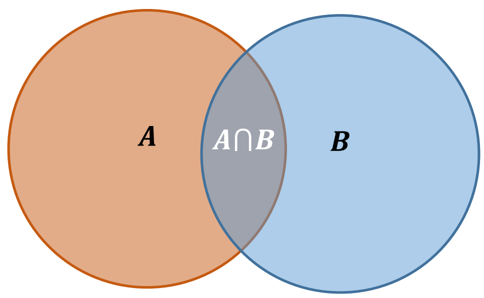
עקרון ההכלה-הפרדה (INCLUSION-EXCLUSION)

נניח שנתונות שתי קב' סופיות A, B ואנחנו רוצים לחשב את $|A \cup B|$. אם הן זרות (כלומר $A \cap B = \emptyset$), אז:

$$|A \cup B| = |A| + |B|$$

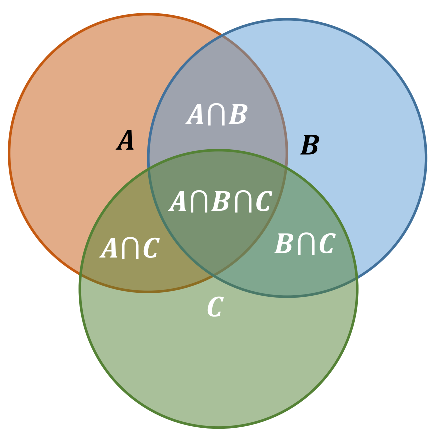
(זהו כלל החיבור). באופן כללי, התמונה היא כזו:



אז בשביל שלא לספור את $A \cap B$ פעמיים:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

אם יש שלוש קב' A, B, C, התמונה היא כזו:



כאן אנו רוצים לא לספור את $A \cap B, A \cap C, B \cap C$ יותר מפעם אחת, אבל לא להחסיר את $A \cap B \cap C$ יותר מדי פעמים, אז:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

טענה – נוסחת ההכלה-הפרדה ל-n קב': תהיינה $A_1, \dots, A_n$ קב' סופיות. אז:

$$\left|\bigcup_{k=1}^{n} A_n\right| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \cdots + (-1)^{l+1} \sum_{1\le i_1<i_2<\cdots<i_l\le n} |A_{i_1} \cap A_{i_2} \cap \ \dots \cap A_{i_l}| + \cdots + (-1)^{n+1} \left|\bigcap_{1\le i\le n} A_i\right|$$

הוכחה: אנחנו נראה שכל איבר של $\bigcup_{k=1}^{n} A_n$ נספר נטו בדיוק פעם אחת באגף ימין. יהי $x \in \bigcup_{k=1}^{n} A_n$, אז x שייך ל-k מבין הקב' $A_1, \dots, A_n$. נניח בהג"כ כי x שייך לקב' $A_1, \dots, A_k$. נשים לב ש- $x \in A_{i_1} \cap A_{i_2} \cap \ \dots \cap A_{i_l}$ אם ורק אם $1 \le l \le k$ ו- $1 \le i_1 < \cdots < i_l \le k$. עבור $1 \le l \le k$ נתון, מס' הבחירות של $i_1, \dots, i_l$ המקיימות את הנ"ל הוא $\binom{k}{l}$. כלומר x נספר בשורה ה-l-ית של הנוסחא $\binom{k}{l}$ פעמים. בהתחשב בסימנים, מס' הפעמים נטו ש-x נספר באגף ימין הוא:

$$\sum_{l=1}^{k} (-1)^{l+1} \binom{k}{l} = \underbrace{\sum_{l=0}^{k} (-1)^{l+1} \binom{k}{l}}_{0} - \underbrace{(-1)^1 \binom{k}{0}}_{-1} = 1$$

כמו שרצינו להראות.

חזרה על מושגים בסיסיים מתורת המספרים

בכל הדיון להלן מדובר על מספרים טבעיים.

הגדרה: אנחנו אומרים ש-m **מחלק את** n, וכותבים $m|n$, אם קיים k כך ש-$n = mk$.

הגדרה: אנחנו אומרים ש-p **הוא ראשוני** אם $p > 1$, ואין לו מחלקים מלבד p ו-עצמו.

טענה (ללא הוכחה)**:** כל מס' $n > 1$ ניתן להצגה בצורה:

$$n = p_1^{k_1} \dots p_t^{k_t}$$

כאשר $p_1, \dots, p_t$ ראשוניים.

הגדרה: **המחלק המשותף המקסימלי** של n, m, המסומן (n, m), הוא המספר הגדול ביותר המחלק את שניהם.

הגדרה: **הכפולה המשותפת המינימלית** של n, m, המסומנת $[n, m]$, הוא המספר הגדול ביותר המחלק את שניהם.

הערה: מתקיים $(m, n)[m, n] = mn$.

טענה: לכל מס' a:

$$a|(m,n) \quad \Leftrightarrow \quad a|m, a|n$$

$$[m,n]|a \quad \Leftrightarrow \quad m|a, n|a$$

הגדרה: שני מס' m, n נקראים **זרים** אם $(m, n) = 1$ או במילים אחרות, אין מס' ראשוני p המחלק את שניהם. עוד תנאי שקול, $[m, n] = mn$.

הגדרה: **פונ' אוילר** φ היא הפונ' המחזירה לכל n את המס' בין $1, \dots, n$ שזרים ל-n.

למשל: $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2$. באופן כללי, עבור p ראשוני, $\varphi(p) = p - 1$.

עבור חזקה של ראשוני, $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$ (כל המס' האפשריים ללא אלה שאינם זרים, כלומר, כל הכפולות של p). כעת נחשב את $\varphi(n)$ באופן הכללי ביותר. יהי $n = p_1^{k_1} \dots p_t^{k_t}$. עבור $i = 1, \dots, t$, נסמן A_i=קב' המספרים בין $1, \dots, n$ המתחלקים ב-p_i. אז $A_1 \cup A_2 \cup \dots \cup A_t$ היא קב' המספרים בין $1, \dots, n$ שאינם זרים ל-n. לכן:

$$\varphi(n) = n - |A_1 \cup A_2 \cup \dots \cup A_t| = n - \sum_{1 \le i \le t} |A_i| + \sum_{1 \le i < j \le t} |A_i \cap A_j| + \cdots$$

כעת, מתוך רצף של n איברים ניקח אחד אחת ל-p_i מס' לקבלת את מס' המתחלקים. לכן:

$$|A_i| = \frac{n}{p_i}$$

מזרות p_i, p_j לכל $i \neq j$, נקבל:

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, \qquad |A_i \cap A_j \cap A_k| = \frac{n}{p_i p_j p_k}, \qquad \dots$$

לפיכך:

$$\varphi(n) = n - \sum_{1 \le i \le t} \frac{n}{p_i} + \sum_{1 \le i < j \le t} \frac{n}{p_i p_j} + \cdots = n\left(1 - \sum_{1 \le i \le t} \frac{1}{p_i} + \sum_{1 \le i < j \le t} \frac{1}{p_i p_j} + \cdots\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\dots$$

כאשר ההסבר לשוויון האחרון זהה להסבר של פיתוח הבינום של ניוטון.

למשל:

$$\varphi(200) = \varphi(2^3 \cdot 5^2) = 200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = \frac{200 \cdot 4}{10} = 80$$

בעיית המזכירה המפוזרת

שאלה: מזכירה מכינה n מכתבים המיועדים ל-n בני אדם שונים, ו-n מעטפות עם כתובות של הממוענים. אבל, בפיזור דעת, היא מכניסה כל מכתב למעטפה שונה באופן אקראי. מה ההסתברות שאף אדם לא יקבל את המכתב המיועד לו?

פתרון: נסמן את המכותבים ע"י $1, \dots, n$. כל סידור של המכתבים במעטפות ניתן לתיאור ע"י תמורה (פונ' חח"ע מקב' לעצמה) $f: \{1, \dots, n\} \to \{1, \dots, n\}$ כאשר f_i פירושו שהמכתב מיועד לאדם i הושם במעטפה הממוענת לאדם j. מספר כל התמורות הנ"ל הוא $n!$. כעת נסמן עבור $i = 1, \dots, n$: A_i = קב' התמורות שבהן $f(i) = i$. אז אנחנו מעוניינים בתמורות שאינן ב-$\bigcup_{i=1}^{n} A_i$. תמורה כזו הקראת **אי-סדר** (**Derangement**) של $\{1, \dots, n\}$. מס' האי-סדרים של $\{1, \dots, n\}$ מסומן ע"י D_n.

$$D_n = n! - |A_1 \cup \dots \cup A_n|$$

נשים לב (ע"י קביעה של המספרים הקבועים בכל קב', וספירת סידורים של המס' האחרים):

$$\forall i: \ \ |A_i| = (n-1)!, \qquad \forall i < j: \ \ |A_i \cap A_j| = (n-2)!, \qquad \dots$$

לכן:

$$D_n = n! - n(n-1)! + \binom{n}{2}(n-2)! + \cdots = n!\left(1 - 1 + \frac{1}{2} - \frac{1}{3!} + \frac{1}{4!} + \cdots + \frac{(-1)^n}{n!}\right)$$

זו הנוסחא עבור D_n. ההסתברות המבוקשת היא:

$$\frac{D_n}{n!} = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} + \cdots$$

כאשר $n \to \infty$, ההסתברות היא e^{-1}. כלומר, כאשר n גדול, ההסתברות שאף אדם לא יקבל את המכתב המיועד לו היא בקירוב e^{-1}.