

סיבוכיות

© ארזים

27 ביוני 2017

1 קודים לתיקון שגיאות

כזכור, קוד לינארי הוא תת מרחב $C \subseteq \mathbb{F}^n$. מימד הקוד הוא $\dim(C) = k$. הקצב שלו הוא $\frac{k}{n}$. המרחק המינימלי הוא

$$\min_{c_1 \neq c_2 \in C} \text{dist}(c_1, c_2) = \min_{0 \neq c \in C} \underbrace{\text{wt}(c)}_{\text{dist}(c, 0)}$$

מטריצה בודקת של קוד היא מטריצה H בגודל $(n - k) \times n$ כך שמתקיים $\ker H = C$.

טענה 1.1 יהיו $C \neq 0, H$ כאלה. אם המרחק המינימלי של C הוא d , אזי כל $d - 1$ עמודות של H הן בלתי תלויות לינאריות, ויש d עמודות תלויות לינאריות של H . במילים אחרות, המרחק המינימלי של C הוא המספר הטבעי המקסימלי d שמקיים שכל $d - 1$ עמודות של H הן בלתי תלויות לינאריות.

הוכחה: נסמן $H = (H_1, \dots, H_n)$. יהי $c \in C$ עם $\text{wt}(c) = d$. אזי

$$Hc = 0$$

$$\sum_{i=1}^n c_i H_i = 0$$

ולכן העמודות $\{H_i \mid c_i \neq 0\}$ הן תלויות לינאריות - ויש d כאלה. כעת, נניח בשלילה שיש $d - 1$ עמודות תלויות, בלי הגבלת הכלליות $H_1, \dots, H_{d-1}$. מההנחה, יש $\alpha_1, \dots, \alpha_{d-1}$ שלא כולם 0 עם

$$\sum_{i=1}^{d-1} \alpha_i H_i$$

נגדיר $c = (\alpha_1, \dots, \alpha_{d-1}, 0, \dots, 0)$. נקבל $c \neq 0, Hc = 0$ וכן $d - 1 < d$. $\text{wt}(c) \leq d - 1$ בסתירה. ■

מסקנה 1.2 $d \leq n - k + 1$ (חסם סינגלטון).

1.1 חסם גילברט ורשמוב

נתמקד בקודים מעל $\mathbb{F}_2$. חסם סינגלטון בצורה אסימפטוטית הוא:

$$\frac{k}{n} = R \leq 1 - \delta + o(1)$$

חסם האמינג:

$$\frac{k}{n} = R \leq 1 - \frac{\log V\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right)}{n}$$

כאשר $V(r, n)$ הוא הנפח של כדור המינג ברדיוס r . זה בדיוק

$$\sum_{i=0}^r \binom{n}{i}$$

מסטירלינג נקבל

$$v\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right) \geq 2^{h\left(\frac{\delta}{2}\right)n - o(n)}$$

עבור h פונקציית האנטרופיה. משמע החסם הוא

$$\frac{k}{n} = R \leq 1 - h\left(\frac{\delta}{2}\right) + o(1)$$

טענה 1.3 (גילברט ורשמוב) לכל $\delta \in (0, \frac{1}{2})$, $\varepsilon \in (0, 1 - h(\delta))$ יש קוד עם מרחק מינימלי δ וכן $R \geq 1 - h(\delta) - \varepsilon$.

הוכחה: אנחנו נראה שקוד מקרי משיג את זה (בעייה פתוחה - למצוא מפורשות אחד כזה). נגדיל מטריצה יוצרת מקרית בגודל $k \times n$, עבור $k = (1 - h(\delta) - \varepsilon)n$ - כלומר כל תא יהיה 0, 1 בהסתברות $\frac{1}{2}$ באופן בלתי תלוי בשאר התאים. נראה שבהסתברות גבוהה, מרחק הקוד שאותו G (המטריצה המקרית) יוצרת הוא לפחות δ . אם $v \neq 0$, אזי vG מתפלג אחיד בתוך $\{0, 1\}^n$:

$$\mathbb{P}(\text{wt}(vG) < \delta) = \frac{V(d-1, n)}{2} \leq \frac{2^{h(\delta)n}}{2^n} = 2^{-n(1-h(\delta))}$$

ההסתברות שקיים $v \neq 0$ שכזה היא לכל היותר

$$2^k 2^{-n(1-h(\delta))} = 2^{-\varepsilon n} < 1$$

בפרט יש G שעבורה זה לא קורה לאף v , ולכן מרחק הקוד שהיא יוצרת הוא לפחות δ .
מההוכחה נובע גם שמימד הקוד הוא k . ■