כללי

הגדרות כלליות:
*** בכל הדף הוקטורים הם וקטורי שורה, פרט לוקטור סינדרום.**

קבוצת אלף-בית:
אוסף אלמנטים המכונים סימבולים (למשל סיביות).
קבוצה המכילה את כל הסימבולים תסומן ב- A.

גודל של אלף-בית:
גודל הא"ב הוא מס' האיברים ב- A.

$$q \triangleq |A|$$

מילה:
מילה היא סדרת סימבולים.

קוד:
קוד הוא אוסף שלך מילים שמכונות מילות קוד.
קוד מאופיין ע"י:

$$C(n,k,d_{\min})$$

n - אורך מילת הקוד
k - אורך מילת המקור
d_{min} - המרחק המינימלי בין כל 2 מילות קוד

קידוד:
העתקה של מילת מקור למילת קוד.

אורך מילת מקור מסומן ב- k.
אורך מילת קוד מסומן ב- n.

קצב הקוד:
קצב של קוד המכיל M מילים באורך n מעל Fq מוגדר כך:

$$k \triangleq \log_q M$$

$$R = \frac{\log_q M}{n} = \frac{k}{n}$$

קוד בלוק:
קוד בלוק הוא קוד שבו לכל מילת קוד יש אורך זהה ואורך זה נקרא אורך הקוד ומסומן ב- n .

מרחק:
"מרחק" היא פונקציה שמקיימת את האקסיומות הבאות:

$$d(x,y) \geq 0 \; ; \; d(\underline{x},\underline{x}) = 0$$

$$d(\underline{x},\underline{y}) = d(\underline{y},\underline{x})$$

$$d(\underline{x},\underline{y}) + d(\underline{y},\underline{z}) \geq d(\underline{x},\underline{z})$$

משקל המינג:
מספר האיברים השונים מאפס (מרחק המילה ממילת האפס).

$$w_H(\underline{x}) = d_H(\underline{x},\underline{0})$$

מרחק המינג:
נתונים 2 וקטורים - x,y 4.
מרחק המינג הוא משקל המניג של הפרש המילים.

$$d_H(\underline{x},\underline{y}) = w_H(\underline{x}-\underline{y})$$

קוד קונבולוציה:
קוד הנוצר ע"י הזנת סדרה אינסופית של סימבולים למעגל LTI.

ערוץ:
הערוץ כולל רעש חיצוני, עיוות מהמודולטור ועיוות מהדה-מודולטור.

ערוץ חסר זיכרון:
זה ערוץ שמקיים:

$$\underline{c} \rightarrow \boxed{h} \rightarrow \underline{r}$$

$$\underline{c} = (c_1,..,c_n) \quad ; \quad \underline{r} = (r_1,..,r_n)$$

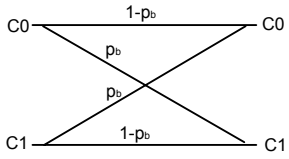
$$\Pr\{\underline{r}/\underline{c}\} = \prod_{i=1}^{n} \Pr\{r_i/c_i\}$$

הערה:
- כל הפעלת ערוץ לא תלויה בהפעלת הערוץ הקודמת (בת"ס).

ערוץ קבוע בזמן (TI):
הסתברות המעבר של הערוץ לא משתנה בזמן:

$$\Pr\{r_i/c_i\} = \Pr\{r_j/c_j\}$$

ערוץ BSC (Binary Symmetric Channel):
ערוץ זה מוגדר מעל שדה בינארי.
זה ערוץ חסר זיכרון, קבוע בזמן ובעל הסתברויות מעבר כדלקמן:



$$r,c,e \in \{0,1\}$$

$$r = c + e$$

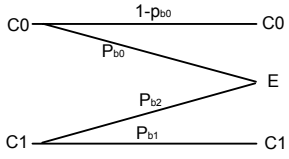
בערוץ זה, אחרי הוספת הרעש, או שהערך נשאר כמו שהיה או שהוא מתהפך.

הסתברות השגיאה:

$$\underline{e} = \underline{r} - \underline{c}$$

$$P(\underline{e}) = p^{W_H(\underline{e})} \cdot (1-p)^{n-W_H(\underline{e})}$$

ערוץ BEC (Binary Erasure Channel):
ערוץ זה מוגדר מעל שדה בינארי.
זה ערוץ חסר זיכרון, קבוע בזמן ובעל הסתברויות מעבר כדלקמן:



בערוץ זה, יכולים להיות 3 מוצאים: 1, 0, מחיקה.
אם קיבלנו 0 אז בטוח שודר 0.
אם קיבלנו 1 אז בטוח שודר 1.
אם קיבלנו מחיקה, אז לא יודעים מה שודר.

קודי בלוק ליניאריים

שדה:
אוסף אלמנטים המקיימים תכונה מסויימת.

שדה Fq:
נגדיר קבוצה הא-ב Zq:

$$Z_q \triangleq \{0,1,2,...,q-1\}$$

הקבוצה Zq ביחד עם פעולות חיבור Modulus ופעולות כפל Modulus, מהווה שדה Fq אמ"מ n ראשוני.

סימוני מודולו:

$$a \bmod b \equiv [a]_b$$

מרחב וקטורי:
מרחב וקטורי מוגדר מעל שדה.

$$F_q^n$$

n - מימד כל וקטור בשדה.
q - גודל קבוצת הא-ב.

מרחב וקטורי חייב להכיל את איבר האפס.
סקלר הוא אלמנט של שדה.

סגירות:
פעולות בין 2 וקטורים במרחב הוקטורי, יתנו וקטור השייך לאותו מרחב.

דוגמא:
מחפשים כמה שווה ¼ מעל השדה F7 (0..6)

$$\frac{1}{4} = ? = x \in F_7$$

$$\bmod(4 \cdot x) = 1 \Rightarrow 4 \cdot 2 = 8 \Rightarrow 8 \bmod 7 = 1$$

קוד ליניארי:
קוד ליניארי C(n,k) מעל שדה Fq הוא תת מרחב k מימדי של F_q^n
תכונות:
- קומבינציה ליניארית של כל 2 מילים היא מילת קוד (סגירות).
- מספר מילות הקוד הוא q^k.
- מילת ה- "0" היא תמיד מילת קוד.

מטריצה יוצרת - G:
מטריצה G, ששורותיה הן וקטורי הבסיס של הקוד C, נקראת מטריצה יוצרת (של הקוד C).

$$\underbrace{\underline{c}}_{[1\times n]} = \underbrace{\underline{m}}_{[1\times k]} \cdot \underbrace{G}_{[k\times n]}$$

הערות:
- לכל קוד C יכולות להיות מספר מטריצות G.
- עבור Gים שונים, למילת מקור עלולה להיות מותאמת מילת קוד שונה (תהליך הקידוד השתנה). אולם, תמיד קבוצת מילות הקוד תישאר זהה.
- פעולות שורה על G לא משנות את מילות הקוד.
- פעולות עמודה על G משנות את מילות הקוד.
- אם הערוץ בעל זיכרון, פעולות על העמודות משנות את ביצועי הקוד.
- אם הערוץ ללא זיכרון, פעולות על העמודות לא משנות את ביצועי הקוד.
- כל שורה במטריצה G היא מילת קוד ב- C.

קידוד ליניארי:
כאשר הפונקציה שיוצרת את הקוד מקיימת ליניאריות.

הערות:
- אם הקוד ליניארי - אז הקידוד **לא בהכרח** ליניארי.
- אם הקידוד ליניארי - אז הקוד בטוח ליניארי.
- אם מילת מקור האפס לא עוברת למילת קוד האפס - אז הקידוד לא ליניארי.

קוד שקול:
2 קודים נקראים שקולים אם ניתן לקבל אחד מהשני ע"י:
- פרמוטציית עמודות (החלפת עמודות).
- הסתכלות על עמודה, והחלפת בין סימבול אחד לאחר בכל המופיעים שלו באותה עמודה:

$$\begin{pmatrix} a & \boxed{a} & c \\ d & e & f \\ a & b & c \end{pmatrix} \xrightarrow{col3:\, b \leftrightarrow a} \begin{pmatrix} a & \boxed{b} & c \\ d & e & f \\ a & a & c \end{pmatrix}$$

- הכפלת כל עמודה בקבוע משלה (D - מטריצה אלכסונית):

$$G' = G \cdot D$$

מטריצת מדורגת קנונית - RRE:
(Row Reduced Echelon)

הגדרת איבר מוביל:
לכל שורה יש איבר מוביל משלה.
האיבר המוביל הוא הראשון משמאל, השונה מאפס, בכל שורה במטריצה.

הגדרת מטריצת RRE:
מטריצה שבה מעל ומתחת כל איבר מוביל יש רק אפסים, ושורותיה מדורגות (משמאל לימין).
אם במטריצת RRE יש שורת אפסים תמיד נעבירה לסוף.

דוגמא:

$$G = \begin{pmatrix} \underline{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \underline{1} & 0 & 1 \\ 0 & 0 & 0 & \underline{1} & 1 \end{pmatrix}$$

(האיברים המובילים המדורגים מסומנים עם קו למטה)

הערות:
- כל מטריצה יכולה להגיע למצב RRE ע"י פעולות שורה.
- לכל מטריצת G יש צורת RRE אחת ויחידה.
- אם קיבלנו שורת אפסים ב- RRE אז אפשר למחוק אותה, (וזה אומר שיש ב- G המקורית שורות תלויות).

קידוד סיסטמטי (שיטתי):
כל קידוד ש- G נראית מהצורה הבאה הוא קידוד סיסטמטי:

$$\underline{m} \cdot \underbrace{\left(I_k \quad P_{k\times(n-k)}\right)}_{G'} = \underline{c} = \left(\underline{m} \quad \underline{m} \cdot P\right)$$

כלומר, במילת הקוד ניתן לזהות את ביטי המקור ואת ביטי היתירות.

הערות:
- קיימת הגדרה נוספת לקידוד סיסטמטי: קוד שבוא כל אחת מסיביות המקור מופיעה במילת הקוד ללא חשיבות לסדר ולמיקום סיביות המקור.
לפני הגדרה זו, אם נבחר את G כ- RRE נבחר כבר קוד סיסטמטי.
- כל קוד ליניארי ניתן לקודד בצורת שיטתית.

סד"פ למציאת קוד סיסטמטי:
- נתונה G שאינה RRE.
- מביאים את G למצב RRE ע"י פעולות שורה בלבד.
- מביאים את GRRE למצב שיטתי ע"י החלפת עמודות בלבד:

$$G' = \left(I_k \quad P_{k\times(n-k)}\right)$$

קוד ססתמטי (שיטתי):
קוד, שאינו בהכרח ליניארי, נקרא ססתמטי אם קיים עבורו קידוד ססתמטי.

מטריצת בדיקת זוגיות - H:
הגדרה:
נתון קוד ליניארי C.
אוסף כל הוקטורים אשר ניצבים ל- C נקרא **קוד דואלי** ומסומן כך:

$C^{\perp}$

המטריצה היוצרת של הקוד הדואלי מסומנת ב- H ונקראת מטריצת בדיקת הזוגיות:

$$\underbrace{\underline{c}^{\perp}}_{1\times n} = \underbrace{\underline{\tilde{m}}}_{1\times n-k} \cdot \underbrace{H}_{n-k\times n}$$

יש לשים לב שאורך מילות המקור m שונה.

הערות:
- מטריצה H בודקת זוגיות רק במקרה הבינארי.
- תמיד מתקיים:

$$H \cdot G^T = \underline{\underline{0}}$$
$$H \cdot \underline{c}^T = \underline{0}$$
$$\underline{c}^{\perp} \cdot \underline{c}^T = 0$$

משפט:
השורות של G ו- H (וקטורי בסיס) לא בהכרח פורשות את כל המרחב.

סד"פ למציאת מטריצה H:
- מביאים את G למצב RRE.
- מביאים את G למצב שיטתי ע"י החלפת עמודות בלבד (יש לזכור את סדר החלפת העמודות).

$$G' = \left(I_k \quad P_{k\times(n-k)}\right)$$

- נגדיר את H' באופן הבא:

$$H' = \left(-\left(P_{k\times(n-k)}\right)^T \quad I_{n-k}\right)$$

- נבצע את פרמוטציית העמודות שוב אך **בסדר הפוך** לקבלת H.

הערה - קשר בין G ל- H:
אם H מהצורה הבאה:

$$H = \left(I \quad -P^T\right)$$

אז G תהיה מהצורה:

$$G = \left(P \quad I\right)$$

מציאת dmin של C באמצעות H:
מספר העמודות התלויות (ליניארית) המינימלי ב- H הוא d_{min}.

הגדרת תלות ליניארית:

$$\underline{h}_0 \cdot c_0 + \underline{h}_1 \cdot c_1 + \ldots + \underline{h}_{n-1} \cdot c_{n-1} = \underline{0}$$

כל n וקטורים שמקיימים את התנאי הנ"ל, תלויים ליניארית.
(אם נניח שאחד ה- c'ים שווה 1 ונעביר את האיבר המתאים אגף, נגלה שהוא קומבינציה ליניארית של השאר).

כללי אצבע (מעל שדה בינארי):
- אם יש עמודת אפסים ב- H אז $d_{min}=1$.
- אם יש **לפחות** 2 עמודות זהות אז $d_{min}=2$.

מספר העמ' בת"ל ב- H =< d_{min}

דוגמא:

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

כאן יש 3 עמודות זהות. כלומר יש תלות מינימלית בין 2 עמודות ולכן dmin=2.

חסמים על dmin (עבור קודים ליניארים):
חסם Singleton -

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

חסם Hamming -

$$\sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i \le q^{n-k}$$

קוד MDS (Max Min Distance Seperable):
קוד MDS הוא קוד ש"משיג" את חסם Singleton כלומר:

$$d = n-k+1$$

קוד מושלם:
קוד ש"משיג" את חסם Hamming נקרא "קוד מושלם".

פענוח קודים

הגדרת סינדרום:

$$\underline{r} = \underline{c} + \underline{e}$$

$$\underbrace{\underline{s}}_{[(n-k)\times 1]} \triangleq \underbrace{H}_{[(n-k)\times n]} \cdot \underbrace{\underline{r}^T}_{[n\times 1]} = H(\underline{c}^T + \underline{e}^T) = \underbrace{H \cdot \underline{c}^T}_{0} + H \cdot \underline{e}^T = H \cdot \underline{e}^T$$

- **הסינדרום הוא בעל k-n ביטים.**

הגדרת Co-Set:

$$co-set = \underline{z} + C \triangleq \left\{\underline{z} + \underline{c} : \underline{c} \in C\right\}$$

הערות:
- הקוסטים פורשים את כל המרחב (לא רק את מילות הקוד).
- בין C ל- co-set שלו יכול להיות חיתוך.

משפטים:
- 2 קוסטים של אותו הקוד **(ליניארי)** - או שהם זהים או שהם זרים (עקב המודלו).
- אם מילת קוד $\underline{c}$ (בקוד ליניארי) שייכת ל- 2 קוסטים אז הם זהים.

כללי פענוח:

$$\underbrace{\max_{\underline{c}\in C}\left\{P(\underline{c}/\underline{r})\right\}}_{MAP} = \underbrace{\max_{\underline{c}\in C}\left\{P(\underline{r}/\underline{c})\right\}}_{ML} = \max_{\underline{e}}\left\{P(\underline{e})\right\}$$

$$\hat{c} = \arg\max_{\underline{c}\in C}\left\{P(\underline{r}/\underline{c})\right\} = \arg\min_{\underline{c}\in C}\left\{d_H(\underline{c},\underline{r})\right\} = \underline{r} - \arg\min_{\underline{e}\ s.t\ H\underline{e}^T=\underline{s}}\left\{w_H(\underline{e})\right\}$$

הערה:
- הסינדרום מממש את כלל Maximum Likelihood (MAP) עובר הסתברויות א-פריוריות שוות).

פענוח בעזרת סינדרום (תיקון שלם):
נתון r (המילה שהתקבלה מהערוץ) ומעוניינים למצוא את c שנשלחה:
- רושמים את כל אפשרויות לוקטורי סינדרום בטבלה.
- ליד כל סינדרום רושמים את e המתאים לו **בעל המשקל המינימלי**.
- אם יש כמה אפשרויות (עם משקל מינימלי) אז בוחרים אחת מהם באופן אקראי.
- ל- e עם משקל מינימלי קוראים "מוביל" (יש לשים לב שאין קשר לאיבר "מוביל" שהוגדר בתוך מטריצת RRE).
- עבור ה- r הנתון, מחשבים את הסינדרום.
- לפי הסינדרום, מוצאים את e מהטבלה ומחסרים אותו מ- r למציאת מילת הקוד המפוענחת.

ובקיצור:
מ- r מוצאים את s. ואז, מחפשים את המילה (בעלת המשקל הנמוך ביותר = e) שמכפלתה ב- H תתן את s.

$$H \cdot \underline{r}^T = \underline{s}$$
$$\Rightarrow \underline{s} = H \cdot \underline{e}^T \Rightarrow \underline{e}$$
$$\Rightarrow \underline{c} = \underline{r} - \underline{e}$$

סיבוכיות הפענוח (כמספר הסינדרומים):

$$2^{n-k}$$

הסתברות השגיאה בפענוח:
P_b - ההסתברות שביט אחד יתהלף.
A_i - מספר המובילים עם משקל המינג i.

$$P_{error} = 1 - \sum_{i=0}^{n} A_i \left(1-P_b\right)^{n-i} P_b^i$$

חסם על הסתברות השגיאה:

$$P_{error} \le 1 - P\left\{\text{the noise created an error with } w_H \le t\right\}$$
$$= 1 - \sum_{i=0}^{t} \binom{n}{i} \left(1-P_b\right)^{n-i} P_b^i \quad ; \quad \binom{n}{i} \triangleq \frac{n!}{i!(n-i)!}$$

תיקון אחיד:
תיקון המסתמך על איזורי החלטה בצורת עיגולים שרדיוסם הוא רדיוס האריזה t:

$$t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$$

t - רדיוס האריזה - יכולת התיקון של הקוד.
בודאות ניתן לתקן t שגיאות (עבור שגיאות מסוימות, לפעמים נוכל לתקן יותר מ- t שגיאות).

הקשר בין תיקון אחיד לתיקון שלם:
- תיקון שלם "אוגר" בתוכו יותר אינפורציה לגבי יכולת התיקון (כלומר, ניתן לדעת איפה השגיאות המסוימות עם יותר מ- t שגיאות, שאותן נוכל לתקן גם כן).
- בתיקון שלם לכל מוביל קיים t משלו.
- יכולת התיקון של תיקון אחיד היא ה- t המינימלי (מבין כל המובילים).

הערה:
ניתן להקטין את יכולת התיקון של הקוד, ועקב כך להגדיל יכולת הגילוי (ע"י יצירת קוד חדש).

סוגי קודים

קוד אוניברסלי:

$$G = I_n$$

לקוד זה אין מטריצת בדיקה.

קוד חזרה:
זהו קוד MDS - מקיים את חסם סינגלטון מעל כל שדה.
קוד חזרה באורך אי-זוגי הוא מושלם (משיג את חסם המינג).

$$\underbrace{G}_{1\times n} = (1 \ldots 1)$$

$$H = \begin{pmatrix} -1 \\ \vdots \ I_{n-1} \\ -1 \end{pmatrix}$$

קוד עם בדיקה בודדת:

$$G = \begin{pmatrix} -1 \\ \vdots \ I_{n-1} \\ -1 \end{pmatrix}$$

$$\underbrace{H}_{1\times n} = (1 \ldots 1)$$

קוד המינג:
קוד ליניארי בעל אורך מקסימלי בעל b=n-k נתון, ומקיים t=1.
b - מספר ביטי בדיקה.

קוד המינג בינארי:

$$b = n-k$$
$$n = 2^b - 1$$
$$t = 1$$
$$d_{\min} = 3$$

הערה:
- כדי שנקבל ב- H מינימום 3 עמודות תלויות, אסור שתהיה עמודת אפסים, ואסור שיהיו 2 עמודות זהות. לכן מספר העמודות ב- h (n) הוא b^2 פחות 1 (עמודת האפס).
- מכיוון ש- b קבוע, אם נחפש n מקסימלי, נקבל גם k מקסימלי.

קוד המינג מעל GF(q):

$$H = \begin{pmatrix} 1 & x & x & & x & x \\ 0 & 1 & x & & \vdots & \vdots \\ \vdots & 0 & 1 & \ldots & x & x \\ \vdots & \vdots & \vdots & & 1 & x \\ 0 & 0 & 0 & & 0 & 1 \\ \underbrace{}_{q^0\ options} & \underbrace{}_{q^1 options} & \underbrace{}_{q^2 options} & & \underbrace{}_{q^{b-2} options} & \underbrace{}_{q^{b-1} options} \end{pmatrix}$$

כל עמודה במטריצה הנ"ל מסמלת מס' רב של עמודות כפי שרשום מתחתיה.

צריך q^b-1 עמודות בלתי תלויות במטריצה H.

$$n = 1 + q + q^2 + \ldots + q^{b-2} + q^{b-1} = \frac{q^b - 1}{q-1}$$

הערה:
עבור n שואף לאינסוף, יכולת התיקון שואפת לאפס (כי אף פעם לא יהיו מספיק ביטי זוגיות שילמדו אותנו כיצד לזהות ולתקן את השגיאות).

שינויים על קודים

סוגי שינויים:

פעולה	משמעות על G ו- H	תכונות
דילול	מחיקת שורה ב- G הוספת שורה (בלתי-תלויה) ב- H	$n'=n$ $k'=k-1$ $d'\geq d$
הגדלה	הוספת שורה (בלתי-תלויה) ב- G מחיקת שורה ב- H	$n'=n$ $k'=k+1$ $d'\leq d$
ניקוב	מחיקת עמודה ב- G מחיקת עמודה ושורה ב- H	$n'=n-1$ $k'=k$ $d'=d\ or\ d-1$
הרחבה	הוספת עמודה ב- G הוספת עמודה ושורה ב- H	$n'=n+1$ $k'=k$ $d'=d\ or\ d+1$
קיצור	מחיקת עמודה ושורה ב- G מחיקת עמודה ב- H	$n'=n-1$ $k'=k-1$ $d'\geq d$
הארכה	הוספת שורה ועמודה ב- G הוספת עמודה ב- H	$n'=n+1$ $k'=k+1$ $d'\leq d$

הערות:
- דילול, ניקוב, או הרחבה הם הגדלה, קיצור או הארכה של הקוד הדואלי בהתאמה.
- אם הממד ירד בדרגה אחת, אז חצי מהמילים נעלמו.
- הוספת שורה של אחדים ב- H (מחיקת שורה ב- G), מורידה חצי מהמילים (בגלל שירד מימד), אבל היא מורידה את כל מילות הקוד עם משקל אי-זוגי או זוגי (תלוי אם n הוא זוגי או אי-זוגי).

טכניקות שינוי (קיצור וניקוב):

אלגוריתם שינוי פרמיטיבי:
- נכתוב את כל מילות הקוד.
- נמחק מתוכן את כל המילים בעלות ערך שונה מאפס בעמודה ה- i.
- נשאר רק עם המילים שהיה להן 0 בעמודה ה- i, ואז פשוט נעלים את הביט ה- i בכל מילת קוד.

לחילופין - אם מדובר במחיקת שורה בודדת או עמודה בודדת - אז פשוט מוחקים את השורה או העמודה הדרושה מ- G או מה- H.

אלגוריתם שינוי לא פרמיטיבי:
כאשר יש צורך למחוק עמודה ושורה מ- G או מ- H, נבצע פעולות שורות עד שנגיע למצב שבו, בעמודה שרוצים למחוק, יש רק "אפסים", מלבד בשורה אחת.
ואז נמחוק את העמודה הדרושה, ואת השורה המתאימה בה אין "אפס".

בניית קודים מקודים פשוטים:

נתונים 2 קודים **שונים** (**בביט אחד לפחות**):

$\underline{c}_1\in C_1(n_1,k_1,d_1)$

$\underline{c}_2\in C_2(n_2,k_2,d_2)$

מתוך קומבינציה של c1,c2 נרכיב מילה חדשה, למשל:

$c_3=(\underline{c}_1,\underline{c}_1+\underline{c}_2)$

ולכן הקוד החדש יקיים:

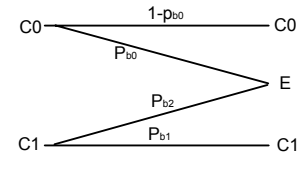
$n_3=2\cdot n\quad ;\quad k_3=k_1+k_2$

$G_3=\begin{pmatrix}G_1 & G_1\\ 0 & G_2\end{pmatrix}\quad ;\quad d_{\min}=\min(2d_1,d_2)$

ערוץ מחיקה

הגדרת ערוץ מחיקה:

ערוץ זה מוגדר מעל שדה בינארי.
זה ערוץ חסר זיכרון, קבוע בזמן ובעל הסתברויות מעבר כדלקמן:



הערה:
ערוץ זה משמש למידול קליטת אות חלש כמחיקה.

הגדרת הבעיה:

נתון קוד C(n,k,d).
למחיקות בערוץ נתייחס כניקוב בקוד.

יכולת התיקון:
קוד המקיים:

$d\geq 2t+1+w_E$

מסוגל לתקן w_E מחיקות ו- t שגיאות.

סד"פ פענוח קוד שעבר ערוץ מחיקה:

- נקלטה מילה עם מחיקה במקום ה- i.
- נבצע ניקוב למטריצה G בעמודה ה- i.
- נמצא את H (לקוד המנוקב).
- נמצא את הסינדרום המתאים (לקוד המנוקב).
- מתוך הסינדרום נמצא את המוביל (e).
- נמצא את מילת הקוד המנוקבת (r-e = c).
- נמצא את מילת הקוד (הלא מנוקבת) ע"י הוספת הביט "המחוק" ובדיקה האם המילה שהתקבלה מאפסת את הסינדרום:

$\underline{s}=\underline{0}=H\cdot\underline{c}^T$

קוד ציקלי

הגדרת קוד ציקלי:

- קוד הוא ציקלי אם הוא לינארי, ואם כל הזזה ציקלית של מילה בקוד, היא גם מילת קוד.
- קודים ציקליים הם תת-קבוצה בקודים הלינאריים.
- הם מקיימים סגירות תחת פעולת ההזזה (כל הזזה של מילה בקוד, או קומבינציה לינארית של הזזות היא גם מילה בקוד).
- היתרון בשימוש בקודים ציקליים הוא ביכולת פענוח ע"י מעגלים פשוטים יחסית.

סימון חלוקה:

$a\,|\,b\Rightarrow b=a\cdot N\ ;\ N\in\mathbb{Z}$

סימון קונגרואנטיות (שקילות):

$a\equiv b \bmod m \Leftrightarrow a \bmod m = b \bmod m$

$\Rightarrow a-b=0 \bmod m \Rightarrow a-b=N\cdot m\ ;\ N\in\mathbb{Z}$

הכוונה היא שמכירים רק מספרים בין 0...m-1 וההפרש בין a ל- b מתחלק ב- m ללא שארית.

הגדרת שארית:

$a=k\cdot b+[a]_b\quad k\in\mathbb{Z}$

$[12]_5=2\ ,\ [7]_5=2\ ,\ [12]_5\neq 7$

כללים:

$[a\cdot b]_c=\big[[a]_c\cdot[b]_c\big]_c$

$[a+b]_c=\big[[a]_c+[b]_c\big]_c$

הזזה ציקלית:

$\underline{y}=(y_0,y_1,...,y_{n-1})\Rightarrow y(x)=y_0+y_1\cdot x+...+y_{n-1}\cdot x^{n-1}$

$\underline{y}'=(y_{n-1},y_0,...,y_{n-2})\Rightarrow y'(x)=y_{n-1}+y_0\cdot x+y_1\cdot x^2+...+y_{n-2}\cdot x^{n-1}$

$\underline{y}'(x)\triangleq[x\cdot y(x)]_{x^n-1}$

פולינום יוצר של קוד ציקלי:

- לכל קוד ציקלי קיים פולינום **מוני** יחיד g(x) בעל מעלה מינימלית מבין כל הפולינומים של מילות הקוד.
- יצירת מילת הקוד מתבצעת ע"י הכפלת פולינום מילת המקור בפולינום היוצר.
- הפולינום היוצר הוא מילת קוד (עם המעלה הנמוכה ביותר).

פולינום מוני = המקדם של ה- x עם המעלה הכי גבוהה הוא 1.

משפט:
מילה שייכת לקוד אמ"מ היא מקיימת:

$\deg(c(x))\leq n-1$

$c(x)=0 \bmod g(x)\Rightarrow g(x)\,|\,c(x)$

הערות:

$b\triangleq\deg(g(x))=n-k$

$x^n-1\equiv 0 \bmod g(x)\Rightarrow g(x)\,|\,x^n-1$

$\dim C=n-b=n-\deg(g(x))$

Dim - מספר וקטורי הבסיס שפורשים את הקוד.

$\deg(m(x))\leq k-1$

g(x) כפול פולינום m(x) ייתן מילת קוד תקינה c(x) אמ"מ המעלה של m(x) קטנה או שווה ל- k-1.

מטריצה היוצרת של קוד ציקלי:

$g(x)=g_0+g_1x+...+g_{b-1}x^{b-1}+\underbrace{g_b}_{=1}\cdot x^b$

$G=\begin{pmatrix}g_0 & g_1 & g_2 & \cdots & g_b & 0 & \cdots & 0\\ 0 & g_0 & g_1 & g_2 & \cdots & g_b & 0 & \vdots\\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & 0\\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_b\end{pmatrix}$

פולינום בדיקה

$h(x)\triangleq\frac{x^n-1}{g(x)}$

המעלה של h(x) היא k.

c היא מילת קוד אמ"מ:

$c(x)h(x)=0 \bmod g(x)$

מטריצת בדיקת הזוגיות של קוד ציקלי:

$h(x)=h_0+h_1x+...+h_{k-1}x^{k-1}+\underbrace{h_k}_{=1}\cdot x^k$

$H=\begin{pmatrix}0 & \cdots & 0 & h_k & \cdots & h_2 & h_1 & h_0\\ 0 & 0 & h_k & \cdots & h_2 & h_1 & h_0 & 0\\ \vdots & \vdots & \iddots & \iddots & \iddots & \cdots & \iddots & 0\\ h_k & \cdots & h_2 & h_1 & h_0 & 0 & \cdots & 0\end{pmatrix}$

יצירת קוד ציקלי:

ניתן להתייחס למילת קוד כפולינום באופן הבא:

$101\Rightarrow m(x)=1+0\cdot x+1\cdot x^2=1+x^2$

באותו אופן ניתן לייצג את g(x). למשל:

$G=\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}\Rightarrow g(x)=1+x+x^2+x^3$

ואז הקוד הציקלי המתקבל הוא:

$c(x)=m(x)\cdot g(x)=1+x^3+x^5+x^6$

קצב הקוד:
- בקודים ציקליים אנו מזינים רצף של ביטי מקור לתוך מעגל בעל רכיבי השהיה, ובמוצא מקבלים רצף של ביטים מקודדים.

קידוד ציקלי שיטתי ולא שיטתי:

קידוד ציקלי לא שיטתי:

$c(x)=m(x)\cdot g(x)$

קידוד ציקלי שיטתי:

$c(x)=m(x)\cdot x^{n-k}-\big[m(x)\cdot x^{n-k}\big]_{g(x)}$

<u>מימוש בעזרת מטריצה G</u>

$G=(B,I_k)$

שורות B נתונות ע"י המשוואה הבאה:

$\big[-x^{n-k}\cdot x^j\big]_{g(x)}\quad j=0,1,2,...,k-1$

דוגמא:

$g(x)=x^4+x+1;\ n=15$

$x^4\equiv x+1\ ,\ x^5\equiv x^2+x\ ,\ x^6\equiv x^3+x^2,\cdots,x^{15}\equiv 1$

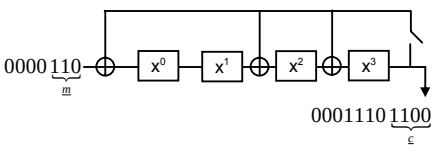
$\underset{[11x15]}{G}=\begin{pmatrix}\overset{x^0}{1} & \overset{x^1}{1} & \overset{x^2}{0} & \overset{x^3}{0} & \\ 0 & 1 & 1 & 0 & I\\ 0 & 0 & 1 & 1 & \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}$

מקודד ציקלי לא שיטתי (מעגל שארית):

המקודדים הבאים מדגימים את חישוב הביטוי:

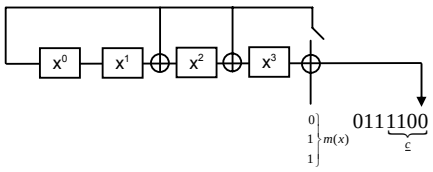
$\big[m(x)\cdot x^{n-k}\big]_{g(x)}=\big[(1+x)\cdot x^4\big]_{1+x^2+x^3+x^4}\triangleq\underline{c}$

$\underline{m}=110$



- למעשה זהו מעגל חלוקה ב- g(x).
- מכניסים את n הביטים המייצגים את $m(x)\cdot x^{n-k}$ (קודם את המעלה הגבוהה).
- לאחר שכל המילה נכנסה למעגל (בדוגמא הנ"ל לאחר 7 הזזות), המתג נפתח (נתק).
- כרגע התשובה אגורה בתוך הרגיסטרים.
- נמשיך לבצע k הזזות עד אשר נקבל את כל מילת הקוד הציקלית ביציאה.
- סה"כ דרוש למעגל n-k+n הזזות לקבלת מילת הקוד.

מקודד ציקלי שיטתי עם הזנה ימנית:



- בדוגמא זו שוב מזינים את k ביטי המקור (מהמעלה הגבוהה לנמוכה).
- המתג ייסגר ואז ויידרשו עוד n-k הזזות כדי לקבל את מילת הקוד במוצא המעגל.
- במעגל זה דרושות n הזזות לקבלת מילת הקוד השיטתית.

הערה:
מקודד זה מספק במוצא גם את ביטי המקור וגם את ביטי המודולו ובכך מספק את כל מילת הקוד השיטתית.

מקודד (שיטתי) מבוסס h(x):

מספר הרגיסטרים במעגל ייקבע ע"י המעלה של h(x) (מעלה k=3 תתקן 3 רגיסטרים).

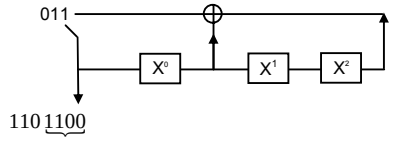
$$H\cdot \underline{c}^T=\underline{0}\Rightarrow c(x)h(x)=0 \bmod x^n-1$$

$$c_i=-\frac{1}{\underbrace{h_k}_{=1}}\sum_{m=0}^{k-1}h_m c_{i-m-k}$$

$$=-h_0\cdot c_{i+k}-h_1\cdot c_{i-1+k}-h_2\cdot c_{i-2+k}-\ldots-h_{k-1}\cdot c_{i+1}$$

מימוש עבור k=3 מעל בינארי:

$$c_i=h_0\cdot c_{i+3}+h_1\cdot c_{i+2}+h_2\cdot c_{i+1}=c_{i+3}+c_{i+1}$$



- בדוגמא זו שוב מזינים את k ביטי המקור בסדר הפוך (ביחס להזנה שמאלית). מתעלמים מהאפסים שמייצגים את המעלות הנמוכות יותר.
- לאחר מכן הוא נסגר (המעגל לא מקבל יותר סיביות בכניסה), ודרושות עוד n-k הזזות נוספות לקבלת מילת הקוד.
- סה"כ במעגל זה דרושות n הזזות לקבלת מילת הקוד.

הערה:
מקודד זה מספק במוצא גם את ביטי המקור וגם את ביטי המודולו ובכך מספק את כל מילת הקוד השיטתית.

מפענח קוד ציקלי (מפענח מגיט):

נתון קוד c(17,9,5) עם פולינום יוצר:

$$g(x)=1+x+x^2+x^4+x^6+x^7+x^8$$

המילה המתקבלת:

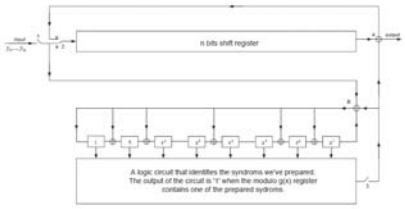
$$y(x)=c(x)+e(x)$$

הסינדרום נתון ע"י:

$$s(x)=\left[y(x)\right]_{g(x)}$$

s(x) הוא ממעלה n-k-1.

מעגל החלוקה המחזיר את המילה המתוקנת עבור y(x):
- בבסיס המעגל הבא יש מעגל חלוקה של g(x) בהזנה ימנית.



- ב- n הזזות הראשונות נכנס הוקטור y למעגל החלוקה.
- בסוף n הזזות הראשונות, מתקבל הסינדרום s בתוך הרגיסטרים של מעגל החלוקה.
- מעגל ROM בוחר את המוביל (מילת השגיאה) המתאים לסינדרום שהתקבל.
- ב- n הזזות הבאות כל ביט מהמוביל מחובר לביט מהמילה שנקלטה y.
- לאחר n הזזות האלו מתקבלת במוצא המילה המתוקנת.

להכניס את מה שאני כתבתי + השלמה מהמחברת של אורי לגבי מפענחים נוספים

שדות סופיים

הגדרת חבורה:

חבורה היא קבוצה עם פעולה אחת המקיימת אקסיומות:

$$G=\{a,b,c,\ldots\}$$

$$a\cdot b\triangleq f(a,b)=c\quad OR\quad a+b\triangleq f(a,b)=c$$

- הפעולה היא פונקציה שמקבלת 2 אברים מהקבוצה G ומחזירה איבר שהוא גם שייך ל G.
- ניתן לסמן את הפעולה בעזרת חיבור או כפל (זו הגדרה ולא באמת חיבור או כפל).
- ניתן להגדיר את הפעולה (פונקציה) בעזרת טבלה דו-מימדית.

סגירות:

$$\forall a,b\in G:\ a\cdot b\in G$$

אסוציאטיביות:

$$\forall a,b,c\in G:\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

קיום איבר היחידה:

$$\exists\, e\in G:\forall\ a\in G:\ e\cdot a=a\cdot e=a$$

איבר היחידה עבור פעולה כפלית הוא 1, ועבור פעולה חיבורית הוא 0.

קיום איבר הופכי:

$$\forall\ a\in G\ \exists\ a^{-1}\in G:$$

$$\Rightarrow a\cdot a^{-1}=a^{-1}\cdot a=e=1$$

$$OR$$

$$\Rightarrow a+a^{-1}=a^{-1}+a=e=0$$

חבורה קומוטטיבית (אבלית):

חבורה קומוטטיבית היא חבורה שמקיימת:

$$\forall\ a,b\in G:a\cdot b=b\cdot a$$

חבורה ציקלית:

חבורה ציקלית היא חבורה שכל אבריה הם חזקות של איבר אחד.

חבורה ציקלית חיבורית:

$$G=\{1,c,c^2,c^3,\ldots,c^{m-1}\}$$

חבורה ציקלית כפלית:

$$G=\{1,c,c+c,c+c+c,\ldots\}$$

הערות:
- כל חבורה ציקלית היא אבלית.
- כל תת-חבורה של חבורה ציקלית היא בעצמה חבורה ציקלית.

הגדרת חוג:

חוג הוא קבוצה עם 2 פעולות המקיימת את האקסיומות הבאות:

$$R=\{a,b,c,\ldots\}$$

$$a\cdot b=f_1(a,b)=c$$

$$a+b=f_2(a,b)=c$$

R היא חבורה אבלית לגבי חיבור.

סגירות:

$$\forall a,b\in R:\ a\cdot b\in R$$

אסוציאטיביות:

$$\forall a,b,c\in R:\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

דיסטריביוטיביות:

$$\forall a,b,c\in R:\ a\cdot(b+c)=a\cdot b+a\cdot c$$

$$(b+c)\cdot a=b\cdot a+c\cdot a$$

הגדרת שדה:

קבוצה F עם 2 פעולות בינאריות המסומנות ב- '+' ו- '·' היא שדה אם מתקיים:
- F היא חבורה קומוטטיבית (אבלית) חיבורית:

$$a+b=b+a$$

- $F\setminus\{0\}$ (החבורה F ללא איבר האפס) היא חבורה קומוטטיבית כפלית.

$$a\cdot b=b\cdot a$$

- מתקיים:

$$a,b,c\in F\Rightarrow a(b+c)=ab+ac$$

הערה:
- שדה הוא חוג גם עם קומטטיביות כפלית (ללא איבר האפס).
- בשדה מתקיים:

$$a\cdot b=0\Rightarrow a=0\ or\ b=0$$

משפט:
Z_n הוא שדה אמ"מ n הוא מספר ראשוני.

$$Z_n\triangleq\{0,1,2,\ldots,n-1\}$$

הגדרת F(x)/f(x):

F(x)/f(x) מוגדר כאוסף הפולינומים סופי 'שארית' פולינום f(x).

הערות:
- F(x) הוא אוסף אינסופי של כל הפולינום, ממעלה כלשהי, שהמקדמים שלהם שייכים לשדה F. למשל, כל הפולינומים ממעלה גדולה מ- 2.
- בגלל השארית F(x)/f(x) הוא אוסף סופי.
- מעלת כל הפולינומים שב- F(x)/f(x) קטנה ממעלת f(x).

משפט:
פולינום p(x) מעל שדה F מתאפס ע"י b אמ"מ p(x)|(x-b).

משפט:
עבור שדה GF(q) מתקיים:

$$\beta_i\neq\beta_j\in GF(q)\ \ \forall i\neq j$$

$$x^q-x=\prod_{i=1}^{q}(x-\beta_i)$$

תכונות עבור שדה גדול שנוצר משדה קטן:

נבנה שדה גדול GF(q^m) מתוך GF(p).

תכונות:
- סדר איבר פרימיטיבי בשדה הגדול:

$$primitive=\alpha\in GF(q^m)$$

$$o(\alpha)=q^m-1$$

- סדר כל איבר בשדה הגדול:

$$\forall b\in GF(q^m)$$

$$o(b)/(q^m-1)$$

הערה חשובה!
המשמעות היא שהסדר של איבר למשל ב- GF(16) יכולה להיות אך ורק 1 או 3 או 5 או 15.
כדי למצוא את הסדר של אלמנט כלשהו, למשל a^7 נעלה אותו ב- 1, 3, 5 או 15 עד אשר התוצאה היא 1.

- לכל איבר בשדה הגדול מתקיים:

$$\forall b\in GF(q^m)$$

$$b^{q^m-1}=1 \bmod q$$

משפט:
אמ"מ קיים m שלם המקיים $GF(q_1)\subset GF(q_2)$

$$q_1^m=q_2$$

משפט:
GF(q) / {0} הוא חבורה ציקלית. כלומר תמיד קיים איבר פרמיטיבי כלשהו שבעזרתו ניתן ליצור חבורה ציקלית.

ואז, עבור β פרמיטיבי תמיד מתקיים:

$$x^{q-1}-1=\prod_{i=1}^{q-1}(x-\beta^i)$$

הגדרת GCD ו- LCM:

הגדרת GCD:
המספר הכי גדול שמחלק גם את a וגם את b (המכנה המשותף הגדול ביותר).

הגדרת LCM:
המספר הכי קטן ש- a מחלק אותו וגם ב- b מחלק אותו.

דוגמא:

$$a=6\ ,\ b=3\Rightarrow lcm=6\ ,\ \gcd=3$$

משפט:

$$\gcd(a,b)\cdot lcm(a\cdot b)=a\cdot b$$

משפט אוקלידס:
אלגוריתם למציאת GCD:

$$\gcd(s(x),r(x))=?$$
$$\deg(s(x))\geq\deg(r(x))$$
$$s(x)=q_0(x)r(x)+r_1(x)$$
$$r(x)=q_1(x)r_1(x)+r_2(x)$$
$$\vdots$$
$$r_{n-2}(x)=q_{n-1}(x)r_{n-1}(x)+r_n(x)$$
$$r_{n-1}(x)=q_n(x)r_n(x)+0$$

$$\gcd=r_n(x)$$

דוגמא מספרית:

$$\gcd(56,77)=?$$
$$77=56+21\rightarrow\gcd(56,21)=\gcd(56,77)$$
$$56=21\cdot2+14\rightarrow\gcd(14,21)=\gcd(56,21)$$
$$21=14+7\rightarrow\gcd(14,7)=\gcd(14,21)$$
$$14=7\cdot2+0\rightarrow\gcd(14,7)=\gcd(0,7)=7$$

הערה:

$$\gcd(s(x),r(x))=a(x)s(x)+b(x)r(x)$$

כאשר ל- a(x) ו- b(x) יכולים להיות מקדמים שליליים (כלומר כאן אין מודולו).

הגדרת פולינום בלתי-פריק מעל שדה F:
פולינום שלא ניתן לפרק אותו למכפלת פולינומים מעל שדה F.

במילים אחרות:
f(x) בלתי פריק אמ"מ:

$$\gcd(f(x),g(x))=1\quad\forall\ g(x)\neq f(x)$$

משפט:
F(x)/f(x) הוא שדה אמ"מ f(x) בלתי פריק מעל שדה F.

הגדרת שדות איזומורפיים:
שדות F_1 ו- F_2 נקראים איזומורפיים אם קיימת העתקה f (בין F_1 ל- F_2) חח"ע ועל המקיימת את התכונות הבאות:

$$f:F_1\rightarrow F_2$$
$$f(a+b)=f(a)+f(b)$$
$$f(a\cdot b)=f(a)\cdot f(b)$$

משפט:
עבור q נתון, כל השדות GF(q) הם איזומורפיים זה לזה.

בניית אברי שדה מתוך פולינום f(x):
הסבר בעזרת דוגמא:
נרצה לבנות את GF(16) מתוך GF(2).
נתון פולינום מעל GF(2) ממעלה m=4.
יהי α שורש של הפולינום, השייך ל GF(2^4)=GF(16).

$$\Pi(x)=x^4+x+1$$
$$\Pi(\alpha)=\alpha^4+\alpha+1=0$$
$$\rightarrow\alpha^4=\alpha+1$$

כל הוקטורים הם 4 ממדיים ולכן צריך 4 וקטורי בסיס שיפרשו את כל השדה הגדול.

$$0000\rightarrow0$$
$$1000\rightarrow1$$
$$0100\rightarrow\alpha$$
$$0010\rightarrow\alpha^2$$
$$0001\rightarrow\alpha^3$$
$$1100\rightarrow\alpha^4=\alpha+1$$
$$0110\rightarrow\alpha^5=\alpha\cdot\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha$$
$$\vdots$$
$$1000\rightarrow\alpha^{15}=1$$
$$0100\rightarrow\alpha^{16}=\alpha$$

הערות:
- בשיטה זו נקבל חבורה ציקלית (שדה ללא איבר האפס שבו ניתן לקבל את כל האיברים ע"י העלאת איבר כלשהו בחזקה כלשהי).
- חיבור עדיף לעשות בצורה פולינומית (בעזרת הביטים) ואילו כפל עדיף לעשות בצורה פולרית (בעזרת האלמנט a).
- דוגמא למציאת הופכי:

$$(1101)^{-1}=?\Rightarrow(\alpha^5)^{-1}=\alpha^{-5}\cdot\underbrace{\alpha^{15}}_{=1}=\alpha^{10}\Rightarrow0101$$

סדר של איבר α:
סדר של איבר השייך לחבורה G הוא המספר החיובי הקטן ביותר (n) המקיים:

$$\alpha^n=1\ ;\ \alpha\in GF(q^m)$$
$$\Rightarrow o(\alpha)=n$$

דוגמא:
נרצה למצוא את איבר מסדר 5 מעל GF(2^4).
נניח ש- α הוא אלמנט פרימיטיבי מעל GF(16) ואז:

$$o(\alpha)=q^m-1=15$$
$$\beta=\alpha^b\ ;\ o(\beta)=5\ ;\ b=?$$
$$\beta^5=1=\alpha^{5\cdot b}$$
$$1=\alpha^{15}\Rightarrow b=3$$

עבור β איבר פרימיטיבי, מתקיים:

$$\alpha,\beta\in GF(q^m)$$
$$\alpha=\beta^k$$
$$o(\alpha)=\frac{q^m-1}{\gcd(k,q^m-1)}$$

איבר פרימיטיבי:
איבר פרימיטיבי הוא איבר שבעזרת חזקותיו ניתן להביע כל אבר בשדה פרט לאיבר האפס.

$$F=GF(q^m)=\{0,1,\alpha,\alpha^2,\alpha^3,....,\alpha^{q^m-2}\}$$
$$o(\alpha)=q^m-1\ \Rightarrow\ \alpha^{q^m-1}=1$$

פולינום פרימיטיבי:
פולינום שכל איבריו פרמיטיביים.

פולינום מוני:
פולינום מוני הוא פולינום שמקדם המעלה הגדולה ביותר שלו הוא 1.

$$f(x)=f_{n-1}\cdot x^{n-1}+...+f_1\cdot x+f_0$$
$$f_{n-1}=1$$

פולינום ראשוני:
פולינום מוני ואי-פריק הוא פולינום ראשוני.

פולינום מינימאלי:
פולינום מינימאלי מעל שדה GF(q) של איבר $\alpha\in GF(q^m)$ הוא הפולינום מוני M(x) מעל GF(q) בעל המעלה הנמוכה ביותר שמקיים:

$$M(\alpha)=0$$

תכונות פולינום מינימאלי:
- פולינום מינימאלי הוא פולינום אי-פריק מעל GF(q).
- פולינום מינימאלי הוא פולינום ראשוני.
- לכל איבר קיים פולינום מינימאלי יחיד.
- $M(x)/\left(x^{q^m}-x\right)$.
- אם α הוא שורש של פולינום מינימאלי M(x) אז גם α^q הוא שורש של M(x).
- פולינום מינימאלי של איבר פרימיטיבי הוא ממעלה m.
- פולינום מינימאלי של איבר כללי הוא ממעלה המחלקת את m.
- כל פולינום מינימאלי מעל השדה הקטן, אשר מעלתו מחלקת את m, שורשיו הם אברים בשדה הגדול. $GF(2^3)$

הערה:
עבור הפולינום:

$$f(x)=x^2+x+1\ \ GF(2^2)$$
$$f(\alpha)=0\ ;\ \alpha\in GF(16)$$

מתקיים:
- הפולינום המינימלי מעל GF(2) של α הוא:

$$M_\alpha(x)=x^2+x+1\ \ GF(2)$$

- הפולינום המינימלי מעל GF(16) של α הוא:

$$M_\alpha(x)=x-\alpha$$

איברים צמודים:
שני אברים השייכים ל- $GF(q^m)$ הם צמודים אם הם שייכים לשדה הגדול ויש להם אותו פולינום מינימאלי מעל GF(q).

הערות:
- מעלת הפולינום המינימאלי של איבר זהה למספר הצמודים שיש לאיבר.

מציאת האיברים צמודים:
אם נתון איבר b:

$$b\in GF(q^m)$$

אז הצמודים של b הם כל האברים השונים:

$$\{b,b^q,b^{q^2},b^{q^3},...\}$$

עוצרים כאשר מגיעים לאיבר הראשון.

מציאת פולינום מינימאלי:
נמצא את הפולינום המינימאלי של b ע"י כך שנמצא תחילה את כל הצמודים של b ונזכור שכל הצמודים של b גם מאפסים את הפולינום המינימאלי של b.
נניח שהצמודים של b נתונים ע"י :

$$\{b^{q^0},b^{q^1},b^{q^2},b^{q^3},...\}$$

אז הפולינום המינימאלי הוא:

$$M_b(x)=(x-b)(x-b^q)(x-b^{q^2})(x-b^{q^3})\cdots$$

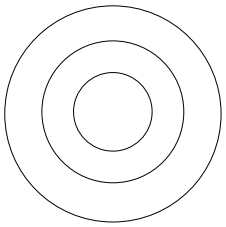
משפט:
f(x) הוא פולינום מינימלי כלשהו מעל שדה GF(q). תמיד מתקיים:

$$GF(q^m)$$
$$o(f(x))/m$$

משפט:
מכפלת כל הפולינומים האי-פריקים ממעלה המחלקת את m נתונה ע"י:

$$x\cdot\left(x^{q^m-1}-1\right)=\prod_{\beta_i\in GF(q^m)}(x-\beta_i)$$

סדרי איברים בתוך שדה:
כל שדה גדול שנבנה מתוך שדה קטן, מכיל את כל השדות היותר קטנים (כלומר מכיל איברים בעלי הסדר של השדות הקטנים).



קרקריסטיקה של שדה - P:
מספר ה"אחדים" שניתן לחבר עד שמגיעים ל- 0 בפעם הראשונה.

הסבר ע"י דוגמא:

$$GF(3):\{0,1,2\}\ ;\ P=?$$
$$1+1+1=0\Rightarrow P=3$$

הערה:
לכל האלמנטים בשדה יש את אותה קרקריסטיקה P.

משפט:

$$\alpha,\beta\in GF(q)=GF(P^m)\ ;\ l,P\in N$$
$$(\alpha\pm\beta)^{P^l}=\alpha^{P^l}\pm\beta^{P^l}$$

משפט:

$$I=\deg(s(x))$$
$$(s(x))^{P^l}=\left(\sum_{i=0}^{I}s_i\cdot x^i\right)^{P^l}=\sum_{i=0}^{I}s_i^{P^l}\cdot x^{i\cdot P^l}$$

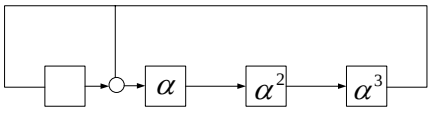
P – הקרקטריסטיקה.

מעגל הכפלה באיבר פרמיטיבי:
יוצרים את המעגל המכפיל בהתאם לפולינום ממנו יצרו את השדה.

מבצעים מכפלה בין איבר כללי בשדה לבין אלפה:

$$g(x)=x^4+x+1\ ;\ GF(2^4)$$
$$\alpha\cdot\left(a_0+a_1\cdot\alpha+a_2\cdot\alpha^2+a_3\cdot\alpha^3\right)=$$
$$=a_3+(a_0+a_3)\cdot\alpha+a_1\cdot\alpha^2+a_2\cdot\alpha^3$$

מתוך התוצאה מייצרים את המעגל הבא:



טוענים את ערכי האיבר שרוצים להכפיל לתוך הרגיסטרים.
מקדמים את המעגל פעם אחת, הפתרון נמצא בתוך הרגיסטרים.

הערה:
- אם מפעילים את המעגל כמה פעמים ברציפות, נקבל הכפלה כמה פעמים ב אלפה.

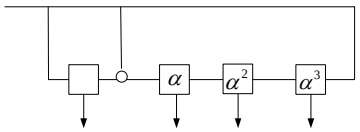
מעגל חלוקה באיבר פרמיטיבי:
- זהה למעגל הכפלה באיבר רק עושים את ה- shift לכיוון השני.

מציאת ערך של פולינום (פונקציה):
- נתון פולינום שרוצים למצוא את הערך שלו מעל שדה GF(q^m).
- נתון α איבר פרמיטיבי.
- נחשב את ערך הפונציה (פולינום) בנק' α.

$$f(x)=f_0+f_1x+f_2x^2+...+f_{q^m-2}x^{q^m-2}$$

$$f(\alpha)=f_0+f_1\alpha+f_2\alpha^2+...+f_{q^m-2}\alpha^{q^m-2}$$

- נבנה מעגל מכפיל ב- α ע"פ הפולינום היוצר של השדה.
- נזין למעגל את המקדמים של הפולינום מהמעלה הגבוהה ביותר לנמוכה ביותר.
- כאשר סיימנו להזין את כל מקדמי הפולינום, ברגיסטרים תהיה התוצאה של $f(\alpha)$.



הערה:
- חישוב הפולינום עבור איבר שאינו פרמיטיבי, למשל:

$$\beta=\alpha^5\Rightarrow f(\beta)=f(\alpha^5)=?$$

- הסבר ע"י דוגמא:

$$f(x)=x^5+x+1\ ;\ GF(2^4)$$

$$f(\alpha)=\alpha^5+\alpha+1\Rightarrow\begin{cases}f_i=1 & i=0,1,5\\ f_i=0 & ow\end{cases}$$

$$\beta=\alpha^5\Rightarrow f(\alpha^5)=\alpha^{25}+\alpha^5+1=\alpha^{10}+\alpha^5+1$$

$$\Rightarrow\begin{cases}f_i=1 & i=0,5,10\\ f_i=0 & ow\end{cases}$$

מעגל מעלה בריבוע:
מעל שדה GF(2^4) עם פולינום יוצר:

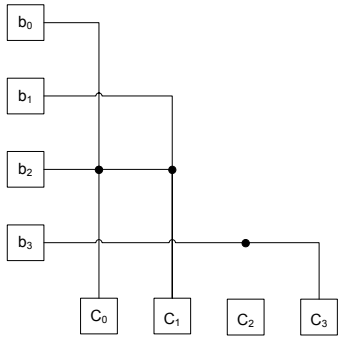
$$g(x)=x^4+x+1\ ;\ GF(2^4)$$

$$\left(b_0+b_1\cdot\alpha+b_2\cdot\alpha^2+b_3\cdot\alpha^3\right)^2=b_0+b_1\cdot\alpha^2+b_2\cdot\alpha^4+b_3\cdot\alpha^8=$$

$$=\left(b_0+b_2\right)+b_2\alpha+\left(b_1+b_3\right)\alpha^2+b_3\alpha^3$$

$$\underline{b}^2=\underline{b}\cdot A=\underline{a}$$

$$A=\begin{bmatrix}1&0&0&0\\0&0&1&0\\1&1&0&0\\0&0&1&1\end{bmatrix}$$



מעגל הוצאת שורש:
מוצאים את מטריצת ההעלאה בריבוע - A, הופכים אותה וממשים את המעגל באותו האופן.

$$\underline{b}^2=\underline{b}\cdot A=\underline{a}$$

$$\Rightarrow \underline{b}=\sqrt{\underline{b}^2}=\underline{a}\cdot A^{-1}$$

משפט:
עבור n נתון ועבור:

$$GF(q)\ ;\ \gcd(n,q)=1$$

קיים m כך שמתקיים:

$$\left(x^n-1\right)/\left(x^{q^m}-1\right)$$

וגם מתקיים:

x^n-1 הוא בעל n שורשים ב- $GF(q^m)$.

קודים צקליים

קוד ציקלי:
קוד ציקלי מעל GF(q) מוגדר באמצעות הפולינום היוצר:

$$g(x)=lcm\left(M_{i_1}(x),M_{i_2}(x),...,M_{i_v}(x),\right)$$

$$\deg\left(g(x)\right)=n-k$$

$$n\,|\,q^m-1\ ,\ n\le q^m-1$$

α הוא אלמנט של GF(q^m) בעל סדר n.

Mi,j(x) הם הפולינומים המינימליים מעל GF(q) של השורש aij.

שורשי הקוד:
השורשים של g(x) נקראים שורשי הקוד.

קוד פרמיטיבי:
אם n=q^m-1 אז הקוד פרמיטיבי.

מטריצת הבדיקה:
ניתן גם להגדיר את הקוד ע"י מטריצת הבדיקה:

$$H=\begin{pmatrix}1&\alpha^{i_1}&\alpha^{2\cdot i_1}&\dots&\alpha^{(n-1)i_1}\\1&\alpha^{i_2}&\alpha^{2\cdot i_1}&\dots&\alpha^{(n-1)j_2}\\\vdots&\vdots&\vdots&\dots&\vdots\\1&\alpha^{i_v}&\alpha^{2\cdot i_v}&\dots&\alpha^{(n-1)i_v}\end{pmatrix}$$

שורות מטריצת הבדיקה הן לא בהכרח בלתי-תלויות, כלומר ממד H הוא לא בהכרח n-k x n אלא הממד n-k עלול לגדול.

משפט:
אם בעמודה מסוימת ב- H יש איברים צמודים, אז ניתן למחוק את השורות של האיברים הצמודים (ולהשאיר רק אחת).

הערה:
ניתן לפרוס כל שורה למספר שורות לפי הייצוג של איבר בשדה. ואז, לאחר הפריסה, נקבל בד"כ מטריצה עם שורות תלויות. את השורות התלויות אפשר לצמצם ולהישאר רק עם השורות הבלתי תלויות.

לבסוף, תמיד נקבל מטריצה בעלת n-k שורות (מעלת g(x)).

משפט:
אם בונים קוד ובמטריצה H מוסיפים שורה. ואם האיבר של השורה שנוספה אינו צמוד של אף אחד מאיברי השורות הקודמות - אז n-k יגדל במספר הצמודים של אותו איבר. וזאת מפני ש-g(x) יתווספו מכפלות כמספר האיברים הצמודים שלא אותו איבר.

קודי BCH

הגדרה:
- קוד BCH הוא מקרה פרטי של קוד ציקלי.

$$H_{(d-1)\,x\,n}=\begin{pmatrix}1&\alpha^{j_0}&\alpha^{2\cdot j_0}&\dots&\alpha^{(n-1)(j_0)}\\1&\alpha^{j_0+1}&\alpha^{2(j_0+1)}&\dots&\alpha^{(n-1)(j_0+1)}\\\vdots&\vdots&\vdots&\dots&\vdots\\1&\alpha^{j_0+d-2}&\alpha^{2(j_0+d-2)}&\dots&\alpha^{(n-1)(j_0+d-2)}\end{pmatrix}$$

$$g(x)=lcm\left(M_i(x):i=j_0,j_0+1,...,j_0+d-2\right)$$

הערה:
עבור GF(q) ניתן למחוק כל שורה q-ית.

חסם BCH:
המרחק המינימלי dmin של קוד BCH מקיים:

$$d_{\min}\ge d$$

קוד BCH פשוט:
כאשר j0=1 הקוד יקרא קוד BCH פשוט.

משפט:
אם n ו- q ראשוניים יחסית (gcd(n,q)=1), אז קיים m כך ש:

$x^n-1\,|\,x^{q^m-1}-1$

וגם x^n-1 הוא בעל n שורשים ב- $GF(q^m)$.

מסקנה:
המשפט מבטיח שאם רוצים לבנות קוד מעל GF(q) באורך n אז קיים שדה הרחבה $GF(q^m)$ המכיל איבר בסדר המתאים.

משפט (חסם BCH):
אם יש קוד כלשהו, וניתן לזהות מתוך ה- H שלו תת-מטריצת BCH, עדיין ניתן לומר ש-

$$d_{\min}\ge d$$

(לפי תת-המטריצה שהיא כן BCH) כי הוספת שורות יכולה רק להגדיל את המרחק בין המילים.

קודי Reed-Solomon

הגדרת קוד RS:
- זהו מקרה פרטי של קוד BCH שבו m=1:

$$g(x)=\left(x-\alpha^{j_0}\right)\left(x-\alpha^{j_0+1}\right)\dots\left(x-\alpha^{j_0+d-2}\right)$$

$$d_{\min}=n-k+1$$

הערות:
- קודי RS הם קודי MDS (מקיימים את חסם Singleton)

אלגוריתם PGZ

כללי:
- מטרת אלגוריתם PGZ לפענח קודי BCH.

סד"פ:
נתון קוד BCH מעל GF(q) באורך n, ומתקיים:

$$\alpha\in GF(q^m)\ ;\ d=2\cdot t+1$$

$$y(x)=c(x)+e(x)$$

$$e(x)=e_{i_1}x^{i_1}+e_{i_2}x^{i_2}+...+e_{i_v}x^{i_v}\ ;\ e_i\in GF(q)$$

1. חישוב סנדרומים

$$\underline{s}\triangleq H\cdot\underline{y}^T=H\cdot\underline{e}^T$$

$$s_i\triangleq y(\alpha^{i+j_0-1})=e(\alpha^{i+j_0-1})\ ;\ i=1,...,2t$$

2. מציאת מספר חילופי הערוץ
V הוא מספר חילופי הערוץ המקסימלי (הקטן מ- t) כך שהמטריצה M הפיכה:

$$M=\begin{pmatrix}s_1&s_2&\dots&s_v\\s_2&s_3&\dots&s_{v+1}\\\vdots&\vdots&\ddots&\vdots\\s_v&s_{v+1}&\dots&s_{2v-1}\end{pmatrix}$$

המטריצה הפיכה אמ"מ ה- det(M)≠0 (בודקים עבור איזה v מקסימלי שעדיין קטן מ- t המטריצה הפיכה).

3. מציאת מקדמי פולינום מיקום השגיאה
הגדרת פולינום מיקום השגיאה:

$$x\in GF(q)$$

$$\Lambda(x)=\prod_{i=1}^{v}(1-x\cdot z_i)=1+\Lambda_1x+\Lambda_2x^2+...+\Lambda_vx^v$$

$$\Lambda(z_i^{-1})=0$$

(Z^{i-1} הוא שורש של פולינום מיקום השגיאה)

מציאת המקדמים של פולינום השגיאה:

$$\begin{pmatrix}\Lambda_v\\\Lambda_{v-1}\\\vdots\\\Lambda_1\end{pmatrix}=-M^{-1}\begin{pmatrix}s_{v+1}\\s_{v+2}\\\vdots\\s_{2v}\end{pmatrix}$$

4. מציאת מיקומי השגיאות
נמצא את שורשי הפולינום $\Lambda(x)$: $z_1^{-1},z_2^{-1},...,z_v^{-1}$.
מיקומי השגיאות הם המקומות ik כך ש- $z_k=\alpha^{i_k}$

5. מציאת ערכי השגיאות
מחשבים את:

$$\begin{pmatrix}Y_1\\Y_1\\\vdots\\Y_v\end{pmatrix}=\begin{pmatrix}z_1&z_2&\dots&z_v\\z_1^2&z_2^2&\dots&z_v^2\\\vdots&\vdots&\ddots&\vdots\\z_1^v&z_2^v&\dots&z_v^v\end{pmatrix}^{-1}\begin{pmatrix}s_1\\s_2\\\vdots\\s_v\end{pmatrix}$$

ואז השגיאות נתונות ע"י:

$$e_{ik}=Y_k\cdot z_k^{-j_0+1}\ \Rightarrow\ e(x)=\sum_{k=1}^{v}e_{ik}x^{i_k}$$

6. תיקון המילה
המילה המתוקנת נתונה ע"י:

$$\hat{c}(x)=y(x)-e(x)$$

כותרת משנה 2:
כותרת משנה 9:
כותרת משנה 5:
כותרת משנה 7:
כותרת משנה 3:
כותרת משנה 12:
כותרת משנה 10:
כותרת משנה 8:
כותרת משנה 13:
כותרת משנה 4:
כותרת משנה 6:
כותרת משנה 11:

שונות:

להוסיף תזכורת לחלוקת פולינומים.

מטריצות:

$$(A,B)^T = \begin{pmatrix} A^T \\ B^T \end{pmatrix}$$

GF(2):
a,b מעל השדה הבינארי, ולכן מתקיים:

$$(a+b)^2 = a^2 + b^2$$

הערות של אורן:

$$GF(p^m)$$

m – אומר כמה סימבולים מייצגים איבר בשדה.
P – אומר כמה אפשרויות יש לסמבול.

כללים חשובים:

1. הסדר של α, ששייכת ל- $GF(q^m)$, תמיד מחלק את q^m-1. כלומר כשבודקים למשל סדר של איבר מעל GF(16) מספיק לבדוק האם האיבר בחזקת כפולות של 1,3,5,15 נותן 1.
2. הפולינום המינימלי Mα(x) הוא ממעלה המחלקת את m (α שייך ל- $GF(q^m)$).
3. הצמודים מעל שדה GF(q) תמיד יהיו בהפרשים של בחזקת q אחד מהשני (מוצאים את הצמודים ע"י העלאה ב- q).
4. אם מחפשים איברים של שדה קטן מתוך איברים של שדה גדול, צריך למצוא את האיברים בשדה הגדול שהסדר שלהם הוא ה- q של השדה הקטן פחות אחד.