מ.מ.למדמ"ח ∼ עמית וינשטיין ∼ קוד לתיקון שגיאות

שחר פרץ

5 ליוני 2024

1 משהו

$$Alice \longrightarrow Bob$$

מה מקשה על אליס ובוב לדבר?

- רעש / noise $\Longleftarrow$ קוד לתיקון שגיאות
- מחיר / cost $\Longleftarrow$ כיווץ (למפל זיוג, האפמן)
- ציטוט / eavesdropping $\Longleftarrow$ הצפנה (דיופי־הלמן)

1.1 ביקורת בתעודה

חישוב ספרת ביקורת:

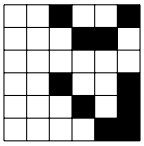
```
_ 9  8 7  6 5 4 3 2 1
_ 1  2 1  2 1 2 1 2 1
  --------------------
n =: 38= 16 7 12 5 6 8 3 4 1
```

ספרת הביקורת תהיה $10 - n \bmod 10$ (כאשר n סכום ספרות לאחר ההכפלות).

כל ספרה שנשנה, תשנה את ספרת הביקורת, וגם לרוב חילופי הספרות העוקבים. כך, ספרת הביקורת תתפוס את רוב השגיאות הנפוצות.

1.2 דוגמה נוספת

נסדר 25 קלפים לבנים (0)/שחורים (1), בסידור של 5×5. אחר כך, נוסיף בכל שורה קלף לכן או שחור כדי שיהיה מספר זוגי של קלפים שחורים בשורה. באופן דומה, נוסיף שורה שישית כך שבכל עמודה יהיה מספר זוגי של קלפים שחורים.



ניתן לתקן שגירה של קלף בודד: נהפוך את הקלף היחיד שבשורה שלו מס' הסלפים השחורים אי־זוגי וגם שבעמודה שלו מס' הקדפים השחורים אי־זוגי. מסתכלים על המודל שבו כל ביט מתחלף בהסתברות של $p \ll 1$. ניתן לזהות שגיאות של עד 3 קלפים/ביטים שיתחלפו.

2 מרחק Hamming

בהינתן $x, y \in \Sigma^n$, המרחק ביניהן מוגדר להיות כמות המקומות שאותם יש לשנות על מנת לעבור מ־x ל־y.

$$\Delta(x, y) = |\{i \in \{0, 1\} \mid x_i \neq y_i\}|$$

תכונות:

- $\forall x.\Delta(x, x) = 0,\ \forall x \neq y.\Delta(x, y) \neq 0$
- $\forall x, y.\Delta(x, y) = \Delta(y, x) \geq 0$
- $\forall x, y, z.\Delta(x, y) \leq \Delta(x, z) + \Delta(z, y)$

ואכן, הוא חיובי/0 קמטטיבי, ומקיים את א"ש המשולש, ושווה ל־0 אמ"מ ערכים זהים.

קוד לתיקון שגיאות הוא פונקציה $C\colon \{0,1\}^k \to \{0,1\}^n \quad (n > k)$

נגדיר **מרחק של קוד לתיקון שגיאות** להיות:

$$d = \Delta(C) = \min_{x \neq y} \Delta(C(x), C(y))$$

באופן פורמלי, נננאפיין קוד בעזרת (n,k,d) כאשר $n =$ אורך ההודעה המשודרת, $k =$ אורך ההודעה המקורית $d =$ מרחק.

מטרה: בהינתן k קבוע, ש־n יהיה כמה שיותר קטן ו־d כמה שיותר גדול.

אלגו' decoding: למצוא מילת קוד קרובה ביותר, ולהחזיר את ההודעה שמתאימה לה. $D\colon \{0,1\}^n \to \{0,1\}^k$. $D(x') =$ הערך $x \in \{0,1\}^k$ כך ש־$D(x') = \Delta(C(x), x') = \min_{y \in \{0,1\}^k} \Delta(C(y), x')$.

לדוגמה, בעבור ספרת ביקורת: $n = 9, k = 8, d = 2$, לזהות שגיאות $= 1$, לתקן שגיאות $= 0$.

ובעבור משחק הקלפים: $d = 4,\ k = 25,\ n = 36$ לזהות שגיאות $= 3$, לתקן שגיאות $= 1$.

ובעבור קוד חזרה ($0 \to 000,\ 1 \to 111$): $(n,k,d) = (3,1,3)$

קוד ביט זוגיות (parity-bit): $(n,k,d) = (3,2,2)$. דוגמאות: $00 \to 000, 01 \to 011, 10 \to 101, 11 \to 110$ (הוספת ביט לפי XOR)

טענה: עבור קוד ממרחק d, לכל מילה x, כדור hummaing (המילים במרחק hummaing שהוא x) ברדיוס $d-1$ סביב $C(x)$ מכיל רק אותה מבין $\mathrm{Im}(C)$. לכן, ניתן לזהות לכל היותר $d-1$ שגיאות.

טענה: עבור קוד ממרחק d ניתן לתקן עד $\left\lfloor \frac{d-1}{2} \right\rfloor$.

באופן דומה, כדורי ה־humming של $C(x), C(y)$ ברדיוס $\left\lfloor \frac{d-1}{2} \right\rfloor$ סביב מילות קוד, זרים (הכדורים), שכן אם קיים איברם בחיתוכם, נקבל שהמרחק בין $C(x)$ ל־$C(y)$ כלשהם קטן ממש מ־d וזו סתירה.

קשר בין n, k, d:

$$d \leq n - k + 1$$

הוכחה. נניח ויש לנו 2^k מילים באורך n ביטים. ידוע שהמרחק בין כל שתי מילים, הוא לפחות d. אם נמחק את $d-1$ התווים הראשונים, יתרת המחרוזות באורך $n-d+1$, שנוכל לדעת שהן שונות. סה"כ, קיבלנו 2^k מחרוזות שונות שנכנסות למרחק של 2^{n-d+1}. סה"כ, $2^k \leq 2^{n-d+1}$. נוציא לוג ונקבל $k \leq n-d+1$, נעביר אגפים וסה"כ $d \leq n-k+1$. ■