קורס: קודים לתיקון שגיאות ושימושיהם במדעי המחשב
מרצה: ד"ר קלים יפרמנקו
סמסטר: סתיו תשפ"א
תאריך: 24/11/2020

הרצאה 12

RM Codes

מבוא

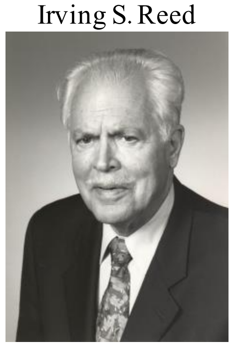
קודי RM (Reed-Muller) הינם קודים לתיקון שגיאות הנמצאים בשימוש בתקשורת אלחוטית (wireless), במיוחד ב Deep Space Communication. בנוסף, סטנדרד 5G מסתמך על קודי Polar לתיקון שגיאות ב Control Channel, אשר קשורים באופן הדוק לקודי RM.

קודי RM הינם הכללה של קודי Reed-Solomon וקודי Walsh-Hadamard. RM הינם קודים ליניאריים אשר Locally Testable, Locally Decodable וגם List Decodable. תכונות אלה הופכות אותם לשימושיים במיוחד ב Probabilistically Checkable Proof. נלמד בהרצאה 22 אודות קודים לוקאליים.

קודי Reed-Muller קרויים על שם David E. Muller אשר המציא אותם בשנת 1954, ו Irving S. Reed, אשר הציע את אלגוריתם הפענוח היעיל הראשון.

David E. Muller

Irving S. Reed



קודי RM ניתנים לייצוג ע"י מספר דרכים שונות (אך שקולות). הייצוג המבוסס על פולינומים מדרגה נמוכה הינו אלגנטי ומותאם במיוחד לאפליקציה שלהם כ Locally Testable וכ Locally Decodable.

ייצוג בעזרת Multilinear Polynomials מעל F_2

$C:\{0,1\}^k \to \{0,1\}^n$, פונקציית הקידוד של $RM[r,m]$ כאשר $n = 2^m$, $\mathrm{k} = \sum_{\mathrm{i}=0}^{\mathrm{r}} \binom{\mathrm{m}}{\mathrm{i}}$, ניתנת לייצוג בעזרת אבלואציה של Multilinear Polynomials מעל F_2, בעלי m משתנים ודרגה r.

<u>הגדרה:</u> Multilinear Polynomial מעל F_2, בעל m משתנים ודרגה r הינו פולינום מהצורה $p(x_1, \ldots, x_m) = \sum_{S \subseteq \{1,\ldots,m\}: |S| \le r} c_S \cdot \prod_{i \in S} x_i$, כאשר $c_S \in \{0,1\}$ הינם המקדמים של הפולינום.

מכיוון שישנם בדיוק k מקדמים לפולינום, ההודעה $t \in \{0,1\}^k$ הינה בעלת k ערכים שיכולים לשמש כמקדמים אלה. מכאן, שכל הודעה t מולידה פולינום p_t ייחודי בעל m משתנים. על מנת לקודד את t למילת הקוד $C(t)$, המקודד מחשב את p_t בכל הנקודות האפשריות $a \in \{0,1\}^m$ מודולו 2. כלומר, פונקציית הקידוד מוגדרת באופן הבא: $C(t) = (p_t(a) mod 2)_{a \in \{0,1\}^m}$.

<u>הערה:</u> העובדה שמילת הקוד $C(t)$ ניתנת לשחזור באופן ייחודי ל t נובעת מאינטרפולציית לאגראנז', שקובעת כי מקדמי פולינום נקבעים באופן ייחודי כאשר ניתנות מספיק נקודות הערכה. בנוסף, מכיוון שלכל $\alpha \in F_q$ ולכל $x, y \in \{0,1\}^k$ מתקיים $C(\alpha x) = \alpha C(x) mod2$ וגם $C(x + y) = C(x) + C(y) mod2$, פונקציית הקידוד C הינה העתקה ליניארית, ומשום כך RM הינו קוד ליניארי.

<u>דוגמא:</u> עבור $r = 2, m = 4$ מתקיים כי $k = 11, n = 16$. עבור הודעה $t = 11010010101$ נקבל כי

$$\boldsymbol{p_t(x_1,x_2,x_3,x_4)} = 1 + 1 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3 + 0 \cdot x_4 + 0 \cdot x_1x_2 + 1 \cdot x_1x_3 + 0 \cdot x_1x_4 + 1 \cdot x_2x_3 + 0 \cdot x_2x_4 + 1 \cdot x_3x_4 = \boldsymbol{1 + x_1 + x_3 + x_1x_3 + x_2x_3 + x_3x_4} \Longrightarrow$$

$$\boldsymbol{C(t)} = C(11010010101) = (p_t(0000), p_t(0001), p_t(0010), \dots, p_t(1111) = \boldsymbol{1111101001010000}$$

<u>ייצוג בעזרת Multilinear Polynomials מעל F_q</u>

מעל שדה F_q ייצוג RM בעזרת Multilinear Polynomials הינו הכללה עבור F_2:

פונקציית הקידוד של $RM_q[r,m]$, $C: \{0, \dots, q-1\}^k \to \{0, \dots, q-1\}^n$ ניתנת לייצוג בעזרת אבלואציה של Multilinear Polynomials מעל F_q, בעלי m משתנים ודרגה r.

<u>הגדרה:</u> Multilinear Polynomial מעל F_q, בעל m משתנים ודרגה r הינו פולינום מהצורה $p(x_1, \dots, x_m) = \sum_{0 \le i_1, \dots, i_m \le q-1 : i_1 + \dots + i_m \le r} c_S \cdot \prod_{j=1}^m x_j^{i_j}$, כאשר $c_S \in \{0, \dots, q-1\}$ הינם המקדמים של הפולינום.

בדומה ל F_2, ישנם בדיוק k מקדמים לפולינום, לכן ההודעה $t \in \{0, \dots, q-1\}^k$ הינה בעלת k ערכים שיכולים לשמש כמקדמים לפולינום. מכאן, שכל הודעה t מולידה פולינום p_t ייחודי בעל m משתנים. על מנת לקודד את t למילת הקוד $C(t)$, המקודד מחשב את p_t בכל הנקודות $a \in \{0, \dots, q-1\}^m$ מודולו q. כלומר, פונקציית הקידוד מוגדרת באופן הבא: $C(t) = (p_t(a) mod q)_{a \in \{0, \dots, q-1\}^m}$.

$$RM_q[m,r] = \{p(a_1), p(a_2), \dots, p(a_{q^m}) : p \text{ is polynomial of degree } r \text{ in } m \text{ variables}\}$$

<u>טענה:</u> האורך $(\boldsymbol{n})$ של $RM_q[m,r]$ הינו q^m.

<u>הסבר:</u> עבור הודעה $t \in \{0, \dots, q-1\}^k$ הקוד מחשב את p_t בכל הנקודות $a \in \{0, \dots, q-1\}^m$ מודולו q. כלומר, מספר הסימבולים במילת הקוד $C(t) = (p_t(a) mod q)_{a \in \{0, \dots, q-1\}^m}$ הינו q^m.

<u>הערה:</u> ניתן להבחין כי מעל F_2 אכן מתקיים כי $n = 2^m$.

<u>טענה:</u> המימד ($\boldsymbol{k}$) של $RM_q[m,r]$ הינו

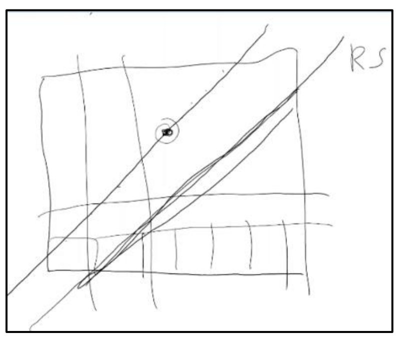
$$\begin{cases} \sum_{i=0}^{r}\binom{m}{i}, & q=2 \\ \sum_{i=0}^{r}\binom{m+i-1}{i}, & q>r \\ there\ isn't\ a\ closed\ formula, & otherwise \end{cases}$$

<u>הסבר:</u> מימד של קוד הינו אוסף של כל ההודעות האפשריות, משמע המימד של $RM_q[m,r]$ הינו אוסף V כל הפולינומים מדרגה r בעלי m משתנים. נבחין כי V הינו מרחב ליניארי, כאשר בסיס עבור מרחב זה יכול להיות אוסף המונומים $B=\{x_1^{i_1}x_2^{i_2}\ldots x_m^{i_m} : 0\le i_1,\ldots,i_m\le q-1 \wedge i_1+\cdots+i_m\le r\}$.

<u>טענה:</u> עבור $q>r$ המרחק של $RM_q[m,r]$ הינו $q^m(1-\frac{r}{q})$.

<u>Locally Decodable</u>

כאמור, אחת מהתכונות החשובות של RM בייצוג ע"י Multilinear Polynomials, הינה שהוא Locally Decodable כאשר $r<q$. למשל עבור $m=2$, ניתן לקחת פולינום בעל 2 משתנים, לצמצם אותו על הישר, ולקבל פולינום בעל אותה הדרגה. כלומר, בהינתן $C(t)=w\in F_q^n$, ה Local Decoder מעביר ישר רנדומלי דרך w, ובעזרת $r+1$ נקודות על ישר זה מבצע אינטרפולציה לפולינום p_t שבעזרתו ניתן לחשב בקלות את t.



<u>טענה:</u> עבור $q=2$ המרחק של $RM_q[m,r]$ הינו 2^{m-r}.

<u>הוכחה:</u> $RM_q[m,r]$ הינו קוד ליניארי לכן נצטרך להוכיח כי:

א. קיימת מילת קוד $c\in RM_2[m,r]$ כך ש $wt(c)=2^{m-r}$.
ב. לכל מילת קוד $c\in RM_2[m,r]$ מתקיים $wt(c)\ge 2^{m-r}$.

א. ראשית, נסתכל על $p_t(x_1,\ldots,x_m)=x_1\cdot x_2\cdot\ldots\cdot x_r$, אשר התקבל ע"י הודעה $t\in\{0,1\}^k$.
נבחין כי $p_t(x_1,\ldots,x_m)\neq 0 \iff x_1=x_2=\cdots=x_r=1$.
מכאן, $wt\big(C(t)\big)=|\{a\in\{0,1\}^m : p_t(a)\neq 0\}|=2^{m-r}$.
כלומר, קיימת מילת קוד $c\in RM_2[m,r]$ כך ש $wt(c)=2^{m-r}$.

ב. יהי פולינום $p_t(x_1, \dots, x_m)$, אשר התקבל ע"י הודעה $t \in \{0,1\}^k$.
נסמן את המונום של $p_t(x_1, \dots, x_m)$ בעל הדרגה המקסימלית כ $x_{i_1}x_{i_2} \dots x_{i_r}$.
בה"כ $x_{i_1}x_{i_2} \dots x_{i_r} = x_1x_2 \dots x_r$.
נקבע את הערכים של $x_{r+1}, \dots, x_m$: $p_t(x_1, \dots, x_r, c_{r+1}, \dots, c_m) = p_{c_{r+1},\dots,c_m}(x_1, \dots, x_r)$.
אזי, גם עבור $p_{c_{r+1},\dots,c_m}(x_1, \dots, x_r)$ המונום בעל הדרגה המקסימלית הינו $x_1x_2 \dots x_r$, מכיוון שבפולינום זה המקדם של $x_1x_2 \dots x_r$ זהה למקדם שלו בפולינום p_t (הקבועים $c_{r+1}, \dots, c_m$ אינם מקדמים של מונום זה ב $p_{c_{r+1},\dots,c_m}$).
מכאן ש $p_{c_{r+1},\dots,c_m}(x_1, \dots, x_r) \neq 0$, לכן קיימים ערכים $\alpha_1, \dots, \alpha_r$ עבור $x_1, \dots, x_r$ כך ש $p_{c_{r+1},\dots,c_m}(\alpha_1, \dots, \alpha_r) \neq 0$. משמע, $p_t(\alpha_1, \dots, \alpha_r, c_{r+1}, \dots, c_m) \neq 0$.
כלומר, לכל $c_{r+1}, \dots, c_m$ קיימים $\alpha_1, \dots, \alpha_r$ כך ש $p_t(\alpha_1, \dots, \alpha_r, c_{r+1}, \dots, c_m) \neq 0$.
מכאן, $wt(C(t)) = |\{a \in \{0,1\}^m : p_t(a) \neq 0\}| \geq 2^{m-r}$.
כלומר, לכל מילת קוד $c \in RM_2[m,r]$ מתקיים $wt(c) \geq 2^{m-r}$.

$$\boxed{RM[m,r] = [2^m, \sum_{i=0}^{r} \binom{m}{i} \sim m^r, 2^{m-r}]}$$

<u>מסקנות:</u>

- אם r קטן אז $\delta(c) = 2^{-r}$ אבל $R\left(\frac{m^r}{2^m}\right) \to 0$.
- אם r גדול אז $R\left(\frac{m^r}{2^m}\right) > 0$ אבל $\delta(c) \to 0$.

<u>**Concatenated Codes**</u>

<u>מבוא</u>

ראינו בעבר כיצד ניתן להמיר קוד RS לקוד בינארי.

<u>דוגמא:</u> פונקציית הקידוד של $RS_{2^m, F_{2^m}^*}[k, 2^m - 1]$ מקודדת הודעה $m_1m_2 \dots m_k$ כל שלכל $1 \leq i \leq k$ מתקיים $m_i \in F_{2^m}$ למילת קוד $c_1c_2 \dots c_n$ כך ש $n = 2^m - 1$.

$$\boxed{m_1}\boxed{m_2}\boxed{\dots}\boxed{m_k} \longrightarrow \boxed{c_1}\boxed{c_2}\boxed{\dots}\boxed{c_n}$$

נסתכל על כל סימבול בהודעה כסדרה של m ביטים. כלומר, לכל $1 \le i \le k$ נסמן $m_i = b_{i_1}b_{i_2}\dots b_{i_m}$.
באופן דומה נסתכל גם על מילת הקוד. כעת, במקום לקודד k הודעות ב F_{2^m} ל n הודעות ב F_{2^m}, פונקציית הקידוד תקודד km ביטים ל cm ביטים.

$$\boxed{b_{1_1}\dots b_{1_m}}\boxed{\dots}\boxed{b_{k_1}\dots b_{k_m}} \longrightarrow \boxed{\bar{b}_{1_1}\dots \bar{b}_{1_m}}\boxed{\dots}\boxed{\bar{b}_{n_1}\dots \bar{b}_{n_m}}$$

<u>טענה:</u> אם מרחק של הקוד RS הינו d אז מרחק של הקוד הבינארי הינו d.

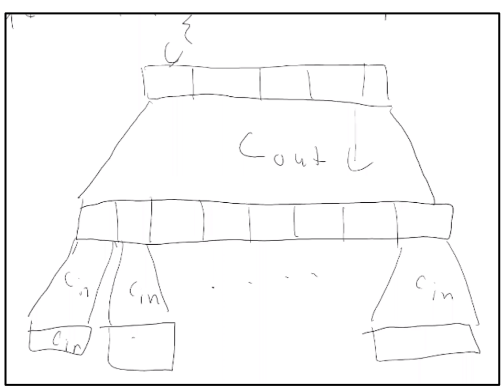
<u>הסבר:</u> אם 2 מילות קוד של RS שונות בסימבולה i, אז 2 מילות הקוד הבינאריות שונות בלפחות ביט אחד במקומות $(i-1)m+1, \dots, im$.

<u>מסקנה:</u> למרות שאורך מילות הקוד גדל, השוני בין שתי מילות קוד בינאריות אינו גדול מהשוני בין 2 מילות הקוד המקוריות.

<u>רעיון:</u> נמיר כל מילת קוד ל $2m$ ביטים, כאשר נרצה שאם 2 מילות קוד מקוריות שונות, אז הייצוג הבינארי שלהן יהיה שונה בהרבה מקומות מתוך $2m$ הביטים. נעשה זאת בעזרת $C_{in}: (F_{2^m}) \to (F_2)^{2m}$, כך שלכל $\sigma_1 \neq \sigma_2 \in F_{2^m}$, אם המרחק של C_{in} הוא d אז $C_{in}(\sigma_1), C_{in}(\sigma_2)$ שונים ב d מקומות.

Concatenated Codes הינם זוג קודים $C_{out}: \Sigma^{k_{out}} \to \Sigma^{n_{out}}, C_{in}: (F_2)^{\log|\Sigma|} \to (F_2)^{n_{in}}$, כך שאם $C_{out} = [n_{out}, k_{out}, d_{out}], C_{in} = [n_{in}, \log_2|\Sigma|, d_{in}]$, ניתן לשרשר אותם ולבנות את הקוד $\boldsymbol{C_{out} \circ C_{in}}$.

$$\boxed{m_1m_2\dots m_k \to C_{out}(m_1m_2\dots m_k) = c_1c_2\dots c_{n_{out}} \to C_{in}(c_1)C_{in}(c_2)\dots C_{in}(c_{n_{out}}) = c'_1c'_2\dots c'_{n_{out}}}$$



<u>טענה:</u> האורך של הקוד $C_{in} \diamond C_{out}$ הינו $n_{in} \cdot n_{out}$ ביטים.

<u>הסבר:</u> האורך של C_{out} הינו n_{out} סימבולים שכל אחד מהם מקודד ל n_{in} ביטים.

<u>טענה:</u> מימד של הקוד $C_{in} \diamond C_{out}$ הינו $k_{in} \cdot k_{out}$ ביטים.

<u>הסבר:</u> מספר הביטים הכולל הינו $k_{in} \cdot k_{out} = \log_2|\Sigma| \cdot k_{out} = \log_2|\Sigma|^{k_{out}}$.

<u>טענה:</u> המרחק של הקוד $C_{in} \diamond C_{out}$ הינו $d_{in} \cdot d_{out}$.

<u>הסבר:</u> יהיו $m_1, m_2 \in \Sigma^{k_{out}}$ כך ש $m_1 \neq m_2$. לכן, $C_{out}(m_1), C_{out}(m_2)$ שונים בלפחות d_{out} מקומות. $C_{out}(m_1) \neq C_{out}(m_2)$, לכן $C_{in}\left(C_{out}(m_1)\right), C_{in}(C_{out}(m_2))$ שונים בלפחות d_{in} מקומות. בסה"כ קיבלנו כי המרחק של הקוד $C_{in} \diamond C_{out}$ הינו $d_{in} \cdot d_{out}$.

$$[n_{out}, k_{out}, d_{out}]_q \diamond [n_{in}, k_{in}, d_{in}]_2 \rightarrow [n_{out} \cdot n_{in}, k_{out} \cdot k_{in}, d_{out} \cdot d_{in}]_2$$

<u>$C_{out} = RS$</u>

לפי מה שלמדנו על RS מתקיים כי:

$$C_{out} = [n = 2^m, k, n-k+1], R_{out} = \frac{k}{n}, \delta_{\text{out}} = 1 - R_{out} = 1 - \frac{k}{n}$$

ע"פ משפט Gillber-Uarshamov קיים קוד C_{in} כך ש:

$$R_{in} = r, \delta_{in} = h^{-1}(1-r)$$

מכאן, נוכל לבנות $C_{in} \diamond C_{out}$ המקיים:

$$R_{conc} = R_{out} \cdot R_{in} = \frac{kr}{n}, \delta_{conc} = \delta_{out} \cdot \delta_{in} = \left(1 - \frac{k}{n}\right) \cdot h^{-1}(1-r)$$

<u>מסקנה:</u> אם $R_{out}, R_{in} > 0$ אזי $R_{conc}, \delta_{conc} > 0$.

<u>בעיה:</u> הקוד הפנימי אינו קוד מפורש! (אך אורכו הינו $logn$, קצר).

<u>Zgablov Bound</u>

<u>משפט:</u> לכל $R \in (0,1)$ קיים קוד מפורש במרחק $\delta_{zgablov}(R)$,

כאשר $\delta_{zgablov}(R) = \max_{R \leq r \leq 1}\{\left(1 - \frac{R}{r}\right) h^{-1}(1-r)\}$.