספר פיבונצ'י חמישי מתחלק ב־5.

תרגיל 15 $f_n < (\frac{7}{4})^n$.

פרק 4

לא רק חשבון

כמעט תמיד מלמדים אינדוקציה בצורה של אינדוקציה מתמטית מעל למספרים השלמים החיוביים. אולם, השיטה מתאימה בכל מצב בו מבנים גדולים בנויים ממבנים קטנים יותר. **אינדוקציה מעל מבנה** נמצאת בשימוש נרחב במדעי המחשב, שם מבני נתונים מוגדרים בצורה רקורסיבית. בפרק זה נציג דוגמאות של השימוש באינדוקציה במבנים מתמטיים שהם לא מספרים שלמים: טריגונומטריה, פוליגונים, גרפים ועצים. נתחיל בדוגמה של אינדוקציה מעל מבנה.

הגדרה 18 ביטוי (חשבוני) מורכב ממשתנים וקבועים ביחד עם הפעולות הבוגות:

אם E_1, E_2 הם ביטויים, אזי גם $(E_1 + E_2), (E_1 - E_2), (E_1 \times E_2), (E_1/E_2)$ הם ביטויים.[1]

תרגיל 16
(א) מספר הסוגרים השמאליים בביטוי שווה למספר הסוגרים הימניים.
(ב) בכל מקום בביטוי, מספר הסוגרים השמאליים משמאל לנקודה גדול או שווה למספר הסוגרים הימניים משמאלה.

דוגמה בביטוי $(x+(y-23))$ קיימים שני סוגרים שמאליים ושני סוגרים ימניים. במקום המסומן על ידי | בביטוי $(x + (y | - 23))$, קיימים שני סוגרים שמאליים משמאל לסימן | ואפס סוגרים ימניים.

4.1 טריגונומטריה

משפט 19 לכל $n \geq 1$, $\cos n\pi = (-1)^n$.

הוכחה טענת הבסיס פשוטה להוכחה: $\cos 1\pi = \cos \pi = -1 = (-1)^1$. הנחת האינדוקציה היא $\cos n\pi = (-1)^n$. הצעד האינדוקטיבי הוא:

$$\cos(n+1)\pi = \cos(n\pi + \pi) = \cos n\pi \cdot \cos \pi - \sin n\pi \cdot \sin \pi .$$

[1] חוקים של קדימויות יכולים להקטין את מספר הסוגריים, כך שהמשמעות של $a \times b + 2$ היא $((a \times b) + c)$ ולא $(a \times (b + c))$. בדיון כאן נתעלם מקדימויות.

מ־$\sin\pi = 0$ ו־$\cos\pi = -1$ מתקבל:

$$\cos(n+1)\pi = \cos n\pi \cdot -1 \overset{\bullet}{=} (-1)^n \cdot -1 = (-1)^{n+1}\,.$$

∎

כאשר הוכחנו משפטים באמצעות אינדוקציה מתמטית מעל למספרים השלמים, ביצעו חישובים חשבוניים ואלגבריים ללא הנמקה. כאן, השתמשנו ללא הנמקה מפורשת בנוסחה טריגונומטית עבור $\cos(\alpha+\beta)$.

תרגיל 17 לכל $n \geq 1$:

$$\cos\theta \cdot \cos 2\theta \cdot \cos 4\theta \cdot \cdots \cdot \cos 2^{n-1}\theta = \frac{\sin 2^n\theta}{2^n \sin\theta}\,.$$

רמז השתמש בנוסחה ל־$\sin 2\theta$.

תרגיל 18 לכל $n \geq 1$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$.

4.2 גיאומטריה

במבט ראשון, קשה לראות איך אפשר להשתמש באינדוקציה בהוכחת משפטים בגיאומטריה. אולם, משפטים רבים מנוסחים בצורה: "לכל פוליגון עם n צלעות, ...", ואינדוקציה מתאימה מאוד במקרים אלה.

משפט 20 לכל פוליגון קמור עם n צלעות, מספר המשולשים הנוצרים מהאלכסונים **שאינם נחתכים** הוא $n-2$.

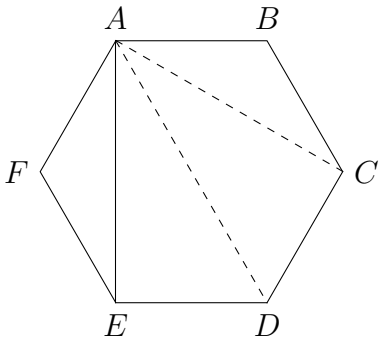
הוכחה במשולש אין אלכסונים, $n=3$ ויש משולש אחד: $3-2=1$. טענת בסיס טובה יותר היא עבור מרובע $n=4$. קיים אלכסון אחד שאינו חותך אלכסון אחר והוא מייצר $4-2=2$ משולשים.
נקח פוליגון עם $n+1$ צלעות ונצייר אלכסון אחד בין שני צמתים השכנים לצומת אחר. האלכסון ביחד עם הצלעות האחרים מהווים פוליגון עם n צלעות. לפי הנחת האינדוקציה, האלכסונים שאינם חותכים אחד את השני מייצרים $n-2$ משולשים. עם המשולש החדש, קיימים $2-(n+1)=(n-2)+1$ משולשים. ∎
דוגמה תרשים 4.1 מראה משושה $n=6$. צייר את הקו AE המחלק את המשושה למשולש AEF ולמחומש $ABCDE$. צייר את האלכסונים שאינם נחתכים AC ו־AD. לפי הנחת האינדוקציה, מספר המשולשים במחומש הוא $5-2=3$: ABC, ACD, ADE. ביחד עם המשולש AEF, קיימים $6-2=4$ משולשים.

תרגיל 19 עבור פוליגון קמור עם n צלעות, מספר האלכסונים (כולל אלה שנחתכים) הוא $\frac{1}{2}n(n-3)$.

תרגיל 20 עבור פוליגון קמור עם n צלעות, סכום הזוויות הפנימיות הוא $180(n-2)^\circ$.

תרגיל 21 נתון קו באורך 1 ומספר שלם $n \geq 1$, בנה קו באורך $\sqrt{n}$.

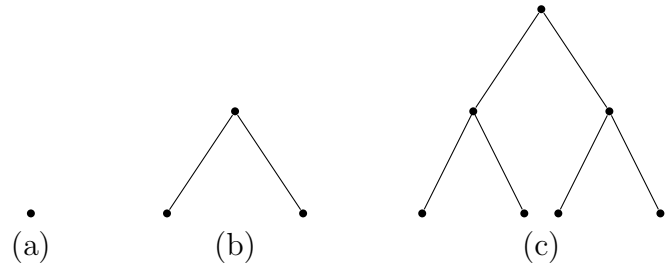
רמז משפט פיתגורס.



איור 4.1: אלכסונים שלא נחתכים

4.3 עצים

עץ בינרי הוא גרף עם צמתים וקשתות, כאשר יש צומת אחד הנקרא השורש ולכל צומת יש אפס, אחת או שתי קשתות היוצאות ממנו אל צמתים אחרים הנקראים בנים. אין מעגלים בעץ. צומת ללא בנים נקרא עלה וצומת שהוא לא עלה נקרא צומת פנימי. גובה עץ h הוא אורך המסלול הארוך ביותר בין השורש לבין עלה. עץ בינרי שכל העלים בו הם באותו גובה ושלכל הצמתים הפנימיים בו יש שני בנים נקרא **עץ בינרי שלם** (תרשים 4.2).



איור 4.2: עצים בינריים שלמים בגובה 0, 1, 2

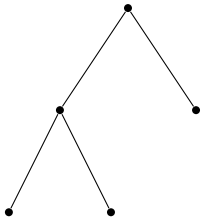
משפט 21 יהי n_h מספר הצמתים בעץ בינרי שלם בגובה h. אזי $n_h = 2^{h+1} - 1$.

דוגמה בתרשים 4.2: $n_0 = 2^1 - 1 = 1$ (a), $n_1 = 2^2 - 1 = 3$ (b), $n_2 = 2^3 - 1 = 7$ (c).

הוכחה הוכחת טענת הבסיס פשוטה: עלה הוא עץ בגובה אפס ו־$1 = 2^{0+1} - 1 = 1$. הנחת האינדוקציה היא שמספר הצמתים בתת־עץ השמאלי n_l ומספר הצמתים בתת־עץ הימני n_r, שניהם בגובה h, ניתנים על יד הנוסחה $n_l = n_r = 2^{h+1} - 1$. כדי להוכיח את הצעד האינדוקטיבי, נשים לב שעץ בגובה $h+1$ בנוי משני תת־עצים בגובה h, ביחד עם צומת אחד נוסף שהוא השורש החדש. לכן:

$$n_{h+1} = n_l + n_r + 1 \overset{\bullet}{=} (2^{h+1} - 1) + (2^{h+1} - 1) + 1 = 2 \cdot 2^{h+1} - 2 + 1 = 2^{(h+1)+1} - 1 \,.$$

∎



איור 4.3: עץ בינרי לא שלם בגובה 2 עם 5 צמתים

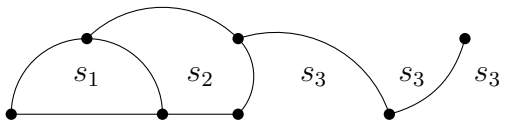
למרות שהאינדוקציה היא אינדוקציה מתמטית על גובה העץ, העץ עצמו בנוי משני תת־עצים שלכל אחד מהם יש מעט פחות ממחצית הצמתים. בתרגיל הבא צורת האינדוקציה הזאת תתבהר.

תרגיל 22 יהי n_h מספר הצמתים בעץ בינרי (לא בהכרח שלם) בגובה h. אזי $n_h \leq 2^{h+1} - 1$.

דוגמה תרשים 4.3 מראה עץ בינרי בגובה 2 עם $5 \leq 2^3 - 1 = 7$ צמתים.

4.4 גרפים

גרף הוא מבנה כללי המורכב מצמתים וקשתות בין הצמתים. אם הקשתות מרכיבות מסלול סגור, הן תוחמות שטח. אנחנו גם סופרים כשטח את כל המישור מחוץ לגרף. התרשים להלן מראה גרף עם 7 צמתים, 8 קשתות, ו־3 שטחים, כאשר s_3 מופיע מספר פעמים כדי להדגיש את השטח של המישור מחוץ לגרף.



תרגיל 23 ***(Euler)*** עבור גרף עם n צמתים, e קשתות ו־s שטחים, מתקיים $s + n = e + 2$.[2]

דוגמה בתרשים, $3 + 7 = 8 + 2$.

רמז הוכח באמצעות אינדוקציה על מספר הקשתות בגרף. יש שני צעדים אינדוקטיביים, תלוי אם הקשת היא חלק ממסלול סוגר או לא.

[2] קיימים מקרים מיוחדים שיש להתייחס אליהם במשפט ובהוכחה שלו. ראו:
David Eppstein, *Twenty Proofs of Euler's Formula: $V - E + F = 2$*,
https://www.ics.uci.edu/~eppstein/junkyard/euler/ .

פרק 5

מוקשים שיש להיזהר מהם

5.1 אינדוקציה היא לא דרך ההוכחה היחידה

אינדוקציה נמצאת בשימוש נרחב בהוכחות במתמטיקה ולפעמים היא השיטה הטובה ביותר להוכחת משפט, אבל היא לא שיטת ההוכחה היחידה. הנה הוכחה של משפט 6 שלא משתמשת באינדוקציה.

משפט 22 לכל $n \geq 1$, $n(n+1)$ מתחלק ב־2.

הוכחה אם n מתחלק ב־2 המשפט נכון. אחרת, $n = 2k+1$ עבור k כלשהו. לכן, $n+1 = 2k+2 = 2(k+1)$ מתחלק ב־2. ∎

זו בעצם אותה הוכחה כמו הצעד האינדוקטיבי בהוכחה באמצעות אינדוקציה.

תרגיל 24 הוכח ללא שימוש באינדוקציה: לכל $n \geq 1$, $n(n+1)(n+2)$ מתחלק ב־3.

Carl Friedrich Gauss היה מגדולים המתמטיקאים בכל הזמנים. לפי האגדה, כאשר התפרע מעט בבית הספר היסודי, המורה הטיל עליו לסכם את המספרים החיוביים מ־ 1 ל־100, בתקווה שזה יעסיק אותו זמן ממושך. Gauss פתר את הבעיה מיד כאשר שם לב שניתן להציג את המספרים כך:

$$\begin{array}{rccccccc} & 1 & 2 & 3 & \cdots & 98 & 99 & 100 \\ + & 100 & 99 & 98 & \cdots & 3 & 2 & 1 \\ \hline & 101 & 101 & 101 & \cdots & 101 & 101 & 101 \end{array}$$

ומיד מקבלים את הנוסחה $\frac{100 \cdot 101}{2}$ שהוכחנו במשפט 4.

ניתן גם להוכיח את המשפט עבור n שרירותי כך:

$$\begin{aligned} \sum_{i=1}^{n} i &= \sum_{i=1}^{n} (n-i+1) \\ &= \frac{1}{2}\left[\sum_{i=1}^{n} i + \sum_{i=1}^{n} (n-i+1)\right] \\ &= \frac{1}{2}\left[\sum_{i=1}^{n} (n+1)\right] \end{aligned}$$

$$= \frac{n(n+1)}{2}.$$

תרגיל 25 הוכח עס ובלי אינדוקציה ש־$x-1$ מחלק את x^n-1. איזו הוכחה עדיפה בעיניך?

רמז להוכחה ללא אינדוקציה, חשב:

$$(x-1)\sum_{i=0}^{i=n} x^i.$$

להוכחה באינדוקציה, מצא פולינומים $p(x), q(x)$ ששניהם מתחלקים ב־$x-1$, כך ש־$x^{n+1}-1 = p(x)+q(x)$.

5.2 לפעמים אי אפשר להשתמש באינדוקציה

ניתן להשמתמש באינדוקציה רק אם המבנים הגדולים נוצרים צעד אחר צעד ממבנים קטנים יותר, ואם יש מבנה קטן ביותר. לא ניתן להרחיב את המשפטים שהוכחנו למספרים רציונליים כי אין מספר רציונלי "ראשון".[1] נניח שאנו רוצים להוכיח שלכל זוג מספרים רציונלים **חיובים** a, b, כך ש־$a < b$ מתקיים $a \leq \frac{a+b}{2} \leq b$.

- מהי טענת הבסיס? נניח ש־a הוא המספר הרציונלי החיובי הקטן ביותר. אבל המספר $\frac{a}{2}$ הוא רציונלי, חיובי וקטן מ־a.
- מהי הנחת האינדוקציה? מהו הצעד האינדוקטיבי? נניח שהנחת האינדוקציה היא שהנוסחה נכונה עבור a, b. בצעד האינדוקטיבי יש להוכיח את נכונות הנוסחה עבור **זוג הערכים הבא**, שניתן לכתוב אותו כ־$a + \frac{p_a}{q_a}$, $b + \frac{p_b}{q_b}$. אבל $a + \frac{p_a}{q_a+1}$ גדול מ־a וקטן מ־$a + \frac{p_a}{q_a}$, כך שאין "זוג הערכים הבא".

5.3 היזהרו מהוכחות לא נכונות

משפט 23 לכל $n \geq 0$ ו־$a \geq 1$, $a^n = 1$.

הוכחה טענת בסיס: $a^0 = 1$. הנחת האינדוקציה: $a^k = 1$ עבור $0 \leq k \leq n$. הצעד האינדוקטיבי הוא:

$$a^{n+1} = a^n \cdot a \stackrel{\bullet}{=} 1 \cdot a = a = \frac{a^{n-1}}{a^{n-2}} \stackrel{\bullet}{=} \frac{a^{n-1}}{1} \stackrel{\bullet}{=} \frac{1}{1} = 1.$$

∎

כמובן שזוהי שטות כי $2^3 = 8 \neq 1$.

תרגיל 26 איפה השגיאה בהוכחה?

[1] Georg Cantor מצא דרך לסדר את המספרים הרציונלים בסדרה: $\{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{1}{5}, \frac{5}{1}, \ldots\}$, אבל סדרה זו היא לא אינטואיטיבית ולא מתאימה להוכחות באינדוקציה.

משפט 24 לכל התלמידים בכיתה מסוייפת יש אותו צבע שיער.

הוכחה טענת בסיס: בחר תלמיד כלשהו s_1. לתלמיד צבע שיער c. הנחת האינדוקציה: בכל קבוצה של n תלמידים, לכולם צבע שיער c. צעד אינדוקטיבי: יהיו $s_1, s_2, \ldots, s_n, s_{n+1}$ התלמידים בקבוצה שבה $n+1$ תלמידים. נבדוק את התת־קבוצה $s_1, s_2, \ldots, s_n$. לפי הנחת האינדוקציה צבע השיער שלהם הוא c. באופן דומה, בתת־קבוצה $s_1, s_2, \ldots, s_{n-1}, s_{n+1}$, לכולם צבע שיער c. לכן, צבע השיער של תלמיד s_{n+1} הוא c, בדיוק כמו צבע השיער של s_1, שהוא אותו צבע שיש לתלמידים $s_2, \ldots, s_n$. לכן, לכל התלמידים $s_1, s_2, \ldots, s_n, s_{n+1}$ צבע שיער c. ∎

ברור שלתלמידים שונים יש צבע שיער שונה (שלא לדבר על אלה שצובעים בכל גווני הקשת) כך שההוכחה שגויה.

תרגיל 27 איפה השגיאה בהוכחה?

פרק 6

לוגיקה מתמטית

אינדוקציה היא כלי חיוני בלוגיקה מתמטית כי המשפטים טוענים לתכונות של **כל** הנוסחאות. בגלל שהנוסחאות בנויות מתת־נוסחאות, המורכבות באמצעות אופרטורים לוגיים, הוכחת משפט היא על ידי אינדוקציה על מבנה הנוסחה. בפרק זה נראה איך משתמשים באינדוקציה, לעתים בצורה לא־מפורשת, בהוכחות בתחשיב הפסוקים.

הגדרה 25 נוסחה A היא **ספיקה** אם ורק אם קיימת השמה של T או F לכל **אטום** כך שערכה של הנוסחה A היא T.

הגדרה 26 נוסחה A **שקולה לוגית** לנוסחה A' אם ורק אם ערכיהן שווים לכל השמה לאטומים. סימון: $A \equiv A'$.

הנה דוגמה המבהירה את ההבדל בין המושגים **שקולה לוגית** ו־ **ספיקה אם ורק אם**.
נתונה שתי נוסחאות:

$$A = (p \vee q \vee \neg r) \ \wedge \ (p \vee \neg q) \ \wedge \ (\neg p \vee q)\,,$$
$$B = (p \vee \neg q) \ \wedge \ (\neg p \vee q)\,.$$

A ספיקה בגלל שערכה הוא T עבור ההשמה $\{p = F, q = F, r = F\}$ ו־ B ספיקה עבור אותה השמה. אולם, עבור ההשמה $\{p = F, q = F, r = T\}$, ערכה של A הוא F וערכה של B הוא T, כך שהנוסחאות אינן שקולות לוגית.

6.1 המרת נוסחה ל־CNF

הגדרה 27 נוסחה בתחשיב הפסוקים היא בצורת ***conjunctive normal form (CNF)*** אם היא חיתוך ("ו") של איחוד ("או") של ליטרלים (אטומים או שלילה של אטומים).

דוגמה הנוסחה שלהלן איננה ב־CNF:

$$(p \wedge \neg q) \ \rightarrow \ (\neg q \wedge p)\,, \tag{6.1}$$

אבל היא שקולה לוגית לנוסחה שלהלן שהיא ב־CNF:

$$(\neg p \vee q \vee \neg q) \ \wedge \ (\neg p \vee q \vee p)\,. \tag{6.2}$$

לצורת CNF חשיבות רבה במדעי המחשב, גם בתיאוריה וגם בשימוש מעשי. בתיאוריה: Stephen Cook הוכיח שהקביעה האם נוסחה ב־ CNF היא ספיקה היא בעיית NP-שלמה. צורת CNF נמצאת בשימוש נרחב בהוכחה אוטומטית של משפטים, בתכנות לוגי ובפתרון בעיות על ידי בדיקת ספיקות.

משפט 28 תהי A נוסחה. אזי ניתן לבנות נוסחה A' בצורת *CNF* שהיא שקולה ל־ A: $A \equiv A'$.

לא נביא כאן את פרטי ההוכחה. במקום זה, נדגים את המשפט על הנוסחה 6.1:

הנוסחה המקורית	$(p \wedge \neg q) \ \rightarrow \ (\neg q \wedge p)$
סלק את האופרטור $\rightarrow$	$\neg(p \wedge \neg q) \ \vee \ (\neg q \wedge p)$
דחוף שלילה פנימה	$(\neg p \vee \neg\neg q) \ \vee \ (\neg q \wedge p)$
סלק את זוג האופרטורים $\neg\neg$	$(\neg p \vee q) \ \vee \ (\neg q \wedge p)$
חוק הפילוג	$(\neg p \vee q \vee \neg q) \ \wedge \ (\neg p \vee q \vee p)$

הנימוקים לצעדים מבוססים על שקילויות לוגיות שניתן להוכיח:

$$\begin{aligned}
A \rightarrow B &\equiv \neg A \vee B \\
\neg(A \vee B) &\equiv \neg A \wedge \neg B \\
\neg(A \wedge B) &\equiv \neg A \vee \neg B \\
\neg\neg A &\equiv A \\
A \vee (B \wedge C) &\equiv (A \vee B) \wedge (A \vee C)\,.
\end{aligned}$$

ההוכחה של משפט 28 היא סדרת למות כגון:

למה 29 תהי A נוסחה. אזי קיימת נוסחה A' ללא האופרטור $\rightarrow$ כך ש־$A \equiv A'$.

הלמה תמימה למראה מהרגע שהוכחנו $A \rightarrow B \equiv \neg A \vee B$, אבל ההוכחה מסתירה אינדוקציה לא־מפורשת:

הוכחה טענת הבסיס היא כאשר הנוסחה A היא אטום p, אבל ברור שהאטום p לא מכיל את האופרטור $\rightarrow$. הנחת האינדוקציה היא שעבור כל נוסחה שגודלה פחות או שווה ל־n,[1] קיימת נוסחה שקולה A' ללא $\rightarrow$. תהי $A_1 \vee A_2$ נוסחה כך שגודלן של A_1, A_2 פחות או שווה ל־n. לפי הנחת האינדוקציה, קיימות נוסחאות A'_1, A'_2 ללא $\rightarrow$, כך ש־$A_1 \equiv A'_1$ ו־$A_2 \equiv A'_2$. ברור ש־$A'_1 \vee A'_2$ שקולה ל־A ולא מכילה $\rightarrow$.

צעדי אינדוקציה דומים מוכיחים את המשפט עבור $\neg A_1$ ו־$A_1 \wedge A_2$.

עבור $A_1 \rightarrow A_2$, לפי הנחת האינדוקציה, קיימות נוסחאות A'_1, A'_2 ללא $\rightarrow$, כך ש־$A_1 \equiv A'_1$ ו־$A_2 \equiv A'_2$. הנוסחה $\neg A'_1 \vee A'_2 \equiv \neg A_1 \vee A_2$, שקולה ל־$A$ ולא מכילה $\rightarrow$. ∎

[1] ניתן להגדיר את גודלה של נוסחה כגובה עץ הבניה שלה, אבל ההגדרה חורגת מתחום מסמך זה.

כדי לסיים את ההוכחה של משפט 28 אנחנו צריכים שלוש למות נוספות עם הוכחות דומות. כל אינדוקציה היא על **מבנה** של הנוסחה, ולכן מספר הצעדים האינדוקטיביים הוא כמספר האופרטורים בלוגיקה.[2] בשום ספר לימוד בלוגיקה מתמטית לא תמצאו הוכחה כל כך מפורטת, כי ההוכחות ברורות משקילויות כגון $A \to B \equiv \neg A \vee B$, אבל חשוב להבין שמשתמשים באינדוקציה בצורה לא־מפורשת.

6.2 מ־ CNF ל־ 3CNF

הגדרה 30 נוסחה בצורת CNF היא בצורת $3CNF$ אם ורק אם בכל איחוד יש בדיוק שלושה ליטרלים.

דוגמה הנוסחה 6.2 היא ב־3CNF.

משפט 31 תהי A נוסחה בתחשיב הפסוקים. ניתן לבנות נוסחה A' ב־$3CNF$, כך ש־A ספיקה אם ורק אם A' ספיקה.

ההוכחה הרגילה של משפט 31 משתמשת באינדוקציה בצורה לא־מפורשת. כאן אנו במביאים הוכחה המציגה את האינדוקציה בצורה מפורשת.

הוכחה מספיק להוכיח שעבור כל איחוד בודד $A = x_1 \vee x_2 \vee \cdots \vee x_n$ ניתן לבנות חיתוך של איחודים עם שלושה ליטרלים כל אחד.

יש שלוש טענות בסיס:

- אם ל־A שלושה ליטרלים, אין מה להוכיח.
- אם ל־A שני ליטרלים $p_1 \vee p_2$, הנוסחה A' תהיה:

$$(p_1 \vee p_2 \vee q) \ \wedge \ (p_1 \vee p_2 \vee \neg q)\,,$$

כאשר q הוא אטום חדש. אם A ספיקה, אזי ההשמה נותנת את הערך T או ל־p_1 או ל־p_2, ולכן גם הערך של A' הוא T. בכיוון ההפוך, אם A' ספיקה, אז אחת מהשמות $\{p_1 = F, p_2 = F, q = T\}$ ו־$\{p_1 = F, p_2 = F, q = F\}$ מספקת את A', כך שאו p_1 או p_2 (או שניהם) צריכים לקבל את הערך T. מכאן שגם A ספיקה.

- **תרגיל 28** אם A הוא ליטרל בודד p או $\neg p$, קיימת נוסחה A' עם בדיוק שלושה ליטרלים שהיא ספיקה אם ורק אם A ספיקה. **רמז** כמה אטומים חדשים נחוצים?

הנחת האינדוקציה היא: אם $A = p_1 \vee p_2 \vee \cdots \vee p_n$ היא איחוד עם $n \geq 3$ ליטרלים, אזי קיימת נוסחה A' בצורת 3CNF שהיא ספיקה אם ורק אם A ספיקה. הצעד האינדוקטיבי הוא: יהי A איחוד $p_1 \vee p_2 \vee \cdots \vee p_n \vee p_{n+1}$ עם $n+1$ ליטרלים. בנה A' כך:

$$(p_1 \vee \cdots \vee p_{n-1} \vee q) \ \wedge \ (\neg q \vee p_n \vee p_{n+1})\,,$$

[2] מקובל להשתמש בלפחות ארבעה אופרטורים $\neg, \vee, \wedge, \to$ ולפעמים ארבעה נוספים $\leftrightarrow$ שקילות, $\oplus$ אי־שקילות, $\uparrow$ nand, $\downarrow$ nor. Raymond Smullyan הגדיר סימון פשוט יותר כך שיש רק שני צעדי אינדוקציה.

כאשר q הוא אטום חדש. ניתן להראות ש־A' ספיקה אם ורק אם A ספיקה בהוכחה דומה להוכחה של טענת הבסיס עבור שני ליטרלים.

לפי הנחת האינדוקציה לאיחוד הראשון עם n ליטרלים קיימת נוסחה A'' בצורת 3CNF שהיא ספיקה אם ורק אם נוסחת האיחוד הראשון ספיקה. מכאן, ש:

$$A'' \ \wedge \ (\neg q \vee p_n \vee p_{n+1})$$

נוסחה בצורת 3CNF שהיא ספיקה אם ורק אם A ספיקה. ∎

פרק 7

מודלים חישוביים

מודלים חישוביים, כגון אוטומטים סופיים ושפות פורמליות, הם מושגים מרכזיים במדעי המחשב. הוכחות בנושאים אלה משתמשות באינדוקציה מעל המבנה של אוטומט או מעל לגזירה של מחרוזות מדקדוק פורמלי. לעתים יש יותר מטענת בסיס אחת וצעד אינדוקציה אחד.

אנו מניחים שהקורא בקיא במושגים של אוטומט לא־דטרמיניסטי סופי NFA, ביטוי רגולרי RE, ודקדוק חסר־הקשר.

7.1 אוטומטים

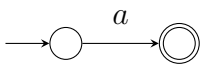
משפט 32 יהי r ביטוי רגולרי. אזי ניתן לבנות NFA שמקבל את השפה של r.

הוכחה יש שלוש טענות בסיס:

- r הוא הקבוצה הריקה $\emptyset$. ה־NFA עם מצב תחילי אחד ומצב סופי אחד וללא מעברים לא מקבל אף מחרוזת:

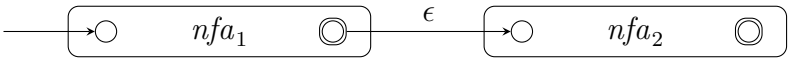
- r הוא המחרוזת הריקה ϵ. ה־NFA עם מצב אחד שהוא גם תחילי וגם סופי מקבל את המחרוזת הריקה:

- r הוא התו הבודד a. ה־NFA שלהלן מקבל את השפה $\{a\}$:

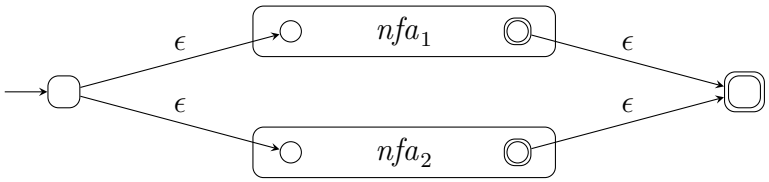


יש שלושה צעדי אינדוקציה, אחד לכל דרך לבניית RE מ־REs פשוטים יותר:

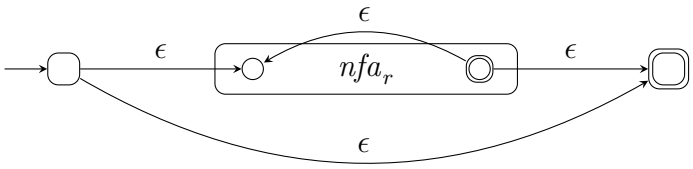
- שירשור $r_1 r_2$: לפי הנחת האינדוקציה קיימים NFAs nfa_1 ו־nfa_2 המקבלים את השפות של r_1 ו־r_2, בהתאמה. בנה nfa_{12} על ידי הוספת מעבר ריק מהמצב הסופי של nfa_1 למצב התחילי של nfa_2. המצב התחילי של nfa_{12} הוא המצב התחילי של nfa_1 והמצב הסופי שלו הוא המצב הסופי של nfa_2:



- איחוד $r_1 + r_2$: לפי הנחת האינדוקציה קיימים NFAs nfa_1 ו־nfa_2 המקבלים את השפות של r_1 ו־r_2, בהתאמה. בנה nfa_{12} על ידי הוספת מצב תחילי ומצב סופי חדשים ומעברים ריקים:



- סגור r^*: לפי הנחת האינדוקציה קיים NFA nfa_r המקבל את השפה של r. הוסף מצב תחילי, מצב סופי ומעברים ריקים כפי שהם מוצגים בתרשים:



המעבר הריק בין המצב התחילי והמצב הסופי הוא עבור מחרוזת המתקבלת מאפס מופעים של r, והמעבר הפנימי מהמצב הסופי של nfa_r למצב התחילי שלו הוא עבור חזרה אחת או יותר של r. ∎

7.2 שפות פורמליות

הוכחות בשפות פורמליות הן באינדוקציה מעל לאורך המחרוזות, שהיא בעצם אינדוקציה מעל לגזירת המחרוזת מהדקדוק. הנה דקדוק חסר־הקשר G:

$$\begin{array}{llll} S \to aB & S \to bA & A \to a & B \to b \\ A \to aS & B \to bS & A \to bAA & B \to aBB \end{array}$$

משפט 33 השפה L של הדקדוק G היא כל המילים מעל $\{a, b\}$ עם מספר שווה של a ו־b. סימון:

$$S \stackrel{*}{\Rightarrow} w \text{ iff } \#a = \#b,$$

כאשר $\#a, \#b$ מסמנים את מספר ה־a וה־b ב־w.

הוכחה נשתמש באינדוקציה **בו־זמנית** על שלוש הטענות האלו:

$$S \overset{*}{\Rightarrow} w \quad \text{iff} \quad \#a = \#b \tag{7.1}$$

$$A \overset{*}{\Rightarrow} w \quad \text{iff} \quad \#a = \#b + 1 \tag{7.2}$$

$$B \overset{*}{\Rightarrow} w \quad \text{iff} \quad \#a + 1 = \#b. \tag{7.3}$$

טענת הבסיס $|w| = 1$ פשוטה כי A ו־B גוזרים את a ו־b, בהתאמה, ו־S לא גוזר אף מחרוזת באורך אחד. עלינו לציין שאין דרכים אחרות לקבל מחרוזת באורך אחד.
תהי w מילה הנגזרת מ־S עם $|w| = n + 1$. יש שלושה צעדי אינדוקציה וכדי להוכיח כל אחד מהם נניח את **כל שלוש הטענות** עבור $|w| = n$ כהנחת האינדוקציה.
תחילה נוכיח את הנוסחה 7.1 עבור w. הגזירה הראשונה היא אחת מ:

$$S \to aB \overset{*}{\Rightarrow} aw', \qquad S \to bA \overset{*}{\Rightarrow} bw'.$$

במקרה הראשון, לפי הנחת האינדוקציה בנוסחה 7.3, עבור המילה w' שנגדרה על ידי B קיים $\#a + 1 = \#b$, כך ש־$\#a = \#b$ ב־w. בדרך דומה ניתן להוכיח את המקרה השני תוך שימוש בנוסחה 7.2.
נשאיר את סיום ההוכחה כתרגיל. ∎

תרגיל 29

- הוכח את הנוסחאות 7.2 ו־7.3.
- הוכח את המשפט ההפוך: אם $\#a = \#b$ ב־w אזי $S \overset{*}{\Rightarrow} w$.

פרק 8

הוכחת נכונות של תכניות

תכנית מחשב היא **נכונה** אם **כל** חישוב תואם את המפרט של התכנית. למשל, אם המפרט של תכנית דורש שהיא תחשב שורש ריבועי של מספר בקלט, אם התכנית מחשבת שורש שלישי, התכנית לא נכונה. אולם התכנית תהפוך לנכונה אם נשנה את המפרט כדי לדרוש חישוב של שורש שלישי. קיימות שיטות לכתיבת מפרטים פורמליים ושיטות **להוכחה** שתכנית עומדת בדרישות המפרט.

אין מגבלה על האורך (מספר הצעדים) של חישוב. כמו כן, אין מגבלה על מספר החישובים השונים שתכנית יכולה לבצע. תכנית לחישוב שורש תבצע חישוב שונה עבור כל מספר אפשרי בקלט. לכן, טבעי שמשתמשים באינדוקציה כדי להוכיח תכונות של תכניות עם אורך חישוב בלתי מוגבל ומספר חישובים בלתי מוגבל.

נדגים כאן הוכחות אינדוקטיביות של תכניות סדרתיות ותכניות מקביליות. תכנית סדרתית היא **פונקציונלית**: היא מקבלת קלט ומפיקה פלט במספר צעדים סופי. נדגים חישוב סדרתי על אלגוריתם למיון סדרת מספרים: הקלט הוא הסדרה והפלט הוא תמורה של הסדרה עם ערכיה בסדר עולה. נשתמש באינדוקציה כדי להוכיח את נכונות האלגוריתם ללא תלות בכמות המספרים בסדרה.

תכניות מקביליות מורכבות ממספר תכניות סדרתיות המכונות **תהליכים** המתבצעים בו־זמנית. בדרך כלל, תכניות מקביליות הן **תגובתיות**, לא פונקציונליות: אנו מצפים שהן תתבצענה ללא נקודת סיום ותייצרנה פלט תוך זמן קצר מקבלת הקלט. למשל, מערכת ההפעלה של סמארטפון מתבצעת תמיד: כאשר אתה נוגע בצלמית מייד יש תגובה נראית. אינדוקציה היא חיונית בהוכחת נכונות של תכניות מקביליות, כי קיים מספר אינסופי של **שילובים** של החישובים של התהליכים המרכיבים את התכנית.

8.1 תכניות סדרתיות

נסתכל על מערך של מספרים שלמים כגון:[1]

$$A = [5, 31, 7, 1, 6, 17, 16, 22, 3, 10] .$$

[1] במדעי המחשב משתמשים במונח מערך עבור מה שמתמטיקאים קוראים וקטור.

דרוש אלגוריתם **למיון** המערך A: בנה מערך B שהאיברים שלו הם תמורה של האיברים של A בסדר עולה:

$$B = [1, 3, 5, 6, 7, 10, 16, 17, 22, 31]\,.$$

נציג שני אלגוריתמים פשוטים למיון.

מיון הכנסה כאשר משחקים קלפים, שחקן אדיב יחכה עד שכל הקלפים חולקו ורק אחר כך יאסוף אותם ויסדר אותם. אם אתה לא אדיב אפשר להשתמש באלגוריתם יעיל המכונה מיון הכנסה: אסוף את הקלפים אחד־אחד והכנס אותם במקומם לפי הסדר:[2]

כל עוד A אינו ריק
קח את הערך הראשון ב־A והכנס לאחר הערך הגדול ביותר ב־B שקטן ממנו

עבור המערך A לעיל, בניית המערך B מתנהלת כך:

B_0	=	$[\,]$	A_0	=	$[5, 31, 7, 1, 6, 17, 16, 22, 3, 10]$
B_1	=	$[5]$	A_1	=	$[31, 7, 1, 6, 17, 16, 22, 3, 10]$
B_2	=	$[5, 31]$	A_2	=	$[7, 1, 6, 17, 16, 22, 3, 10]$
B_3	=	$[5, 7, 31]$	A_3	=	$[1, 6, 17, 16, 22, 3, 10]$
B_4	=	$[1, 5, 7, 31]$	A_4	=	$[6, 17, 16, 22, 3, 10]$
B_5	=	$[1, 5, 6, 7, 31]$	A_5	=	$[17, 16, 22, 3, 10]$
B_6	=	$[1, 5, 6, 7, 17, 31]$	A_6	=	$[16, 22, 3, 10]$
B_7	=	$[1, 5, 6, 7, 16, 17, 31]$	A_7	=	$[22, 3, 10]$
B_8	=	$[1, 5, 6, 7, 16, 17, 22, 31]$	A_8	=	$[3, 10]$
B_9	=	$[1, 3, 5, 6, 7, 16, 17, 22, 31]$	A_9	=	$[10]$
B_{10}	=	$[1, 3, 5, 6, 7, 10, 16, 17, 22, 31]$	A_{10}	=	$[\,]$

נוכיח את הנכונות של מיון הכנסה עבור מערך A באורך שרירותי n.

טענת נכונות כאשר הביצוע של מיון הכנסה מסתיים, כל האיברים של B הם תמורה של האיברים של A בסדר עולה.

למה 1: לכל i, הסדרה המורכבת מהערכים של B_i ולאחריהם האיברים של A_i היא תמורה של A.

למה 2: לכל i, האיברים ב־B_i מסודרים בסדר עולה.

טענת הנכונות נובעת מיד מהלמות: כאשר החישוב מסתיים, A_n ריקה, ולכן לפי למה 1, הסדרה B_n לבדה היא תמורה של האיברים של A, ולפי למה 2, B_n סדורה בסדר עולה.

לא נביא את ההוכחה הפשוטה של למה 1.

הוכחת למה 2: טענת בסיס: B_0 היא סדרה ריקה ולכן היא סדורה. צעד אינדוקטיבי: נניח כהנחת האינדוקציה ש־B_i סדורה. יהי a_i האיבר הראשון של A_i ו־b_k האיבר הגדול ביותר של B_i כך ש־$b_k < a_i \le b_{k+1}$. אזי $B_{i+1} = [\ldots, b_k, a_i, b_{k+1}, \ldots]$ היא סדרה סדורה.

[2] השמטנו את הפקודות עבור המקרה שהקלף הוא קטן יותר מכל הקלפים שסודרו עד כה.

מיון בחירה מיון בחירה הוא אלגוריתם פשוט שקל יותר לישום ממיון הכנסה:

כל עוד A אינו ריק
קח את הערך הקטן ביותר של A ושרשר אותו לסוף B

עבור המערך בדוגמה, החישוב הוא:

$$
\begin{array}{lcl|lcl}
B_0 & = & [\,] & A_0 & = & [5,31,7,1,6,17,16,22,3,10] \\
B_1 & = & [1] & A_1 & = & [5,31,7,6,17,16,22,3,10] \\
B_2 & = & [1,3] & A_2 & = & [5,31,7,6,17,16,22,10] \\
B_3 & = & [1,3,5] & A_3 & = & [31,7,6,17,16,22,10] \\
B_4 & = & [1,3,5,6] & A_4 & = & [31,7,17,16,22,10] \\
B_5 & = & [1,3,5,6,7] & A_5 & = & [31,17,16,22,10] \\
B_6 & = & [1,3,5,6,7,10] & A_6 & = & [31,17,16,22] \\
B_7 & = & [1,3,5,6,7,10,16] & A_7 & = & [31,17,22] \\
B_8 & = & [1,3,5,6,7,10,16,17] & A_8 & = & [31,22] \\
B_9 & = & [1,3,5,6,7,10,16,17,22] & A_9 & = & [31] \\
B_{10} & = & [1,3,5,6,7,10,16,17,22,31] & A_{10} & = & [\,]
\end{array}
$$

כדי להוכיח את הנכונות של מיון בחירה דרושות שתי למות. הראשונה זהה ללמה 1 הפשוטה של מיון הכנסה.

תרגיל 30 נסח את הלמה השנייה הנחוצה להוכחת הנכונות של מיון בחירה. הוכח את הלמה.

8.2 תכניות מקביליות

בתכניות מקביליות מופיעות שגיאות מסוג הידוע לשמצה: שגיאות מירוץ. מהירויות ההרצה היחסיות של התהליכים יכולות לגרום לתקלות שכמעט בלתי אפשרי לשחזר אותן כדי לאתר את השגיאות ולבדוק אם תוקנו. **סמפור** הוא אמצעי סינכרון פשוט ויעיל שמאפשר לכתוב תכניות עם פחות שגיאות מירוץ. אנו מניחים שאתה בקיא בהגדרת הסמפור והפעולות עליו ומכיר את התכניות הפשוטה לפתרון בעיית הקטע הקריטי עם סמפור:

```
                    global int sem = 1
process p                           process q
    loop forever                        loop forever
        p1:  wait(sem)                      q1:  wait(sem)
        p2:  critical section               q2:  critical section
        p3:  signal(sem)                    q3:  signal(sem)
```

טענת הנכונות היא שרק תהליך אחד נמצא בקטע הקריטי בבת־אחת.
הנוסחאות שלהלן הן **שמורות**, כלומר, הן נכונות בכל מצב של כל חישוב:

$$(sem = 0) \vee (sem = 1) \tag{8.1}$$

$$\#CS + sem = 1, \tag{8.2}$$

כאשר sem הוא ערכו של המשתנה sem ו־$\#CS$ הוא מספר התהליכים בקטע הקריטי. התהליך p נמצא בקטע הקריטי אם החישוב נמצא במקום p2 או p3, והתהליך q נמצא בקטע הקריטי אם החישוב נמצא במקום q2 או q3.
לפי נוסחה 8.2, $\#CS = 1 - sem$, ולפי נוסחה 8.1:

$$(\#CS = 1 - 0) \vee (\#CS = 1 - 1),$$

כלומר, $\#CS \leq 1$, שהיא טענת הנכונות למניעה הדדית.
נוכיח את הנוסחה 8.1 באינדוקציה מעל למצבי החישוב.
טענת הבסיס פשוטה ביותר כי המשתנה sem מקבל ערך תחילי של 1.
קיימים 18 צעדי אינדוקציה! **המיקום הנוכחי של החישוב** הוא אחד מ־9 הזוגות:

$$(p_1, q_1), (p_1, q_2), (p_1, q_3), (p_2, q_1), (p_2, q_2), (p_2, q_3), (p_3, q_1), (p_3, q_2), (p_3, q_3),$$

ועבור כל אחד מהם, הפקודה הבאה יכולה לבוא או מתהליך p או מתהליך q. נבדוק שני צעדי אינדוקציה:

- נניח שהחישוב נמצא במצב (p_1, q_1) והפקודה הבאה לביצוע היא p1:wait(sem). הנחת האינדוקציה היא ש־(8.1) נכונה. אם $sem = 0$, לפי ההגדרה, פעולת הסמפור wait(sem) לא ניתנת לביצוע כך ש־(8.1) נשארת נכונה. אם $sem = 1$, לפי ההגדרה של פעולת המספור wait(sem) מחסירים 1 מערכו של sem, כך ש־$sem = 0$ ו־(8.1) נשארת נכונה.
- נניח שהחישוב נמצא ב־(p_2, q_1) והפקודה הבאה לביצוע היא p2:critical section. הנחת האינדוקציה היא ש־(8.1) נכונה. הפקודה critical section לא משנה את ערכו של sem כך ש־(8.1) נשארת נכונה.

למרות שיש מספר רב של צעדי אינדוקציה, לרובם הוכחה פשוטה ביותר בגלל התכונה הלוגית של "גורר": ל־$A \to B$ ערך שקר אם ורק אם A מקבל ערך אמת ו־B מקבל ערך שקר.
נבדוק את השמורה־8.2 שהיא שקולה לשתי הנוסחאות:

$$(p_1 \wedge q_1) \quad \to \quad (sem = 1) \tag{8.3}$$

$$(sem = 1) \quad \to \quad (p_1 \wedge q_1)\,. \tag{8.4}$$

נוכיח את נוסחה 8.3 באינדוקציה. טענת הבסיס נכונה בגלל האיתחול. הנחת האינדוקציה היא ש־(8.3) נכונה. יש שתי דרכים בהן הנוסחה יכולה לקבל ערך שקר:

1. ל־$p_1 \wedge q_1$ ו־$sem = 1$ ערך אמת ואז הנוסחה $sem = 1$ מקבלת ערך שקר בזמן ש־$p_1 \wedge q_1$ נשארת אמת.
2. ל־$p_1 \wedge q_1$ ו־$sem = 1$ ערך שקר ואז הביטוי $p_1 \wedge q_1$ מקבל ערך אמת בזמן ש־$sem = 1$ נשארת שקר.

(1) הנוסחה $sem = 1$ מקבלת ערך שקר רק אם מבצעים p1 או q1, אבל אז גם הביטוי $p_1 \wedge q_1$ מקבל שקר.
(2) הביטוי $p_1 \wedge q_1$ מקבל אמת רק אם מבצעים p3 או q3, אבל אז גם הנוסחה $sem = 1$ מקבלת אמת.

תרגיל 31 הוכח נוסחה 8.2.

פרק 9

אינדוקציה ודדוקציה

עורבים הם ציפורים שחורות. נהוג לומר ש־**כל העורבים שחורים**. מה ההצדקה לטיעון זה? ברור שיש מספר סופי של עורבים בעולם, ובאופן תיאורטי ניתן לבדוק את כולם ולוודא שכולם שחורים. ברור שאף אחד לא עשה כך. לאחר בחינת צבעם של מספר מסויים של עורבים, אפשר **להכליל** ממספר קטן של תצפיות ולטעון שכל העורבים שחורים.

התהליך של הכללה ממספר קטן של מקרים נקרא **אינדוקציה**. מדענים ופילוסופים מכירים בעובדה שאינדוקציה יכולה להטעות. תמיד יש אפשרות שקיים עורב ירוק, ואם אכן יתגלה עורב ירוק, הטיעון הכללי לא יהיה תקף יותר.[1] למרות שלא ניתן לסמוך לגמרי על אינדוקציה, נראה שאין ברירה אלא להשתמש בה במדע.

סוד כמוס הוא שמתמטיקאים משתמשים בצורה זו של אינדוקציה. המתמטיקאי בודק מקרים פרטיים רבים, ורק אחר כך מכליל אותם למשפט שמוכיחים אותו בתהליך הנקרא **דדוקציה**. לפעמים עוברות שנים רבות בין ניסוחו של משפט לבין ההוכחה שלו. כאשר מציגים את המשפט במאמר או בספר לימוד, משמיטים את תהליך האינדוקציה ומציגים רק את המשפט וההוכחה הדדוקטיבית. כך נראה כאילו שהמתמטיקאי שלף את המשפט מהאוויר!

בלוגיקה מתמטית חוקרים מערכות דדוקטיביות (אקסיומות וכללי היסק). בפועל, מתמטיקאים משתמשים בגרסאות לא־פורמליות של מערכות דדוקטיביות, אבל קיימת הסכמה על מה נחשב כשיטת הוכחה תקפה.[2] אינדוקציה מתמטית היא כלל היסק שמתמטיקאים מקבלים כתקף ומשמתמשים בה בצורה שגרתית. אין לה קשר עם המושג המדעי־פילוסופי של אינדוקציה.

[1] מי שרואה עורב ירוק עלול להתפתות ולטעון שהציפור איננה באמת עורב! טיעון זה הוא מקרה של כשל לוגי הנקרא "לא סקוטי אמיתי". ההסקה אינה תקפה כי חייב להיות אוסף קריטריונים קבוע המגדיר מתי ציפור נחשבת כעורב. ציפור התואמת את הקריטריונים היא עורב גם אם צבעה ירוק.

[2] קיימות מערכות דדוקטיביות כגון intuitionism השונות מהמערכות המקובלות. מערכות אלו נחקרות בלוגיקה מתמטית.

פרק 10

עיקרון הסדר הטוב

עיקרון הסדר הטוב שקול לאינדוקציה מתמטית, אבל קל יותר להשתכנע בנכונותו. בפועל, קל יותר להשתמש באינדוקציה.

10.1 סדר מלא ועיקרון הסדר הטוב

הגדרה 34 תהי S קבוצה עם יחס בינרי $\leq$.

1. קבוצה S **מסודרת בסדר מלא** אם עבור כל זוג איברים $x, y \in S$, מתקיים $x \leq y$ או $y \leq x$ או $x = y$.
2. לקבוצה מסודרת בסדר מלא S **חסם תחתון** אם קיים b כך ש $b \leq n$ לכל $n \in S$.
3. לקבוצה מסודרת בסדר מלא S **איבר קטן ביותר** אם קיים $b \in S$ כך ש־$b \leq n$ לכל $n \in S$.

איבר קטן ביותר הוא גם חסם תחתון, אבל cנוסף הuא איבר בתוך הקבוצה.
כל תת־קבוצה של המספרים השלמים היא מסודרת בסדר מלא, למשל, $S_1 = \{8, 3, 19, 5, 6, 23\}$ וקבוצת המספרים הזוגיים $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. חלק מהחסמים התחתונים של S_1 הם $3, 0, -10$. למעשה, כל $b \leq 3$ הוא חסם תחתון עבור S_1. האיבר הקטן ביותר הוא של S_1 הוא 3. ברור שלקבוצה E אין חסם תחתון ובוודאי שאין לה איבר קטן ביותר.
לקבוצת המספרים הרציונליים **החיוביים** מספר אינסופי של חסמים תחתונים (אפס וכל המספרים הרציונליים השליליים), אבל אין לה איבר קטן ביותר כי לכל מספר רציונלי חיובי x, $x/2$ הוא מספר רציונלי חיובי קטן יותר.

הגדרה 35 תהי S קבוצה המסודרת במסדר מלא. S היא **מסודרת היטב** אם **בכל** תת־קבוצה לא ריקה של S קיים איבר קטן ביותר.

הקבוצה S_1 היא מסודרת היטב כי לכל תת־קבוצה לא ריקה קיים איבר קטן ביותר. האיבר הקטן ביותר של S_1 הוא 3, האיבר הקטן ביותר של $\{8, 19, 5\}$ הוא 5, ואתם יכולים לבדוק שלכל אחת מ־63 התת־קבוצות הלא־ריקות של S_1 קיים איבר קטן ביותר. הקבוצה E **אינה**

מסודרת היטב כי E היא תת־קבוצה של עצמה ואין מספר זוגי קטן ביותר. אולם, הקבוצה $E_6 = \{6, 12, 18, \ldots\}$, קבוצת המספרים הזוגיים החיוביים המתחלקים ב־6 היא כן מסודרת היטב כי לכל תת־קבוצה קיים איבר קטן ביותר.

אקסיומה 3 (עיקרון הסדר הטוב) כל תת־קבוצה לא ריקה של המספרים השלמים שיש לה חסם תחתון היא מסודרת היטב.

נשתמש במקרה פרטי של האקסיומה:

אקסיומה 4 בכל תת־קבוצה לא ריקה של המספרים החיוביים קיים איבר קטן ביותר.

10.2 השקילות של עיקרון הסדר הטוב ואינדוקציה מתמטית

משפט 36 עיקרון הסדר הטוב גורר את העיקרון של אינדוקציה מתמטית.

הוכחה אם העיקרון של אינדוקציה מתמטית לא נכון, חייבת להיות תכונה כלשהי $P(n)$, כך ש־$P(1)$ נכונה והצעד האינדוקטיבי נכון (לכל m, $P(m)$ גורר $P(m+1)$), אבל, עבור $n > 1$ כלשהו $P(n)$ אינה נכונה. תהי S קבוצת המספרים השלמים החיוביים k כך ש־$P(k)$ אינה נכונה. הקבוצה S אינה ריקה כי $n \in S$. לפי עיקרון הסדר הטוב, לקבוצה איבר קטן ביותר $b \in S$. לפי ההגדרה של S, $P(b)$ איננה נכונה. אבל $b-1$ קטן מ־b כך ש־$b-1 \notin S$ ולכן $P(b-1)$ נכונה. לפי צעד האינדוקציה, $P(b)$ נכונה וקיימת סתירה. ∎

נדגים את ההוכחה באמצעות דוגמה. תהי $P(n)$ תכונה כך ש־$P(1)$ נכונה (מסומן ב־$+$), צעד האינדוקציה נכון, אבל $P(244)$ לא נכונה (מסומן על ידי $-$). תהי $S = \{244, 57, 102, \ldots\}$ קבוצת המספרים החיוביים k עבורם $P(k)$ לא נכונה. הקבוצה S אינה ריקה כי $244 \in S$. לפי עיקרון הסדר טוב ל־S איבר קטן ביותר 57. אבל, $56 \notin S$ כך ש־$P(56)$ נכונה. לפי צעד האינדוקציה $P(57)$ נכונה וזו סתירה (מסומן על ידי $\mp$).

$P(1)$	$P(2)$	$\cdots$	$P(56)$	$P(57)$	$\cdots$	$P(102)$	$\cdots$	$P(244)$
$+$	$+$	$+$	$+$	$\mp$	$+$	$-$	$+$	$-$

משפט 37 העיקרון של אינדוקציה מתמטית גורר את עיקרון הסדר הטוב.

הוכחה תהי S תת־קבוצה לא־ריקה של המספרים החיוביים. נניח שאין איבר קטן ביותר בקבוצה S. נגדיר את התכונה $P(n)$:

$P(n)$ נכונה אם לכל $k \leq n$, k הוא חסם תחתון של S אבל $k \notin S$.

נוכיח ש־$P(n)$ נכונה לכל המספרים החיוביים, ולכן כל המספרים החיוביים אינם איברים של S, סתירה להנחה ש־S לא ריקה.

טענת בסיס: 1 הוא חסם תחתון של S כי הוא המספר החיובי הקטן ביותר. לפי ההגדרה של S, אין ב־S איבר קטן ביותר, כך ש־$1 \notin S$ ו־$P(1)$ נכונה.

צעד אינדוקטיבי: נניח ש־$P(n)$ נכונה כך ש־n הוא חסם תחתון עבור S, אבל $n \notin S$, כלומר, לכל $k \leq n$, $k < s$ לכל $s \in S$. אזי $n+1 \leq s$ לכל $s \in S$, ולכן $n+1$ הוא חסם תחתון ל־S. אם $n+1 \in S$, $n+1$ הוא איבר קטן ביותר ב־S (כי $k \notin S$ לכל $k \leq n$), סתירה להגדרה של S. מכאן ש־$n+1 \notin S$, כלומר, $P(n+1)$ נכונה. ∎

10.3 אינדוקציה מוזרה ביותר

אנו קושרים אינדוקציה עם הוכחת תכונות של מספרים שלמים ומסמך זה הראה את החשיבות של אינדוקציה מבנית. כאן אנו מביאים הוכחת באינדוקציה על קבוצה מוזרה של מספרים שלמים. האינדוקציה תקפה כי הדרישה היחידה היא שהקבוצה מקיימת את עיקרון הסדר בטוב עם אופרטור יחס כלשהו.

להלן פונקציה רקורסיבית מעל למספרים השלמים:

$$f(x) = \text{if } \; x > 100 \; \text{ then } \; x - 10 \; \text{ else } \; f(f(x+11))\,.$$

עבור מספרים גדולים מ־ 100, חישוב הפונקציה פשוטה ביותר:

$$f(101) = 91, \;\; f(102) = 92, \;\; f(103) = 93, \;\; f(104) = 94\,.$$

מה עם מספרים גדולים או שווים ל־100?

$$\begin{aligned}
f(100) &= f(f(100+11)) = f(f(111)) = f(101) = 91 \\
f(99) &= f(f(99+11)) = f(f(110)) = f(100) = 91 \\
f(98) &= f(f(98+11)) = f(f(109)) = f(99) = 91 \\
&\cdots \\
f(91) &= f(f(91+11)) = f(f(102)) = f(92) = f(f(103)) = f(93) = \cdots \\
&\quad\; f(99) = f(f(110)) = f(100) = f(f(111)) = f(101) = 91 \\
f(90) &= f(f(90+11)) = f(f(101)) = f(91) = 91 \\
f(89) &= f(f(89+11)) = f(f(100)) = f(f(111)) = f(101) = 91\,.
\end{aligned}$$

כפי שאמרה עליסה: "יותר מיותר מוזר!" נשער שעבור כל המספרים השלמים, הפונקציה f שווה לפונקציה g:

$$g(x) = \text{if } \; x > 100 \; \text{ then } \; x - 10 \; \text{ else } \; 91\,.$$

הפונצקיה f הוגדרה לראשונה על ידי John McCarthy, אחד מחלוצי מדעי המחשב, ונקרא פונקצית 91־ של McCarthy.

משפט 38 עבור כל מספר שלם x, $f(x) = g(x)$.

ההוכחה מבוססת על הוכחה ב־Z. Manna. *Mathematical Theory of Computing*, 1974, 411–12, ומיוחס ל־R.M. Burstall.
ההוכחה באינדוקציה מעל לקבוצת המספרים:

$$S = \{x \,|\, x \leq 101\}$$

אם אופרטור היחס $\prec$ המוגדר כך:

$$x \prec y \;\text{ iff }\; y < x\,,$$

כאשר בצד הימני $<$ הוא אופרטור היחס הרגיל מעל למספרים שלמים. הנה סדר המספרים הנובע מהיחס $\prec$:

$$101 \prec 100 \prec 99 \prec 98 \prec 97 \prec \cdots .$$

הקבוצה S עם האופרטור $\prec$ מסודר בסדר טוב כי כל תת־קבוצה של S מכילה איבר קטן ביותר.
הוכחה נוכיח את המשפט בשלושה חלקים.
מקרה 1 $x > 100$. ההוכחה מיידית מההגדרות של f ו־ g.
מקרה 2 $90 \leq x \leq 100$.
טענת הבסיס היא:

$$f(100) = f(f(100 + 11)) = f(f(111)) = f(101) = 91 = g(100)\,,$$

לפי ההגדרה של g לכל המספרים השלמים פחות או שווה ל־100.
הנחת האינדוקציה היא $f(y) = g(y)$ עבור $y \prec x$.
הצעד האינדוקטיבי הוא:

$$\begin{aligned}
f(x) &= f(f(x + 11)) && (10.1)\\
&= f(x + 11 - 10) = f(x + 1) && (10.2)\\
&= g(x + 1) && (10.3)\\
&= 91 && (10.4)\\
&= g(x)\,. && (10.5)
\end{aligned}$$

משוואה 10.1 נכונה מההגדרה של f כי $x \leq 100$. השוויון בין משוואה 10.1 לבין משוואה 10.2 נכון מההגדרה של f כי $x \geq 90$ ולכן $x + 11 > 100$. השוויון בין משוואה 10.2 ומשוואה 10.3 נובע מהנחת האינדוקציה:

$$x \leq 100 \Rightarrow x + 1 \leq 101 \Rightarrow x + 1 \in S \Rightarrow x + 1 \prec x\,.$$

השוויון בין המשוואות 10.3, 10.4, 10.5 נכון מההגדרה של g ו־$x + 1 \leq 101$.

מקרה 3 $x < 90$.

טענת הבסיס היא:

$$f(89) = f(f(100)) = f(f(f(111))) = f(f(101)) = f(91) = 91 = g(89)\,,$$

לפי ההגדרה של g כי $89 < 100$.

הנחת האינדוקציה היא $f(y) = g(y)$ עבור $y \prec x$.

הצעד האינדוקטיבי הוא:

$$\begin{aligned} f(x) &= f(f(x+11)) && (10.6)\\ &= f(g(x+11)) && (10.7)\\ &= f(91) && (10.8)\\ &= 91 && (10.9)\\ &= g(x)\,. && (10.10) \end{aligned}$$

משוואה 10.6 נכונה לפי ההגדרה של f ו־$x < 90 \leq 100$. השוויון בין המשוואות 10.6 ו־ 10.7 נובע מהנחת האינדוקציה:

$$x < 90 \Rightarrow x + 11 < 101 \Rightarrow x + 11 \in S \Rightarrow x + 11 \prec x\,.$$

השוויון בין המשוואות 10.7 ו־ 10.8 נכון לפי ההגדרה של g ו־$x + 11 < 101$. לבסוף, כבר הוכחנו ש־$f(91) = 91$, ולפי ההגדרה, $g(x) = 91$ עבור $x < 90$. ∎

פרק 11

מסקנות

אינדוקציה היא **אקסיומה** שמשתמשים בה לעתים קרובות במתמטיקה. ראינו שאינדוקציה מופיעה בתחפושות רבות היכולות לבלבל, אבל בכל מקרה המושגים הבסיסיים הם אחידים:

- הוכח תכונה עבור מבנים קטנים שהם כל כך פשוטים שההוכחה ברורה מאליו. ייתכן שיהיו מספר טענות בסיס ויש להתייחס אל כולן.
- בדומה להפלת שורה של לבני דומינו, הראה שההנחה שהתכונה נכונה עבור מבנים קטנים יכולה לשמש להוכחת התכונה עבור מבנים גדולים יותר. ייתכן שיהיו מספר צעדי אינדוקציה.
- לפי עיקרון האינדוקציה ניתן עכשיו להסיק שהתכונה נכונה לכל מבנה.

האינדוקציה יכולה להיות מעל למספרים השלמים, מעל למספר הקווים בתרשים גיאומטרי או מעל לנוסחאות לוגיות או אוטומטים.

לעתים השימוש באינדוקציה הוא לא־מפורש ומסתתר מתחת לביטויים כמו "בלי הגבלת הכלליות" או "החלף את כל המופעים של". יש לזהות את השימוש באינדוקציה במקרים אלה גם אם לא רושמים את כל הפרטים.

נספח א'
תרגילי אתגר

בתרגילים אלה נדרשת רק אלגברה ברמה של בית ספר תיכון, אבל התרגילים לא פשוטים.
נסה לפתור אותם בלי להסתכל ברמזים בעמוד הבא.

1.א' התרגילים

תרגיל 32 הנח שיש לך מספר בלתי מוגבל של מטבעות בערכים של 4 ש"ח ו־7 ש"ח. מה המספר הקטן ביותר n המקיים את התכונה הבאה: ניתן לשלם **כל** סכום גדול או שווה ל n ש"ח עם המטבעות האלה?

דוגמה לא ניתן לשלם את הסכום 10 ש"ח, כי לא ניתן לחלק אותו ב־4 או 7 בלבד, וכל צירוף של ערכים אלה יהיה גדול מ־10.

תרגיל 33 **שבר אמיתי** הוא שבר שהמונה שלו קטן מהמכנה שלו. **שבר יסודי** הוא שבר אמיתי שהמונה שלו הוא 1. הוכח שכל שבר אמיתי שווה לסכום של שברים יסודיים **שונים**.

דוגמה קל מאוד לבטא שבר אמיתי כסכום של שברים יסודיים:

$$\frac{4}{5} = \frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5},$$

אבל קשה למצוא סכום של שברים יסודיים שונים:

$$\frac{4}{5} = \frac{16}{20} = \frac{1}{2} + \frac{1}{4} + \frac{1}{20}.$$

תרגיל 34 הוכח את הנוסחה של Binet למספרי פיבונצ'י:

$$f_n = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}}, \qquad \phi = \frac{1+\sqrt{5}}{2},\ \bar{\phi} = \frac{1-\sqrt{5}}{2}.$$

תרגיל 35 הוכח:

$$f_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots.$$

2.א' רמזים

תרגיל 32

- הנח שיכולת לבנות כל המספרים הזוגיים (מעל למספר מסויים). הראה שניתן לבנות את כל המספרים (מעל למספר מסויים).
- אם n מתחלק ב־4, האם ניתן לבנות את n?
- מצא את המספר הגדול ביותר k שכנראה לא ניתן לבנות.
- הראה באמצעות אינדוקציה שניתן לבנות n, עבור כל $n \geq k+1$, n זוגי ו־n לא ניתן לחלוקה ב־4.

תרגיל 33

- מהי טענת הבסיס הפשוטה?
- עבור $\frac{a}{b}$, כאשר $a > 1$, יהי

$$\frac{1}{q} < \frac{a}{b}\,.$$

אזי:

$$\frac{a}{b} = \frac{1}{q} + \left(\frac{a}{b} - \frac{1}{q}\right).$$

עכשיו השתמש באינדוקציה.

- הראה שאם $\frac{1}{q}$ הוא השבר היסודי הגודל ביותר שהוא פחות מ־$\frac{a}{b}$ כך ש:

$$\frac{a}{b} < \frac{1}{q-1}\,,$$

אזי כל השברים היסודיים שונים.

תרגיל 34 הוכח $\phi^2 = \phi + 1$ ו־$\bar{\phi}^2 = \bar{\phi} + 1$.

תרגיל 35 הוכח את החוק של Pascal:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

נספח ב'

פתרונות

1.

$$\sum_{i=1}^{4} i = \sum_{i=1}^{3} i + 4 \overset{\bullet}{=} \frac{3(3+1)}{2} + 4 = \frac{20}{2} = \frac{4(4+1)}{2}\,.$$

2. טענת בסיס: $1^2 = 1 = \frac{1}{6} \cdot 2 \cdot 3$. צעד אינדוקטיבי:

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&\overset{\bullet}{=} \frac{n}{6}(n+1)(2n+1) + (n+1)^2 \\
&= \frac{(n+1)}{6}(n(2n+1) + 6(n+1)) \\
&= \frac{(n+1)}{6}(2n^2 + 7n + 6) \\
&= \frac{(n+1)}{6}(n+2)(2n+3) \\
&= \frac{(n+1)}{6}((n+1)+1)(2(n+1)+1)\,.
\end{aligned}$$

3. טענת בסיס: $2 \cdot 1! = 2 \geq 2^1 = 2$. צעד אינדוקטיבי:

$$2(n+1)! = 2n!(n+1) \overset{\bullet}{\geq} 2^n(n+1) \geq 2^n(2) = 2^{n+1}\,,$$

בגלל ש־$n \geq 1$ ולכן $n+1 \geq 2$.

4. טענת בסיס: $1 \cdot 2 \cdot 3 = 6$ מתחלק ב־3. צעד אינדוקטיבי: לפי הנחת האינדוקציה $n(n+1)(n+2)$ מתחלק ב־3. אם $(n+1)$ או $(n+2)$ מתחלק ב־3. גם

$$(n+1)((n+1)+1)((n+1)+2)$$

מתחלק ב־3. אחרת, n מתחלק ב־3 ו־$n = 3k$. מכאן ש:

$$(n+1)+2 = n+3 = 3k+3 = 3(k+1)$$

מתחלק ב־3.

5. טענת בסיס: $1^3 - 1 = 0$ מתחלק ב־6. צעד אינדוקטיבי:

$$n^3 - n = n(n^2-1) = n(n+1)(n-1) = (n-1)n(n+1)\,.$$

לפי תרגיל 4, אחד מתוך $(n-1), n, (n+1)$ מתחלק ב־3. אם $n-1$ מתחלק ב־3 אז לפי משפט 6 $n(n+1)$ מתחלק ב־2, ולכן המכפלה מתחלקת ב־6. באופן דומה, אם $n+1$ מתחלק ב־3 אז $(n-1)n$ מתחלק ב־2, ולכן המכפלה מתחלקת ב־6. לבסוף, אם n מתחלק ב־3, או ש־n הוא גם זוגי ולכן מתחלק ב־6, או שהוא אי־זוגי וגם $n-1$ ו־$n+1$ זוגיים ומתחלקים ב־2, כך שהמכפלה מתחלקת ב־6.

6. טענת בסיס: עבור $n = 1$, ברור שלא ניתן לשים $2 = 1+1$ יונים בתא אחד כך שיש לכל היותר יונה אחת בתא. צעד אינדוקטיבי: נתונים $n+1$ יונים ו־n תאים. שים יונה אחת בתא שרירותי. אסור לשים יונה נוספת באותו תא, לכן נשארו לנו n יונים שיש לשים ב־$n-1$ תאים. לפי הנחת האינדוקציה הדבר בלתי אפשרי.

7. נבדוק את האי־שוויון למספר ערכים קטנים:

$$\begin{aligned}
2^1 = 2 &\geq 1^2 = 1\,,\\
2^2 = 4 &\geq 2^2 = 4\,,\\
2^3 = 8 &\not\geq 3^2 = 9\,,\\
2^4 = 16 &\geq 4^2 = 16\,,\\
2^5 = 32 &\geq 5^2 = 25\,.
\end{aligned}$$

נראה שהנוסחה נכונה עבור כל מספר פרט ל־$n = 3$. אז ניקח בטענת הבסיס את הערך $n = 4$.

הצעד האינדוקטיבי הוא:

$$2^{n+1} = 2^n \cdot 2 \overset{\bullet}{\geq} n^2 \cdot 2 = n^2 + n^2 \overset{?}{\geq} n^2 + 2n + 1 = (n+1)^2\,.$$

הצעד האינדוקטיבי נכון עבור n כאשר $n^2 \geq 2n+1$, כלומר עבור $n > 2$.

מכאן אנו מבינים מדוע אי־אפשר להוכיח את הנוסחה באינדוקציה עבור טענת בסיס לערך $n = 2$. הצעד האינדוקטיבי מ־$n = 2$ ל־$n+1 = 3$ לא עובד.

8. טענת בסיס: $2 = 1(1+1)$. הצעד האינדוקטיבי הוא:

$$\sum_{i=1}^{n+1} 2i = \sum_{i=1}^{n} 2i + 2(n+1) \overset{\bullet}{=} n(n+1) + 2(n+1) = (n+1)(n+2)\,.$$

9. הוכחת טענת הבסיס זהה להוכחה עבור משפט 10. הצעד האינדוקטיבי הוא:

$$\begin{aligned}\overbrace{kkk}^{3^{n+1}} &= \overbrace{kkk}^{3^n}\cdot\overbrace{kkk}^{3^n}\cdot\overbrace{kkk}^{3^n}\\ &\overset{\bullet}{=} (3^n m)10^{2\cdot 3n}+(3^n m)10^{3n}+(3^n m)\\ &= (3^n m)(10^{2\cdot 3n}+10^{3n}+1)\,.\end{aligned}$$

חילוק של כל חזקה של 10 על ידי 3 משאיר שארית של 1, לכן $(10^{2\cdot 3n}+10^{3n}+1)$ מתחלק ב־3 ו־ $(3^n m)(10^{2\cdot 3n}+10^{3n}+1)$ מתחלק ב־3^{n+1}.

10. טענת בסיס: $a_1 = 5 = 3+2^1$, $a_2 = 7 = 3+2^2$. הצעד האינדוקטיבי הוא:

$$\begin{aligned}a_{n+1} &= 3a_{n+1-1}-2a_{n+1-2}\\ &\overset{\bullet}{=} 3(3+2^n)-2a_{n+1-2}\\ &\overset{\bullet}{=} 3(3+2^n)-2(3+2^{n-1})\\ &= 9+3\cdot 2^n-6-2^n\\ &= 3+2\cdot 2^n\\ &= 3+2^{n+1}\,.\end{aligned}$$

11. יהי $S=\{x=an_1+bn_2 : x>0\}$. בגלל ש־S היא קבוצה לא ריקה, לפי עיקרון הסדר הטוב קיים איבר קטן ביותר $d\in S$, כאש $d=a'n_1+b'n_2>0$. לפי אלגוריתם החלוקה:

$$\begin{aligned}n_1 &= qd+r, \quad \text{for } 0\le r<d\\ r &= n_1-qd\\ &= (1-qa')n_1+(-b'q)n_2\,,\end{aligned}$$

כך ש־$r\in S$. אבל לא ייתכן $0<r<d$ כי d הוא האיבר הקטן ביותר ב־S, ולכן $r=0$ ו־$d\mid n_1$. הוכחה דומה מראה ש־$d\mid n_2$, ולכן d הוא מחלק משותף של n_1,n_2. אם c הוא מחלק משותף כלשהו של n_1,n_2, $d=(a'n_1+b'n_2)$ ומכאן ש־$c\mid d=\gcd(n_1,n_2)$.

12. יהי $p\mid n_1n_2$ והנח ש־p **לא מחלק** את n_1. מכאן ש־p ו־n_1 הם ראשוניים אחד לשני. לפי הזהות של Bezout קיימים a,b כך ש־$an_1+bp=1$. נכפיל ב־n_2 ונקבל:

$$an_1n_2+bpn_2=n_2\,.$$

לפי ההנחה $p\mid n_1n_2$ אז $p\mid an_1n_2$ וברור ש־$p\mid bpn_2$ ולכן $p\mid n_2$.

13. טענת בסיס: $a_1=2=1(1+1)$. הצעד האינדוקטיבי הוא:

$$\sum_{i=1}^{n+1}a_i=\sum_{i=1}^{n}a_i+a_{n+1}\overset{\bullet}{=}n(n+1)+a_{n+1}=n(n+1)+2(n+1)=(n+1)(n+2).$$

נשמתמש במשפט 16 כדי להציב $2(n+1)$ במקום a_{n+1}.

14. טענת בסיס: $f_5 = 5$ מתחלק ב־5. הצעד האינדוקטיבי הוא:

$$\begin{aligned} f_{5(n+1)} &= f_{5n+5} \\ &= f_{5n+4} + f_{5n+3} \\ &= 2f_{5n+3} + f_{5n+2} \\ &= 3f_{5n+2} + 2f_{5n+1} \\ &= 5f_{5n+1} + 3f_{5n}\,. \end{aligned}$$

הגורם הראשון $5f_{5n+1}$ מתחלק ב־5 ולפי הנחת האינדוקציה גם $3f_{5n}$ מתחלק ב־5.

15. טענות בסיס: $f_1 = 1 < (\frac{7}{4})^1$ ו־$f_2 = 1 < (\frac{7}{4})^2 = \frac{49}{16}$. הצעד האינדוקטיבי הוא:

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &\overset{\bullet}{<} \left(\frac{7}{4}\right)^n + f_{n-1} \\ &\overset{\bullet}{<} \left(\frac{7}{4}\right)^n + \left(\frac{7}{4}\right)^{n-1} \\ &= \left(\frac{7}{4}\right)^{n-1} \cdot \left(\frac{7}{4} + 1\right) \\ &< \left(\frac{7}{4}\right)^{n-1} \cdot \left(\frac{7}{4}\right)^2 \\ &= \left(\frac{7}{4}\right)^{n+1}, \end{aligned}$$

בגלל ש־

$$\left(\frac{7}{4} + 1\right) = \frac{11}{4} = \frac{44}{16} < \frac{49}{16} = \left(\frac{7}{4}\right)^2.$$

16. טענת בסיס ($n = 2$): $F_2 = 2^{2^2} + 1 = 17$.

הנחת האינדוקציה: $F_n = 10k_n + 7$.

הצעד האינדוקטיבי:

$$\begin{aligned} F_{n+1} &= 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1 \\ &= \left(\left(2^{2^n} + 1\right) - 1\right)^2 + 1 \\ &\overset{\bullet}{=} (10k_n + 7 - 1)^2 + 1 = (10k_n + 6)^2 + 1 \\ &= 100k_n^2 + 120k_n + 36 + 1 \\ &= 10(10k_n^2 + 12k_n + 3) + 6 + 1 \\ &= 10k_{n+1} + 7\,. \end{aligned}$$

17. טענת בסיס:

$$5 = F_1 = \prod_{k=0}^{0} F_k + 2 = F_0 + 2 = 3 + 2\,.$$

הצעד האינדוקטיבי:

$$\begin{aligned}
\prod_{k=0}^{n} F_k &= (\prod_{k=0}^{n-1} F_k)F_n \\
&\overset{\bullet}{=} (F_n - 2)F_n \\
&= (2^{2^n} + 1 - 2)(2^{2^n} + 1) \\
&= 2^{2^{n+1}} - 1 \\
&= (2^{2^{n+1}} + 1) - 2 \\
&= F_{n+1} - 2 \\
F_{n+1} &= \prod_{k=0}^{n} F_k + 2\,.
\end{aligned}$$

18. (א) טענות בסיס: אין סוגריים בתוך משתנה או קבוע. יש ארבעה צעדי אינדוקציה, אחד לכל פעולה, אבל ניתן להוכיח אותם ביחד. עבור הביטוי $E = (E_1 \,\mathrm{op}\, E_2)$ עם הפעולה op, לפי הנחת האינדוקציה, מספרי סוגריים השמאליים n_1^l, n_2^l ומספרי הסוגריים הימניים n_1^r, n_2^r ב־E_1, E_2, בהתאמה, שווים: $n_1^l = n_2^l$ ו־$n_1^r = n_2^r$. עבור E:

$$n^l = n_1^l + n_2^l + 1 \overset{\bullet}{=} n_1^r + n_2^r + 1 = n^r\,.$$

(ב) טענות הבסיס כמו ב־(א). עבור $E = |(|E_1|\mathrm{op}|E_2|)|$, קיימים צעדי אינדוקציה לכל אחד משש המקומות הסומנים ב־|. עבור כל אחד מהמקומות האלו, הערכים של n^l ו־n^r הם:

n^l	0	1	$n_1^l + 1$	$n_1^l + 1$	$n_1^l + n_2^l + 1$	$n_1^l + n_2^l + 1$
n^r	0	0	n_1^r	n_1^r	$n_1^r + n_2^r$	$n_1^r + n_2^r + 1$

לפי הנחת האינדוקציה, $n_1^l \geq n_1^r$ ו־$n_2^l \geq n_2^r$, כך ש־$n^l \geq n^r$ בכל המקומות.

19. טענת הבסיס: $\cos\theta \overset{?}{=} \frac{\sin 2\theta}{2\sin\theta}$. כן, כי $\sin 2\theta = 2\cos\theta\sin\theta$. הצעד האינדוקטיבי הוא:

$$\begin{aligned}
\cos\theta\cdots\cos 2^n\theta &= (\cos\theta\cdots\cos 2^{n-1}\theta)\cdot\cos 2^n\theta \\
&\overset{\bullet}{=} \frac{\sin 2^n\theta}{2^n\sin\theta}\cdot\cos 2^n\theta \\
&= \frac{1}{2^n\sin\theta}\cdot\cos 2^n\theta\sin 2^n\theta \\
&= \frac{1}{2^n\sin\theta}\cdot\frac{\sin 2\cdot 2^n\theta}{2} \\
&= \frac{\sin 2^{n+1}\theta}{2^{n+1}\sin\theta}\,.
\end{aligned}$$

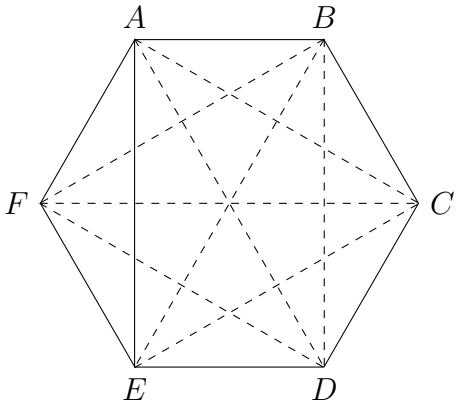
20. טענת הבסיס עבור $n=1$ פשוטה ביותר. הצעד האינדוקטיבי הוא:

$$\begin{aligned}
(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)\cdot(\cos\theta + i\sin\theta)^n \\
&\overset{\bullet}{=} (\cos\theta + i\sin\theta)\cdot(\cos n\theta + i\sin n\theta) \\
&= (\cos\theta\cos n\theta - \sin\theta\sin n\theta) + i(\cos\theta\sin n\theta + \sin\theta\cos n\theta) \\
&= \frac{1}{2}[(\cos(1-n)\theta + \cos(1+n)\theta) - \\
&\qquad (\cos(1-n)\theta - \cos(1+n)\theta) + \\
&\qquad i[(\sin(1+n)\theta - \sin(1-n)\theta) + \\
&\qquad (\sin(1+n)\theta + \sin(1-n)\theta)]] \\
&= \cos(n+1)\theta + i\sin(n+1)\theta\,.
\end{aligned}$$

21. טענת בסיס: עבור מרובע $n=4$, קיימים $\frac{1}{2}(4)(4-3)=2$ אלכסונים. עבור הצעד האינדוקטיבי לפוליגון עם $n+1$ צלעות, צייר אלכסון בין שני צמתים שהם שכנים של אותו צומת k. לפי הנחת האינדוקציה, קיימים $\frac{1}{2}n(n-3)$ אלכסונים בפוליגון עם n צלעות שנוצר. למספר זה יש להוסיף את האלכסון שצוייר ועוד $n+1-3$ אלכסונים מ־k. התוצאה היא:

$$\frac{1}{2}n(n-3)+1+(n+1-3)=\frac{1}{2}(n^2-n-2)=\frac{1}{2}(n+1)(n-2)\,.$$

איור 1.ב' מראה את הבנייה עבור משושה עם $\frac{1}{2}(6)(6-3)=9$ אלכסונים.

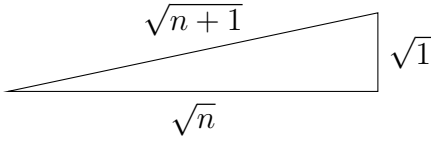


איור 1.ב': אלכסונים נחתכים

22. טענת בסיס: סכום הזוויות הפנימיות של משולש הוא $180(3-2)=180$. עבור הצעד האינדוקטיבי צייר קו כדי לייצר פוליגון עם n צלעות ומשולש. אז:

$$180(n-2)+180=180((n+1)-2)\,.$$

23. עבור טענת הבסיס, קו באורך $\sqrt{1}=1$ נתון. הצעד האינדוקטיבי מוצג באיור 2.ב'. לפי הנחת האינדוקציה, ניתן לבנות קווים באורך $\sqrt{1}$ ו־$\sqrt{n}$ וניתן לבנות אותם ניצבים אחד לשני. לפי משפט פיתגורס, אורך היתר הוא $\sqrt{n+1}$.



איור 2.ב': בניית קו באורך $\sqrt{n+1}$

24. טענת בסיס: עלה הוא צומת בודד עם גובה אפס: $1=1-2^{0+1}\leq 1$. הצעד האינדוקטיבי הוא: נניח ש־$n_h\leq 2^{h+1}-1$ והראה ש־$n_{h+1}\leq 2^{(h+1)+1}-1$. כפי שניתן לראות באיור 4.3, תת־עץ השמאלי ותת־עץ הימני של שורש העץ **אינם** באותו גובה. אולם, $h+1=\max(h_l,h_r)+1$, כי הגובה של השורש הוא אחד יותר מהגובה של התת־עץ עם הגובה המקסימלי. לפי הנחת האינדוקציה:

$$\begin{aligned} n_l &\leq 2^{h_l+1}-1\leq 2^{\max(h_l,h_r)+1}-1=2^{h+1}-1\\ n_r &\leq 2^{h_r+1}-1\leq 2^{\max(h_l,h_r)+1}-1=2^{h+1}-1\,. \end{aligned}$$

ולכן:

$$n_{h+1}=n_l+n_r+1\overset{\bullet}{\leq}(2^{h+1}-1)+(2^{h+1}-1)+1=2^{(h+1)+1}-1\,.$$

25. טענת בסיס: קשת אחת נושקת לשני צמתים וקיים שטח אחד שהוא כל המישור: $1+2=2+1$. יש שני צעדי אינדוקטיביים: אם צומת נושק לקשת אחת, מחק את הצומת והקשת. השוויון $s+(n+1)=(e+1)+2$ נובע מהנחת האינדוקציה. אם אין צמתים כאלה אז כל קשת הוא חלק ממסלול מעגלי. מחיקת הקשת משאירה את מספר הצמתים ללא שינוי, מורידה ב־1 את מספר הקשתות ומורידה את מספר השטחים גם הוא ב־1. השוויון $(s-1)+n=(e-1)+2$ נובע מהנחת האינדוקציה.

26. אם n מתחלק ב־3 סיימנו. אחרת, $n=3k+1$ או $n=3k+2$. מכאן:

$$n+1=3k+2+1=3k+3$$

או:

$$n+2=3k+1+2=3k+3$$

מתחלק ב־3.

27. הוכחה ללא אינדוקציה:

$$\begin{aligned}(x-1)\sum_{i=0}^{i=n} x^i &= x\sum_{i=0}^{i=n} x^i - \sum_{i=0}^{i=n} x^i \\ &= x^{n+1} + \sum_{i=1}^{i=n}(x^i - x^i) - x^0 \\ &= x^{n+1} - 1\,.\end{aligned}$$

הוכחה באינדוקציה: טענת בסיס: $x^0 - 1 = 0$ מתחלק על ידי כל פולינום. הצעד האינדוקטיבי:

$$x^{n+1} - 1 = x^{n+1} - x^n + x^n - 1 = x^n(x-1) + (x^n - 1)\,.$$

ברור שהגורם הראשון מתחלק ב־$x-1$ ולפי הנחת האינדוקציה גם הגורם השני מתחלק ב־$x-1$.

28. בצעד האינדוקטיבי עבור $n+1$, השתמשנו ב־$a^n = 1$ שהיא נוסחה נכונה, אבל השתמשנו גם ב־$a^{n-1} = 1$ u־$a^{n-2} = 1$, שאינן נכונות אלא אם נוכיח טענות בסיס נוספות $a^{-1} = 1$ ו־$a^{-2} = 1$, לכל $a \geq 1$. אולם, שתי הטענות אינן נכונות.

29. השתמשנו בהנחת האינדוקציה עבור קבוצות שונות עם n איברים: $s_1, s_2, \ldots, s_{n-1}, s_n$ ו־$s_1, s_2, \ldots, s_{n-1}, s_{n+1}$. אולם, קבוצות אלו שונות רק אם $n \geq 3$ ולא הוכחנו טענת בסיס עבור $n = 2$. כמובן שזה בלתי אפשרי כי ייתכן שתלמיד s_1 צבע את שיערו ירוק ותלמידה s_2 צבעה את שיערה כחול.

30. הנוסחה $A = p$ ספיקה אם ורק אם הנוסחה

$$A' = (p \vee q \vee r) \ \wedge \ (p \vee \neg q \vee r) \ \wedge \ (p \vee q \vee \neg r) \ \wedge \ (p \vee \neg q \vee \neg r).$$

ספיקה עם אטומים חדשים q ו־r. ברור שאם A ספיקה אז גם A' על ידי הצבת T ב־p. מה קורה אם A' ספיקה? אם ההצבה כוללת הצבה של T ל־p גם A ספיקה. אחרת p קיבל הצבה של F. מה עם ההצבות ל־q ו־r? אחד מ:

$$q \vee r, \neg q \vee r, \vee q \vee \neg r, \neg q \vee \neg r$$

יקבל ערך F. לכן A' ספיקה רק אם p מקבל הצבה T. הוכחה דומה קיימת עבור הליטרל $\neg p$.

31. יהי $A \stackrel{*}{\Rightarrow} w$. קיימים שלושה מקרים בהתאם לכלל היצירה הראשון בגזירה. אם הכלל היה $A \to a$, ברור ש־$\#a = \#b + 1$ כי $1 = 0 + 1$. אם הכלל היה $A \to aS$, לפי הנחת האינדוקציה בנוסחה 7.1, $S \stackrel{*}{\Rightarrow} w'$ כך ש־$\#a = \#b$ ב־w'. לכן $\#a = \#b + 1$ ב־w. אם $A \to bAA$, אז נשתמש פעמיים בהנחת האינדוקציה 7.2 ונקבל $AA \stackrel{*}{\Rightarrow} w'$

כך ש־$\#a = \#b + 2$ ב־w', ולכן $\#a = \#b + 1$ ב־w. ההוכחה עבור נוסחה 7.3 היא סימטרית.

ההוכחה בכיוון הנגדי: יהי $S \overset{*}{\Rightarrow} w$ כך ש־$\#a = \#b$ ב־w. נניח שהכלל הראשון בגזירה היה $S \to aB$. מכאן של המחרוזת w' שנגזרת מ־B יש $\#a + 1 = \#b$. לפי הנחת האינדוקציה בנוסחה 7.3, קיימת גזירה $B \overset{*}{\Rightarrow} w'$, כך שיש גזירה $S \to aB \overset{*}{\Rightarrow} w$. המקרה שהגזירה הראשונה היא $S \to bA$ דומה, כמו ההוכחות של הכיוונים הנגדיים של הנוסחות 7.2 ו 7.3.

32. למה 2: לכל i, האיברים ב־B_i ממויינים **וגם** כל האיברים ב־A_i גדולים או שווים לכל האיברים ב־B_i.

טענת בסיס: B_0 היא קבוצה ריקה והטענה ריקה. הצעד האינדוקטיבי: הנחת האינדוקציה היא שלמה 2 נכונה עבור A_i ו־B_i. לכן, כאשר מוסיפים את האיבר a_i לסוף של B_i כדי לקבל B_{i+1}, הוא גדול או שווה לכל האיברים ב־B_i, ומכאן ש־B_{i+1} ממויינת. כל האיברים של A_{i+1} גדולים או שווים לכל האיברים של B_{i+1}: (1) לפי הנחת האינדוקציה האם כבר היו גדולים אל שווה לכל האיברים ב־B_i, ו־(2) a_i היה האיבר הקטן ב־A_i כך שהם גדולים או שווים ל־a_i שהתווסף ל־B_i כדי לקבל B_{i+1}.

33. טענת בסיס: הערך התחילי של המשתנה sem הוא 1 ו־ $\#CS = 0$ כי אין אף תהליך בקטע הקריטי. לפי הנחת האינדוקציה, נניח שהנוסחה נכונה. היא יכולה להפוך ללא נכונה רק אם ערכים של $\#CS$ או sem משתנים. התהליכים סימטריים, ולכן ללא הגבלת הכלליות אפשר לבדוק רק פקודות מתהליך p. שגיאה יכולה לקרות רק אם ביצוע הפקודה p1 או הפקודה p3. ביצוע p1 מוסיף 1 לערך של $\#CS$ אבל גם מחסיר 1 מערכו של sem. באופן דומה, ביצוע של p3 מחסירה 1 מערכו של $\#CS$ אבל מוסיף 1 לערכו של sem.

34. אם n אי־זוגי, $n - 7$ זוגי, ולכן אם ניתן לבנות מספרים זוגיים גדולים ככל שנרצה, נוכל לבנות מספרים אי־זוגיים גדולים ככל שנרצה על ידי הוספת מטבע אחד של 7 ש"ח. ברור, שניתן לבנות מספרים שהם כפולות של 4, $n = 4k$, מ־k מטבעות של 4 ש"ח. לכן, כל מה שנשאר הוא להוכיח שניתן לבנות מספר זוגי שאינו כפולה של 4.

קל להראות שהמספרים $1, 2, 3, 5, 6, 9, 10, 11, 13, 15, 17$ לא ניתנים לבנייה. למשל, 17 אי־זוגי, לכן חייבים להשתמש במטבע של 7, ולהשתמש בו פעם אחד בלבד כי לא ניתן לייצר $17 - 2 \cdot 7 = 3$. אבל $17 - 7 = 10$ לא מתחלק ב־4 ולכן הבנייה בלתי אפשרית.

נוכיח באינדוקציה שניתן לבנות כל מספר זוגי גדול או שווה ל־18 שלא מתחלק ב־4.

טענת בסיס: $18 = 2 \cdot 7 + 4$.

מספרים זוגיים שלא ניתן לחלק ב־4 ניתן לבטא כ־$2(2k + 1)$. הצעד האינדוקטיבי:

$$2(2(n + 1) + 1) = 4n + 6 = (4n + 2) + 4.$$

לפי הנחת האינדוקציה, ניתן לבנות $4n + 2 = 2(2n + 1)$. נוסיף מטבע אחד של 4 ונקבל $2(2(n + 1) + 1)$.

35. טענת הבסיס: השבר $\frac{a}{b}$ הוא שבר יסודי $a=1$. הצעד האינדוקטיבי הוא שהטענה נכונה עבור כל שבר שהוא קטן מ־$\frac{a}{b}$. לפי הנחת האינדוקציה והבחירה של $\frac{a}{b} > \frac{1}{q}$, ניתן לבטא את

$$\left(\frac{a}{b}-\frac{1}{q}\right) < \frac{a}{b}$$

כסכום של שברים יסודיים. מכאן שניתן לבטא את:

$$\frac{a}{b} = \frac{1}{q} + \left(\frac{a}{b}-\frac{1}{q}\right)$$

כסכום של שברים יסודיים.

אם $\frac{1}{q}$ הוא השבר היסודי **הגדול ביותר** שהוא פחות מ־$\frac{a}{b}$, אזי $\frac{a}{b} > \frac{1}{q-1}$, ולכן $aq-b<a$ ו־

$$\left(\frac{a}{b}-\frac{1}{q}\right) = \frac{aq-b}{bq} = (aq-b)\cdot\frac{1}{b}\cdot\frac{1}{q} < a\cdot\frac{1}{b}\cdot\frac{1}{q} < \frac{1}{q}\,,$$

כי $\frac{a}{b}$ הוא שבר אמיתי. מכאן שאף אחד מהשברים היסודים בסכום המבטא את $\left(\frac{a}{b}-\frac{1}{q}\right)$ יכול להיות גדול או שווה ל־$\frac{1}{q}$.

36. נוכיח קודם ש־$\phi^2 = \phi + 1$:

$$\begin{aligned}
\phi^2 &= \left(\frac{1+\sqrt{5}}{2}\right)^2 \\
&= \frac{1}{4}+\frac{2\sqrt{5}}{4}+\frac{5}{4} \\
&= \frac{2}{4}+\frac{2\sqrt{5}}{4}+\frac{4}{4} \\
&= \frac{1+2\sqrt{5}}{2}+1 \\
&= \phi+1\,.
\end{aligned}$$

ההוכחה של $\bar{\phi}^2 = \bar{\phi}+1$ דומה.

טענת הבסיס עבור $n=1$ היא:

$$\frac{\phi^1-\bar{\phi}^1}{\sqrt{5}} = \frac{(1+\sqrt{5})/2-(1-\sqrt{5})/2}{\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1\,.$$

נניח את הנחת האינדוקציה לכל $k \le n$. הצעד האינדוקטיבי הוא:

$$\begin{aligned}
\phi^n-\bar{\phi}^n &= \phi^2\phi^{n-2}-\bar{\phi}^2\bar{\phi}^{n-2} \\
&= (\phi+1)\phi^{n-2}-(\bar{\phi}+1)\bar{\phi}^{n-2} \\
&= (\phi^{n-1}-\bar{\phi}^{n-1})+(\phi^{n-2}-\bar{\phi}^{n-2}) \\
&\overset{\bullet}{=} \sqrt{5}f_{n-1}+\sqrt{5}f_{n-2}\,,
\end{aligned}$$

לכן

$$\frac{\phi^n - \bar{\phi}^n}{\sqrt{5}} = f_{n-1} + f_{n-2} = f_n \,.$$

37. הוכחת החוק של Pascal:

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} \\
&= \frac{n![(k+1)+(n-k)]}{(k+1)!(n-k)!} \\
&= \frac{n!(n+1)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} \\
&= \binom{n+1}{k+1} .
\end{aligned}$$

טענת בסיס:

$$f_1 = 1 = \binom{1}{0} = \frac{1!}{0!(1-0)!} \,.$$

הצעד האינדוקטיבי הוא:

$$\begin{aligned}
f_{n-1} + f_{n-2} &\overset{\bullet}{=} \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \binom{n-4}{3} + \cdots \\
&\qquad\qquad \binom{n-2}{0} + \binom{n-3}{1} + \binom{n-4}{2} + \cdots \\
&= \binom{n-1}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots \\
&= \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots .
\end{aligned}$$

השוויון האחרון משתמש ב־:

$$\binom{k}{0} = \frac{k!}{0!(k-0)!} = 1$$

עבור כל k.