מבוא לתורת הקודים לתיקון שגיאות

שיעור ראשון – 21/10/2015

בירוקרטיה וכאלה

מרצה: אמיר שפילקה בנבנישתי.
אין תרגול, יהיו תרגילים. יהיו בערך פעם בשבוע-שבועיים, התרגיל הראשון יהיה השבוע. הוא יכלול בעיקר חישובים.
כל התרגילים הם להגשה. הציון הוא 80% בחינה 20% תרגילים.
שעת קבלה בשני ב־11:00 בחדר 118 בשרייבר.
מייל: shpilka@post.tau.ac.il

חומר

הקדמה

במאמר מ־1948 Shannonכתב על התרחיש הבא:
Aliceרוצה לשלוח הודעה ל־Bob. מה קורה כשבתווך יש רעש?
מודל: Binary Symmetric Channel: כשרוצים לשלוח ביט מקבלים בהסתברות $1-p$ את אותו הביט, ובהסתברות p את הביט השונה.
מודל נוסף: noiseless: אם נרצה לשלוח פקס, רוב הפיקסלים שנרצה לשלוח הם לבנים. כלומר מרחב ההודעות שלנו הוא **לא אחיד**. ולכן נרצה לחסוך, כלומר נרצה **לדחוס**.
במצב שבו אנחנו noiseless, יתקיימו מצבים שבהם נרצה לחסוך, ולכן נרצה לבצע compression.
נתמקד במודל noiseless בדוגמא של פקס.
פיקסל לבן: 99%, פיקסל שחור: 1%.
נחשוב על לבן כעל 0 ועל שחור כעל 1.
מסכימים מראש על הקידוד הבא:
נחתוך את הביטים לקבוצות של 10 ביטים. כשהבלוק הוא 10 אפסים, נשלח 0 יחיד. כשיש בו רק אחדות, נשלח 1 ואז את הבלוק.
נשאלת השאלה – **האם חסכנו בקידוד הזה?**
נניח שהפקס המקורי הכיל n פיקסלים. ננסה להבין כמה פיקסלים אנחנו מעבירים באמצעות הקידוד הזה בממוצע.

$$P(\text{block with only zeros}) = 0.99^{10} > 0.9$$

$$P(\text{block with at least one in it}) < 0.1$$

לכן כמות הביטים שנשלח יהיה:

$$\frac{n}{10}(0.9 \cdot 1 + 0.1 \cdot 11) = \frac{n}{5}$$

כלומר, חסכנו **פי 5** בערך.
Shannon שאל: מה האופטימום שאפשר להשיג מבחינת דחיסה?
הוא אפיין **בדיוק** כמה אפשר לחסוך.

אנטרופיה

Ω מרחב סופי. D התפלגות על Ω: $D : \Omega \to [0,1]$. $\sum_{x\in\Omega} D(X) = 1$.
נגדיר את האנטרופיה:

$$h(x) = \log \frac{1}{D(x)}$$

$$H(D) = Eh(x) = \sum_{x\in\Omega} D(X) \log \frac{1}{D(X)} = \sum_{x\in\Omega} -D(x) \cdot logD(X)$$

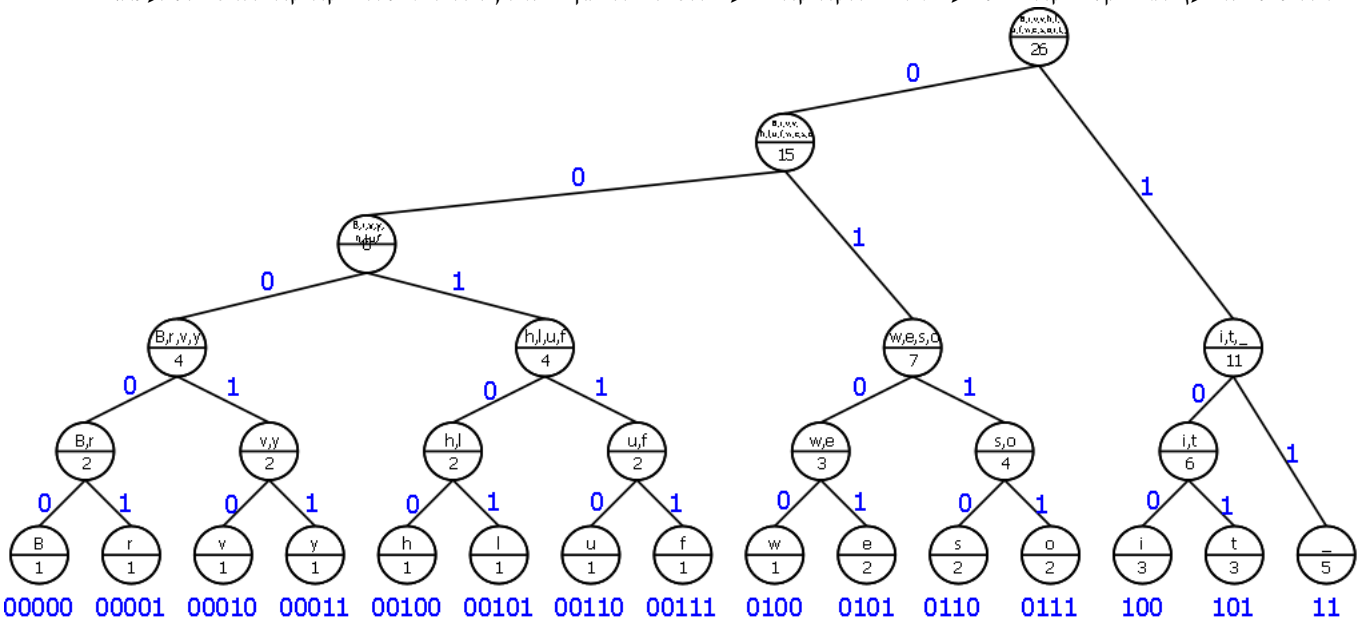
<u>משפט שאנון לערוץ ללא רעש:</u>
לכל D, Ω כנ"ל יש פונקציית $Enc : \Omega \to \{0,1\}^\star$, $Dec : \{0,1\}^\star \to \Omega$ כך שלכל $x \in \Omega$ מתקיים:

$$Dec(Enc(x)) = x$$

וגם

$$\mathbb{E}_{X\sim D}[|Enc(X)|] \in [H(D), H(D)+1]$$

ואי אפשר טוב יותר.
הוכחה: <u>Huffman tree</u>
לשם פשטות, נניח שכל ההסתברויות מהצורה $\frac{1}{2^i}$, $i \in \mathbb{N}$.
נתחיל לבנות עץ האפמן. ניקח בכל פעם את 2 הקודקודים עם הסכום הנמוך ביותר, ונחבר אליהם קודקוד חדש מלמעלה.



נשים לב שאף מחרוזת בקידוד אינה רישא של מחרוזת אחרת.
תכונה מרכזית של הקידוד: איבר שההסתברות שלו היא $\frac{1}{2^i}$ יקבל מחרוזת באורך i.
ניתן להוכיח תכונה זו באינדוקציה על כמות האיברים ב-Ω.
נראה שהבנייה הזו משיגה **בדיוק** את האנטרופיה.

$$\mathbb{E}_{X\sim D} = \sum_x \frac{1}{2^{i_x}} i_x = \sum_x D(x) \log \frac{1}{D(x)} = H(D)$$

במקרה שבו החזקות הן לא כאלה, ניתן לקחת את המספר הכי קרוב אליו מלמעלה מהצורה $\frac{1}{2^i}$, ואז ניתן לראות שאנחנו "מבזבזים" לכל היותר 1+.

Noisy channel

אלפבית הודעות מקור Σ.

אלפבית שהערוץ מציג Γ.

לכל הודעה ב-Σ קיימת הסתברות מסוימת לקבל הודעה מ-Γ.

דוגמא: BSC (Binary Symmetric Channel) עם פרמטר p.

עוד דוגמא: BEC: Binary Erasure Channel עם פרמטר p, בו יש הסתברות שהודעה מגיעה מחוקה במקום לקבל את הביט ההפוך. ואז ניתן לדעת שהייתה בעיה.

משפט שאנון עבור BSC(p)

לכל $0 \leq p < \frac{1}{2}$ קיים קבוע $0 < c < \infty$ וזוג פונקציות Enc, Dec

$$Enc : \{0,1\}^k \to \{0,1\}^n$$

$$Dec : \{0,1\}^n \to \{0,1\}^k$$

$$n = c \cdot k$$

כך שאם בוחרים באקראי הסתברות אחידה $x \in \{0,1\}^k$, מקודדים ל $Enc(x)$ ו"שולחים בערוץ הרועש". מסתכלים על המחרוזת $Enc(x) \oplus \eta$ כאשר $Pr(\eta_i = 1) = p$, $\eta \in \{0,1\}^n$ אז בהסתברות גבוהה

$$Dec(Enc(x) + \eta) = x$$

עבור BSC מספיק לקחת $c > \frac{1}{1-H(p)}$. (כאשר $H(p) = -p \cdot \log p - (1-p) \cdot \log(1-p)$).

הוכחה:

לכל $x \in \{0,1\}^k$ נבחר את $Enc(x)$ באקראי מתוך $\{0,1\}^n$.

נגדיר Hamming distance:

$$u, v \in \{0,1\}^n, dist(u,v) = |\{i | u_i \neq v_i\}|$$

$$Dec(y) = x : dist(y, Enc(x)) \text{ is minimal}$$

(כשיש כמה מחרוזות מתאימות, נבחר אחת מהן).

נקבע איזשהו $x \in \{0,1\}^k$ ואת $Enc(x)$.

נגדיר $y = Enc(x) \oplus \eta$

1. בהסתברות גבוהה המשקל של η הוא לכל היותר $(p+\varepsilon)n$.

$$wt(\eta) = |\{i | \eta_i = 1\}| = dist(\eta, 0)$$

2. נראה שההסתברות שאיזשהו $x' \neq x$ מקיים $dist(Enc(x'), y) \leq (p+\varepsilon)n$ היא "קטנה".

נוכיח את 1:

1.

$$Pr\left(wt(\eta) > (p+\varepsilon)n\right) \overset{chernoff}{<} e^{-\frac{\varepsilon^2}{3}n}$$

2. נקבע x' כלשהו.

$$Pr\left(dist\left(Enc\left(x\right), y\right) \leq \left(p+\varepsilon\right)n\right) = \frac{Vol\left(Ball\left(y, \left(p+\varepsilon\right)n\right)\right)}{2^n}$$

ולכן ההסתברות שאיזשהו x' יפול ב"כדור" היא לכל היותר $\frac{2^k \cdot Vol(Ball(y,(p+\varepsilon)n))}{2^n}$.

$$Vol(Ball(0,r)) = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{r} = 2^{H(\frac{r}{n})n + O(\log n)}$$

אפשר להראות את זה עם קירוב סטירלינג.
ולכן

$$Vol(Ball(y,(p+\varepsilon)n)) = 2^{n(\frac{k}{n} + H(p+\varepsilon) - 1 + O(1))}$$

אם אנחנו בוחרים את n בצורה הבאה:

$$n > \frac{k}{1 - H(p+\varepsilon)}$$

אנחנו מקבלים את התוצאה הרצויה.

$$Pr_{E,\eta}\left(Dec\left(Enc\left(x\right) \oplus \eta\right) \neq x\right) < e^{-\frac{\varepsilon^2}{3}n} + 2^{-n(1-\frac{k}{n} - H(p+\varepsilon) - o(1))}$$

לכל $c > \frac{1}{1-H(p)}$ אם $n = c \cdot k$ אז ההסתברות שניכשל בפענוח של x היא קטנה מהחלק הימני של האי שוויון האחרון עבור איזשהו $\varepsilon' > 0$.
היחס $\frac{k}{n}$ נקרא **קצב**. $1 - H(p)$ נקרא הקיבול של $BSC(p)$.

<u>משפט:</u>
לכל $0 < p < \frac{1}{2}$ ולכל $0 < \delta$ יש n_0 כך שאם $n \geq n_0$ וגם $k \geq (1 - H(p)) + \varepsilon)n$ אז לכל זוג פונקציות

$$E : \{0,1\}^k \to \{0,1\}^n, D : \{0,1\}^n \to \{0,1\}^k$$

מתקיים:

$$Pr_{\eta, x \in \{0,1\}^k}\left(D\left(E(x) \oplus \eta\right) = x\right) < \delta$$

שיעור שני – 28/10/2015

בשיעור שעבר:

- מודל של שאנון לרעש BSC, BEC.
- קיבול של ערוץ
- משפט שאנון לערוץ רועש
- משפט הדחיסה (לערוצים בלי רעש)

היום נדבר על העבודה של Hamming.

Hamming

אנחנו רוצים להיות מסוגלים לפענח ב**וודאות** וב**יעילות**.

סימונים

Σ- אלפבית.

$$Enc : \Sigma^k \to \Sigma^n$$

k הוא אורך ההודעה – message length
n הוא אורך מילת קוד – codeword/block length.
d: המרחק המינימלי של הקוד

$$d = \min_{x \neq y} dist(Enc(x), Enc(y)) \neq \{i | Enc(x)_i \neq Enc(y)_i\}$$

q - $|\Sigma|$ גודל האלפבית.
נסמן $C = Image(Enc)$ - קבוצת מילות הקוד.
קוד מסומן ע"י $(n, k, d)_q$.
נסמן ב-e את מספר הטעויות שקרו. מהו ה-e המקסימלי עבורו אנו יכולים לדעת שקרתה טעות?
קיבלנו $w = Enc(x) + \eta$, מהו ה-e המקסימלי ($w + (\eta) = e$) כך שנוכל לדעת בוודאות $w \notin C$? תשובה: $d - 1$.
מהו ה-e המקסימלי עבורו נוכל לשחזר בוודאות את $Enc(x)$? תשובה: $\lfloor \frac{d-1}{2} \rfloor$.
אנחנו רוצים ש:

- n יהיה קטן ככל האפשר
- k יהיה גדול ככל האפשר
- d יהיה גדול ככל האפשר.
- q "קטן" (אנחנו עובדים עם מחשבים אז אנחנו מעדיפים ש-q יהיה חזקה של 2.). הערה: יותר קל לבנות קודים עם q גדול.

דוגמאות:

$d = 1$: ניתן לבחור $Enc(x) = x$.
$d = 2$: ניתן לבחור $Enc(x) = (x, x)$ (זה repition code).
עוד אפשרות: $Enc(x) = (x_1, ..., x_k, \sum_{i=}^{k} x_i)$ (חיבור מודולו 2).
נראה כי באפשרות זו אכן מתקיים $d = 2$:
אם $dist(x, y) \geq 2$ אז בכל מקרה המרחק גדול שווה ל-2.
אחרת $dist(x, y) = 1$.
נשים לב שמספר האחדות ב-x בהכרח שונה ממספר האחדות ב-y, אם אחד זוגי אז השני אי זוגי. ובמקרה כזה גם ה-parity bit שונה.
$d = 3$: כאן המקרה יותר קשה, ונטפל בו בקרוב.

קוד ליניארי

קוד עבורו Enc הוא העתקה ליניארית הוא קוד ליניארי.
צריך Σ^k מרחב וקטורי. Σ הוא שדה.
דוגמא: $\mathbb{F}_2$: $\{0, 1\}$ עם חיבור וכפל מודולו 2.
באופן שקול: $C \subseteq \Sigma^n$ יהיה מ"ו.
ניתן לתאר קידוד ע"י מטריצה $G_{n \times k}$:

$$Enc(x) = [\![G]\!]_{n \times k} \cdot (x)$$

העמודות במטריצה הן **בסיס** ל-C. $dim(C) = k$.

G נקראת ה**מטריצה היוצרת** – **G**enerating Matrix.

Parity Check Matrix - מטריצת בדיקת זוגיות. מסומנת H (נקראת גם PCM). ומתקיים: $C = \{w|H \cdot w = 0\} = Ker(H)$.
H היא מטריצה מסדר $(n-k) \times n$.
ה**קוד הדואלי** ל-C מסומן כ-$C^{\perp} = \{v \in \{0,1\}^n | v \perp w \forall w \in C\}$ – המרחב הנפרש ע"י שורות H.
תכונות:

1. $C^{\perp}$ הוא מ"ו.
2. מספיק לדרוש שאם $w_1, ..., w_k$ הם בסיס ל-G אז $C^{\perp} = \{v|v \perp w_1, ..., v \perp w_k\}$.

כזכור, עמודות G הן בסיס ל-C. ולכן:

$$C = \{v|v \cdot [\![G]\!] = 0\} = \{v|v \cdot G = 0\}$$

מרחב הפתרונות: $dim(C^{\perp}) = n - k$.
הערה: יש אפשרות שהחיתוך בין C ל-$C^{\perp}$ לא יהיה ריק. לדוגמא, תרגיל שמדגים את הקיצוניות של המצב הזה: מצאו C ממימד $\frac{n}{2}$ כך ש-$C = C^{\perp}$. (כדי למצוא פתרון לתרגיל מייצרים k משוואות: $\sum_{i=1}^{n} a_{i_1} x_i = 0, ..., \sum_{i=1}^{n} a_{i_k} x_i = 0$ – k משוואות בת"ל.
יהי $v_1, ..., v_{n-k}$ בסיס ל-$C^{\perp}$.

$$H = \begin{bmatrix} v_1 \\ . \\ . \\ . \\ v_{n-k} \end{bmatrix}$$

תרגיל: $C = \{x|H \cdot x = 0\}$.
מה הקשר (אם יש בכלל) בין המרחק המינימלי בקוד ל-H?
הבחנה: אם C הוא קוד לינארי, אז $dist(C) = \min_{0 \neq x \in C} wt(x) = \min_{0 \neq x \in C} dist(x, 0)$. הוכחה:

$$dist(x, y) = |\{i|x_i \neq y_i\}| = |\{i|x_i - y_i \neq 0\}| = dist(x - y, 0)$$

אבל מכיוון ש-x, y הן מילות קוד, אז גם הפרש שלהם הוא מילת קוד (כי מדובר בקוד לינארי).
המרחק המינימלי בקוד לינארי C הוא גדול שווה ל-d אמ"ם אין ב-C מילות קוד ממשקל קטן מ-d, פרט ל-0.

$$H \cdot (x) = x_1 \cdot \overline{c_1} + ... + x_k \cdot \overline{c_{n-k}} = 0$$

$dist(C) \geq d$ אמ"ם כל צירוף לינארי של **פחות** מ-d עמודות של H אינו שווה ל-0.
נחזר למקרה בו $d = 3$: מעל $G\mathbb{F}_2$ ניקח את H להיות מטריצה שכל עמודותיה שונות, (כלומר, כל צירוף של 2 עמודות מהמטריצה יהיה שונה מ-0, ולכן כל 2 עמודות מהמטריצה צריכות להיות שונות, ולכן נדרוש שכל העמודות במטריצה יהיו שונות.) ואף עמודה אינה 0.
איך נוכל לגרום לכך ש-k ו-n יהיו כמה שיותר קרובים? נסמן $n - k = l$. אז המטריצה היא מסדר $l \times n$, ונרצה ש-l יהיה כמה שיותר קטן ביחס ל-n. אם נרצה לבחור כמה שיותר עמודות במטריצה כך שהן יהיו שונות אחת מהשנייה ונרצה להגדיל את n, המקסימום שנוכל לבחור הוא $n = 2^{l-1}$.

$$H = []_{l \times (2^l - 1)}$$

עמודות H יהיו $\{0,1\}^l - \{\overline{0}\}$. מסקנה: לכל $l > 0$ טבעי קיים קוד $(2^l - 1, 2^l - l - 1, 3)_2$.
האמינג הוכיח משפט שאומר שזהו הקוד "הטוב ביותר". מה זה אומר? שעבור $d = 3, q = 2$, אם $n = 2^l - 1$ עבור l טבעי כלשהו, אז ה-k הטוב ביותר שנוכל לקבל הוא $k = 2^l - l - 1$.
הקוד שלקחנו הוא מושלם במובן שאם נסתכל על ה"כדורים" של מילות הקוד (שמייצגים את המילת קוד והמילים שקרובות למילות הקוד לאחר שיבוש של מספר ביטים), אז הכדורים **מכסים** את כל המרחב ואין חיתוך בין 2 כדורים.
נוכיח את זה:

כמה מילות קוד יש לנו? $2^k = 2^{(2^l - l - 1)}$. מה גודל הכדור ברדיוס $\frac{d-1}{2} = 1$? הגודל הוא $n+1$.
כמה מילים בתוך כל הכדורים יש לנו?

$$(n+1) \cdot 2^k = 2^l \cdot 2^{2^l - l - 1} = 2^{2^l - 1} = 2^n$$

כלומר – אנחנו מכסים את כל המרחב ע"י המילים בכל הכדורים.
טענה נחמדה: אם יש לנו קוד עם d אי זוגי, נוכל להוסיף לו parity bit ולהגדיל את d ב-1.

חסמים על קודים

ראינו כבר חסם על קודים: חסם הכדורים של המינג. נובע מכך שכדורים ברדיוס $\frac{d-1}{2}$ סביב מילות קוד הם זרים.

$$2^k \cdot \left| Ball(0, \left\lfloor \frac{d-1}{2} \right\rfloor) \right| \leq 2^n$$

סימונים:
קצב של קוד (Rate): $R = \frac{n}{k}$. $(0 < R \leq 1)$.
מרחק יחסי: $\delta = \frac{d}{n}$.
אנחנו רוצים: $2^{R \cdot n} \cdot \left| Ball\left(0, \frac{\delta}{2} n\right) \right| \leq 2^n$.

$$2^{R \cdot n} \cdot \left| Ball\left(0, \frac{\delta}{2} n\right) \right| = 2^{R \cdot n} \cdot 2^{H(\frac{\delta}{2}) \cdot n + O(n)} \leq 2^n$$

קיבלנו את החסם: $R + H(\frac{\delta}{2}) \leq 1$ (מעל $\Sigma = \{0,1\}$).

חסם סינגלטון (Singleton):
בכל $[n,k,d]_q$ קוד, מתקיים:

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

(אסימפטוטית – $\delta \leq 1 - R$).
הוכחה:
יהי $C \subseteq \Sigma^n$.
נביט בהטלה על $k-1$ הקואורדינטות הראשונות. יש $|\Sigma|^{k-1}$ מחרוזות שונות. $|C| = |\Sigma|^k$. לפי שובך היונים, יש $x, y \in C$ המסכימים על $k-1$ הקואורדינטות הראשונות. בפרט: $dist(x,y) \leq n - (k-1) = n - k + 1$.
קוד Maximum Distance Separable (MDS-Code) הוא קוד שמשיג את חסם סינגלטון, כלומר הוא $[n,k,n-+1]_q$-קוד.
מעל $\mathbb{F}_2$ לא ניתן להגיע לסינגלטון. נראה עבור קודים ליניארים:
ב-Parity Check Matrix (PCM) של קוד MDS כל $n-k$ עמודות הן בת"ל.
נראה כי מעל $\mathbb{F}_2$ לא ניתן להגיע לתוצאה הרצויה.
נניח כי $n-k$ העמודות הראשונות הן בת"ל (אחרת סיימנו). נרצה להוסיף עמודה אחת נוספת, נרצה עמודה נוספת שתהיה תלויה ב-$n-k$ העמודות הראשונות. אבל מעל $\mathbb{F}_2$ צירוף של העמודות האלה הוא חיבור שלהן. אבל כעת לא נוכל להוסיף עמודה נוספת שתהיה תלויה בכל עמודות הקודמות, מכיוון שאז נקבל את אותה עמודה נוספת או 0.
הסבר:

1. אם $n-k$ העמודות הראשונות ת"ל, אז יש צ"ל באורך קצר או שווה ל-$n-k$ ובפרט יש מילה בגרעין (כלומר, מילת קוד) ממשקל קטן שווה ל-$n-k$.
2. אם $n-k$ העמודות הראשונות בת"ל, אז הן בסיס. אם עמודה אחרת היא צ"ל של $t < n-k$ מהן אז יש מילה בגרעין ממשקל גדול שווה ל-$n-k \geq t+1$. (ואז הקוד אינו MDS).
3. אם כל עמודה אחרת היא צרוף של בדיוק כל $n-k$ איברי הבסיס, ו-$k \geq 2$, אז יש 2 עמודות זהות.

כדי ש-H תהיה PCM של MDS-קוד, חייב להתקיים שכל $n-k$ עמודות ב-H הן בת"ל. נחפש מטריצה כזו:
moment curve: יהיו $\alpha_1, ..., \alpha_n$ איברים שונים. נביט במטריצה הבאה:

$$\begin{bmatrix} 1 & & 1 \\ \alpha_1 & ... & a_n \\ \alpha_1^2 & ... & \alpha_n^2 \\ ... & & .... \\ \alpha_1^{t-1} & ... & a_n^{t-1} \end{bmatrix}$$

כל t עמ' הן בת"ל.

שדה Field:
כל מה שמקיים את אקס' השדה. (כפל וחיבור שמתנהגים "יפה" ויש הופכי ונגדי).
דוגמאות:

1. $\mathbb{F}_2$ עם חיבור וכפל מודולו 2.
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. אם p ראשוני, אז $\mathbb{F}_p = GF(p) = \{0, 1, ..., p-1\}$ עם חיבור וכפל מודולו p.

לכל שני שלמים n, m יש שלמים a, b כך ש-$a \cdot n + b \cdot m = gcd(n, m)$.
אם m ראשוני ו-$n < m$ נקבל: $a \cdot n + b \cdot m = 1$. אז במקרה שיש לנו מספר p ראשוני, נוכל למצוא בעזרת האלגוריתם של אוקלידס למציאת gcd את ההופכי של מספר מסוים בשדה $\mathbb{F}_p$.
מסקנה: לכל q ראשוני ו-$n \leq q$ יש קוד $[n, k, n-k+1]_q$.
הוכחה: יהיו $\alpha_1, ..., \alpha_n$ איברי שדה שונים. נגדיר:

$$H = \left[\alpha_j^i\right]_{i=0...n-k-1, j=1...n}$$

נובע מכך שהדטרמיננטה של מטריצה ונדרמונדה היא $\prod_{i<j}(\alpha_i - \alpha_j)$ בכל שדה.

מציין של שדה: כל שדה מכיל 0,1. נסתכל על הקבוצה: $\{..., 1, 1+1, 1+1+1, ...\}$.
שדה הוא ממציין סופי אם הקבוצה הנ"ל סופית. והמציין במקרה הזה הוא גודל הקבוצה.
דוגמא: המציין של $\mathbb{F}_p$הוא p.
נאמר שהמציין הוא 0 אם הקבוצה אינסופית, לדוגמא ב-$\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
טענה: המציין הוא 0 או ראשוני.
הוכחה: אם המציין הוא $n = a \cdot b$, אז $0 = \overbrace{1 + ... + 1}^{a \cdot b = n} = \overbrace{(1 + ... + 1)}^{b} \cdot \overbrace{(1 + ... + 1)}^{a} = n$.
ומכך שבשדה לכל איבר שונה מ-0 יש הופכי, נקבל $a = n$ או $b = n$. בפרט, n ראשוני.
הסבר: אם $a \cdot b = 0$ ו-a הפיך אז $b = 0$ (כפל ב-a^{-1}) ואז $|\{1, 1+1, ..., \}| \leq b < n$ בסתירה להגדרת n.
הערה: נשים לב שאם המציין של שדה $\mathbb{F}$ הוא p אז $\mathbb{F}$ מכיל את $\{1, 2, ..., p-1, 0\}$ וכמו כן החיבור של שני איברים מהקבוצה (וכן הכפל שלהם) מתבצע מודולו p. ולכן $\mathbb{F}_p \subseteq \mathbb{F}$.
טענה: $\mathbb{F}$ עם מציין p הוא מ"ו מעל $\mathbb{F}_p$.
הוכחה: ברור.
דוגמא: $\mathbb{F}_4 = \{0, 1, x, x+1\}$ עם חיבור מודולו 2 וכפל: $x \cdot x = x + 1$.
מסקנה: אם $\dim \mathbb{F}/\mathbb{F}_p = k$ אז $|\mathbb{F}| = p^k$.

שיעור שלישי – 4/11/2015

חזרה על שיעורים קודמים

$(\mathrm{n,k,d})_q$ קוד.
k מימד/אורך ההודעה. $R = \frac{k}{n}$ קצב.
d מרחק מינימלי. $\delta = \frac{d}{n}$ מרחק יחסי.

דיברנו על קודים ליניארים, G מטריצה יוצרת, מטריצה H לבדיקת זוגיות.
קוד המינג - $(2^{l-1}, 2^l - l - 1, 3)_2$.
חסם הרדיוסים של המינג: $2^k \cdot Vol(Ball(0, \lfloor \frac{d-1}{2} \rfloor)) \leq 2^n$. קוד שמשיג חסם זה נקרא perfect code (קוד המינג הוא כזה).
חסם סינגלטון $d \leq n - k + 1$. קוד שמשיג חסם זה ייקרא MDS.

היום

- קוד Reed-Solomon
- קוד Reed-Muller.
- קוד האדמרד.
- חסם Gilbert-Varshamov.
- הקודים של Wozenkraft.

קודי Reed-Solomon

יהי $\mathbb{F}$ שדה בגודל $q \geq n$. לכל k נגדיר קוד $(n, k, n - k + 1)_q$.
$\mathbb{F}^k$: נחשוב על כל איבר ב-$\mathbb{F}^k$ כמתאר פולינום.

$$(a_1, ..., a_{k-1}) \in \mathbb{F}^k \rightsquigarrow \sum_{i=0}^{k-1} a_i x^i$$

הודעות = $\{f(x) | f \text{ is polynom with degree lower than } k \text{ over } \mathbb{F}\}$.
נקבע n איברים שונים בשדה $\alpha_1, ..., \alpha_n \in \mathbb{F}$. (נשים לב שזה מכריח את q להיות גדול שווה ל-n.)

$$Enc(f) = (f(\alpha_1), ..., f(\alpha_n))$$

כיוון שהקוד ליניארי (כי מדובר בפולינומים) מספיק להבין מה המספר המינימלי של קוארדינטות שונות מ-0 לכל מילת קוד שאינה 0.
עובדה: לפולינום ממעלה $k - 1$ יש לכל היותר $k - 1$ שורשים.
לכן בכל מילת קוד ששונה מ-0 יש לכל היותר $k - 1$ אפסים, ובפרט מרחקה מ-0 הוא לפחות $n - (k - 1) = n - k + 1$.

דוגמא: הודעה: $(x - \alpha_1) \cdot ... \cdot (x - \alpha_{k-1})$. ובמילת הקוד המתאימה יש בדיוק $n - k + 1$ קוארדינטות שאינן 0.

המטריצה היוצרת של הקוד:

$$\begin{pmatrix} 1 & \alpha_1 & ... & \alpha_1^{k-1} \\ 1 & \alpha_2 & ... & \alpha_2^{k-1} \\ ... & ... & & ... \\ 1 & \alpha_n & ... & \alpha_n^{k-1} \end{pmatrix}_{n \times k} \begin{pmatrix} a_0 \\ ... \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ ... \\ f(\alpha_n) \end{pmatrix}$$

כלומר זוהי מטריצת ונדרמונדה.

דוגמא: $\mathbb{F} = GF(2^8)$. קוד $(256, 240, 17)_{2^8}$.
ובבינארית (ביטים ולא בייטים): $(8 \cdot 256, 8 \cdot 240, 17)_2$.
מעל $\mathbb{F}_2$ ידועים קודים טובים יותר.
הסיבה שמשתמשים דווקא בקוד הזה ולא בקודים אחרים היא שסוג הטעויות שלנו הוא burst error (לדוגמא, שריטה), ואז קיימת דריסה של כמה תאים רצופים. אז אפילו אם קיימות 30 טעויות, אבל הן רצופות, נקבל שבעצם הן "הרסו" רק 5 תווים של השדה $\mathbb{F}_{2^8}$.

קודי Reed-Muller

דוגמא: 2 משתנים. הודעות: פולינומים ב-2 משתנים ממעלה קטנה שווה ל-l, בכל משתנה מעל $\mathbb{F}_q$.

$$f(x,y) = \sum_{i,j=0}^{l} a_{i,j} \cdot x^i y^j$$

מספר משתנים: $(l+1)^2$.

$$Enc(f) = (f(\alpha,\beta))_{(\alpha,\beta)\in\mathbb{F}_q^2}$$

זה נותן לנו קוד $(n = q^2, k = (l+1)^2, d =?)_q$.
נשים לב: $q = \sqrt{n}$.
טענה: $d = (q-l)^2$
ניתן לכתוב את f בתור: $f = \sum_{i=0}^{l} x^i \cdot f_i(y)$.
בסופו של דבר הקוד הוא קוד $(q^2, (l+1)^2, (q-l)^2)_q$.

באופן כללי, m משתנים, דרגה l, שדה בגודל q.
מקרה א': $l < q$.
הודעות: פולינומים ב-m משתנים מדרגה כוללת $\leq l$ (total degree).
קידוד:

$$f \to (f(\alpha))_{\alpha\in\mathbb{F}_q^m}$$

נשים לב שזה לא לגמרי מכליל את קוד Reed-Muller, כי כאן אנחנו חוסמים את הדרגה הכוללת, ולא את המעלה של כל אחד מהפולינומים.
הפולינום הכללי:

$$f = \sum_{\substack{d_1,\ldots,d_m \\ \sum d_i \leq l \\ 0\leq d_i}} a_{d_1,\ldots,d_m} \cdot x_1^{d_1} \cdot \ldots x_m^{d_m}$$

אורך = $n = q^m$.
מימד = $\binom{m+l}{m}$.
מרחק $\leq (1 - \frac{l}{q}) \cdot q^m$ (נוכיח את זה בשיעורי הבית).

דוגמא: $(x_1 - 1) \cdot \ldots \cdot (x_1 - l)$ (פולינום ממעלה l עם "משתנים שקטים". במקרה כזה המרחק הוא **שווה** לחסם:

$$(q-l) \cdot q^{m-1} = (1 - \frac{l}{q}) \cdot q^m$$

בסופו של דבר הקוד הוא קוד $(q^m, \binom{m+l}{m}, (1-\frac{l}{q})q^m)_q$.

דוגמא (לא מדויקת):
$q \approx log^2 k$, $m \approx \frac{logk}{\log\log k}$, $l \approx \frac{\log^2 l}{\log\log k}$.
עבור l, m, q כנ"ל:

$$\binom{m+l}{m} \approx \left(\frac{m+l}{m}\right)^m \approx \left(\frac{l}{m}\right)^m \approx k$$

$$q^m \approx k^2$$

$$d = \left(1 - \frac{l}{q}\right) \cdot q^m \approx \left(1 - \frac{1}{\log\log k}\right) \cdot k^2 = (1 - o(1)) \cdot k^2$$

וסך הכל הקוד הוא

$$(k^2, k, (1 - o(1)) \cdot k^2)_{\log^2 k}$$

או בצורה אחרת:

$$(n, \sqrt{n}, (1 - o(1))n)_{O(\log^2 n)}$$

מקרה ב': $l \geq q$
ההודעות הן פולינומים ב-mמשתנים מדרגה כוללת קטנה שווה ל-l, אך אף משתנה לא מופיע מדרגה גדולה מ-$q - 1$.
$n = q^m$, $k =?$
$l = a(q-1) + b$, כאשר $0 \leq b < q - 1$.
$d = q^{m-a}(1 - \frac{b}{q})$.
דוגמא: $((x_{a+1} - b) \cdot ... \cdot (x_{a+1} - 1)) \cdot (((x_1 - 0) \cdot ... \cdot (x_1 - (q-2)))$ $\prod_{i=1}^{a}$. במקרה כזה אנחנו רואים ש-d הוא קטן שווה מהחסם.
דוגמא: $q = 2$. $n = 2^m$.

$$k = \binom{m}{0} + \binom{m}{1} + ... + \binom{m}{l} \triangleq \binom{m}{\leq l}$$

$d = 2^{m-l}$.
הקוד הוא קוד $(2^m, \binom{m}{\leq l}, 2^{m-l})_2$ - $RM(m, l)$.

עבור $l = \frac{m}{2}$, נקבל $(n, \frac{n}{2}, \sqrt{n})_2$.

מה קורה כאשר $l = 1$?
נקבל $(2^m, m+1, \frac{1}{2} \cdot 2^m)_2$ - קוד האדמרד: $RM(m, 1)$. זה קוד עם מרחק מאוד טוב, אבל נשים לב ש-$k = \log n + 1$, שזה לא נהדר.
דרך נוספת להסתכל על קודי האדמרד:
תהי A מטריצה של ± 1 כך ש-$A \cdot A^t = n \cdot I$.
דוגמא: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
ואם $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes k}$ אז $A \cdot A^t = 2^k \cdot I$.
כאשר $\otimes$ זו מכפלה טנזורית.
תהיינו $v_1, ..., v_n$ שורות A, $v_i \to \tilde{v_i} \in \{0,1\}^n$ (כאשר $1 \to 0$, $-1 \to 1$).
וחוץ מזה ניקח $\tilde{u_i} = \bar{1} - \tilde{v_i}$.
נקבל קבוצה של n הודעות: $\{\tilde{u_i}\} \cup \{\tilde{v_i}\}$.
טענה: כל A כנ"ל נותנת $(n, \log n + 1, \frac{n}{2})_2$ קוד.
הוכחה: $\langle v_i, v_j \rangle = 0$ לכל $i \neq j$. מתקיים מכיוון ש-$A \cdot A^t = n \cdot I$.
נקבל שכל 2 מילות קוד "מסכימות" בדיוק על $\frac{n}{2}$ מקומות. כלומר, לכל $i \neq j$ מתקיים $dist(v_i, v_j) = \frac{n}{2}$.
ובפרט גם $dist(\tilde{v_i}, \tilde{v_j}) = \frac{n}{2}$. ולכן גם $dist(\tilde{v_i}, \tilde{u_j}) = \frac{n}{2}$ וגם $dist(\tilde{u_i}, \tilde{u_j}) = \frac{n}{2}$ לכל $i \neq j$.

סיכום עד כה
קודים בינאריים: $(2^l - 1, 2^l - l - 1, 3)_2$, $(2^l, l+1, \frac{1}{2}2^l)_l$, $(n \cdot \log q, k \cdot \log q, n - k + 1)_2$ (מתקבל מ-RS).
חסמים: $d \leq n - k + 1$, $2^k Vol(Ball(0, \lfloor \frac{d-1}{2} \rfloor)) \leq 2^n$.

התנהגות אסימפטוטית של קודים:

משפחה של קודים $C = \{C_i\}$, $C_i = (n_i, k_i, d_i)_{q_i}$.
הקצב של המשפחה:

$$R(C) = \liminf_{i\to\infty} \frac{k_i}{n_i}$$

$$\delta(C) = \liminf \frac{d_i}{n_i}$$

משפחה היא אסימפטוטית טובה אם $R(C), \delta(C) > 0$.
לדוגמא $RS : (n, \frac{1}{2}n, \frac{1}{2}n + 1)_n$ היא אינה משפחה טובה.

משפט Gilbert-Varshamov

לכל R, δ כך ש-$R + H(\delta) < 1$ יש משפחה עם $R(C) \geq R$ וגם $\delta(C) \geq \delta$.
הוכחה: בנייה חמדנית.
נתחיל עם $C_0 = \emptyset \subseteq \{0,1\}^n$.
בכל שלב, כל עוד נשארו מילים שלא נמחקו, נוסיף ל-C אחת המילים, ונמחק את כל המילים במרחק $\geq \delta n$ מהמילה שהוספנו. (למה $d = \delta n$? כי δn).
בכל שלב זורקים $Vol(Ball(0, \delta n)) \approx 2^{H(\delta)} \leq 2^{(H(\delta)+\varepsilon)n}$.
ולכן $|C| \geq \frac{2^n}{2^{(H(\delta)+\varepsilon)n}} = 2^{(1-H(\delta)-\varepsilon)n}$ ומכאן $R \geq 1 - H(\delta) - \varepsilon$.
בקוד הנ"ל ניתן לתקן כל $\frac{1}{2}\delta n$ טעויות.
בקוד של שאנון, עבור אחוז $\frac{1}{2}\delta$ של טעויות **מקריות**, ייתן קוד מקצב $1 - H(\frac{1}{2}\delta)$.
הוכחה 2: (קוד ליניארי)
תהי G מטריצה $k \times n$. כאשר $k = (1 - H(\delta) - 2\varepsilon)n$ אקראית מעל $GF(2)$. (כל קוארדינטה היא 0/1 באופן ב"ת אחיד).
טענה: בהסתברות טובה, אין אף מילת קוד בכדור ברדיוס δn מסביב ל-0.
הוכחה: עבור הודעה $x \in \{0,1\}^k$ מסוימת,

$$Pr\left(wt(x) \leq \delta n\right) \leq \frac{Vol(Ball(0, \delta n))}{2^n}$$

ההסתברות שתהיה הודעה "רעה" היא קטנה שווה ל-$\frac{2^k \cdot 2^{(H(\delta)+\varepsilon)n}}{2^n} = 2^{-\varepsilon n}$.