קידוד עבור אילוצים ספקטראליים

ויטלי סקצ׳ק

קידוד עבור אילוצים ספקטראליים

חבור על מחקר
לשם מילוי חלקי של הדרישות לקבלת התואר
מגיסטר למדעים במדעי המחשב
מאת
ויטלי סקצ׳יק

הוגש לסנט הטכניון - מכון טכנולוגי לישראל
חשון תשנ״ח   חיפה   נובמבר 1997

המחקר נעשה בהנחית פרופ׳ טובי עציון ופרופ׳ רוני רוט בפקולטה למדעי המחשב.

אני מודה לפרופ׳ טובי עציון ופרופ׳ רוני רוט על ההנחיה ועל התמיכה לאורך כל הדרך.

אני מודה לטכניון על התמיכה הכספית הנדיבה בהשתלמותי.

תוכן עניינים

CONTENTS

תקציר

בעבודה זו אנו חוקרים את משפחת הצפנים הידועה בשם **צפנים בעלי אפסים ספקטראליים**. הצפנים האלה מוגדרים מעל אלפבית $F=\{+1,-1\}$. לכל מילה $\underline{x} = (x_1, x_2, ..., x_n)$ מעל F נגדיר את **הפולינום המייצג** שלה במשתנה z מעל הממשיים

$$X(z) = x_1z + x_2z + ... + x_n z^n$$

אם הפולינום המייצג של מילה $\underline{x}$ מתחלק ב - $(z-1)^k$ אז $\underline{x}$ תיקרא **מילה בעלת אפס ספקטראלי מסדר k**. אוסף כל המילים באורך n מעל F בעלות אפס ספקטראלי מסדר k יסומן ע״י $S(n,k)$. כל תת-קבוצה C של $S(n,k)$ תיקרא צופן בעל אפס ספקטראלי מסדר k ואורך n. ניתן להשתמש בצפנים האלה בתור צפני בלוקים, כי שירשור של l מילים מתוך C מהווה מילה ב-$S(ln,k)$. הערך $\rho(C) = n - \log_2|C|$ ייקרא **היתירות** של הצופן C והוא משקף את הניפוח של הנתונים כאשר ההודעה מוצפנת באמצעות C .

בחלק הראשון של העבודה אנו עוסקים בבעית הצפנה ופענוח יעילים של צפנים בעלי אפסים ספקטראליים מסדר 3. אנחנו מציגים אלגוריתם יעיל להצפנה של סדרת סיביות שרירותית באורך n אל תוך צופן בעל אפס ספקטראלי מסדר 3. האלגוריתם הינו רקורסיבי והוא מורכב מחמישה שלבים בסיסיים. היתירות של הצופן המיוצר ע״י האלגוריתם הינה $9 \log_2 n + O(\log \log n)$. סיבוכיות החישוב של האלגוריתם היא $O(n)$ פעולות חיבור מעל השלמים ו-$O(n \log n)$ פעולות קידום מונים. הזיכרון הנדרש הוא $O(n)$.

בחלק השני של העבודה זו אנו חוקרים תכונות שונות של צפנים בעלי אפסים ספקטראליים. בפרט אנו משפרים את החסמים התחתון והעליון על האורך המינימלי של מילה בעלת אפס ספקטראלי מסדר k. אנו מחשבים את היתירות של $S(n,k)$ לערכים מסוימים של n ו k. כמו כן אנו מראים תנאי חלוקה חדשים על אורך n של מילה בעלת אפס ספקטראלי מסדר k. אנו גם מציגים חסם תחתון חדש על מספר שינויי סימן במילה בעלת אפס ספקטראלי מסדר k.

רשימת סמלים

- $|S|$ מספר איברים של קבוצה S
- $k|n$ מספר שלם k מחלק מספר שלם n
- $\lceil c \rceil$ ערך שלם עליון של מספר ממשי c
- $\lfloor c \rfloor$ ערך שלם תחתון של מספר ממשי c
- $O(f(n))$ פונקציה מתנהגת בסדר גודל כמו פונקציה $f(n)$
- $\binom{n}{t}$ מספר צרופים של t איברים מתוך n איברים שונים ללא חזרות
- $|w|$ אורך של מילה w
- $\mathrm{Re}(z)$ החלק הממשי של מספר מרוכב z
- $\mathrm{Im}(z)$ החלק המדומה של מספר מרוכב z
- $S(n,k)$ הצופן בעל אפס ספקטראלי מסדר k באורך n
- $H(n,k;c)$ המטריצה הבודקת של הצופן $S(n,k)$
- $\rho(S(n,k)) = n - \log_2|S(n,k)|$ היתירות של הצופן $S(n,k)$
- $R(S(n,k)) = \frac{\log_2|S(n,k)|}{n}$ הקצב של הצופן $S(n,k)$
- $q_j(\underline{x}) = \sum_{i=-h}^{h-1} i^j \cdot x_j$ המומנט ה-i של מילה $\underline{x}$ באורך $2h$
- $(\underline{x})_A$ תת-מילה של מילה $\underline{x}$ באורך n אשר האינדקסים שלה ניתנים ע״י קבוצה A
- $\underline{y} \to (\underline{x})_A$ הצבה של כניסות של מילה $\underline{y}$ לתוך כניסות של מילה $\underline{x}$ המסומנות באמצעות קבוצת האינדקסים A

1 צפנים בעלי אפסים ספקטראליים

1.1 מבוא

משפחת הצפנים בעלי אפסים ספקטראליים הינה תת-משפחה של קבוצה גדולה מאוד של צפנים לערוצים מוגבלי קלט (constrained codes). צפנים אלו נועדו להצפין סדרה שרירותית של סיביות קלט אל תוך סדרה של סיביות אשר תקיים את אילוצי הערוץ. אילוצים אלו יכולים להיות בעלי אופי אלגברי או קומבינטורי.

ערוצים אמיתיים רבים הם ערוצים מוגבלי קלט. כך למשל דיסקים מגנטיים ואופטיים הם ערוצים מוגבלי קלט. גם ערוצי תקשורת מעל סיבים אופטיים הם ערוצים מוגבלי קלט. הנושא של צפנים לערוצים מוגבלי קלט מצא ביטוי נרחב בספרות מדעית בשנים האחרונות, הקורא יכול למשל לפנות אל [MSW92], [MRS94]. שימושים של צפנים מאולצים בהתקנים לאחסון מידע מוזכרים ביתר פרוט בספרות [Pohl92], [Imm91].

צפנים בעלי אפסים ספקטראליים מתאימים לשימוש במערכות לאחסון מידע, כגון דיסקים מגנטיים ואופטיים [Imm91], [ImmB87]. הם ניתנים לשימוש גם בתקשורת מעל סיבים אופטיים [ImmB87]. הערוצים במערכות אחסון מידע ובתקשורת מעל סיבים אופטיים הם ערוצים כאלה שפונקצית צפיפות הספקטרום מתאפסת באזור של התדר $f = 0$ (או במילים אחרות קיים אפס ספקטראלי). זה נובע בין השאר בגלל שראש קורא של דיסק מגנטי או אופטי אינו מסוגל לקרוא אות בתחום זה של ספקטרום. אם נשדר אות שרירותי דרך ערוץ כזה ביציאה מהערוץ נקבל אות מעוות אשר מרכיבים שלו בתדרים נמוכים סביב $f = 0$ יהיו נמוכים מהאות המקורי. העוותים האלה עלולים לגרום לשגיאות בערוץ. לכן רצוי שלאות המעובר דרך הערוץ מרכיבים באזור $f = 0$ יהיו מאופסים. ניתן להשיג את זה ע״י שימוש בצופן בעל אפס ספקטראלי. ככל שסדר של האפס הספקטראלי בצופן יהיה גבוה יותר, כך פונקצית צפיפות הספקטרום תהיה ״שטוחה״ יותר באזור $f = 0$ וכך גם העוותים יהיו קטנים יותר.

התכונות של צפנים בעלי אפסים ספקטראליים נחקרו הרבה בעשור האחרון. בהקשר זה ניתן למשל לציין את העבודות [ImmB87], [KS91], [Knu86], [MPi89], [RSV94], [Roth93], [TAlB95]. אבל הנושא הינו חדש יחסית ולכן קיים מספר רב של בעיות פתוחות חשובות אשר טרם נפתרו. בעיות אלה הן בעלות היבט ישומי ופתרונן יכול לקדם התקדמות טכנולוגית בתחום אחסון מידע ותקשורת.

העבודה הנוכחית מתחלקת לשלושה חלקים. הפרק הראשון מהווה מבוא שמכיל בתוכו הגדרות ותכונות בסיסיות של צפנים בעלי אפסים ספקטראליים. הוא גם כולל סקירה של תוצאות חשובות בנושא. הפרק השני מתרכז בנושא של הצפנה ופיענות. הוא מציג את התוצאה העיקרית של העבודה הנוכחית, אלגוריתם הצפנה יעיל עבור צופן בעל אפס ספקטראלי מסדר 3. הפרק השלישי של העבודה הנוכחית עוסק בתכונות שונות של צפנים בעלי אפסים ספקטראליים. הוא מציג את תוצאות המחקר שלנו בנושאים של אורכים אפשריים של מילות הצופן, חסמים על היתירות, מספר שינויי סימן ותוצאות חישוביות שונות.

1.2 הגדרות

נסמן ע״י F את הא״ב $\{+1,-1\}$. לכל מילה $\underline{x} = (x_1, x_2, ..., x_n)$ מעל F נגדיר את **הפולינום המייצג** שלה בעל משתנה z:

$$X(z) = x_1z + x_2z + ... + x_n z^n$$

אם הפולינום המייצג של המילה $\underline{x}$ מתחלק בפולינום $(z\text{-}1)^k$ אז המילה $\underline{x}$ תקרא **בעלת אפס ספקטראלי מסדר k**. $S(n,k)$ יסמן את אוסף של כל המילים בעלות אפס ספקטראלי מסדר k אשר אורכן שווה ל-n. כל תת-קבוצה C של $S(n,k)$ תקרא צופן בעל אפס ספקטראלי מסדר k ואורך n. אוסף של כל המילים בעלות אפס ספקטראלי מסדר k יסומן ע״י $S(k)$. לפעמים כשנדבר על סיביות של מילות הצופן, נכתוב '+' ו '-' במקום '1+' ו '1-' בהתאמה.

נציין תכונות בסיסיות של צפנים בעלי אפסים ספקטראליים (המופיעות למשל ב-[RSV94]):

א. אם $\underline{x} = (x_1, x_2, ..., x_n)$ היא מילה עם אפס ספקטראלי מסדר k, אז גם השלילה שלה $\underline{x}' = (-x_1, -x_2, ..., -x_n)$ היא בעלת אפס ספקטראלי מסדר k.

ב. אם $\underline{x} = (x_1, x_2, ..., x_n)$ היא מילה עם אפס ספקטראלי מסדר k, אז גם המילה האחורית $\underline{x}'' = (x_n, x_{n-1}, ..., x_1)$ היא בעלת אפס ספקטראלי מסדר k.

ג. אם $\underline{x} = (x_1, x_2, ..., x_n)$ ו $\underline{y} = (y_1, y_2, ..., y_m)$ שתיהן מילים עם אפס ספקטראלי מסדר k, אז גם השרשור שלהן $\underline{z} = (x_1, x_2, ..., x_n, y_1, y_2, ..., y_m)$ היא מילה בעלת אפס ספקטראלי מסדר k.

ד. אם $\underline{x} = (x_1, x_2, ..., x_n)$ היא מילה עם אפס ספקטראלי מסדר k, אז המילה $\underline{w} = (x_1, x_2, ..., x_n, -x_n, -x_{n-1}, ..., -x_1)$ היא בעלת אפס ספקטראלי מסדר k+1.

על סמך תכונה ג' ניתן להשתמש בצפנים האלה בתור צופני בלוקים, כי שירשור של l מילים מתוך C מהווה מילה ב-$S(ln,k)$.

הקצב של הצופן $S(n,k)$ מוגדר ע״י

$$R(S(n,k)) = \frac{\log_2 |S(n,k)|}{n}$$

ידוע שלכל k, $\overline{\lim}_{n\to\infty} R(S(n,k)) = 1$, ראה [KS91] ו [RSV94].

לכל מילה $\underline{x} = (x_1, x_2, ..., x_n)$ מעל F^n נגדיר **מומנטים**. המומנט ה-j שלה יסומן ע״י $\rho_j(\underline{x})$ והוא מוגדר ע״י הנוסחא

$$q_j(\underline{x}) \equiv \sum_{i=-h}^{h-1} i^j \cdot x_i \qquad (1.1)$$

ידוע שהמילה $\underline{x}$ היא בעלת אפס ספקטראלי מסדר k אם ורק אם

$$q_j = 0, \quad j = 0, \dots, k-1 \qquad (1.2)$$

ניתן להגיד שמטריצה $H(n,k;c)$ היא המטריצה הבודקת של הצופן $S(n,k)$.

$$H(n,k;c)=\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1+c & 2+c & 3+c & \dots & n+c \\ (1+c)^2 & (2+c)^2 & (3+c)^2 & \dots & (n+c)^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (1+c)^{k-1} & (2+c)^{k-1} & (3+c)^{k-1} & \dots & (n+c)^{k-1} \end{pmatrix} \quad (1.3)$$

כי לכל מילה $\underline{x}$ מעל F^n מתקיים:

$$\underline{x} \in S(n,k) \Leftrightarrow H(n,k;c)\cdot\underline{x} = \underline{0}$$

1.3 סקירת תוצאות

<u>אורך</u>

מילה בעלת אפס ספקטראלי מסדר k יכולה להיות באורכים מסוימים בלבד. במאמר [RSV94] משתמשים בעובדה ש $+1=-1 \pmod 2$ בישביל להוכיח כי אורך של מילה $\underline{x}$ מתוך $S(n,k)$ תמיד מתחלק בגודל $2^{\lfloor \log_2 k \rfloor+1}$.

באותו המאמר הוכח כי האורך המינימלי של מילה בעלת אפס ספקטראלי מסדר k קטן או שווה ל-2^k. ההוכחה היא באמצעות הבניה: המחברים מראים כי המילה שנוצרת ע"י 2^k הסיביות הראשונות של סדרה מסוימת הנקראת סדרת Morse היא למעשה מילה עם אפס ספקטראלי מסדר k בעלת אורך n. ב [RSV94] צוין שע"י תוכנת מחשב ניתן לוודא שעבור סדר k, $1 \le k \le 5$, המילה הקצרה ביותר היא זו שנוצרת מתוך סדרת Morse. אבל לסדרים גבוהים יותר בדיקה ע"י תוכנה פשוטה אינה מעשית בגלל מספר רב של החישובים. לכן השאלה האם המילים שנוצרות מסדרות Morse הן מילים קצרות ביותר לכל סדר k נשארת פתוחה ב [RSV94].

באמצעות תכונה יחודית שמצאנו עבור מילים בעלות אפסים ספקטראליים מסדר גבוה ניתן לכתוב תוכנית שדורשת הרבה פחות חישובים למעבר על כל המילים בעלות אפס ספקטראלי מסדר גבוה. באמצעותה גילינו מילה באורך 48 בעלת אפס ספקטראלי מסדר 6. תגלית זו איפשרה לשפר את החסם העליון על האורך המינימלי של מילה בעלת אפס ספקטראלי מסדר k.

<u>שינויי סימן</u>

נאמר שלמילה $\underline{x} = (x_1, x_2, \dots, x_n)$ יש **שינוי סימן במקום i** אם $x_i \ne x_{i+1}$. חסם תחתון על מספר מינימלי של שינויי סימן במילה עם אפס ספקטראלי מסדר k הוצג ב-[KS91] והוא שווה ל-k. ההוכחה התבססה על שימוש במקרה פרטי של כלל הסימנים של Descartes עבור פולינום ממשי עם k שורשים ממשיים חיוביים. בעבודה נוכחית אנו מראים סדרה של חסמים תחתונים חדשים על מספר שינויי הסימן במילה בעלת אפס ספקטראלי מסדר k.

יתירות

כאשר מצפינים סדרה של סיביות באמצעות צופן C בעל מילים באורך n יש חשיבות רבה למושג של **יתירות**. יתירות מוגדרת ע״י $\rho(C) = n - \log_2|C|$ והיא משקפת את ניפוח הנתונים כאשר מבצעים הצפנה באמצעות C. ידועים חסמים תחתונים ועליונים על יתירות של $S(n,k)$ [RSV94]. שימוש בחסם על מרחק Hamming מתוך [ImmB87] ובהוכחה זהה ל ״חסם הכדורים״ מאפשרים להגיע לנוסחא הבאה:

$$\rho(S(n,k)) \geq (k-1)(\log_2(n) - \log_2(k-1)) = O(k \log n) \qquad (1.4)$$

כמו כן אם n מתחלק ב 2^k אזי שימוש באינדוקציה על k ובניה של מילים מסדר גבוה מתוך מילים מסדר נמוך יותר נותן כי

$$\rho(S(n,k)) \leq O((2^k - 1)(\log_2(n) - k + 1)) = O(2^k \log n) \qquad (1.5)$$

כפי שניתן לראות קיים פער רחב בין החסם התחתון לחסם העליון.

באמצעות התכונה היחודית שהוזכרה לעיל אנו מחשבים את ערכי היתירות עבור צפנים $S(n,k)$ למספר זוגות (n,k).

אלגוריתמים להצפנה

צפנים בעלי אפס ספקטראלי מסדר ראשון ידועים גם בשמות **צפנים מאוזנים** ו dc-free codes . ידועים הרבה אלגוריתמי הצפנה לשימוש בצפנים אלו. גם תכונות של צפנים מאוזנים נחקרו הרבה, ראה למשל [Knu86], [AlB90], [AlB94], [Bose91], [TCB96], [ABCO88], [Etz90]. האלגוריתמים הידועים מייצרים צפנים בעלי יתירות של $\log_2 n + O(1)$, כאשר n הוא אורך הנתונים לפני ההצפנה. לעומת זאת היתירות של $S(n,1)$ היא $0.5 \log_2 n + O(1)$ [Knu86] (ע״י נימוקים קומבינטוריים פשוטים) והיא ניתנת להשגה ע״י הצפנה ממספרת (enumerative encoding) [Imm91]. אבל שיטה זו פחות טובה מבחינת סיבוכיות זמן החישוב ביחס לאלגוריתמים הקודמים.

עבור המקרה k=2 ידועים כמה אלגוריתמי הצפנה המופיעים בספרות [RSV94], [TAlB95]. הם מבוססים על סדרה של החלפות והצבות של סיביות בתוך המילה המוצפנת. האלגוריתמים האלה מייצרים צופן בעל יתירות של $3 \log_2 n + O(\log \log n)$ סיביות וסיבוכיות הזמן שלהם היא $O(n)$ חיבורים של מספרים שלמים בעלי $O(\log n)$ סיביות. הצפנה ממספרת כבר במקרה זה הופכת להיות בלתי שימושית לחלוטין. היתירות של $S(n,2)$ היא $2 \log_2 n + O(1)$ [TAlB95].

לערכים k גבוהים יותר של סדר של אפס ספקטראלי, Karabed ו-Siegel הציגו ב [KS91] שיטת הצפנה המבוססת על דיאגרמות מצבים אינסופיות (שהיא הכללה של עבודה של Monti ו-Pierobon [MPi89]). מאחר וקצב של הבניה שלהם קטן ממש מ-1, היתירות של האלגוריתם היא גודל לינארי באורך הצופן n. לפיכך היתירות שמיוצרת ע״י אלגוריתם כזה עבור כל k קבוע ועבור n גדול מספיק היא גדולה משמעותית מהחסם העליון (1.5). אלגוריתם רקורסיבי שהוצג ב-[RSV94] מייצר צופן בעל יתירות של $O(n^{1-\varepsilon(k)})$ כאשר $0 < \varepsilon(k) < 1$ ו $\lim_{k\to\infty} \varepsilon(k) = 0$.

אבל גם יתירות זו היא גדולה משמעותית ביחס ליתירות האמיתית של $S(n,k)$.

בעבודה הנוכחית אנו מציגים אלגוריתם הצפנה לצופן בעל אפס ספקטראלי מסדר 3. האלגוריתם מייצר צופן בעל יתירות של $9 \log_2 n + O(\log \log n)$ סיביות. סיבוכיות הזמן שלו היא $O(n)$ חיבורים/חיסורים של מספרים שלמים ו $O(n \log n)$ הגדלות/הקטנות מונים בני $O(\log n)$ סיביות. סיבוכיות המקום היא $O(n)$.

2 אלגוריתם לצפנים בעלי אפס ספקטראלי מסדר 3

2.1 איפיון של מילות הצופן

מתוך [RSV94] ידוע כי אורך של מילת צופן בעל אפס ספקטראלי מסדר 3 הוא כפולה של 4. נרצה להצפין נתונים אל תוך מילות של צופן $S(n,3)$ כאשר $n=2h$ עבור h זוגי. עבור n כזה נגדיר m באופן הבא:

$$m = \lceil \log_2 n \rceil = 1 + \lceil \log_2 h \rceil$$

האלגוריתם ימפה מילת קלט $\underline{y}$ באורך גדול או שווה ל $2h$-$6m$+2 מעל F לתוך מילים $\underline{x}$, $\underline{x}'$ כאשר $\underline{x} \in S(2h,3)$, $\underline{x}' \in S(3m+\mu,3)$ ו μ מתנהג כמו $O(\log\ m)$. שירשור של $\underline{x}$ ו-$\underline{x}'$ מהווה מילת פלט בעלת אפס ספקטראלי מסדר 3.

בפרק **1** ציינו שכל מילה $\underline{x} = (x_1, x_2, ..., x_n)$ מעל F^n היא בעלת אפס ספקטראלי מסדר k אם ורק אם $H(n,k;c)\cdot\underline{x} = \underline{0}$ כאשר $H(n,k;c)$ מוגדרת ע״י (1.3). לפיכך $S(n,3)$ מאופיין באופן שקול ע״י $H(n,3;-h\text{-}1)$. נסמן את האינדקסים של המילה $\underline{x}$ ע״י $\underline{x} = (x_{-h}, x_{-h+1}, \dots, x_{h-1})$. **המומנטים** של המילה $\underline{x}$ מעל הממשיים יוגדרו באופן הבא:

$$q_j(\underline{x}) \equiv \sum_{i=-h}^{h-1} i^j \cdot x_i, \quad j = 0,1,2,\ldots \tag{2.1}$$

ברור כי $\underline{x} \in F^n$ הינו בתוך $S(n,3)$ אם ורק אם $q_0(\underline{x}) = q_1(\underline{x}) = q_2(\underline{x}) = 0$.

2.2 אלגוריתם הצפנה

האלגוריתם המוצע מתחיל ממילה $\underline{x}$ מעל {-1, +1, 0} אשר מכילה את מילת הקלט $\underline{y}$ כתת-מילה בכניסות מסוימות שלה. שאר הכניסות של $\underline{x}$ נקבעות להיות 0. בהמשך האלגוריתם מקטין לאפס את הערכים המוחלטים של $q_0(\underline{x})$, $q_2(\underline{x})$ ו- $q_1(\underline{x})$ (בסדר זה) ע״י סדרה של הפיכות, הזזות והחלפות של ביטים וע״י הצבה של ערכים 1+, 1- לכניסות של $\underline{x}$ ששוות ל 0. התהליך מסתיים ע״י הצפנה רקורסיבית של מונים מסוימים אשר חושבו במהלך ביצוע של השלבים הקודמים באלגוריתם. אם האורכים של המונים האלה קצרים מספיק אז משתמשים בשיטת ההצפנה הממספרת (enumerative encoding). תוצאת ההצפנה הרקורסיבית, $\underline{x}'$, משורשרת ל-$\underline{x}$, וכך מתקבלת מילת הפלט הסופית.

נסתכל בקבוצת האינדקסים $S = \{-h, -h+1, ..., h\text{-}1\}$ ונגדיר את תת-הקבוצות $S_{3.2}$, $S_{3.3}$ ו-S_4. השם של כל תת-הקבוצה נובע ממקום באלגוריתם בו תת-הקבוצה מוגדרת.

- $S_{3.2} = \{d_i\}_{i=0}^{2m-8} \bigcup \{c_i\}_{i=0}^{2m-8}$

כאשר

$$(d_i, e_i) = \begin{cases} (-10\cdot 2^{i/2}, -6\cdot 2^{i/2}) & \text{אם } i \text{ זוגי} \\ (-9\cdot 2^{(i+1)/2}, -7\cdot 2^{(i+1)/2}) & \text{אם } i \text{ אי-זוגי} \end{cases}$$

עבור $0 \le i \le 2m\text{-}10$.

בנוסף נגדיר $(d_{2m-8}, e_{2m-8}) = (-\tau_1, 7)$ וגם $(d_{2m-9}, e_{2m-9}) = (\tau_1, \tau_2)$, כאשר τ_1 הוא האינדקס האי-זוגי הקטן ביותר בתוך S אשר גודלו לפחות $\sqrt{(h^2/2)+49}$ ו-τ_2 הוא האינדקס הגדול ביותר בתוך S אשר גודלו לכל היותר $h/2$. נסלק זוג $\{d_i, e_i\}$ מתוך $S_{3.2}$ אם מתקיים $d_i < -h$. כפי שיפורט בהמשך, זה יכול לקרות רק לזוגות (d_{2m-10}, e_{2m-10}) ו (d_{2m-11}, e_{2m-11}).

- $S_{3.3} = \{0,-3,3,-5,5,6,-7,-9,9,10,-11,12,-13,14\}$.

- $S_4 = \{\pm 2^i\}_{i=0}^{m-2}$.

נניח שהערך של h גדול מספיק כדי שהקבוצות $S_{3.2}$, $S_{3.3}$ ו-S_4 תהיינה כולן זרות בזוגות. כפי שניתן יהיה לראות בדוגמא בסיום הפרק וכמו שצוין קודם, חלק מאברי $S_{3.2}$ ניתן לפעמים לסלק מהקבוצה. זה מאפשר ל-h להיות כל מספר זוגי שלא קטן מ 18.

נסמן $S_0 = S_{3.2} \bigcup S_{3.3} \bigcup S_4$

שים לב כי $|S_0| \le 2(2m-7) + 14 + 2(m-1) = 6m-2$.

בהמשך נשתמש בסימון $(\underline{x})_A$ כדי לסמן תת-מילה של מילה $\underline{x}$ באורך n אשר האינדקסים שלה ניתנים ע״י קבוצה A. הסימון $\underline{y} \to (\underline{x})_A$ ישמש אותנו בכדי לסמן הצבה של כניסות של מילה $\underline{y}$ לתוך כניסות של מילה $\underline{x}$ המסומנות באמצעות קבוצת האינדקסים A.

להלן מוצג האלגוריתם:

<u>צעד 1: איתחול של x</u>

$\underline{0} \to (\underline{x})_{S_0}$

$\underline{y} \to (\underline{x})_{S \backslash S_0}$

<u>צעד 2: הקטנת $|q_0(x)|$</u>

עבור סדרת האינדקסים $j = -h, -h+1, \ldots,$ הפוך את x_j (כלומר הפוך את הסימן שלו). המשך עד אשר $q_0(\underline{x})$ הופך להיות שווה ל-0. סמן ע״י j_2 את מספר הסיביות שערכן שונה.

<u>צעד 3: הקטנת $|q_2(x)|$</u>

1. בצע הזזה סיבובית של סיביות של $(\underline{x})_{S \backslash S_0}$ ימינה עד אשר יתקיים $|q_2(\underline{x})| \le h^2$. נסמן ע״י j_3 את מספר ההזזות האלה.
2. עבור סדרת האינדקסים $i = 2m-8, 2m-9, \ldots, 0$ הקטן ערך של $|q_2(\underline{x})|$ ע״י הצבה $x_{d_i} = -x_{e_i} = -1$ אם $q_2(\underline{x}) \ge 0$ וע״י הצבה $x_{d_i} = -x_{e_i} = 1$ אחרת.
3. $\to (\underline{x})_{S_{3.3}}$ שורה של טבלה 2.1 המתאימה ל-$|q_2(\underline{x})|$. אם $q_2(\underline{x}) \ge 0$, הפוך את הכניסות של $(\underline{x})_{S_{3.3}}$.

צעד 4: הקטנת $|q_1(x)|$

1. עבור סדרת האינדקסים $j = 1, 2, ..., h-1$ החלף בין x_j לבין x_{-j} עד אשר $|q_1(\underline{x})| \le 2(h\text{-}1)$. סמן ע״י j_4 את מספר ההחלפות שבוצעו.

2. עבור סדרת הערכים $i = m\text{-}2, m\text{-}3, ..., 0$, הקטן את הערך של $|q_1(\underline{x})|$ ע״י הצבה $x_{2^i} = -x_{-2^i} = -1$ אם $0 \le q_1(\underline{x})$ וע״י הצבה $x_{2^i} = -x_{-2^i} = 1$ אחרת.

צעד 5: הצפנה רקורסיבית

נפעיל צעדים 1 עד 4 באופן רקורסיבי על ההצגה הבינארית של (j_2, j_3, j_4). את התוצאה נשרשר אל $\underline{x}$ בתור הפלט הסופי של המצפין.

טבלה 2.1
יצירת מספרים אי-זוגיים עד 63 ע״י הצבות מאוזנות

Table 2.1
Generating odd integers up to 63 by balanced assignments

$\lvert q_2(x)\rvert$	0	-3	3	-5	5	6	-7	-9	9	10	-11	12	-13	14
1	+	+	-	-	+	-	+	-	-	+	-	+	-	+
3	+	+	-	+	+	-	-	-	-	+	-	-	+	+
5	-	+	-	-	-	+	+	+	+	+	-	-	+	-
7	-	-	-	+	+	-	+	+	+	-	+	+	-	-
9	+	-	-	-	+	+	+	-	-	+	+	-	-	+
11	+	+	-	+	-	-	-	+	-	+	-	+	+	-
13	+	+	-	-	+	-	+	-	+	-	-	-	+	+
15	-	-	-	+	+	-	+	+	+	+	-	-	+	-
17	+	-	-	-	-	+	+	+	-	+	+	+	-	-
19	-	-	-	+	+	+	-	+	-	+	+	+	-	-
21	+	+	-	-	-	-	+	+	+	-	-	+	+	-
23	+	+	-	-	-	+	+	-	-	+	-	+	-	+
25	+	+	-	-	+	+	-	-	-	+	-	-	+	+
27	+	+	-	-	-	-	-	+	+	+	+	+	-	-
29	-	-	-	+	-	+	+	+	+	-	+	+	-	-
31	-	-	-	+	+	+	-	+	+	-	+	-	+	-
33	+	-	-	+	+	-	+	-	-	+	-	+	-	+
35	+	+	-	-	-	+	+	-	+	-	-	-	+	+
37	-	+	-	+	+	+	-	-	+	-	-	-	+	+
39	-	+	-	+	+	-	+	-	-	-	+	+	+	-
41	+	+	-	-	-	+	-	-	+	+	+	-	-	+
43	+	+	-	-	+	-	+	-	-	-	+	+	-	+
45	+	+	-	+	+	-	-	-	-	-	+	-	+	+
47	-	+	-	-	-	+	+	+	+	-	+	-	+	-
49	+	-	-	+	+	+	-	-	-	-	+	+	-	+
51	+	+	-	-	+	-	+	-	-	+	-	-	+	+
53	+	-	-	+	-	-	+	+	+	-	-	+	+	-
55	+	-	-	-	+	+	+	-	-	+	-	+	-	+
57	+	-	-	+	+	+	-	-	-	+	-	-	+	+
59	+	-	-	+	-	-	-	+	+	+	+	+	-	-
61	+	-	-	-	+	-	+	+	+	-	+	-	-	+
63	-	+	-	+	+	-	+	-	+	-	-	-	+	+

2.3 ניתוח האלגוריתם

צעד אחר צעד נוודא שהאלגוריתם אכן עוצר כאשר הפלט שלו היא מילה בעלת אפס ספקטראלי מסדר 3 מעל F^n.

צעד 1 מסתיים כאשר המילה $\underline{x}$ מכילה מספר זוגי של כניסות מתוך F. צעד 2 הוא למעשה אלגוריתם של Knuth המופעל על אותן הכניסות. כפי שהדבר הוכח ב-[Knu86] , תמיד קיימת רישא של $\underline{x}$ אשר עבורה, אם הופכים אותה, המילה המתקבלת היא מאוזנת. לפיכך המונה j_2 מוגדר היטב.

נעבור כעת לשלב 3 ונראה כי המונה j_3 מוגדר היטב.

<u>למה 2.1</u> תמיד קיימת הזזה סיבובית של $(\underline{x})_{S\setminus S_0}$ בשלב 3.1 שעבורה $|q_2(\underline{x})| \le h^2$.

<u>הוכחה.</u> נסמן ע״י $\underline{x}^{(0)}$ את הערך של $\underline{x}$ בתחילתו של צעד 3.1 וע״י

$$\underline{x}^{(s)} = (x^{(s)}_{-h}, x^{(s)}_{-h+1}, \ldots, x^{(s)}_{h-1})$$

נסמן את המילה שמתקבלת מ-$\underline{x}^{(0)}$ באמצעות s הזזות סיבוביות ימינה של $(\underline{x}^{(0)})_{S\setminus S_0}$.
שים לב כי $(\underline{x}^{(0)})_{S_0}$ נשארת להיות מילה של אפסים לכל שלם s.

קודם נראה ש $\left|q_2(\underline{x}^{(s+1)}) - q_2(\underline{x}^{(s)})\right| \le 2h^2$ לכל $0 \le s$. נניח כי $j_1 < j_2 < \ldots < j_t$ הן מקומות של שינויי הסימן של המילה $\underline{x}^{(s)}$. קל להשתכנע כי

$$\left|q_2(\underline{x}^{(s+1)}) - q_2(\underline{x}^{(s)})\right| = \left|2\sum_{i=1}^{t}(-1)^i \cdot j_i^2\right| \qquad (2.2)$$

יהיה r האינדקס הקטן ביותר עבורו $j_r \ge 0$. נגדיר

$$B^+ = \sum_{i=r}^{t}(-1)^i \cdot j_i^2 \qquad\qquad B^- = \sum_{i=1}^{r-1}(-1)^i \cdot j_i^2$$

לפי ההגדרה B^- הוא הסכום של השלמים עם הסימנים המתחלפים והערך המוחלט הולך וקטן. השלם הראשון בסדרה (אם קיים בכלל) הוא שלילי. לפיכך מתקיים

$$-h^2 \le -j_1^2 \le B^- \le 0 \qquad (2.3)$$

באופן דומה, B^+ הוא הסכום של השלמים עם הסימנים המתחלפים והערך המוחלט הולך וקטן. מאחר ו-t זוגי, האיבר האחרון בסכום חייב להיות חיובי. לפיכך נקבל

$$0 \le B^+ \le j_i^2 \le (h-1)^2 \qquad (2.4)$$

ע״י שילוב של 2.2, 2.3 ו-2.4 נקבל כי

$$\left|q_2(\underline{x}^{(s+1)}) - q_2(\underline{x}^{(s)})\right| = 2 \cdot \left|B^- + B^+\right| \le 2h^2 \qquad (2.5)$$

כעת נבחין כי

$$\sum_{s=0}^{|S\setminus S_0|-1} q_2(\underline{x}^{(s)}) = 0$$

מאחר ו $\underline{x}^{(0)}$ מאוזן, נובע כי

$$\sum_{s=0}^{|S\setminus S_0|-1} x_j^{(s)} = 0$$

לכל $j \in S$.

לפיכך

$$\sum_{s=0}^{|S\setminus S_0|-1} q_2(\underline{x}^{(s)}) = \sum_{s=0}^{|S\setminus S_0|-1}\sum_{j\in S} j^2 \cdot x_j^{(s)} = \sum_{j\in S} j^2 \sum_{s=0}^{|S\setminus S_0|-1} x_j^{(s)} = 0$$

לכן, קיימים ערכי s "שמחליפים סימן" בהם $q_2(\underline{x}^{(s)})\cdot q_2(\underline{x}^{(s+1)}) \le 0$.

לפי (2.5) חייב להתקיים ש $|q_2(\underline{x}^{(s)})| \le h^2$ או $|q_2(\underline{x}^{(s+1)})| \le h^2$, וזה משלים את ההוכחה.

צעד 3.2 מקטין את הערך המוחלט של $q_2(\underline{x})$ כדלקמן:

<u>למה 2.2</u> הערך של $q_2(\underline{x})$ אחרי צעד 3.2 הוא מספר שלם אי-זוגי בין 63- לבין 63.

<u>הוכחה.</u> נניח כי לכל שני זוגות עוקבים מקבוצה $S_{3.2}$ מתקיים

$$2(d_{i-1}^2 - e_{i-1}^2) \ge d_i^2 - e_i^2, \quad i = 2m-8, 2m-9, \ldots, 1. \quad (2.6)$$

פרט אולי לזוג אחד או שניים שהוצאנו מקבוצה S. (אם הוצאנו זוג (d_i, e_i) אז עלינו להוכיח שמתקיים $2(d_{i-1}^2 - e_{i-1}^2) \ge d_{i+1}^2 - e_{i+1}^2$ ובאופן דומה גם אם הוצאנו שני זוגות עוקבים.)

כמו כן $2(d_{2m-8}^2 - e_{2m-8}^2) \ge h^2$

בפרט עבור $i \le 2m$ -10 מתקיים $d_i^2 - e_i^2 = 2^{i+6}$

מכאן נובע שאחרי הפעלה מספר i של שלב 3.2, הערך המוחלט של $q_2(\underline{x})$ חסום מלמעלה ע"י d_i^2-e_i^2. בפרט עבור i=0, הערך של $q_2(\underline{x})$ הוא מספר שלם בין 64- לבין 64. שים לב שבשלב זה הכניסות היחידות של $\underline{x}$ ששוות לאפס הן אלה שהאינדקסים שלהן שייכים לקבוצה $S_{3.3}$ או לקבוצה S_4. ישנו מספר אי-זוגי של האינדקסים הלא זוגיים שלא שייכים לקבוצות האלה. מכאן נובע כי $\rho_2(\underline{x})$ חייב להיות אי-זוגי.

נחזור להוכחה של (2.6).

$$d_{2m-10} = -10\cdot 2^{\frac{2m-10}{2}} = -\frac{10}{32}\cdot 2^m = -\frac{10}{32}\cdot 2^{1+\lceil \log_2 h\rceil} = -\frac{10}{16}\cdot 2^{\lceil \log_2 h\rceil}$$

התנאי $d_{2m-10} < -h$ יתקיים אם ורק אם $\frac{16}{10}h < 2^{\lceil \log_2 h\rceil}$, כלומר כאשר $2^{i-1} < h < \frac{10}{16}\cdot 2^i$ עבור i מסוים. במקרה זה מוציאים מקבוצה S את הזוג (d_{2m-10}, e_{2m-10}).

באופן דומה

$$d_{2m-11} = -9\cdot 2^{\frac{2m-10}{2}} = -\frac{9}{32}\cdot 2^m = -\frac{9}{32}\cdot 2^{1+\lceil \log_2 h\rceil} = -\frac{9}{16}\cdot 2^{\lceil \log_2 h\rceil}$$

התנאי $d_{2m-11} < -h$ יתקיים אם ורק אם $\frac{16}{9}h < 2^{\lceil \log_2 h \rceil}$, כלומר כאשר $2^{i-1} < h < \frac{9}{16}\cdot 2^i$ עבור i מסוים. במקרה זה מוציאים מקבוצה S את הזוג (d_{2m-11}, e_{2m-11}).

עבור $i \le 2m-12$ אם i זוגי אזי

$$d_i = -10\cdot 2^{\frac{i}{2}} \ge -10\cdot 2^{m-6} = -\frac{10}{64}\cdot 2^{1+\lceil \log_2 h \rceil} = -\frac{10}{32}\cdot 2^{\lceil \log_2 h \rceil} > -h$$

אם $i \le 2m-13$ ו i אי-זוגי אזי

$$d_i = -9\cdot 2^{\frac{i+1}{2}} \ge -9\cdot 2^{m-6} = -\frac{9}{64}\cdot 2^{1+\lceil \log_2 h \rceil} = -\frac{9}{32}\cdot 2^{\lceil \log_2 h \rceil} > -h$$

לכן הזוגות היחידים שמוציאים מקבוצה S הם (d_{2m-10}, e_{2m-10}) ו (d_{2m-11}, e_{2m-11}).

לפיכך ייתכנו שלושה מקרים :

1. $h \in \left(2^{i-1}; \frac{9}{16}2^i\right)$. מוציאים את הזוגות (d_{2m-10}, e_{2m-10}) ו (d_{2m-11}, e_{2m-11}) מהקבוצה S.
2. $h \in \left[\frac{9}{16}2^i; \frac{10}{16}2^i\right)$. מוציאים את הזוג (d_{2m-10}, e_{2m-10}) מהקבוצה S.
3. $h \in \left[\frac{10}{16}2^i; 2^i\right]$. כל הזוגות שבקבוצה $S_{3.2}$ נמצאים גם ב-S.

לפני הקטנת המומנט השני הערך המוחלט שלו הוא לכל היותר h^2. בוחרים τ_1 להיות אי-זוגי הקטן ביותר כך ש $\tau_1 \ge \sqrt{\frac{h^2}{2}+49}$

ואז $\tau_1 < \sqrt{\frac{h^2}{2}+49}+2$.

לכן אחרי הקטנת המומנט השני ע"י השמת איברי F לתוך זוג מקומות $(\tau_1, 7)$ המומנט השני חסום ע"י

$$\max\{h^2-(\tau_1^2-7^2),\ \tau_1^2-7^2\} = \max\{\tau_1^2-7^2\} \ge$$
$$\ge \frac{h^2}{2}+49+4+4\sqrt{\frac{h^2}{2}+49}-49 = \frac{h^2}{2}+4+4\sqrt{\frac{h^2}{2}+49}$$

בוחרים τ_2 להיות האי-זוגי הגדול ביותר כך ש $\tau_2 \le h/2$

ואז $\tau_2 > h/2 - 2$

אחרי הקטנת המומנט השני ע"י השמת איברי F לתוך זוג המקומות (τ_1, τ_2) המומנט השני חסום ע"י

$$\max\left\{\begin{array}{l}\left(\frac{h^2}{2}+4+4\sqrt{\frac{h^2}{2}+49}\right)-\left(\frac{h^2}{2}+49\right)+\left(\frac{h^2}{2}+4-2h\right),\\ \left(\frac{h^2}{2}+49+4+4\sqrt{\frac{h^2}{2}+49}\right)-\left(\frac{h^2}{2}+4-2h\right)\end{array}\right\}=$$

$$=\max\left\{\frac{h^2}{4}-41+4\sqrt{\frac{h^2}{4}+49}-2h,\frac{h^2}{4}+49+4\sqrt{\frac{h^2}{4}+49}+2h\right\} \quad (2.7)$$

הביטוי השני ב $\max\{\,\cdot\,,\,\cdot\,\}$ שב-(2.7) הוא יותר גדול מהביטוי הראשון ולכן הערך המוחלט של המומנט השני אחרי הקטנה באמצעות $(\tau_1,\ \tau_2)$ חסום מלמעלה ע״י הגודל

$$\frac{h^2}{4}+2h+49+4\sqrt{\frac{h^2}{2}+49}$$

כעת נראה שהגודל הזה גדול לכל היותר פי 2 בהשוואה לתרומה של הזוג הבא מתוך אוסף הזוגות הנותרים בקבוצה S בהתאם לדרישת תנאי (2.6).

מקרה 1: $d_{2m-12}^2-e_{2m-12}^2=2^6\cdot 2^{2m-12}=\frac{1}{64}\cdot 2^{2(1+\lceil\log_2 h\rceil)}=\frac{1}{16}\cdot 2^{2\lceil\log_2 h\rceil}$

זה קורה אם ורק אם מסלקים שני זוגות $(d_{2m\text{-}10},\ e_{2m\text{-}10})$ ו $(d_{2m\text{-}11},\ e_{2m\text{-}11})$ מקבוצה S.

אזי $2^{\lceil\log_2 h\rceil}>\frac{16}{9}h$

ולכן $d_{2m-12}^2-e_{2m-12}^2>\frac{16}{81}h^2$

מקרה 2: $d_{2m-11}^2-e_{2m-11}^2=2^5\cdot 2^{2m-10}=\frac{1}{32}\cdot 2^{2(1+\lceil\log_2 h\rceil)}=\frac{1}{8}\cdot 2^{2\lceil\log_2 h\rceil}$

זה קורה אם ורק אם מסלקים זוג $(d_{2m\text{-}10},\ e_{2m\text{-}10})$ בלבד מקבוצה S.

אזי $2^{\lceil\log_2 h\rceil}>\frac{16}{10}h$

ולכן $d_{2m-12}^2-e_{2m-12}^2>\frac{8}{25}h^2>\frac{16}{81}h^2$

מקרה 3: $d_{2m-10}^2-e_{2m-10}^2=2^6\cdot 2^{2m-10}=\frac{1}{16}\cdot 2^{2(1+\lceil\log_2 h\rceil)}=\frac{1}{4}\cdot 2^{2\lceil\log_2 h\rceil}\ge\frac{h^2}{4}>\frac{16}{81}h^2$

נבדוק מהם ערכי h עבורם מתקיים

$$\frac{16}{81}h^2\ge\frac{1}{2}\left(\frac{h^2}{4}+2h+49+4\sqrt{\frac{h^2}{2}+49}\right). \quad (2.8)$$

h=42 הוא הערך הקטן ביותר עבורו האי-שוויון (2.8) מתקיים. עבור $h>42$ נשווה את הנגזרות של שני הצדדים באי-שוויון (2.8). הנגזרת של צד שמאל היא $\frac{32}{81}h$.

הנגזרת של צד ימין היא

$$\frac{h}{4}+1+\frac{2h}{\sqrt{\frac{h^2}{2}+49}} \le \frac{h}{4}+1+\frac{2}{\sqrt{\frac{1}{2}+\frac{49}{h^2}}} < \frac{h}{4}+3 < \frac{32}{81}h$$

המעבר האחרון נכון לכל $h > 42$. ולכן האי-שוויון (2.8) מתקיים לכל $h \le 42$. וזה משלים את ההוכחה של למה 2.2.

יש לציין שאף על פי שאנו מוכיחים נכונות של למה 2.2 עבור h-ים החל מ 42, הבחירה של האינדקסים עובדת נכון גם עבור h-ים קטנים יותר. בדיקה ממוחשבת מראה שניתן להשתמש באלגוריתם זה החל מ h=18.

ההקטנה הסופית של $|q_2(\underline{x})|$ לאפס נעשית ע״י שימוש בהצבות של טבלה 2.1 בצעד 3.3. עבור r = 1, ..., 63, הערכים בשורה r של הטבלה תורמים בדיוק r לערכו של $q_2(\underline{x})$. אם התרומה הרצויה ל-$q_2(\underline{x})$ בשלב זה היא שלילית בגודל r- אז נהפוך את כל הסיביות מהשורה המתאימה של הטבלה. שים לב כי שום פעולה של צעד 3 לא משפיעה על ערכו של $q_0(\underline{x})$, שנשאר להיות שווה לאפס גם אחרי הצעד הזה של האלגוריתם.

כעת נעבור לצעד 4 של האלגוריתם. הצעד הזה דומה לפאזה A של אלגוריתם לצפנים בעלי אפס ספקטראלי מסדר שני מתוך [RSV94, פרק IV]. נראה כי מונה ההחלפות j_4 מוגדר היטב.

<u>למה 2.3</u> קיימת מילה $\underline{x}$ המתקבלת ע״י פחות מ-h החלפות סיביות בצעד 4.1 אשר מקיימת $|q_1(\underline{x})| \le 2(h\text{-}1)$.

<u>הוכחה.</u> נסמן ע״י $\underline{x}^{[0]}$ את הערך של $\underline{x}$ בתחילת צעד 4 ונסמן ע״י $\underline{x}^{[j]}$ את המילה אחרי החלפה ה-j של הסיביות. קודם כל, מתקיים $|q_1(\underline{x}^{[j+1]}) - q_1(\underline{x}^{[j]})| \le 4(h\text{-}1)$ לכל $0 \le j$. נניח כי ממשיכים להחליף את הסיביות עד אשר $j = h\text{-}1$ ונניח ש $\underline{x}^{[h]}$ היא מילה שמתקבלת מ $\underline{x}^{[h\text{-}1]}$ ע״י החלפת הסימן של הכניסה שהאינדקס שלה h-. במקרה כזה נקבל כי

$$|q_1(\underline{x}^{[h]}) - q_1(\underline{x}^{[h\text{-}1]})| = 2h \quad \text{ו} \quad q_1(\underline{x}^{[h]}) = - q_1(\underline{x}^{[0]}) \ .$$

לפיכך חייב להיות אינדקס j, $h > j$, ״העובר את האפס״ שמקיים
$$q_1(\underline{x}^{[j]})\, q_1(\underline{x}^{[j+1]}) \le 0 \ .$$

עבור האינדקס הזה נקבל ש $|q_1(\underline{x}^{[j]})| \le 2(h\text{-}1)$ או ש $|q_1(\underline{x}^{[j+1]})| \le 2(h\text{-}1)$. אם האינדקס הוא $j = h\text{-}1$ אז $|q_1(\underline{x}^{[h\text{-}1]})| \le h$ או $|q_1(\underline{x}^{[h]})| = |q_1(\underline{x}^{[0]})| \le h$. בכל מקרה טענת הלמה מתקיימת.

כעת נחזור לצעד 4.2. קל לוודא שאחרי האיטרציה ה-i בצעד הזה הערך של $|q_1(\underline{x})|$ חסום מלמעלה ע״י 2^{i+1}. בפרט, עבור i=0, הערך של $q_1(\underline{x})$ הוא מספר שלם בין 2- ל 2. הלמה הבאה גוררת ש-$q_1(\underline{x})$ כבר שווה לאפס בשלב הזה.

<u>למה 2.4</u> עבור n שמתחלק ב 4 ועבור כל $\underline{w}$ מעל F^n,
$$q_1(\underline{w}) \equiv q_2(\underline{w}) \pmod 4 .$$

הוכחה. נסמן $n = 2h$ ונרשום את $\underline{w}$ בצורה $\underline{w} = (w_{-h}, w_{-h+1}, ..., w_{h-1})$. אזי

$$q_2(\underline{w}) - q_1(\underline{w}) = \sum_{j=-h}^{h-1} j(j-1) \cdot w_j =$$

$$= \sum_{l=-h/2}^{(h/2)-1} ((2l)(2l-1) \cdot w_{2l} + (2l+1)(2l) \cdot w_{2l+1}) =$$

$$= \sum_{l=-h/2}^{(h/2)-1} (2l)((2l-1) \cdot w_{2l} + (2l+1) \cdot w_{2l+1}).$$

המסקנה נובעת מאחר והביטוי

$$(2l)((2l-1) \cdot w_{2l} + (2l+1) \cdot w_{2l+1})$$

הוא כפולה של 4 לכל l.

אף פעולה מבין אלה שבוצעו במהלך צעד 4 אינה משפיעה על ערכי $q_0(\underline{x})$ ו $q_2(\underline{x})$ אשר נשארים להיות שווים לאפס. בסיום צעד 4 מתקיים $q_1(\underline{x}) \equiv 0 \pmod 4$. מאחר ו $-2 \le q_1(\underline{x}) \le 2$ נובע ש $q_1(\underline{x}) = 0$.

לבסוף, נכונות של צעד 5 מבוססת על העובדה ששירשור של שתי מילים בעלות אפס ספקטראלי מסדר k מהווה מילה בעלת אפס ספקטראלי מסדר k.

על-מנת לפענח את המילה $\underline{y}$ צריך קודם לשחזר את ערכי המונים j_2, j_3 ו-j_4 מתוך הידיעה של המילה $\underline{x}'$. כאשר ערכי המונים האלה ידועים, נוכל לשחזר את המילה $\underline{x}$ בהתחלה של שלבים 4, 3, 2 (בסדר זה, מימין לשמאל).

2.4 יתירות

נעריך את היתירות של הצופן המוגדר ע"י מילים שמיוצרות ע"י האלגוריתם עבור כל אורך נתון.

בצעד 2 אנו זקוקים ל-m סיביות ליצג את מונה ההפיכות j_2. הסיביות האלה תתרומנה ליתירות בצעד 5.

צעדים 3 ו-4 דורשים $|S_0| \le 6m - 2$ סיביות עבור הקטנה של $|q_2(\underline{x})|$ ו-$|q_1(\underline{x})|$ לאפס. בנוסף אנו זקוקים ל-m סיביות לייצג את מונה ההזזות j_3 ו m-1 סיביות לייצג את מונה ההחלפות j_4.

בצעד 5 האלגוריתם מופעל רקורסיבית על $3m$-1 סיביות שמיצגות את שלישית המונים (j_2, j_3, j_4). בצורה כזאת האלגוריתם מייצר מילה $\underline{x}'$, $\underline{x}' \in S(m', 3)$, בעלת אורך של $m' = 3m + O(\log m)$ סיביות. מאחר ש $\log_2 n + 1 > m$, נובע כי היתירות הכוללת של האלגוריתם היא $9 \log_2 n + O(\log \log n)$ סיביות. הביטוי הזה יהווה חסם עליון על היתירות גם אם נציב במקום n את האורך הכולל $n + m'$ של פלט האלגוריתם.

2.5 סיבוכיות זמן ומקום

צעד 2 ניתן לממוש ע״י חישוב של הערך ההתחלתי של $q_0(\underline{x})$ ועדכון של הערך הזה לאחר היפוך של כל סיבית. זה דורש $O(n)$ הקטנות והגדלות של המונה בעל $\lceil \log_2 n \rceil$ סיביות.

בצעד 3 אנו זקוקים לערך של $q_2(\underline{x})$ לכל הזזה סיבובית בצעד 3.1. נניח שהריבועים של המספרים בין 1 ל-h מחושבים בשלב האיתחול ורשומים בטבלה. אז ערכו ההתחלתי של $q_2(\underline{x})$ ניתן לחישוב ב-$O(n)$ חיבורים של שלמים בעלי $O(\log n)$ סיביות. נסמן ע״י $\underline{x}'$ את המילה המתקבלת מ-$\underline{x}$ ע״י הזזה סיבובית אחת ימינה של $(\underline{x})_{S\setminus S_0}$ ונסמן ע״י $\underline{x}''$ את המילה המתקבלת מ-$\underline{x}$ ע״י הזזה סיבובית אחת שמאלה של המילה $\underline{x}$. נתאר איך ניתן לחשב ביעילות את $q_l(\underline{x}')$ מתוך ידיעה של $q_l(\underline{x})$ עבור l=1,2. נבצע את הצעד 3.1 באופן איטרטיבי וכל פעם נסמן ע״י $\underline{x}'$ את הערך החדש של $\underline{x}$.

נציין כאן כי $q_0(\underline{x})=0$ ואז קל לבדוק כי

$$q_1(\underline{x}'') = q_1(\underline{x}) - 2h \cdot x_{h-1}$$
$$q_2(\underline{x}'') = q_2(\underline{x}) + 2q_1(\underline{x})$$

לפיכך, אם אנחנו יודעים את $q_1(\underline{x})$ ו-$q_2(\underline{x})$, קל לחשב את $q_1(\underline{x}'')$ ו-$q_2(\underline{x}'')$.

נסמן ע״י S_1 את קבוצת האינדקסים j, $j \in S_0$, כך ש- $j-1 \in S_0 \setminus S$ (עבור $j = -h$ האינדקס j-1 יוחלף ב h-1). עבור אינדקס j , $j \in S_1$, נסמן ע״י j^* את האינדקס הקטן ביותר בתוך קבוצה $S\setminus S_0$ אשר גדול מ-j. אם אין אינדקס כזה, אז נגדיר את j^* בתור האינדקס הקטן ביותר בתוך הקבוצה $S\setminus S_0$. עבור l=1,2, נגדיר

$$\alpha_l(\underline{x}) = \sum_{j \in S_1} (j^{*l} - j^l) \cdot x_{j-1}$$

קל לוודא כי

$$q_l(\underline{x}') = q_l(\underline{x}'') + \alpha_l(\underline{x}), \quad l = 1,2$$

הביטוי $\alpha_l(\underline{x})$ ניתן לחישוב ע״י $O(\log n)$ חיבורים של מספרים שלמים בני $O(\log n)$ סיביות. בהמשך הדיון נראה איך ניתן לשפר את סיבוכיות החישוב של $\alpha_l(\underline{x})$ ע״י שימוש בטבלאות. נחלק את S_1 ל-$O(1)$ קבוצות $S_1(t)$, כל אחת בגודל קטן מ-m:

$$S_1 = \bigcup_t S_1(t)$$

לכל קבוצה $S_1(t)$ בחלוקה נבנה טבלה לחישוב הביטוי

$$\alpha_l((\underline{x})_{S_1(t)}) = \sum_{j \in S_1(t)} (j^{*l} - j^l) \cdot x_{j-1}$$

כפונקציה של כניסות x_{j-1}, $j \in S_1(t)$. כל טבלה מכילה פחות מ-n כניסות וכל כניסה מכילה מספר שלם בעל $O(\log n)$ סיביות. הטבלאות האלה ניתנות לחישוב בזמן $O(n)$ והן תלויות ב-n אבל לא תלויות במילה מוצפנת. על מנת לגשת לסיביות x_{j-1}, $j \in S_1(t)$, אשר מופיעות בתוך $(\underline{x})_{S\setminus S_0}$, נשתמש ב-$|S_1(t)|$ מצביעים (מונים), אשר יוגדלו ב-1 אחרי כל הזזה סיבובית. אחרי שחישבנו $O(1)$ ביטויים $\alpha_l((\underline{x})_{S_1(t)})$, נקבל את $\alpha_l(\underline{x})$ כסכום שלהם. החישובים האלה של $q_2(\underline{x})$ מאפשרים לנו למצוא את j_3 מבלי שנבצע הזזה סיבובית של ממש של המילה $(\underline{x})_{S\setminus S_0}$.

הצעדים 3.2, 3.3 ו 4 הם די פשוטים מבחינת סיבוכיות החישוב וניתנים לממוש ע״י $O(n)$ חיבורים של מספרים שלמים. לפיכך הסיבוכיות הכללית של הזמן והמקום של האלגוריתם היא כדלקמן :

- $O(n)$ חיבורים של מספרים שלמים בעלי $O(n)$ סיביות.
- $O(n)$ גישות ל-$O(1)$ טבלאות, כל אחת בגודל קטן מ-n.
- הקטנות או הגדלות של $O(\log n)$ מונים, כל אחד באורך $O(\log n)$ סיביות.

2.6 דוגמא

בסעיף זה נביא דוגמא להפעלת האלגוריתם. נקח את המקרה n=60 (עבור n קטן כל-כך היתירות גדולה יחסית, ולכן הדוגמא הזאת ניתנת רק למטרת ההמחשה בלבד). במקרה כזה h=30 ו m=6. קבוצה $S_{3.2}$ ניתנת ע״י

$$S_{32} = \{-10,-18,-20,-23\} \bigcup \{-6,-14,-12,7\}$$

כאשר τ_1=23.

שים לב שהוצאנו את האיברים $\{d_3. e_3\} = \{\tau_1, \tau_2\} = \{23, 15\}$ מהקבוצה $S_{3.2}$ מכיוון שהם לא נחוצים בצעד 3.2 : הערך של $d_2^2 - e_2^2 = (-12)^2 - (-20)^2 = 256$ והוא גדול ממחצית הערך $d_4^2 - e_4^2 = 7^2 - (-23)^2 = 480$. הקבוצה $S_{3.3}$ היא בגודל 14 ו S_4 נתונה ע״י $\{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$. לכן $|S_0| = 32$.

נניח שמילת הקלט $\underline{y}$ באורך $n - |S_0| = 28$ נתונה ע״י

++++−−+++++++−+−+++−−++−+−−+

אחרי השמה של המילה $\underline{y}$ לתוך המילה $\underline{x}$ נקבל את המילה

↓

++++−−+0++0+0+0+0000000000000000000000000+0−0+0−+++−−++−+−−+

למילה זו $q_0(\underline{x}) = 10$ (החץ מצביע על הכניסה שהאינדקס שלה הוא אפס). סדרה של היפוכי הסיביות בשלב 2 יוצרת את המילים בעלות $q_0(\underline{x})$ השווים ל-8, 6, 4, 2, 4, 6, 4, 2, 0. לכן $j_2 = 10$ ושלב 2 מסתיים עם המילה

↓

−−−−++−0−−0+0+0+0000000000000000000000000+0−0+0−+++−−++−+−−+

עבור המילה הזאת $q_2(\underline{x}) = -2047$ וכאשר מפעילים הזזות סיבוביות בשלב 3.1, נוצרת המילה $\underline{x}$ עם $q_2(\underline{x})$ השווה ל 1853-, 1755-, 1357- ו 625-. הערך האחרון מתקבל עבור המילה

↓

+−−+−−−0−+0+0−0−0000000000000000000000000−0+0+0++−+−+++−−++−

זוהי המילה הראשונה בשלב זה המקיימת $|q_2(\underline{x})| \le h^2 = 900$. לכן $j_3 = 4$. הצבה של ערכים לכניסות שהאינדקסים שלהן ב-$S_{3.2}$ בצעד 3.2 נותנת את המילה

↓

+−−+−−−+−+++−−0−+0−0+000−000000000000−000−0+0+0++−+−+++−−++−

שעבורה 47 = $q_2(\underline{x})$. בצעד **3.3** נשלים את הכניסות שהאינדקסים שלהן ב-$S_{3.3}$ עם ההיפוך של הכניסות מהשורה של 47 בטבלה **3.1**. זה יוצר את המילה

$$\downarrow$$
+--+---+-++++--0-+---+-0--+0-00+00+0+--0-+-++++0++-+-+++---++-

צעד **4.1** מתחיל מהמילה הזאת כאשר 174 = $q_1(\underline{x})$. החלפות הסיביות יוצרות את המילים עם $q_1(\underline{x})$ השווים ל-194-, 194, 182 (לאורך 9 צעדים), 134, 82, 82 ו-22-. הערך האחרון מתאים למילה

$$\downarrow$$
+--+---+-++++--0++++-+-0--+0+00+00-0+--0-+---+-0++-+-+++---++-

וזוהי המילה הראשונה עבורה $\left|q_1(\underline{x})\right| \le 2(h-1) = 58$, וכך קיבלנו כי $j_4 = 15$. צעד **4.2** משלים כניסות של $\underline{x}$ אשר האינדקסים שלהן ב-S_4. התהליך הזה יוצר את המילה

$$\downarrow$$
+--+---+-++++-+++++-+----+++-++-+--+--+-+---+--++-+-+++---++-

עבורה $q_0(\underline{x}) = q_1(\underline{x}) = q_2(\underline{x}) = 0$.

קיימת דרך יותר חסכונית לספור את מספר ההיפוכים וההחלפות של הסיביות. ניתן להתעלם מהאפסים בכניסות של $\underline{x}$ כאשר מבצעים את ההיפוכים בצעד 2. כמו כן ניתן לא להתייחס לאינדקס של זוג $(-j, j)$ עם $x_{-j} = x_j$ כאשר סופרים את מספר ההחלפות של סיביות בצעד 4 (במקרה הזה ההחלפות האלה הן למעשה כמו היפוך של הסיביות x_j ו x_{-j} בכל פעם כאשר $x_{-j} \ne x_j$).

לבסוף, השלישיה (j_2, j_3, j_4) מיוצגת ע"י $3 \cdot 6 - 1 = 17$ סיביות והרקורסיה של צעד **5** מופעלת על השלישיה הזאת.

3 תכונות של צפנים בעלי אפסים ספקטראליים מסדר גבוה

3.1 כללי

פרק 3 מכיל אוסף תוצאות המחקר שונות הקשורות בצפנים בעלי אפסים ספקטראליים. נעזרנו בחלק מהתוצאות (תכונת החלוקה, החסם התחתון על האורך של המילה המינימלית) למילוי טבלת היתירות של הקבוצות $S(n,k)$ עבור זוגות (n,k) מסוימים (טבלה 3.1) ולמציאת מילות הצופן. השימוש במילה באורך 48 בעלת אפס ספקטראלי מסדר 6 שמצאנו הביא לשיפור של החסם העליון בפרק 3.4. לעומת זאת התוצאות שמוצגות בפרקים 3.5, 3.6 אינן קשורות בתוצאות אחרות.

3.2 תכונת החלוקה

ידוע [RSV94] שאורך של מילה בעלת אפס ספקטראלי מסדר k מתחלקת ב $2^{\lfloor \log_2 k \rfloor + 1}$. ההוכחה מתבססת על העובדה שהפולינום המייצג של מילת הצופן המתאימה מתחלק ב $(z-1)^k$ מעל הממשיים, ולכן חייב להתחלק בפולינום $(z+1)^k$ מעל השדה GF(2). נראה כי אם אורך מילת הצופן לא עולה על 2^k אזי לפולינום המייצג שלה קיימות חלוקות נוספות בפולינומים $z+1$ ו z^2+1 מעל המספרים הממשיים. החלוקות מתורגמות לחלוקות בפולינום $z+1$ מעל השדה GF(2).

<u>למה 3.1</u> יהי $C(z)$ הפולינום המייצג של מילת הצופן בעלת אפס ספקטראלי מסדר k ויהי t שלם אי-שלילי כך שמתקיים

$$k > 1 + \log_2\left(\left\lceil \frac{n+t}{2} \right\rceil \left\lceil \frac{n-t-2}{2} \right\rceil\right)$$

אזי $C(z)$ מתחלק בפולינום $(z+1)^{t+1}$.

<u>הוכחה.</u> נסמן ע"י d את הריבוי של $z+1$ בפירוק של הפולינום $C(z)$ מעל הממשיים. נניח בשלילה כי $d \le t$.

עבור $0 \le i \le d$ נסמן ע"י $C^{(i)}(z)$ את הפולינום שמתקבל מהפולינום $C(z)$ על-ידי i חלוקות בפולינום $z+1$. נסמן ע"י $\underline{C}^{(i)} = [c_1^{(i)}, c_2^{(i)}, \ldots, c_{n-i}^{(i)}]$ את וקטור המקדמים של $C^{(i)}(z)$. בפרט $\underline{C}^{(0)}$ יהיה וקטור המקדמים של $C(z)$. לפי הגדרת הצופן לכל l המקיים $1 \le l \le n$ מתקיים $|c_l^{(0)}| = 1$. כמו כן קל לוודא כי עבור $1 \le i \le n$ מתקיימות הזהויות הבאות:

$$c_1^{(i-1)} = c_1^{(i)} \qquad (3.1)$$

$$c_{n-i+1}^{(i-1)} = c_{n-i}^{(i)} \qquad (3.2)$$

עבור $1 < l < n - i + 1$ מתקיים

$$c_l^{(i-1)} = c_{l-1}^{(i)} + c_l^{(i)} \tag{3.3}$$

ע״י שימוש ב-(3.3) ניתן לרשום

$$|c_l^{(i)}| = |c_l^{(i-1)} - c_{l-1}^{(i)}| \le |c_l^{(i-1)}| + |c_{l-1}^{(i)}| \le \cdots \le \sum_{r=1}^{l} |c_r^{(i-1)}| \tag{3.4}$$

בצורה דומה נסיק כי

$$|c_l^{(i)}| = |c_{l+1}^{(i)} - c_{l+1}^{(i-1)}| \le |c_{l+1}^{(i)}| + |c_{l+1}^{(i-1)}| \le \ldots \le \sum_{r=l+1}^{n-i+1} |c_r^{(i-1)}| \tag{3.5}$$

ע״י שימוש באינדוקציה על i נראה כי

$$|c_l^{(i)}| \le \binom{i+l-1}{l-1} \tag{3.6}$$

<u>בסיס האינדוקציה</u>

עבור $i = 0$

$$|c_l^{(0)}| = 1 \le \binom{l-1}{l-1}$$

<u>צעד האינדוקציה</u>

נניח כי עבור $0 \le i \le m\text{-}1$ תנאי (3.6) מתקיים. אזי

$$c_l^{(m)} \le \sum_{r=1}^{l} |c_r^{(m-1)}| \le \sum_{r=1}^{l} \binom{m+r-2}{r-1} = \binom{m+l-1}{l-1}$$

קל להוכיח את השוויון האחרון באינדוקציה פשוטה, אם כי הקורא יכול למצוא אותו גם בספרות [Tuck84, עמוד 207]. וזה משלים את הוכחת האינדוקציה.

ע״י שימוש באינדוקציה על i נראה כי באופן דומה מתקיים

$$|c_l^{(i)}| \le \binom{n-l}{n-l-i} \tag{3.7}$$

<u>בסיס האינדוקציה</u>

עבור $i = 0$

$$|c_l^{(0)}| = 1 = \binom{n-l}{n-l}$$

<u>צעד האינדוקציה</u>

נניח כי עבור $0 \le i \le m\text{-}1$ תנאי (3.7) מתקיים. אזי באופן דומה להוכחה הקודמת

$$c_l^{(m)} \le \sum_{r=l+1}^{n-m+1} |c_r^{(m-1)}| \le \sum_{r=l+1}^{n-m+1} \binom{n-r}{n-r-m+1} = \binom{n-l}{n-l-m}$$

השוויון האחרון מתקיים על-סמך [Tuck84, עמוד 207]. וזה משלים את ההוכחה של אי-שוויון (3.7).

כעת נציב $z = -1$ לתוך השוויון $C^{(d)}(z) = A^{(d)}(z)\ (z-1)^k$. הפולינום $A^{(d)}(z)$ קיים מכיוון ש-$C(z)$ הוא הפולינום המייצג של המילה בעלת אפס ספקטראלי מסדר k ולכן גם $C(z)$ וגם $C^{(d)}(z)$ שניהם מתחלקים ב- $(z-1)^k$. $A^{(d)}(-1)$ ו $C^{(d)}(-1)$ שניהם מספרים שלמים.

כעת נניח הנחת שלילה נוספת: נניח ש $A^{(d)}(-1) \neq 0$. אזי

$$2^k \le |A^{(d)}(-1)||(-2)^k| = |C^{(d)}(-1)| \le \sum_{l=1}^{n-d} |c_l^{(d)}| \qquad (3.8)$$

לכן ניתן לרשום

$$2^k \le \sum_{l=1}^{n-d} |c_l^{(d)}| = \sum_{l=1}^{\left\lceil \frac{n-d}{2} \right\rceil} |c_l^{(d)}| + \sum_{l=\left\lceil \frac{n-d+2}{2} \right\rceil}^{n-d} |c_l^{(d)}|$$

ע"י שימוש ב-(3.6) ו-(3.7) עבור $i = d$ ניתן לרשום

$$\begin{aligned} 2^k &\le \sum_{l=1}^{\left\lceil \frac{n-d}{2} \right\rceil} \binom{d+l-1}{l-1} + \sum_{l=\left\lceil \frac{n-d+2}{2} \right\rceil}^{n-d} \binom{n-l}{n-l-d} = \\ &= \binom{\left\lceil \frac{n+d}{2} \right\rceil}{\left\lceil \frac{n-d-2}{2} \right\rceil} + \binom{n-\left\lceil \frac{n-d+2}{2} \right\rceil + 1}{n-d-\left\lceil \frac{n-d+2}{2} \right\rceil} = \\ &= \binom{\left\lceil \frac{n+d}{2} \right\rceil}{\left\lceil \frac{n-d-2}{2} \right\rceil} + \binom{\left\lfloor \frac{n+d}{2} \right\rfloor}{\left\lfloor \frac{n-d-2}{2} \right\rfloor} \le 2\binom{\left\lceil \frac{n+d}{2} \right\rceil}{\left\lceil \frac{n-d-2}{2} \right\rceil} \end{aligned} \qquad (3.9)$$

אבל לפי הנתון

$$k > 1 + \log_2 \binom{\left\lceil \frac{n+t}{2} \right\rceil}{\left\lceil \frac{n-t-2}{2} \right\rceil} \qquad (3.10)$$

מתוך (3.10) וההנחה כי $t \le d$ ניתן לרשום

$$k > 1 + \log_2 \binom{\left\lceil \frac{n+d}{2} \right\rceil}{\left\lceil \frac{n-d-2}{2} \right\rceil}$$

התנאי הזה שקול לאי-שוויון

$$2^k > 2\binom{\left\lceil \frac{n+d}{2} \right\rceil}{\left\lceil \frac{n-d-2}{2} \right\rceil}$$

אשר מהווה סתירה לאי-שוויון (3.9). לכן על מנת למנוע את הסתירה יש להניח כי $C^{(d)}(-1) = A^{(d)}(-1) = 0$. במילים אחרות הפולינום $C^{(d)}(z)$ מתחלק בפולינום $z + 1$. וזה מהווה סתירה להגדרה של d כריבוי של $z + 1$ בפירוק של $C(z)$ מעל הממשיים. הסתירה האחרונה נובעת מתוך ההנחה $d \le t$. לכן $C(z)$ מתחלק בפולינום $(z + 1)^{t+1}$. בזה השלמנו את ההוכחה של למה **3.1**.

דוגמא

נניח שעבור מילה מסוימת מתקיים $n < 2^k$. הצד הימני של התנאי בלמה **3.1** עבור בחירה $t = 0$ ייכתב כדלקמן

$$1+\log_2\binom{\lceil n/2\rceil}{\lceil n/2-1\rceil} < 1+\log_2\binom{2^{k-1}}{2^{k-1}-1} = 1+\log_2 2^{k-1} = k$$

ולפיכך התנאים של הלמה מתקיימים. ניתן להסיק מכך כי במקרה הזה הפולינום $C(z)$ מתחלק בפולינום $z + 1$.

ניתן לשפר את התוצאה של למה **3.1** למקרה של מילה המקיימת $n = 2^k$ ו $k>1$. ניתן להראות כי $C(z)$ המתאים מתחלק בפולינום $z + 1$ אף על פי שהתנאים של למה **3.1** לא מתקיימים.

נניח בשלילה כי $A^{(d)}(-1) \neq 0$. אזי בדומה ל (3.8) נרשום

$$2^k \le |A^{(0)}(-1)||(-2)^k| = |C^{(0)}(-1)| \le \sum_{l=1}^{n} |c_l^{(0)}|$$

האי-שוויון האחרון מתקיים בשיוויון רק עבור פולינום $C(z)$ כזה ש $c_b^{(0)} = c_1^{(0)}$ עבור b אי-זוגי ו $c_b^{(0)} = c_2^{(0)} = -c_1^{(0)}$ עבור b זוגי. הפולינום $C(z)$ הזה מתאים למילה בעלת אפס ספקטראלי מסדר ראשון. לכן עבור $k>1$ נקבל

$$2^k < \sum_{l=1}^{n} |c_l^{(0)}| = n = 2^k$$

וזה מהווה סתירה שנובעת מההנחה השגויה כי $A^{(d)}(-1) \neq 0$. לכן הפולינום $C(z)$ מתחלק בפולינום $z + 1$.

למה 3.2 יהי $C(z)$ הפולינום המיצג של המילה בעלת אפס ספקטראלי מסדר $k > 2$ ויהי t שלם אי-שלילי כך שמתקיים

$$k > 3 + 2\log_2\left(\begin{matrix}\left\lceil \frac{n+3t}{4} \right\rceil \\ \left\lceil \frac{n-t-4}{4} \right\rceil\end{matrix}\right) \qquad (3.11)$$

אזי הפולינום $C(z)$ מתחלק בפולינום $(z^2 + 1)^{t+1}$.

הוכחה ההוכחה דומה מאוד להוכחה של הלמה הקודמת. לא נחזור על כל הפרטים, אבל נציין את הקווים הכלליים של ההוכחה. הפעם נסמן ע"י d את הריבוי של הפולינום $z^2 + 1$ בפירוק של $C(z)$ מעל הממשיים. נניח בשלילה כי $d \le t$.

משוואת המפתח שקושרת את המקדמים היא

$$c_l^{(i-1)} = c_{l-2}^{(i)} + c_l^{(i)}$$

לפיכך ניתן לרשום

$$|c_l^{(i)}| = |c_l^{(i-1)} - c_{l-2}^{(i)}| \le |c_l^{(i-1)}| + |c_{l-2}^{(i)}| \le \ \ldots \ \le |c_l^{(i-1)}| + |c_{l-2}^{(i-1)}| + \ \ldots \ + |c_b^{(i-1)}|$$

כאשר b=1 אם l אי-זוגי ו b=2 אם l זוגי.

באינדוקציה דומה לזו שמופיעה בהוכחה של למה **3.1** ניתן להראות כי

$$|c_l^{(i)}| \le \binom{i + \lceil l/2 \rceil - 1}{\lceil l/2 \rceil - 1} \qquad (3.12)$$

<u>בסיס האינדוקציה</u>

עבור $i = 0$

$$|c_l^{(0)}| = 1 \le \binom{\lceil l/2 \rceil - 1}{\lceil l/2 \rceil - 1}$$

<u>צעד האינדוקציה</u>

נניח כי עבור $0 \le i \le m\text{-}1$ אי-שוויון (3.12) מתקיים. אזי

$$c_l^{(m)} \le |c_l^{(m-1)}| + |c_{l-2}^{(m-1)}| + \ldots + |c_b^{(m-1)}| \le$$

$$\le \binom{m + \lceil l/2 \rceil - 2}{\lceil l/2 \rceil - 1} + \binom{m + \lceil l/2 \rceil - 3}{\lceil l/2 \rceil - 2} + \ldots + \binom{m-1}{0} =$$

$$= \binom{m + \lceil l/2 \rceil - 1}{\lceil l/2 \rceil - 1}$$

כאשר b=1 או b=2 בהתאם לזוגיות של l.

באופן דומה ניתן להראות כי

$$|c_l^{(m)}| = |c_{l+2}^{(m-1)} - c_{l+2}^{(m)}| \le |c_{l+2}^{(m-1)}| + |c_{l+2}^{(m)}| \le \ldots \le |c_{l+2}^{(m-1)}| + |c_{l+4}^{(m-1)}| + \ldots + |c_b^{(m-1)}|$$

כאשר $b = n - m + 1$ או $b = n - m$ בהתאם לזוגיות של l.

באינדוקציה על i נוכיח כי

$$|c_l^{(i)}| \le \binom{\left\lfloor \frac{n-l+i}{2} \right\rfloor}{\left\lfloor \frac{n-l-i}{2} \right\rfloor} \qquad (3.13)$$

<u>בסיס האינדוקציה</u>

עבור $i = 0$

$$|c_l^{(0)}| = 1 \le \binom{\left\lfloor \frac{n-l}{2} \right\rfloor}{\left\lfloor \frac{n-l}{2} \right\rfloor}$$

<u>צעד האינדוקציה</u>

נניח כי עבור $0 \le i \le m\text{-}1$ אי-שוויון (3.13) מתקיים. אזי מתוך משוואת המפתח נובע

$$|c_l^{(m)}| \le |c_{l+2}^{(m-1)}| + |c_{l+4}^{(m-1)}| + \ldots + |c_b^{(m-1)}|$$

לפי הנחת האינדוקציה

$$|c_l^{(m)}| \le \binom{\left\lfloor \frac{n-l-2+m-1}{2} \right\rfloor}{\left\lfloor \frac{n-l-2-m+1}{2} \right\rfloor} + \binom{\left\lfloor \frac{n-l-4+m-1}{2} \right\rfloor}{\left\lfloor \frac{n-l-4-m+1}{2} \right\rfloor} + \ldots + \binom{\left\lfloor \frac{n-b+m-1}{2} \right\rfloor}{\left\lfloor \frac{n-b-m+1}{2} \right\rfloor} =$$

$$= \binom{\left\lfloor \frac{n-l+m-3}{2} \right\rfloor}{\left\lfloor \frac{n-l-m-1}{2} \right\rfloor} + \binom{\left\lfloor \frac{n-l+m-5}{2} \right\rfloor}{\left\lfloor \frac{n-l-m-3}{2} \right\rfloor} + \ldots + \binom{\left\lfloor \frac{n-b+m-1}{2} \right\rfloor}{0}$$

לפי [Tuck84, עמוד 207] נקבל כי

$$|c_l^{(m)}| \le \binom{\left\lfloor \frac{n-l+m-1}{2} \right\rfloor}{\left\lfloor \frac{n-l-m-1}{2} \right\rfloor} \le \binom{\left\lfloor \frac{n-l+m}{2} \right\rfloor}{\left\lfloor \frac{n-l-m}{2} \right\rfloor}$$

וזה משלים את ההוכחה האינדוקציה.

כעת נרשום

$$C^{(d)}(z) = (z-1)^k A^{(d)}(z) \qquad (3.14)$$

ונציב $z = j = \sqrt{-1}$

בעת נניח עוד הנחת שלילה אחת: נניח כי $A^{(d)}(j) \ne 0$. אזי $\left|A^{(d)}(j)\right| \ge 1$ מאחר ו $A^{(d)}(j)$ הוא פולינום עם מקדמים שלמים. ניקח ערך מוחלט משני הצדדים של שוויון (3.14) ונקבל

$$2^{k/2} \le |A^{(d)}(j)|\sqrt{2^k} = |C^{(d)}(j)| = \sqrt{|\mathrm{Re}(C^{(d)}(j))|^2 + |\mathrm{Im}(C^{(d)}(j))|^2}$$

כמו כן

$$|\mathrm{Im}(C^{(d)}(j))| \le \sum_{l=1}^{\left\lceil \frac{n-d}{2} \right\rceil} |c_{2l-1}^{(d)}|$$

לכן ניתן לרשום

$$|\mathrm{Im}(C^{(d)}(j))| \le \sum_{l=1}^{\left\lceil \frac{n-d}{4} \right\rceil} |c_{2l-1}^{(d)}| + \sum_{l=\left\lceil \frac{n-d}{4} \right\rceil+1}^{\left\lceil \frac{n-d}{2} \right\rceil} |c_{2l-1}^{(d)}|$$

ע"י שימוש בהנחת האינדוקציה נקבל

$$|\mathrm{Im}(C^{(d)}(j))| \le \sum_{l=1}^{\left\lceil \frac{n-d}{4} \right\rceil} \binom{d+\left\lceil \frac{2l-1}{2} \right\rceil - 1}{\left\lceil \frac{2l-1}{2} \right\rceil - 1} + \sum_{l=\left\lceil \frac{n-d}{4} \right\rceil+1}^{\left\lceil \frac{n-d}{2} \right\rceil} \binom{\left\lfloor \frac{n-2l+d+1}{2} \right\rfloor}{\left\lfloor \frac{n-2l-d+1}{2} \right\rfloor} =$$

$$= \sum_{l=1}^{\left\lceil \frac{n-d}{4} \right\rceil} \binom{d+l-1}{l-1} + \sum_{l=\left\lceil \frac{n-d}{4} \right\rceil+1}^{\left\lceil \frac{n-d}{2} \right\rceil} \binom{\left\lfloor \frac{n+d+1}{2} \right\rfloor - l}{\left\lfloor \frac{n-d+1}{2} \right\rfloor - l} \qquad (3.15)$$

מאחר שמתקיים $\left\lceil \frac{n-d}{2} \right\rceil = \left\lfloor \frac{n-d+1}{2} \right\rfloor$ ע"י שימוש ב-[Tuck84, עמוד 207]
האי-שוויון (3.15) הופך להיות

$$\binom{\left\lceil \frac{n-d}{4} \right\rceil + d}{\left\lceil \frac{n-d}{4} \right\rceil - 1} + \binom{\left\lceil \frac{n+d}{2} \right\rceil - \left\lceil \frac{n-d}{4} \right\rceil}{\left\lceil \frac{n-d}{2} \right\rceil - \left\lceil \frac{n-d}{4} \right\rceil - 1} \qquad (3.16)$$

לכל מספר שלם x מתקיים $\left\lceil \frac{x}{2} \right\rceil - \left\lceil \frac{x}{4} \right\rceil = \left\lceil \frac{x-2}{4} \right\rceil$; אכן קל לבדוק את זה ע"י בדיקה
של ארבע האפשרויות לשארית החלוקה של x ב-4. לפיכך מ (3.16) נקבל

$$\binom{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1} + \binom{\left\lceil \frac{n+3d-2}{4} \right\rceil}{\left\lceil \frac{n-d-2}{4} \right\rceil - 1} \le 2\binom{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1}$$

ניתן לסכם את החישובים ע"י

$$\left|\mathrm{Im}(C^{(d)}(j))\right| \le 2\binom{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1}$$

אי-שוויון זהה לאי-שוויון האחרון מתקיים גם עבור $\left|\mathrm{Re}(C^{(d)}(j))\right|$. ולכן

$$2^{k/2} \le \sqrt{|\mathrm{Re}(C^{(d)}(j))|^2 + |\mathrm{Im}(C^{(d)}(j))|^2} \le 2\sqrt{2}\binom{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1} \qquad (3.17)$$

מצד שני לפי הנתון מתקיים

$$k > 3 + 2\log_2\left(\frac{\left\lceil \frac{n+3t}{4} \right\rceil}{\left\lceil \frac{n-t}{4} \right\rceil - 1}\right)$$

מאחר והנחנו בשלילה כי $d \le t$, חייב להתקיים

$$k > 3 + 2\log_2\left(\frac{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1}\right)$$

ניתן לרשום את התנאי האחרון בתור

$$2^{k/2} > 2\sqrt{2}\left(\frac{\left\lceil \frac{n+3d}{4} \right\rceil}{\left\lceil \frac{n-d}{4} \right\rceil - 1}\right) \qquad (3.18)$$

וזה מהווה סתירה ל-(3.17). הסתירה נובעת מההנחה השגויה כי j אינו שורש של $A^{(d)}(z)$. לכן $A^{(d)}(j) = C^{(d)}(j) = 0$ וכמו כן גם $C^{(d)}(-j) = 0$. מסקנה: הפולינום $z^2 + 1$ מחלק את הפולינום $C^{(d)}(z)$. המסקנה האחרונה סותרת את הגדרת d שהוגדר כריבוי של הפולינום $z^2 + 1$ בפירוק של הפולינום $C(z)$ מעל הממשיים. הסתירה הזאת נובעת מההנחה כי $d \le t$. לכן הפולינום $C(z)$ מתחלק בפולינום $(z^2 + 1)^{t+1}$. בזה השלמנו את הוכחת למה 3.2.

כעת ניזכר בתוצאה של רוט, סיגל וורדי [RSV94], שהראו שאם הפולינום $C(z)$ מתחלק מעל השדה GF(2) בפולינום $z + 1$ מספר t של פעמים אז אורך של המילה C מתחלק ב- $2^{\lfloor \log_2 t \rfloor + 1}$. נגדיר $\lambda(k,n)$ להיות השלם הקטן ביותר המקיים

$$k \le 1 + \log_2\left(\frac{\left\lceil \frac{n+\lambda(k,n)}{2} \right\rceil}{\left\lceil \frac{n-\lambda(k,n)-2}{2} \right\rceil}\right)$$

ובאופו דומה נגדיר $\mu(k,n)$ להיות השלם הקטן ביותר המקיים

$$k \le 3 + 2\log_2\left(\frac{\left\lceil \frac{n+3\mu(k,n)}{4} \right\rceil}{\left\lceil \frac{n-\mu(k,n)-4}{4} \right\rceil}\right)$$

<u>**משפט 3.3**</u> אם C היא מילה באורך n בעלת אפס ספקטראלי מסדר k אזי n מתחלק ב $M = 2^{\lfloor \log_2(k+\lambda(k,n)+2\mu(k,n)) \rfloor + 1}$.

<u>**הוכחה**</u> עבור מילה בעלת אפס ספקטראלי מסדר k הפולינום המיצג שלה מתחלק בפולינום $(z - 1)^k$. לפי למה 3.1 הפולינום המיצג מתחלק בפולינום $(z+1)^{\lambda(k,n)}$. לפי למה 3.2 הפולינום המיצג מתחלק בפולינום $(z^2+1)^{\mu(k,n)}$.

מעל GF(2) החלוקות האלה מתורגמות לחלוקה בפולינום $(z+1)^{k+\lambda(k,n)+2\mu(k,n)}$. על סמך נימוקים שהוצגו ב-[RSV94] נסיק כי n מתחלק ב $M = 2^{\lfloor \log_2 (k+\lambda(k,n)+2\mu(k,n)) \rfloor + 1}$. מש"ל.

3.3 חסם תחתון על אורך מינימלי של מילה בעלת אפס ספקטראלי

בהנתן מילה $\underline{w}$ בעלת אפס ספקטראלי מסדר k נגדיר p באופן הבא:

(3.19) p הוא המספר הראשוני הגדול ביותר המקיים $p \le k$.

נתבונן במטריצה $H(n,k;-1)$ המוגדרת ע"י (1.3). ההצגה של p השורות הראשונות שלה מעל שדה GF(p) היא כדלקמן

$$H(n,k;-1) = [V|V|V|\ldots|V|V']$$

כאשר המטריצה הריבועית V נתונה ע"י

$$V = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 1 & 2 & \ldots & p-2 & p-1 \\ 0^2 & 1^2 & 2^2 & \ldots & (p-2)^2 & (p-1)^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0^{p-1} & 1^{p-1} & 2^{p-1} & \ldots & (p-2)^{p-1} & (p-1)^{p-1} \end{pmatrix}$$

והמטריצה V' מורכבת מ $n \bmod p$ העמודות הראשונות של V. שים לב כי המטריצה V היא מטריצת ואנדרמונד (Vandermonde matrix). לכן היא הפיכה בשדה GF(p) וקיימת מטריצה הפוכה לה שנסמנה ב V^{-1}. אם נכפיל בשדה GF(p) את $H(n,k;-1)$ משמאל ב V^{-1}, נקבל את הזהות הבאה:

$$G(p) \equiv [I|I|I|\ldots|I|I'] = V^{-1}H(n,k;-1) \bmod p \qquad (3.20)$$

כאשר I היא מטריצת הזהות בעלת p שורות ו p עמודות ו I' היא המטריצה שמורכבת מ $n \bmod p$ העמודות הראשונות של I.

הלמה הבאה נובעת באופן ישיר מתוך (3.20).

<u>**למה 3.4**</u> לכל מילה $\underline{w}$ בעלת אפס ספקטראלי מסדר k ולכל מספר ראשוני p, $p \le k$, מתקיים

$$G(p)\underline{w} = \underline{0} \bmod p .$$

<u>**סימון**</u> נסמן ע"י $|\underline{w}|$ את האורך של המילה $\underline{w}$.

למה 3.5 אם המילה $\underline{w}$ היא בעלת אפס ספקטראלי מסדר $k > 2$ אזי $|\underline{w}| > p(p\text{-}1)$ כאשר p מוגדר ע"י (3.19).

הוכחה בדרך השלילה. נניח ש-$\underline{w}$ היא מילה אשר אורכה קטן או שווה ל-$p(p\text{-}1)$. קודם נראה כי $|\underline{w}|$ הוא כפולה של p. על סמך למה 3.4 לכל ערך r בתחום $0 \le r \le p\text{-}1$ המכפלה של השורה ה-r- של המטריצה $G(p)$ בוקטור $\underline{w}$ היא

$$(G(p)\underline{w})_r = \sum_{i=0}^{\left\lfloor \frac{n-r}{p} \right\rfloor} w_{r+pi} = 0 \bmod p \qquad (3.21)$$

אם האורך של $\underline{w}$ אינו כפולה של p אז ניתן לבחור מספר שורה r, כך שבסכום שבנוסחה (3.21) יופיע מספר אי-זוגי של איברים, כאשר כל איבר הוא 1 או 1-. לכן הסכום הזה יהיה שווה למספר אי-זוגי שנמצא בתחום בין $-p + 1$ לבין $p - 1$. ואז הוא לא יכול להיות $0 \bmod p$ בסתירה ל-(3.21). ולכן $|\underline{w}|$ היא כפולה של p.

מחד גיסא הסקנו כי $|\underline{w}|$ הוא כפולה של p. מאידך גיסא ב-[RSV94] הוכח כי $|\underline{w}|$ מתחלק במספר $m = 2^{\lfloor \log_2 k \rfloor + 1}$. באופן ברור $k \le m$. בנוסף p ו-m הם מספרים זרים אחד לשני כי p ראשוני גודל מ-2 ו m הוא חזקה של 2. לכן האורך של $\underline{w}$ הוא כפולה של mp, כאשר $mp > kp > (p\text{-}1)p$, וזה בסתירה להנחה כי $|\underline{w}| < (p\text{-}1)p + 1$. מש"ל.

3.4 חסם עליון על אורך מינימלי

כפי שהוכח ב-[RSV94] לכל מספר טבעי k קיימת מילה בעלת אפס ספקטראלי מסדר k בעלת אורך 2^k אשר מורכבת מ-2^k סיביות ראשונות של סדרת מורס (השם הלועזי הוא Morse sequence). ע"י חיפוש באמצעות המחשב נקבע כי עבור $k \le 5$ המילה שמתקבלת מסדרת מורס היא הקצרה ביותר בין כל המילים מאותו הסדר [RSV94]. השאלה האם קיימות מילים יותר קצרות מהמילים המתקבלות מתוך סדרת מורס עבור $k>5$ נשארה פתוחה ב-[RSV94].

התנאי (3.21) מכתיב אילוץ לכל r על ערכי הסיביות המופיעות במקומות r, $r+p$, ..., $r + \left\lfloor \frac{n-r}{p} \right\rfloor p$: סכום של הסיביות האלה חייב להתחלק ב p. השימוש בתכונה הזאת מאפשר להקטין בצורה משמעותית את מספר החישובים הדרושים לבדיקה של כל "המועמדים" להיות המילים הקצרות ביותר עבור סדרים שונים. הוא גם מאפשר לחשב את היתירות של הצפנים $S(n,k)$ עבור זוגות (n,k) אשר עבורם לא ניתן היה לעשות חישוב כזה קודם בגלל סיבוכיות גדולה מדי של החישובים.

מתוצאות החיפוש מתברר שקיימת מילה בעלת אפס ספקטראלי מסדר 6 אשר אורכה הוא 48. סה"כ קיימות שתי מילים כאלו: מילה שמובאת בהמשך וההיפוך שלה. המילה הזאת, נסמן אותה $\underline{w}_{\min}$, היא סימטרית והיא מופיעה להלן:

```
++−−  −−+−  −+++  ++−+  +−−−  ++−−
−−++  −−−+  +−++  +++−  −+−−  −−++
```

כאשר '+' מופיע במקום 1+ ו-'−' מופיע במקום 1-. בעזרתה ניתן ליצר מילה בעלת אפס ספקטראלי מסדר $6+i$ בעלת אורך $48\cdot 2^i$ לכל $i \geq 0$. המילה המבוקשת מסדר $6+i$ תיוצג ע"י הפולינום המייצג

$$P(z) = P_{\min}(z)(z^{48}-1)(z^{2\cdot 48}-1)\cdots(z^{i\cdot 48}-1)$$

כאשר $P_{\min}(z)$ הוא הפולינום המיצג של $\underline{w}_{\min}$. להוכחה ניתן לפנות אל הספרות, למשל [RSV94, למה 2.5].

מקרה מעניין אחר הוא $(n,k) = (40,5)$. גם לצופן הזה שייכות רק שתי מילים כאשר אחת היא היפוך של השניה. שתי המילים האלה הן סימטריות ואחת מביניהן היא

−−++ +++− −−−+ −−++ −++−
+−−+ −−++ −+++ +−−− −−++

ניתן להשתמש באילוץ של השוויון (3.21) גם לחישוב את ערכי היתירות של הצפנים $S(n,k)$ עבור זוגות (n,k) שטרם חושבו. התוצאות מופיעות בטבלה 3.1. סימן '-' בכניסת הטבלה מציין שהקבוצה $S(n,k)$ מתאימה ריקה. סימן שאלה מציין שלא הצלחנו לחשב את היתירות לאותו הצופן $S(n,k)$.

עבור $k = 7$ לא קיימות מילים ספקטראליות באורך עד 64. האורך "החשוד" הבא הוא 80. לא ידוע אם קיימות מילים ספקטראליות באורך זה, אם כי בדקנו ומצאנו שמילים סימטריות/אנטיסימטריות באורך זה לא קיימות.

טבלה 3.1 **Table 3.1**

ערכי יתירות **Redundancy values**

	n					
k	36	40	44	48	52	56
1	2.92	3.00	3.06	3.13	3.18	3.24
2	9.25	9.55	9.82	10.07	?	?
3	17.92	18.41	19.18	?	?	?
4	-	27.89	-	?	?	?
5	-	39	-	40.33	-	47.24
6	-	-	-	47	-	-

3.5 על שינויי סימן

בפרק זה נפעיל את למה 3.4 לצורך חקר מספר שינויי הסימן במילה בעלת אפס ספקטראלי. עבור המילה הנתונה

$$\underline{w} = (w_1, w_2, \ldots, w_n) \in S(n,k)$$

נגדיר מילה $\underline{u}$ באמצעות הפולינום

$$P_u(z) = P_w(z)(z-1)$$

כאשר $P_w(z)$ הוא הפולינום המייצג של $\underline{w}$. הפולינום $P_u(z)$ מתחלק בפולינום $(z-1)^{k+1}$. נסמן את הרכיבים של $\underline{u}$ ע"י

$$\underline{u} = (u_1, u_2, \ldots, u_n, u_{n+1})$$

כאשר

$$u_1, u_{n+1} \in F,\ u_i \in \{-2, 0, 2\}$$

עבור $i = 2, \ldots, n$.

יש לנו אינדיקציה טובה האם במקום ה-i בתוך המילה $\underline{w}$ המקורית היה שינוי הסימן. זה יקרה אם ורק אם $u_i \in \{-2, 2\}$. במקרה שב-$\underline{w}$ לא היה שינוי הסימן במקום ה-i נקבל כי $u_i = 0$.

נגדיר את p באופן הבא:

p הוא הראשוני הגדול ביותר אשר מקיים $p \le k+1$. (3.22)

מאחר ו-$\underline{u}$ היא מילה בעלת אפס ספקטראלי מסדר $k + 1$ (מעל השלמים), מתקיים

$$\left(\begin{array}{ccc|ccc|c|ccc}1 & & & 1 & & & \ldots & 1 & & 1\\ & 1 & & & 1 & & \ldots & & 1 & & 1\\ & & \ddots & & & \ddots & \ldots & & & \ddots\\ & & 1 & & & 1 & \ldots & & & 1\end{array}\right)\begin{pmatrix}u_1\\u_2\\ \vdots\\u_{n+1}\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}\bmod p \quad (3.23)$$

כאשר כל הבלוקים במטריצה פרט לאחרון הם בעלי סדר $p\times p$.

אם n איננו כפולה של p, האחדים של העמודה הראשונה ושל העמודה האחרונה מופיעים בשורות שונות. מכיוון שמבצעים את כל הפעולות מודולו p, הכפלה של כל שורת המטריצה בוקטור $\underline{u}$ נותנת 0 מודולו p. אבל הכפלה של השורה הראשונה ב-$\underline{u}$ נותנת מספר אי-זוגי כי $u_1 \in F$. המספר הזה מתחלק ב-p. לכן האחדים בשורה הראשונה של המטריצה הוכפלו בלפחות $(p-1)/2$ רכיבי 2 ו-2- של הוקטור $\underline{u}$. אותו נימוק נכון גם לגבי השורה שמכילה את האחד האחרון. מכאן נסיק כי בוקטור $\underline{u}$ ישנם לפחות p-1 רכיבים ששווים ל-2 או ל 2- ולכן מילה בעלת אפס ספקטראלי מסדר k מכילה לפחות p-1 שינויי סימן.

עבור מקרים כאשר $p = k + 1$, אנחנו חוזרים על התוצאה של [RSV94] האומרת כי למילה בעלת אפס ספקטראלי מסדר k יש לפחות k שינויי סימן. אבל התוצאה שלנו היא חזקה יותר במובן מסוים, כי אנחנו מציינים שתי תת-קבוצות של האינדקסים "החשודים" בהם ורק בהם יכולים שינויי הסימן האלה להופיע.

הגישה הזאת ניתנת להרחבה ע"י שימוש ביותר ממספר ראשוני אחד. למשל, אם ניקח שני מספרים ראשונים r_1 ו-r_2 הקטנים או שווים ל k+1, ונעריך את המספר המכסימלי של החיתוכים בין הקבוצה של המקומות "החשודים" עבור r_1 לבין הקבוצה של המקומות "החשודים" עבור r_2 , נוכל להגיע לביטוי החוסם מלמטה את מספר שינויי הסימן במילה:

$$(r_1-1)+(r_2-1)-2\left\lceil\frac{n-1}{r_1r_2}\right\rceil-2\left\lfloor\frac{n-1}{r_1r_2}\right\rfloor \qquad (3.24).$$

שני המחוברים האחרונים מבטאים את מספר החיתוכים בין הקבוצות של האינדקסים "החשודים". הקבוצות האלה הן

$$\{u_{1+r_1}, u_{1+2r_1}, u_{1+3r_1}, \ldots; u_{n+1-r_1}, u_{n+1-2r_1}, u_{n+1-3r_1}, \ldots\}$$
$$\{u_{1+r_2}, u_{1+2r_2}, u_{1+3r_2}, \ldots; u_{n+1-r_2}, u_{n+1-2r_2}, u_{n+1-3r_2}, \ldots\}$$

החסם (3.24) יכול להוות שיפור של התוצאה המיוצגת ב-[RSV94] עבור המילים שאורכן n מקיים $n < k^3$. אנחנו לא יודעים אם מילים כל כך קצרות קיימות.

את הגישה הזאת ניתן להרחיב ליותר משני מספרים ראשוניים.

3.6 חסם תחתון על יתירות

חסם תחתון של $O(k \log n)$ על יתירות הצופן $S(n,k)$ הוצג ב-[RSV94]. אבל התוצאה הזאת התבססה על תוצאה מורכבת מתורת המספרים. להלן נציג הוכחה אחרת יותר פשוטה לאותה התוצאה.

הלמה הבאה היא פשוטה להבנה ואינה דורשת הוכחה.

<u>למה 3.6</u> נתונה סדרה של מספרים $\{a_i\}_{i=0}^{m}$, כאשר $|a_{i+1}| \geq 2\,|a_i|$ עבור $i = 0, ..., m\text{-}1$. אם קיים מספר h המיוצג ע״י

$$h = \sum_{i=0}^{m} c_i a_i\,, \quad c_i \in F$$

אזי ההצגה הזאת היא יחידה.

<u>משפט 3.7</u> היתירות של קבוצת כל המילים מעל F^n אשר המומנט ה-k שלהם שווה לאפס היא $\Theta(k \log n)$.

<u>הוכחה</u>

נקבע אינדקסים ע״י האלגוריתם הבא:

- $a_0 = b_0 = 1$, $i = 0$
- כל עוד $b_i \cdot 2^{1/(k-1)} < n/2$ חזור:

  $i = i + 1$

  $b_i = \lceil 2^{1/(k-1)} b_{i-1} \rceil$

  $a_i = b_i^{(k-1)}$
- סוף

כתוצאה מהרצה של האלגוריתם הזה נקבל קבוצת האינדקסים $\{b_0, b_1, ..., b_m\}$ המייצגים את הערכים $\{a_0, a_1, ..., a_m\}$ כאשר $2a_i \leq a_{i+1}$. לפיכך ערכי a_i מקיימים את כל הדרישות של למה 3.6 ביחס לכל ערך h של המומנט ה-k. אזי לכל h קיימת הצבה יחידה של ערכים לסיביות שהאינדקסים שלהם ניתנים ע״י הקבוצה $\{b_0, b_1, ..., b_m\}$. בקבוצה הזאת מופיעים m+1 אינדקסים ולכן היתירות של אוסף מילים בעלות המומנט ה-k השווה ל-0 היא m+1 לפחות.

מכיוון שקיים קבוע c כך שלכל n מתקיים

$$b_m \geq c \cdot 2^{m/(k-1)} \geq n/4$$

נובע כי $m = \Theta(k \log n)$ וזה החסם התחתון על היתירות של $S(n,k)$. מש״ל.

4 מחקר עתידי

בתחום של צופנים בעלי אפסים ספקטראליים קיים מספר רב של בעיות פתוחות בעלות חשיבות מעשית רבה. בפרק הנוכחי נתאר מקצת הבעיות האלה אשר בדרך כלל קשורות לבעיות שנותחו בפרקים הקודמים של החיבור.

<u>אורך</u>

בעבודה הנוכחית היצגנו חסם תחתון וחסם עליון חדשים על האורך המינימלי של מילה בעלת אפס ספקטראלי מסדר k. החסם העליון הוא $48\cdot 2^{k-6}$ סיביות עבור מילה מסדר $k > 5$. לא ידוע אם החסם הזה הדוק עבור סדרים $k > 6$. מאידך הצגנו הוכחה שהאורך מתנהג כ $\Omega(k^2)$. ניתן לראות שקיים פער רחב בין החסם התחתון לחסם העליון. הבעיה של מציאת החסמים ההדוקים יותר על אורך המילה המינימלית נשארת פתוחה בשלב זה.

<u>שינויי סימן</u>

חסם תחתון על מספר שינויי סימן במילה בעלת אפס ספקטראלי מסדר k שהוצג ב-[KS91] שווה ל-k. מאידך ב-[RSV94] הוכח שהחסם הזה הדוק עבור k=1 ו k=2 והוא לא הדוק עבור k=3. ככל הנראה החסם הזה אינו הדוק גם לסדרים k גבוהים יותר. מציאת חסמים יותר טובים על מספר שינויי סימן במילה היא שאלה פתוחה.

<u>יתירות</u>

החסמים התחתון והעליון על יתירות של $S(n,k)$ הטובים ביותר שידועים הם מתוך [RSV94]:

$$\rho(S(n,k)) \geq (k-1)(\log_2(n) - \log_2(k-1)) = O(k\log n)$$
$$\rho(S(n,k)) \leq O((2^k - 1)(\log_2(n) - k + 1)) = O(2^k \log n)$$

לפיכך קיים פער רחב בין החסם התחתון לחסם העליון. מציאה של חסמים יותר הדוקים על יתירות של $S(n,k)$ היא שאלה נוספת שעדיין לא נמצא לה פתרון.

<u>אלגוריתמים להצפנה</u>

בכדי שניתן יהיה להשתמש בצופנים בעלי אפסים ספקטראליים מסדר גבוה במערכות אמיתיות לאיחסון נתונים קיים צורך בפיתוח אלגוריתמים יעילים להצפנה ופיענוח. על האלגוריתמים האלה להיות בעלי סיבוכיות חישוב קטנה (פולינומיאלית באורך הקלט) ולייצר צופנים בעלי יתירות קטנה ככל האפשר (בדרך כלל נרצה יתירות לוגריתמית באורך הקלט). אלגוריתמים שמקיימים את שתי דרישות היעילות האלה ידועים רק עבור k=1,2,3 כאשר האלגוריתם עבור k=3 הוצג בעבודה הנוכחית. פיתוח של אלגוריתמים יעילים לסדרים מסוימים עם k>3 ואולי לסדר כללי מהווה אתגר בעל חשיבות מעשית. מחקר עתידי בנושא של צפנים בעלי אפסים ספקראליים יכול להתמקד גם בנושא זה.

References

[AlB90] S. Al-Bassam, B. Bose, *On balanced codes, IEEE Trans. Inform. Theory*, IT-36 (1990), 406-408.

[AlB94] S. Al-Bassam, B. Bose, *Design of efficient balanced codes, IEEE Trans. Comput.*, C-43 (1994), 362-365.

[ABCO88] N. Alon, E. E. Bergmann, D. Coppersmith, A. M. Odlyzko, *Balancing sets of vectors, IEEE Trans. Inform. Theory*, IT-34 (1988), 128-130.

[Bose91] B. Bose, *On unordered codes, IEEE Trans. Comput.*, C- 40 (1991), 125-131.

[Etz90] T. Etzion, *Constructions of error-correcting DC-free block codes, IEEE Trans. Inform. Theory*, IT-36 (1990), 899-905.

[Imm91] K. A. S. Immink, *Coding Techniques for Digital Recorders,* Prentice Hall, New York, 1991.

[ImmB87] K. A. S. Immink, G. Beenker, *Binary transmission codes with higher order spectral zeros at zero frequency, IEEE Trans. Inform. Theory*, IT-33 (1987), 452-454.

[KS91] R. Karabed, P. H. Siegel, *Matched spectral-null codes for partial-response channels, IEEE Trans. Inform. Theory*, IT-37 (1991), 818-855.

[Knu86] D. E. Knuth, *Efficient balanced codes, IEEE Trans. Inform. Theory*, IT-32 (1986), 51-53.

[MS77] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[MRS94] B. H. Marcus, R. M. Roth, P. H. Siegel, *Constrained systems and coding for recording channels,* to appear in *Handbook of Coding Theory,* W. C. Huffman, V. Pless, R. A. Brualdi (Eds.), Elsevier Science Publishers, Amsterdam.

[MSW92] B. H. Marcus, P. H. Siegel, J. K. Wolf, *Finite-state modulation codes for data storage, IEEE J. Sel. Areas Comm.*, 10 (1992), 5-37.

[MPi89] C. M. Monti, G. L. Pierobon, *Codes with a multiple spectral null at zero frequency, IEEE Trans. Inform. Theory*, IT-35 (1989), 463-472.

[Pohl92] K. C. Pohlmann, *The Compact Disc Handbook,* Second Edition, Madison, Wisconsin, 1992.

[RSV94] R. M. Roth, P. H. Siegel, A. Vardy, *High-order spectral-null codes: Constructions and bounds, IEEE Trans. Inform. Theory*, IT-40 (1994), 1826-1840.

[Roth93] R. M. Roth, *Spectral-null codes and null spaces of Hadamard submatrices, Design, Codes, and Cryptography,* 9 (1996), 177-191.

[SER97] V. SKACHEK, T. ETZION, R. M. ROTH, *Efficient encoding algorithm for third-order spectral-null codes*, to appear in *IEEE Trans. Inform. Theory,* March 1998, see also *Proc. IEEE Information Theory Workshop*, July 1997, p.33-34, Longyearbyen, Norway.

[TAlB95] L. G. TALLINI, S. AL-BASSAM, B. BOSE, *On efficient high-order spectral-null codes, Proceedings of IEEE International Symposium On Information Theory,* Sept. 1995, p.144, Whistler, BC, Canada.

[TCB96] L. G. TALLINI, R. M. CAPOCELLI, B. BOSE, *Design of some new efficient balanced codes, IEEE Trans. Inform. Theory*, IT-42 (1996), 790-802.

[Tuck84] A. TUCKER, *Applied Combinatorics*, Second Edition, John Wiley & Sons, 1984.

CODING FOR SPECTRAL-NULL CONSTRAINTS

VITALY SKACHEK

CODING FOR SPECTRAL-NULL CONSTRAINTS

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Computer Science

VITALY SKACHEK

Submitted to the Senate of the Technion - Israel Institute of Technology
Heshvan, 5758 Haifa November, 1997

THE WORK DESCRIBED HEREIN
WAS SUPERVISED BY PROF. TUVI ETZION AND PROF. RON M. ROTH
UNDER THE AUSPICES OF THE FACULTY OF COMPUTER SCIENCE

ACKNOWLEDGMENT

I would like to thank Prof. Tuvi Etzion and Prof. Ron M. Roth for the supervising, and for the help all along.

The generous financial help of Technion is gratefully acknowledged.

ABSTRACT

In this work, we investigate the family of codes known as spectral-null codes. These codes are defined over the alphabet $F = \{-1,+1\}$. For each word $\underline{x} = (x_1, x_2, ..., x_n)$ over F, we shall define a so-called z-polynomial in the indeterminate z,

$$X(z) = x_1 z + x_2 z + ... + x_n z^n.$$

If the z-polynomial of word $\underline{x}$ is divisible by $(z\text{-}1)^k$, $\underline{x}$ is said to have a kth order spectral null. The set of all kth order spectral-null words of length n over F will be denoted by $S(n,k)$. Any subset C of $S(n,k)$ will be called a spectral-null code of length n and order k. Spectral-null codes can be used as block codes since the concatenation of any l codewords of C is a word in $S(ln,k)$. The value $\rho(C) = n - \log_2|C|$ is called the redundancy of the code C and it reflects the increase in length of the data when a message is coded using the code C.

In the first part of the work, we deal with the problem of efficient encoding and decoding of third-order spectral-null codes. We present an efficient algorithm for encoding an arbitrary information sequence of length n into a third-order spectral-null code. The algorithm uses a recursion and consists of five basic stages. The redundancy of the code produced by the algorithm is $9 \log_2 n + O(\log \log n)$. The computational complexity of the algorithm is $O(n)$ integer additions and $O(n \log n)$ counter increments. The memory needed is $O(n)$.

In the second part of the work, we investigate different properties of spectral-null codes. In particular, we improve both the lower and upper bounds on the minimal length of kth order spectral-null words. We compute the redundancy of sets $S(n,k)$ for some values of n and k. We show a new divisibility condition on the length n of kth order spectral-null words. We also present a new lower bound on the number of sign changes in kth order spectral-null words.