ניתוח ביצועים של קודי LDPC לתיקון שגיאות

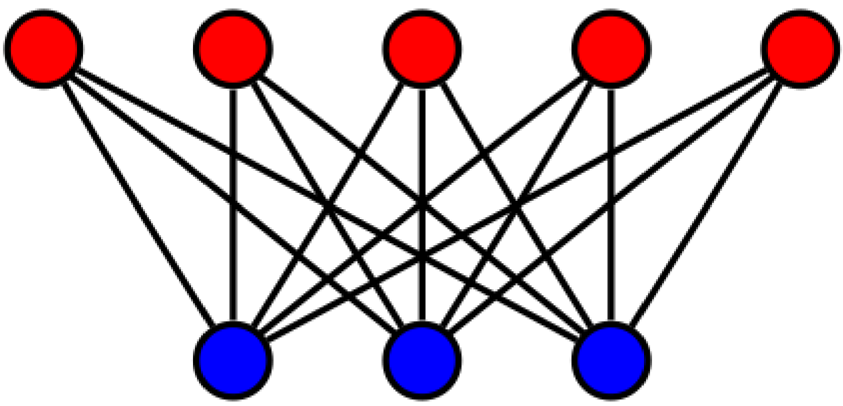
נועם שילוני — Noam Shilony

דור קליינשטרן — Dore Kleinstern

מנחה: רמי כהן — Rami Cohen

סמסטר רישום: חורף תשע"ט

תאריך הגשה: אוגוסט, 2019



תקציר

התקני אחסון מודרניים מבוססי טכנולוגיית Flash מאפשרים אחסון אמין בצפיפות גבוהה יחד עם ביצועי קריאה/כתיבה טובים. בפרוייקט זה נעסוק במודל q-ary bit measurement channel (QBMC) עבור התקני Flash. במודל זה מידע מיוצג באמצעות רמות מתח/זרם המקודדות סיביות. אובדן מידע מתרחש כאשר במהלך קריאת המידע רמת המתח/זרם אינה ידועה במדויק. קודי Low Density Parity Check (LDPC) הם קודים המאפשרים הן ביצועים נאותים והן יכולת פענוח מהירה באמצעות אלגוריתם איטרטיבי שנקרא "belief propagation". בפרויקט זה בחנו את הביצועים של הקודים הללו במודל הנתון, בצורה אמפירית, אנליטית ואנליטית-מקורבת עבור פרמטרים שונים.

Abstract

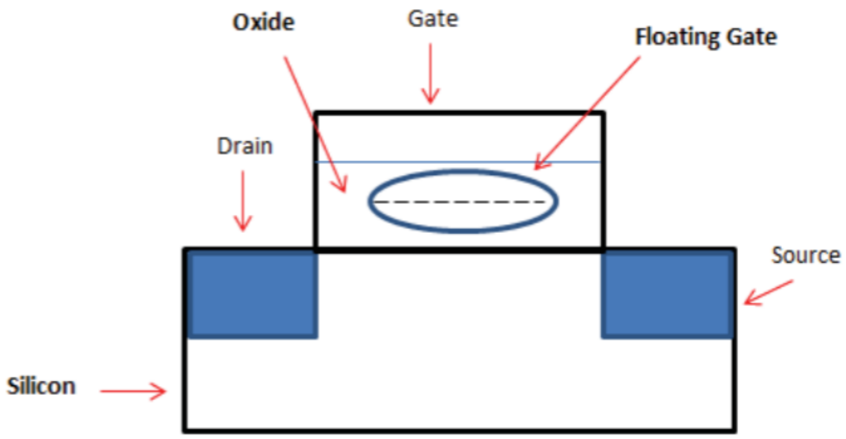
Modern storage devices based on flash technology allow reliable storage along with decent read/write performance. In our project we work with the q-ary bit measurement channel (QBMC) model for flash devices. In this model information is stored in a form of voltage/current levels encoded to bits. An erasure occurs when during the reading process the voltage/current level isn't completely known. Low Density Parity Check (LDPC) codes are known for their reliability and their capability of fast decoding using iterative algorithm called "belief propagation". In our work we analyzed the performance of these codes in the QBMC model, empirically, analytically, and analytically – approximated.

תוכן עניינים

רשימת גרפים

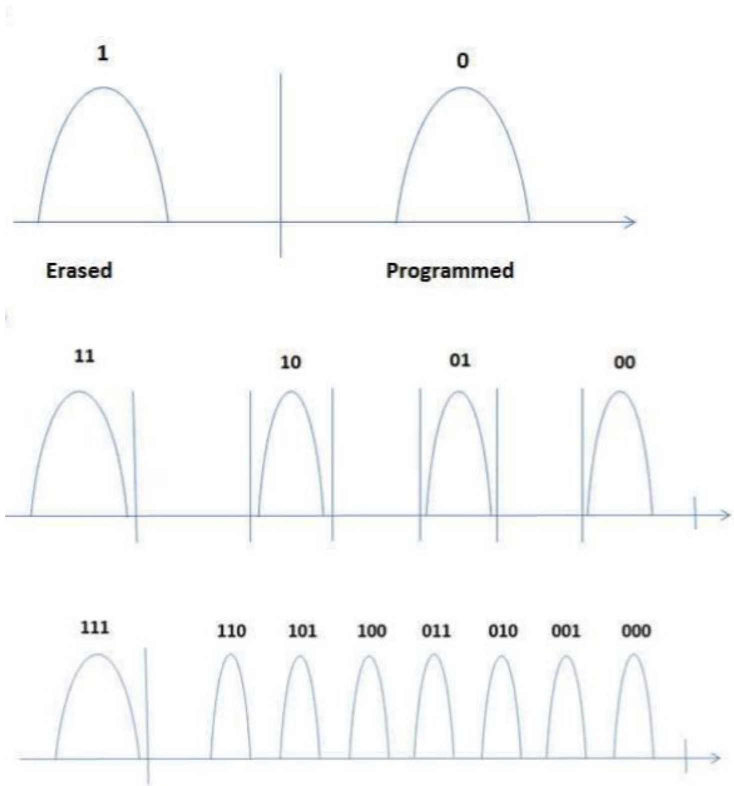
1 מבוא

בשנים האחרונות ההתפתחות המהירה בטכנולוגיות לאחסון זיכרון האיצה את ההכרח בקידוד מהיר ואמין. התקני אחסון מבוססי טכנולוגיית flash צוברים פופולריות רבה יותר בשוק. עם הזמן כונני SSD המשתמשים בטכנולוגיית NAND flash תופסים את מקומם של כונני דיסקים קשיחים (HDD) ששולטים באחסון בגלל מהירויות כתיבה וקריאה גדולות יותר משמעותית, יחד עם צריכת חשמל נמוכה יחסית. התקנים אלו מבוססים על טכנולוגיית Floating Gate (FG) שמורכבת מטרנזיסטורים מסוג MOS או MOSFET. ה-floating gate מבודד משכבת הסיליקון על ידי שכבת מבודד (oxide) ועל ידי אופרטור מתאים מוסיף מטען שנשאר שם עד שמתבצע אופרטור מחיקה. מחיקה בטכנולוגיה זאת מתבצעת על ידי מנהור – FN הדורש הפעלת מתח חיובי גבוה על שער התא ביחס למצע שמושך אלקטרונים ל-floating gate [1].



איור 1 floating gate [1]

במשפחת ה-NAND flash יש סוגים שונים של זיכרון – SLC (Single Level Cell), MLC (Multi-level Cell) ו-TLC (Triple Level Cell). בכל סוג מספר שונה של ביטים המתארים מידע בתא. למשל עבור TLC מאוחסנים 3 ביטים של מידע (000 עבור "מתוכנת לחלוטין" ו-111 עבור "מחוק לחלוטין"). הרמות הללו מתאפשרות באמצעות פילוג מתחי סף לרמות מתאימות כמתואר באיור 2.

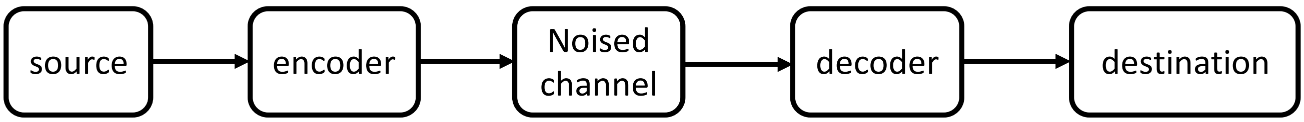


איור 2 פילוג רמות מתח עבור flash משלושה סוגים - SLC, MLC, TLC [1]

2 סקירה ספרותית

2.1 ערוצי תקשורת

המודל הבסיסי של מערכת תקשורת הוא כמתואר באיור 1. ישנו מקור (source) שרוצה לשדר סיביות מידע. המקודד (encoder) מעביר אותם למילת קוד על פי אלגוריתם קידוד נתון. מילה זו עוברת בערוץ הרועש (noised channel) ולאחר מכן עוברת במפענח (decoder) שמשחזר את המילה שנשלחה ומעבירה למוצא (destination).

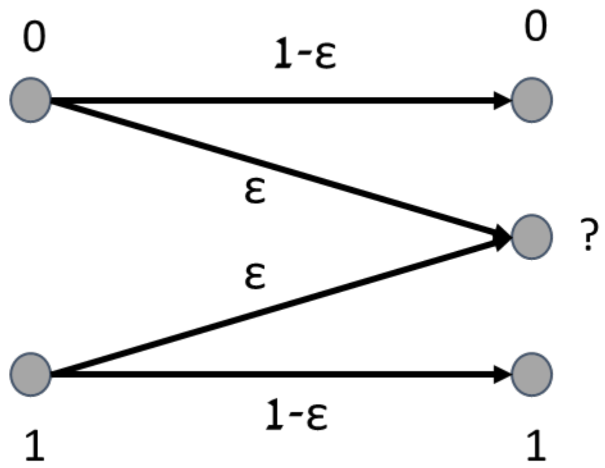


איור 3 מודל בסיסי של ערוץ תקשורת רועש

2.2 ערוץ מחיקה בינארי (BEC)

אחת מהבעיות בהתקני אחסון היא אירועי מחיקה, כאשר מידע שמאוחסן נמחק וידוע שהוא נמחק. המודל הפשוט ביותר לתיאור מחיקה הוא ערוץ המחיקה הבינארי. בערוץ משודרת סיבית 0/1 והמוצא הוא 0/1 בהתאמה אם לא הייתה מחיקה, ו-"?" אם הייתה מחיקה (כאשר מחיקה מתרחשת בהסתברות ε). הסכמה של מודל זה מתוארת באיור 2.

דוגמה למודל היא הסתכלות על מתח בתור דרך לשמור מידע, 0V מתאר את הסיבית 0, ו-5V מתאר את הסיבית 1. אך בעולם האמיתי יש רעשים ואין דבר כזה מתח מדויק של 0 או 5 וולט, לכן לוקחים מרווח בטחון של למשל 1V וכעת כל ערך מתח בין 0 ל 1 יהיה 0, וכל ערך מתח בין 4 ל 5 יהיה 1.



איור 4 סכמת ערוץ מחיקה בינארי

2.3 קודים ליניאריים בינאריים

2.3.1 קודי בלוק ליניאריים

קוד בלוק (n,k) בינארי ליניארי הוא קבוצה של 2^k מילות קוד בינאריות באורך n. קוד ליניארי משמעותו שכל חיבור של שתי מילות קוד הינו מילת קוד.

$$\mathcal{C} = \begin{Bmatrix} (0000000), (1000101), (0100110), (0001111), \\ (0010011), (1100011), (1001010), (1101100), \\ (0110101), (1101100), (0011100), (1110000), \\ (1011001), (1011001), (0111010), (1111111). \end{Bmatrix}$$

איור 5 תיאור קוד בלוקים בינארי עבור (n,k)=(7,4) [7]

מילת קוד ליניארי בינארי x נוצרת על ידי מטריצה יוצרת מעל שדה בינארי $G \in \mathbb{F}_2{}^{n\times k}$ ועל ידי מילת מידע $u \in \mathbb{F}_2^k$ כצירוף של שורות המטריצה היוצרת, $x = G \otimes u$. אוסף מילות הקוד הנוצרות כך $\mathcal{C}$ מהווה קוד ליניארי בינארי. קצב הקוד מוגדר להיות $R = \frac{k}{n}$.

קיבול של ערוץ תקשורת הוא הקצב המרבי בו ניתן לשדר כך שהתקשורת תהיה אמינה. לדוגמה, קיבול הערוץ BEC הוא $C_{BEC} = 1 - \varepsilon$ [2].המטריצה הדואלית $H \in \mathbb{F}_2^{m\times n}$ למטריצה היוצרת G מקיימת $H \otimes G = 0$ ולכל מילת קוד $H \otimes x = 0$. נעסוק בקודים שמימד המטריצה היוצרת שלהם הוא k ולפיכך המטריצה הדואלית הפורשת את המרחב הדואלי לקוד תהיה בעלת ממד $m = n - k$.

2.3.2 קודי LDPC בינאריים

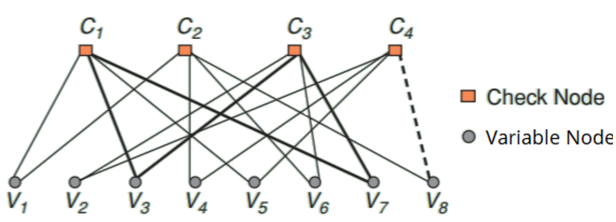
קוד Low Density Parity Check (LDPC) רגולרי מאופיין על ידי שני ערכים d_v, d_c כאשר d_v הוא מספר ה-'1' בכל עמודה במטריצה H ו-d_c הוא מספר ה-'1' בכל שורה במטריצה, כאשר הם קבועים לכל שורה ולכל עמודה.

נגדיר $R_d = 1 - \frac{dv}{dc}$ אזי מתקיים עבור קוד רגולרי $R_d = 1 - \frac{d_v}{d_c} = R = \frac{k}{n}$.

ניתן לתאר קוד על ידי tanner graph המייצג מטריצת בדיקת זוגיות H כמטריצת שכנויות. זהו גרף דו צדדי (bipartite) המורכב מ-n צמתים של משתנים (variable nodes) ו-$m = n - k$ צמתים של בדיקה (check nodes). בגרף תהיה קשת בין variable node ל-check node כאשר יש '1' במקום המתאים במטריצת השכנויות H. לפיכך, לכל variable node ישנן d_v קשתות יוצאות ולכל check node יש d_c קשתות נכנסות.

באיור 4 מתואר tanner graph עבור קוד LDPC לא רגולרי. בחלקו התחתון של האיור אלו ה-variable nodes שמייצגים את n הסימבולים שעוברים ומעליהם נמצאים ה-check nodes המייצגים את m משוואות בדיקת הזוגיות. המשוואות הן בהתאם ל-$H \otimes x = 0$. נקרא לקודי LDPC רגולרים אם עבור כל check node או variable node, מספר הקשתות היוצאות ממנו תהיה זהה ל-d_c ו-d_v בהתאמה.

$$\begin{array}{cc} & \begin{array}{cccccccc} V_1 & V_2 & V_3 & V_4 & V_5 & V_6 & V_7 & V_8 \end{array} \\ \mathbf{H} = & \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{array}{c} C_1 \\ C_2 \\ C_3 \\ C_4 \end{array} \end{array}$$



איור 6 tanner graph עבור קוד LDPC רגולרי עם $(d_v, d_c) = (2,4)$ [9]

2.3.3 אלגוריתם העברת הודעות לפענוח (message passing decoding)

מכיוון שמטריצת H הינה מטריצה דלילה עם ממדים קבועים d_v, d_c שאינם תלויים בגודל הקוד ניתן לקבל מימוש מפענח על ידי אלגוריתם איטרטיבי עם סיבוכיות נמוכה (מספר קטן של הודעות ביחס לאורך הקוד) וביצועים טובים.

אלגוריתם message passing פשוט עבור פענוח בערוץ BEC מתבצע על ידי העברת הודעות איטרטיבית מ-variable nodes ל-check nodes והפוך.

Let x be a word to decode
Initialize $VTC_0(v,c) = x(v)\ \forall v \in V\ and\ c \in Neighbour(v)$
Init $i = 1$
While $VTC_i \neq VTC_{i-1}$

- $CTV_{i-1}(c,v) = XOR\ of\ all\ VTC_{i-1}(v',c)\ for\ v' \in N(c)\backslash v\ if\ none\ of\ them\ is\ erasure$
- $VTC_i(v,c) = Intersection\ of\ all\ CTV_{i-1}(c',v)\ for\ c' \in N(v), erasure\ if\ all\ erasure$

End
Decoded word = VTC_{final}

אלגוריתם 1 Message Passing עבור קודי LDPC בערוץ BEC

2.3.4 Density evolution (DE) וסף פענוח (decoding threshold)

אחד ממדדי הטיב של תהליך הפיענוח של קוד מסוים הוא תחום הפרמטרים בערוץ עבורם המפענח יכול לשחזר את המילה בהסתברות גבוהה. עבור ערוץ BEC פשוט עם הסתברות מחיקה ε, נאמר שקיים סף (threshold) כך שעבור $\varepsilon < thresh$ שגיאת הפענוח שואפת לאפס ועבור $\varepsilon > thresh$ שואפת לאחד.

ניתן למדוד את סף הפענוח של אלגוריתם 1 בצורה אמפירית, על ידי הגרלה של מילים ולבדוק את יכולת הפענוח להסתברויות מחיקה שונות ε. עבור אלגוריתם איטרטיבי זה, קיים פיתוח מתאים בשם Density Evolution [3] העוסק בפילוג ההסתברות של ההודעות באלגוריתם. הפיתוח מניח את פילוג ההודעה ההתחלתית לפי הסתברות השגיאה, ומעדכן את הפילוג של ההודעות בכל שלב לפי האופרטורים באלגוריתם. כך האלגוריתם מתבצע באופן איטרטיבי ונותן פילוג הסתברות על ההודעה בכל איטרציה באלגוריתם וניתן להשיג את פילוג ההסתברות על ערך המוצא של המפענח לאחר מספר רב של איטרציות. על ידי פיתוח זה ניתן לחשב את הסף פענוח התאורטי.

טבלה 1 המציינת את הסף לפי הקיבול ולפי פיתוח ה-Density Evolution עבור שני קודי LDPC בעלי קצב $R = \frac{1}{2} = 1 - \frac{d_v}{d_c}$.

d_v	d_c	$\epsilon^{shannon}$	$\epsilon^{MessagePassing}$
3	6	0.5	0.4294
4	8	0.5	0.3834

טבלה 1 הסיפים לשגיאת פענוח לפי שאנון ולפי DE עבור קודים בעלי קצב $\frac{1}{2}$

2.4 q-ary Bit-Measurement Channel (QBMC)

מודל ערוץ QBMC מאפיין התקן זיכרון כאשר יש $q = 2^s$ סימבולים (מורכבים מ-s ביטים) שמאוחסנים בצורת מתח/זרם ב-q רמות שונות. מילה מורכבת מרצף של סימבולים מעל $\chi = \{0,1,\dots,q-1\}$ האלפבית, כאשר כל סימבול מיוצג על ידי s ביטים. תהליך הקריאה מתבצע כך שהסימבולים נקראים באמצעות קריאה של ביט בודד, החל מה-MSB, ובכל צעד מדידה קוראים ביט נוסף. אירוע מחיקה חלקית מתרחש כאשר לא כל הביטים נקראו (המדידה נעצרה באמצע) כלומר, יש לנו רק כמה מהביטים הראשונים של הסימבול.

בתהליך הקריאה בכל ביט שנקרא ברצף אנו מצמצמים את כמות הסימבולים האפשריים בחצי (עבור מחיקה מלאה q, לאחר מכן $\frac{q}{2}$ וכן הלאה). עבור כל אירוע מחיקה חלקית ב-j ביטים יש הסתברות ε_j. לכן תוצאת המחיקה החלקית היא קבוצה של סימבולים אפשריים בגודל שהוא חזקה של 2.

למשל עבור $q = 8, s = 3$ (TLC) אם המילה המאוחסנת היא $6 \rightarrow (110)$ ותהליך הקריאה נעצר לאחר הביט השני, הרי שראשית קראנו את ה-MSB ('1'), קבוצת הסימבולים עברה מ-$(0,1,\dots 7)$ ל-$(4,5,6,7)$. לאחר מכן קראנו שוב '1' וקיבלנו את הקבוצה $(6,7)$. כעת נעצרה הקריאה וקיבלנו את המילים האפשריות $(6,7) \rightarrow (11?)$.

ערוץ המחיקה הבינארי הבסיסי BEC הוא מקרה פרטי של ערוץ $QBMC$ עבור $s = 1, q = 2$.

עבור ערוץ מחיקה חלקית זה מוצע להשתמש בקודי $LDPC$ מעל $GF(q)$ שידועים ביעילות בביצועים ובמהירות פענוח על ידי מימוש אלגוריתם איטרטיבי לפענוח. יחד עם האלגוריתם מוצע פיתוח הסתברותי אנליטי להסתברות השגיאה במוצא כתלות ב-$\varepsilon = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_s)$.

נגדיר את "אזור השחזור" להיות ערכי ε כך שהשגיאה במוצא שואפת אסימפטוטית ל 0, ושפת אזור זה יקרא אזור סף פענוח. בפרויקט זה בחנו ביצועים של אלגוריתמים שונים לשחזור הודעות מעל ערוצים שונים, והשוונו את הביצועים שלהם הן מבחינת גודל אזור השחזור והן מבחינת מהירות שחזור של האלגוריתם. כמו כן לצורך השוואה חישבנו את הסף התאורטי לחלק מהם, ולחלק חישבנו קירוב לסף התאורטי.

נתייחס לכל סימבול כאל אלמנט ב-$\mathrm{GF}(q)$ - שדה סופי בעל q איברים [4]. אלמנט בשדה זה $x \in \chi$ ניתן לייצוג על ידי פולינום אופייני $f_x(z) = \sum_{i=0}^{s-1} a_i z^i$ כאשר a_i הם מקדמי הייצוג הבינארי של האלמנט y.

עבור מחיקה מסדר j, מוצא הערוץ הוא קבוצה של סימבולים שבייצוגם יש את אותו מספר $s-j$ של סיביות שמאליות כמו סימבול הקלט x. עבור $j=0$ אין מחיקה, עבור $j=s$ מתרחשת מחיקה "מלאה" כאשר קבוצת המוצא היא כל הסימבולים האפשריים. נסמן קבוצות אלה ב-M_x^j.
כעת נגדיר את הסתברות המחיקה החלקית j.

$$\Pr\left(Y=M_x^j \middle| X=x\right)=\varepsilon_j$$

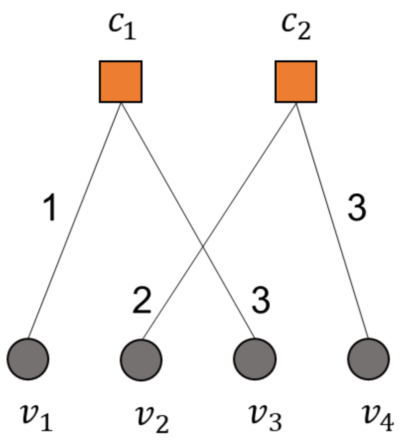
משוואה 1 הסתברות למחיקה חלקית j בערוץ QBMC

קיבול הערוץ QBMC נתון על ידי $C_{QBMC}=1-\sum_{j=1}^{s}\frac{j\epsilon_j}{s}\ [\frac{symbols}{channel\ use}]$ [3].

2.4.1 קודי LDPC עבור ערוץ QBMC

בדומה לקודים בינאריים, בהכללה קוד LDPC עבור ערוץ QBMC הוא בפרט קוד ליניארי שנוצר על ידי מטריצה יוצרת מעל שדה סופי $G\in {GF_q}^{n\times k}$. באופן דומה כעת ה-tanner graph יהיה עם תיוגים לקשתות המתאימים לערכים במטריצה הדואלית $H\in GF_q^{m\times n}$.

$$H=\begin{bmatrix}1&0&3&0\\0&2&0&3\end{bmatrix}$$



איור 7 מטריצת בדיקת זוגיות ו-tanner graph עבור קוד LDPC מעל GF_4

2.4.2 Message Passing עבור LDPC בערוץ QBMC ותחום הפענוח

הצגנו ב-2.3.3 את אלגוריתם Message Passing עבור ערוץ BEC. בערוץ QBMC המפענח אף הוא לפי אלגוריתם איטרטיבי שהוצג ב- [5]. כעת, ההודעות המועברות VTC ו-CTV הן תת קבוצות של GF_q. משוואה 2 ומשוואה 3 מקורן ב- [3] ומגדירות את ההודעות ל-Message Passing.

$$\mathrm{CTV}_{(\mathrm{i})}(c,v)=\sum_{v'\in N(c)\backslash v}\left(\frac{h_{c,v'}}{h_{c,v}}\right)\cdot VTC_{i-1}(v',c)$$

משוואה 2 הודעת Check to Variable עבור ערוץ QBMC

$$VTC_{(i)}(v,c)=\mathrm{V}TC_0(v,c)\bigcap\left\{\bigcap_{c'\in N(v)\backslash c}CTV_{(i)}(c',v)\right\}$$

משוואה 3 הודעת Variable to Check עבור ערוץ QBMC

הערך $h_{c,v}$ מתאר את האיבר המתאים במטריצת בדיקת הזוגיות H והפעולות האריתמטיות מתבצעות מעל השדה, הסימון $\mathrm{N}(\cdot)$ מתאר את קבוצת השכנים של הצומת.

האלגוריתם מאותחל כך שערך $\mathrm{VTC}_0(\mathrm{v},\mathrm{c})$ הוא המוצא של הערוץ הרועש (עד כדי המרת הרעש לתתי קבוצות כפי שהסברנו). לאחר מכן האלגוריתם האיטרטיבי מתחיל במשוואה 2, לאחר מכן מבצעים את משוואה 3 ואלגוריתם זה חוזר חלילה כמה איטרציות שנרצה.

לפי [3] הסתברות השגיאה אינה תלויה במילה המשודרת, ולכן ניתן לשדר את מילת האפס לתוך הערוץ ולבצע את החישובים השונים עליה. כמו כן, במקרה הזה נקבל שתתי הקבוצות הן למעשה תתי חבורות של השדה GF_q.

בדומה ל-decoding threshold עבור ערוץ BEC, נגדיר את תחום הפענוח של האלגוריתם עם קוד LDPC בערוץ QBMC כערכי $\varepsilon=(\varepsilon_0,\varepsilon_1,\dots,\varepsilon_s)$ עבורם שגיאת הפענוח שואפת לאפס.

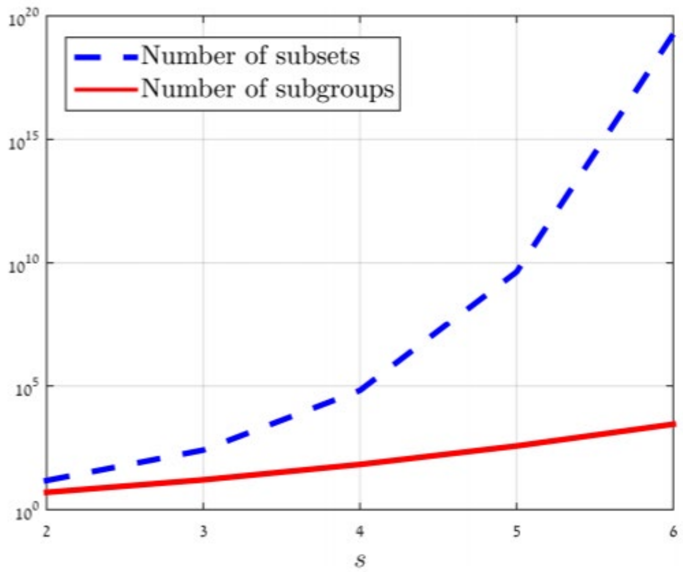
$$Decoding\ Domain=\{(\varepsilon_0,\varepsilon_1,\dots,\varepsilon_s)|P_{error}\rightarrow 0\}$$

2.4.3 Density Evolution בערוץ QBMC

העובדה שבמקרה של שידור מילת האפס ההודעות הן תתי חבורות מפשטת את הניתוח ההסתברותי של האלגוריתם, כיוון שמספר תתי החבורות קטן בסדרי גודל ממספר תתי הקבוצות, כפי שנראה בגרף 1 הלקוח מ- [3]. נסמן את מספר תתי החבורות של שדה סופי GF_q כ-t_q והוא מתואר במשוואה 4 הלקוח מ- [3].

$$t_q = \sum_{j=0}^{s} \left(\frac{\prod_{i=1}^{j} (2^s - 2^{i-1})}{\prod_{i=1}^{j} (2^j - 2^{i-1})} \right)$$

משוואה 4 נוסחה עבור מספר תתי חבורות עבור שדה סופי GF_q



גרף 1: מספר תתי החבורות לעומת מספר תתי הקבוצות עבור שדה סופי מסדר $q = 2^s$ [3]

כאמור, בניגוד לקודי LDPC בינאריים שם התיוגים של הקשתות ב-*tanner graph* הם '0' ו-'1', כעת התיוגים נמצאים בשדה הסופי GF_q. בניתוח הסתברותי של ה-Message Passing יש לכלול את פילוג ההסתברות על התיוגים מבין הערכים בשדה. נסמן את הפילוג הזה כ-$\mathbb{L}$.

$$w_i^{(l)} = \sum_{S_{VTC}} \left(\prod_{m \in S_{VTC}} z_m^{(l-1)} \right) \cdot P_i(S_{VTC}, \mathbb{L})$$

משוואה 5 density evolution עבור הודעת CTV בערוץ QBMC

$$z_i^{(l)} = \sum_{j=0}^{s} \varepsilon_j \sum_{S_{CTV}} \left(\prod_{m \in S_{CTV}} w_m^{(l)} \right) \cdot I_i^j(S_{CTV})$$

משוואה 6 density evolution עבור הודעת VTC בערוץ QBMC

במשוואה 4 ובמשוואה 5 מתוארים המשתנים w_i ו- z_i בהתאמה, המשמעות שלהן היא ההסתברות שהודעה מסוג CTV (או VTC בהתאמה) תהיה H_i, כאשר H_i זה תת החבורה של GF_q.

S_{VTC} ו-S_{CTV} הן מערכים של אינדקסים של תתי החבורות המתאימים להודעות המועברות ל-*check node* או ל-*variable node* וגודלם $d_c - 1$ ו-$d_v - 1$ בהתאמה.

$P_i(S_{VTC}, \mathbb{L})$ מוגדר להיות ההסתברות שבהינתן הודעות S_{VTC} ופילוג $\mathbb{L}$ המוצא יהיה H_i.

$I_i^j(S_{CTV})$ היא פונקציית אינדיקטור ששווה ל-1 אם החיתוך של $H_{m \in S_{CTV}}$ כלומר תתי החבורות ב-S_{CTV} עם התת חבורה-M_0^j נותן את המוצא H_i.

איתחול האלגוריתם נתון על ידי – $z_i^{(0)} = \begin{cases} \varepsilon_{i-1}, & 1 \le i \le s+1 \\ 0, & i > s+1 \end{cases}$.

הסתברות השגיאה באיטרציה ה-*l* (ההסתברות שבאיטרציה זו הודעת ה-*VTC* אינה $\{0\}$) נתונה על ידי משוואה 6.

$$P_{error}^{(l)} = 1 - z_1^{(l)}$$

משוואה 7 הסתברות השגיאה באיטרציה ה-l בפיתוח density evolution

מתברר שעבור פילוג לא אחיד של $\mathbb{L}$ (המקבל רק שני ערכים באחידות ולא שלושה) מתקבל סף גדול יותר בהסתברות המחיקה בביט אחד (ε_1) [3].

2.4.4 שיטות לקירוב באלגוריתם Density Evolution

באלגוריתם ה-DE שמפורט ב-2.4.3 הגורמים $P_i(S_{VTC}, \mathbb{L})$ ו-$I_i^j(S_{CTV})$ עבור q גדול הינם מסובכים לחישוב (סיבוכיות אקספוננציאלית ב-t_q), לכן אנו מציעים קירוב שיאפשר סיבוכיות חישוב קטנה יותר.

הקירוב מתבצע באמצעות מעקב אחרי גדלים של תתי חבורות במקום על תתי החבורות עצמן, בהתחשב בכך שתת חבורה בגודל 1 היא תת החבורה $\{0\}$, דהיינו – אין מחיקה. המעבר למעקב אחר גדלים מאפשר לנו להסתמך על מודלים מתמטיים לקירוב של פילוג ההסתברות על גודל תת החבורה במוצא בהינתן הגדלים בכניסה בהודעות. אנו השתמשנו בשני מודלים המבצעים קירוב, מודל Balls and Bins ומודל Union כאשר השני יותר מדויק בערוץ QBMC.

2.4.4.1 מודל Balls and Bins (BaB)

תחת מודל זה מתייחסים לתוצאה של מכפלת הגדלים כמספר של כדורים (*balls*), ולגודל השדה q כמספר של כדים (*bins*). כעת הבעיה שלנו היא בעיה הסתברותית – אם מטילים כל כדור באופן אקראי (הסתברות שווה שהכדור ייפול בכל כד), נרצה לחשב את פילוג ההסתברות של מספר כדים מלאים (לא ריקים).

פתרון מלא של בעיה זו מתוארת בפרק B ב- [5] ומשתמשת בתיאור המערכת כשרשרת מרקוב הומוגנית. במודל המתאים לערוץ שלנו אנחנו מתעניינים רק בתת חבורות שגודלן הוא חזקה שלמה של 2, לכן נסמן את המטריצה המייצגת של השרשרת כ-Γ_{BaB}, וכ-$g_m^{(N)}$ את ההסתברות למצב 2^m לאחר השלכה של N כדורים. מתקבל שפילוג ההסתברות הכולל לאחר השלכה של N כדורים מתואר במשוואה 7.

$$P_m^{(BaB)} = \frac{g_m^{(N)}}{\sum_{m'=0}^{s} g_{m'}^{(N)}}$$

משוואה 8 פילוג ההסתברות על גדלי תתי חבורות לפי מודל Balls and Bins

2.4.4.2 מודל Union

מודל זה דומה מאוד למודל ה-BaB שהוסבר ב-2.4.4.1, אך הוא לא מניח שהכדורים הם בלתי תלויים, ולכן נקבל תוצאות מדויקות יותר. הבסיס של המודל נובע מהעובדה שמעל שדה, אם $y \neq z$ אז גם $x + y \neq x + z$ לכל x, ולכן כל הכדורים שמתחילים עם אותו איבר (x) אך האיבר השני שונה ($y \neq z$) אז נקבל שהכדורים לא יכולים להיכנס לאותו כד, כלומר שיפלו בהכרח לכדים שונים.

לדוגמה, אם הגדלים בכניסה הם 1 ו 2, במודל ה-BaB נקבל שיש $2 \cdot 1 = 2$ כדורים ועבור $q = 4$ יש 4 כדים, והסתברות שווה של כל כדור להיכנס לכל כד. כעת במודל ה-Union נקבל שיש את אותם מספר של כדורים וכדים, אך מכיוון שבהכרח האיבר של הכניסה 1 יהיה זהה בשני המקרים, והאיברים של כניסה 2 הם שונים זה מזה ($y \neq z$) ולכן נקבל שהם לא יכולים להגיע לאותו הכד כשמחשבים את ההתפלגות.

פתרון מלא של בעיה זו מתוארת בפרק C ב- [5] ומשתמש אף הוא בשרשרת מרקוב הומוגנית בעלת מטריצה מייצגת שונה.

נסמן את המטריצה המייצגת עבור מודל *Union* כ-Γ_{Union}. באופן דומה נסמן כ-$\mathrm{u}_m^{(N/\kappa)}$ את ההסתברות למצב 2^m לאחר השלכה של κ קבוצות של N/κ כדורים, מתקבל הביטוי במשוואה 8.

$$P_m^{(Union)} = \frac{u_m^{(N/\kappa)}}{\sum_{m'=0}^{s} u_{m'}^{(N/\kappa)}}$$

משוואה 9 פילוג ההסתברות על גדלי תתי חבורות לפי מודל Union

3 תיאור הסימולציות

חילקנו את מהלך הפרויקט לשלבים.
ראשית בנינו מודל של ערוץ BEC ומימשנו אותו ב-MATLAB – בנינו מטריצות בדיקת זוגיות שונות (קודים שונים) לפי (d_v, d_c) המקבלים את הערכים $(3,6), (4,8)$ עבור אורכי קוד שונים. שידרנו את מילת האפסים תוך הוספת רעש מחיקה בהסתברויות שונות ופענחנו אותה לפי אלגוריתם ה- Message Passing (אלגוריתם 1). ביצענו מספר איטרציות שבהן מוגרל רעש אחר.
בחנו את הסף של שחזור מלא כתלות באורך הקוד והממדים של מטריצת בדיקת הזוגיות - d_v, d_c.

לאחר מכן הכללנו את המודל לערוץ QBMC – עברנו למטריצות ומילים מעל השדה GF_q עם מחיקות חלקיות בהתאם ל-2.4. הסתכנו על השדה עבור $q = 4$ ובמקרה הזה יש לנו שתי הסתברויות מחיקה, ויצרנו תמונה דו-ממדית של השגיאה לאחר פיענוח כתלות בהסתברויות המחיקה. ראינו בקירוב את הסף שיש לכל ציר, שמהווה שיפור משמעותי לערוץ BEC הקודם.
הסיבוכיות של האלגוריתם הייתה גבוהה מאוד, לכן הרזולוציה של התמונות היא נמוכה, ולא יכולנו לבדוק סימולציות של ערוץ זה עבור q גדול מ-4.

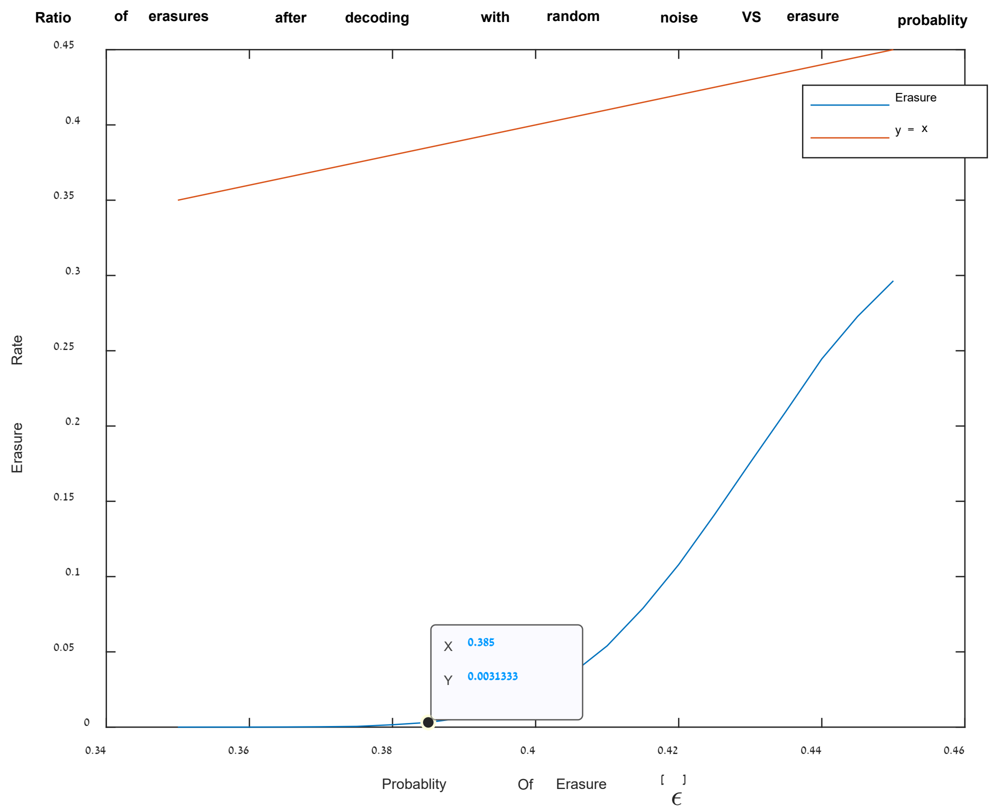
על מנת לעשות ניתוח אנליטי-הסתברותי של הביצועים, עברנו למימוש של משוואות density evolution המתוארות ב2.4.3 עבור q=4. משוואות density evolution מאפשרות לבחון את הביצועים בסיבוכיות נמוכה יותר מהמימוש האמפירי שעשינו עד כה. יצרנו תמונה המייצגת את הביצועים עבור פילוג הסתברות אחיד ולא אחיד של התיוגים במטריצת בדיקת הזוגיות. הסיבוכיות עבור q=8 בחישוב הביטויים הלא-סגורים $P_i(S_{VTC}, \mathbb{L})$ ו-$I_i^j(S_{CTV})$ במשוואה 4 ובמשוואה 5 נותרה מורכבת מדי.

המשכנו בחישוב קירובים לביטויים שלעיל על ידי מודל Balls and Bins (BaB) ומודל Union.
לאחר המימוש התאפשר לנו לבחון את הביצועים עבור q=8 ולאמוד את טיב הקירובים עבור q=4 בהשוואה למימוש המדויק שעשינו לפני כן.

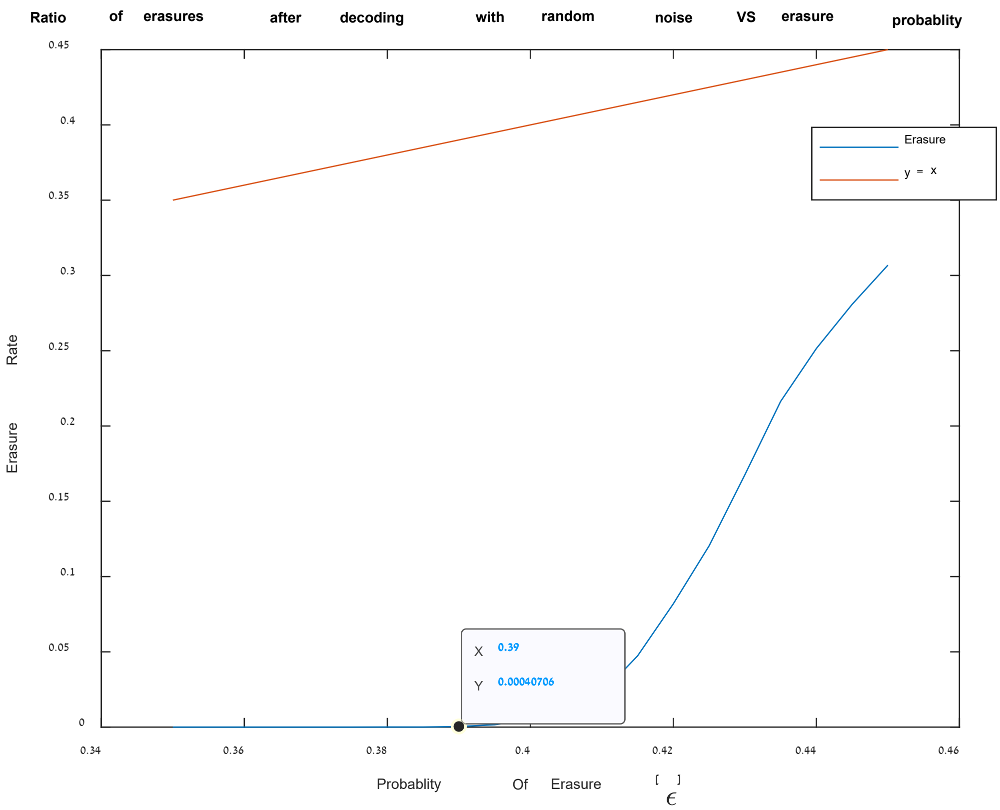
4 תוצאות

4.1 BEC

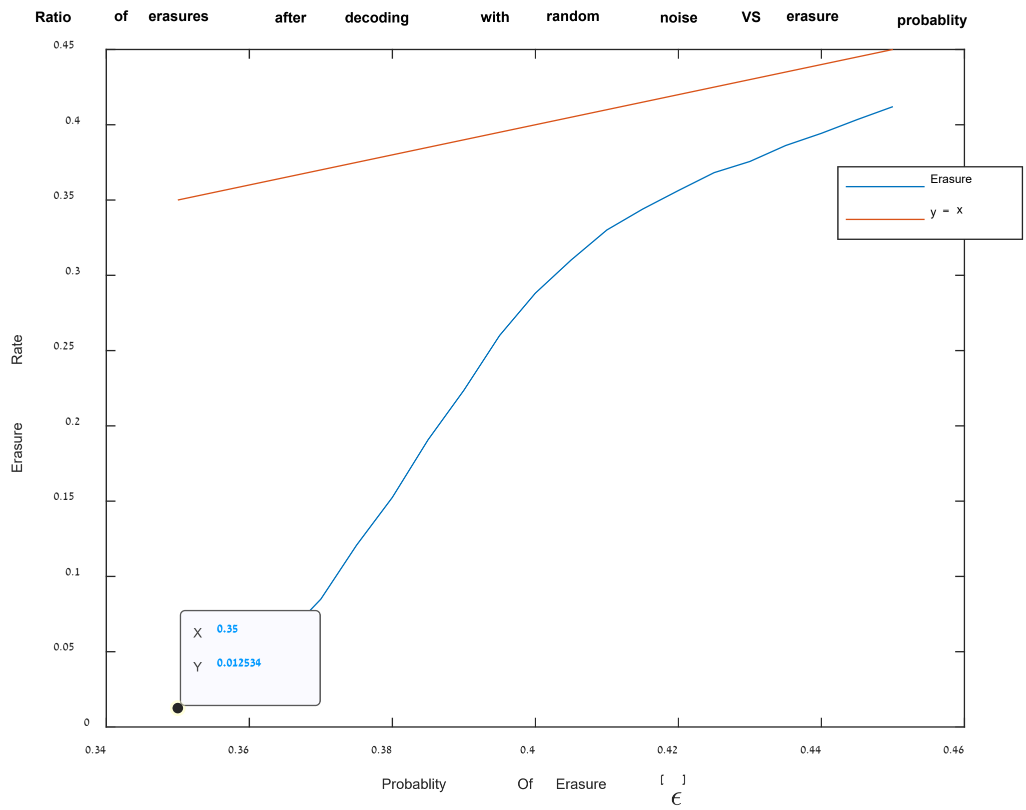
עבור מודל ה BEC בדקנו את טיב הפיענוח על ערכי מילים שונות (n שונה) וכן ההשפעה של מימדיהם של variable nodes ו-check nodes (ערכי dc ו-dv שונים).



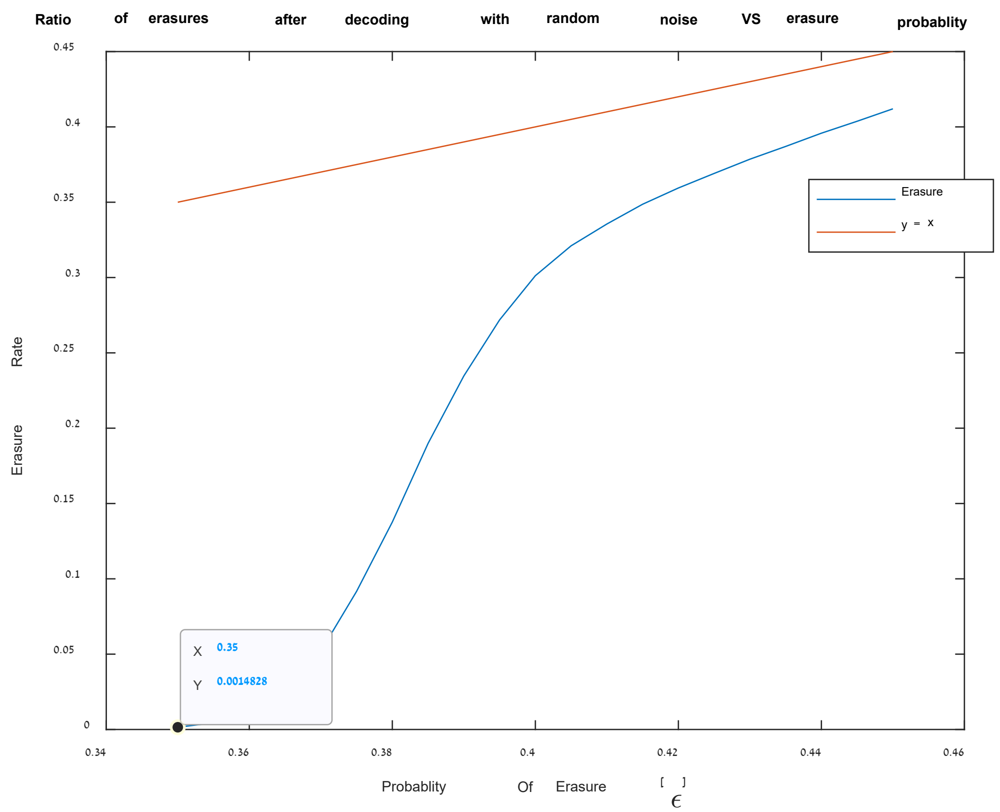
גרף 2: שיעור שגיאה לאחר פענוח עבור n=1000 ו- [dv,dc] =[3,6]



גרף 3: שיעור השגיאה לאחר פענוח עבור $n=2004$ ו- $[dv,dc]=[3,6]$

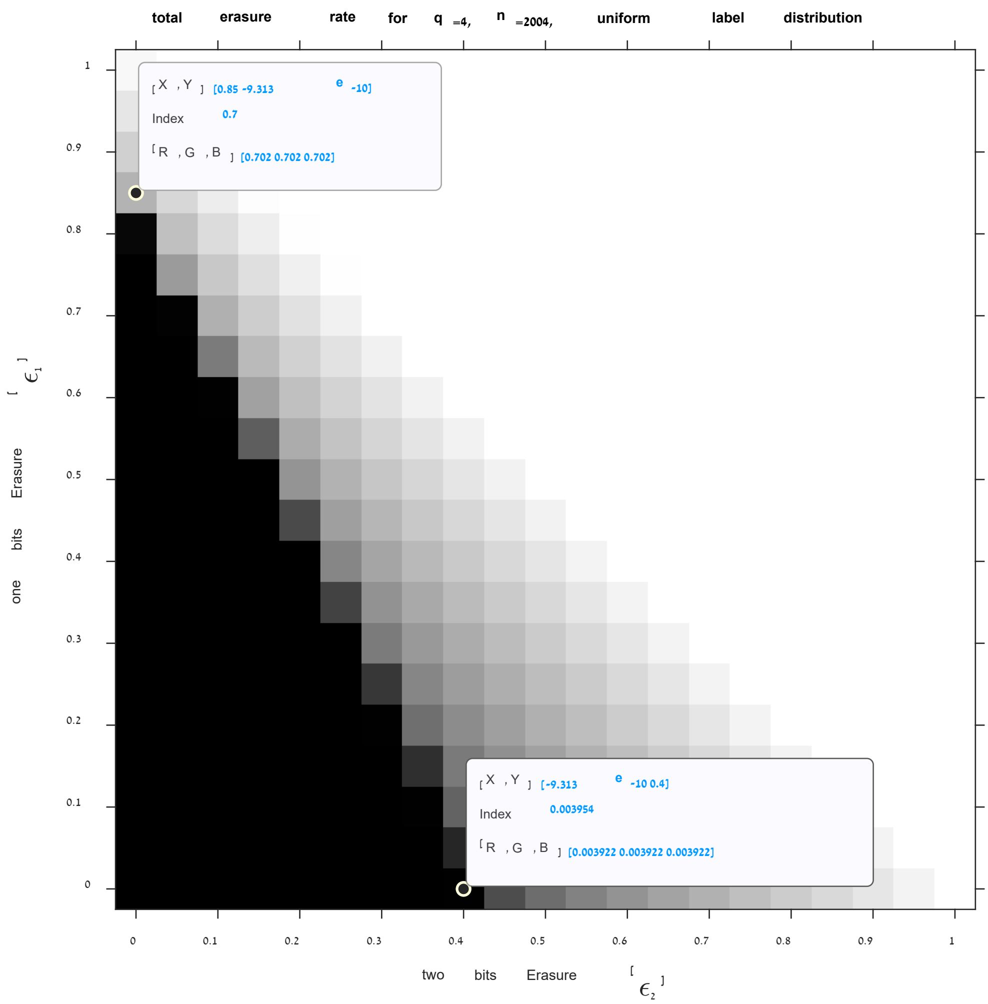


גרף 4 : שיעור השגיאה לאחר פענוח עבור n=1024 ו-[dv,dc]=[4,8]

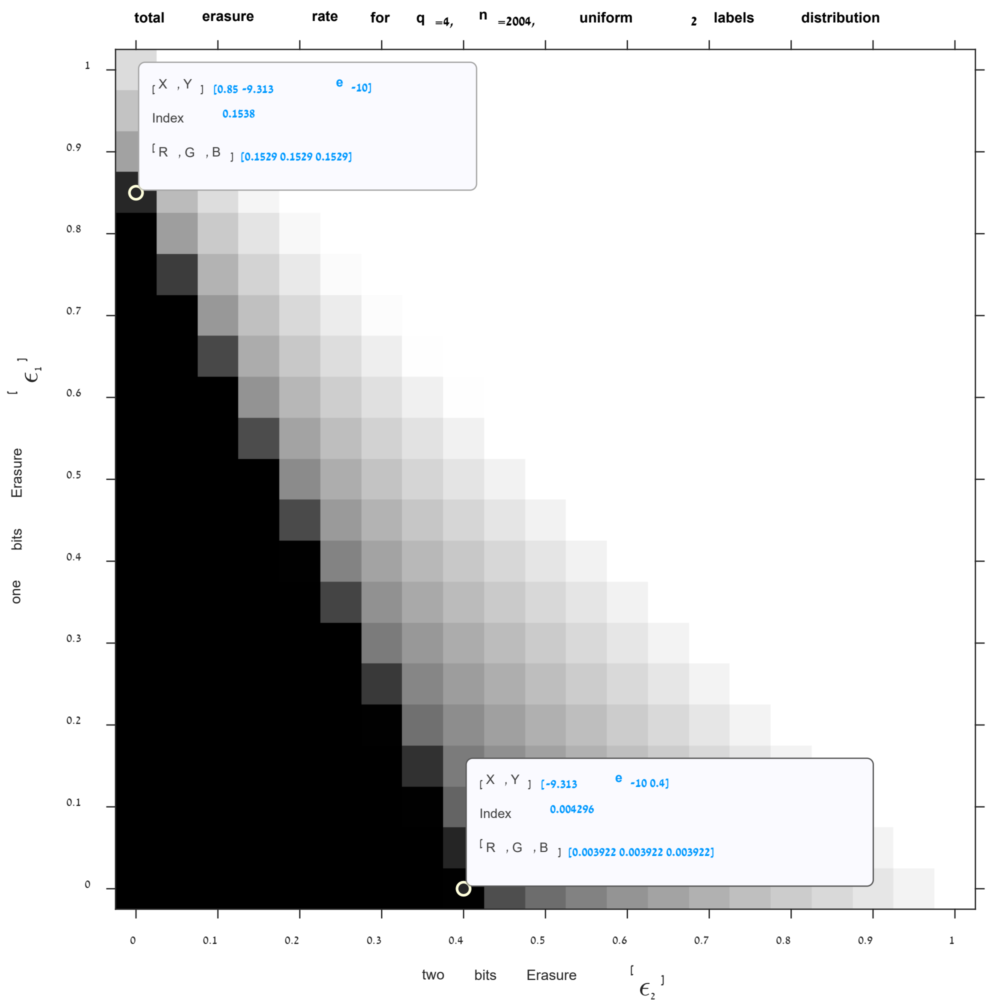


גרף 5 : שיעור השגיאה לאחר פענוח עבור n=2048 ו-[dv,dc]=[4,8]

4.2 פענוח Message passing עבור q=4, ערוץ QBMC מוכלל

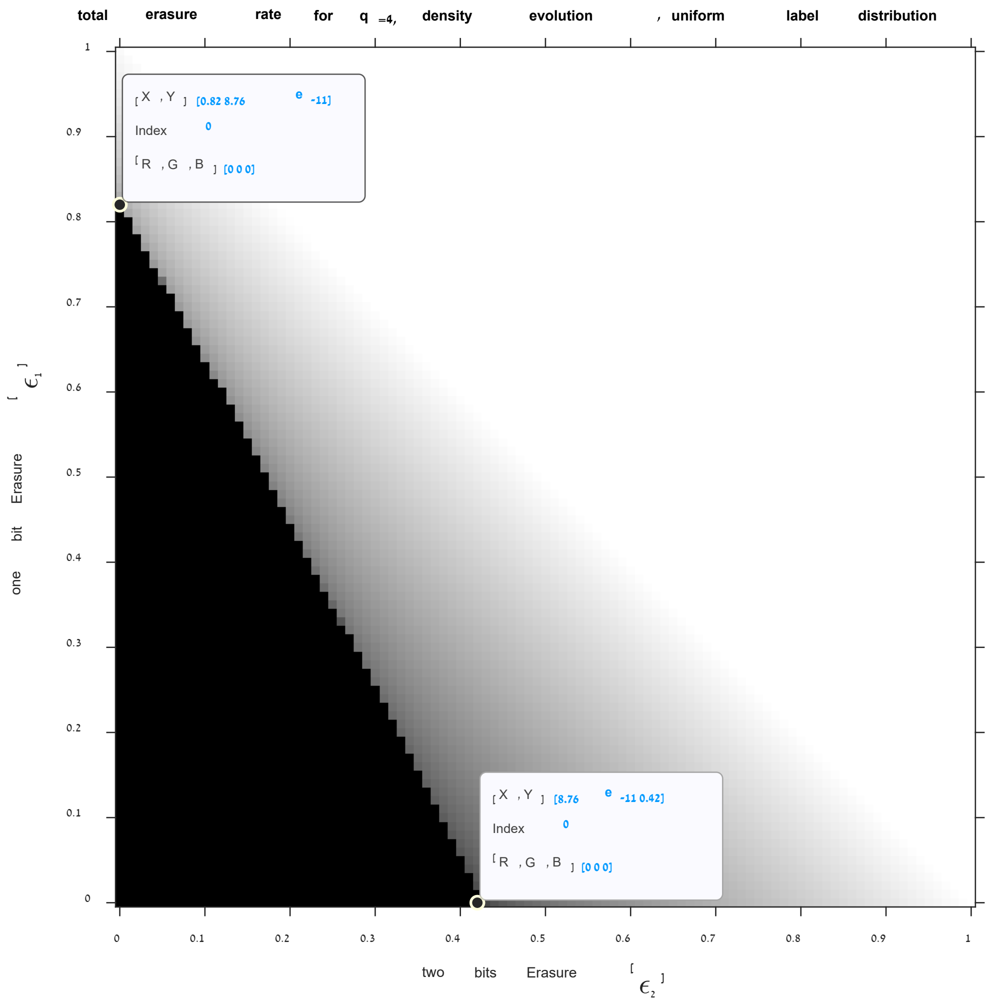


גרף 6 : שיעור השגיאה לאחר פענוח עבור n=2004 ו-[dv,dc]=[3,6], כל הערכים במטריצה H

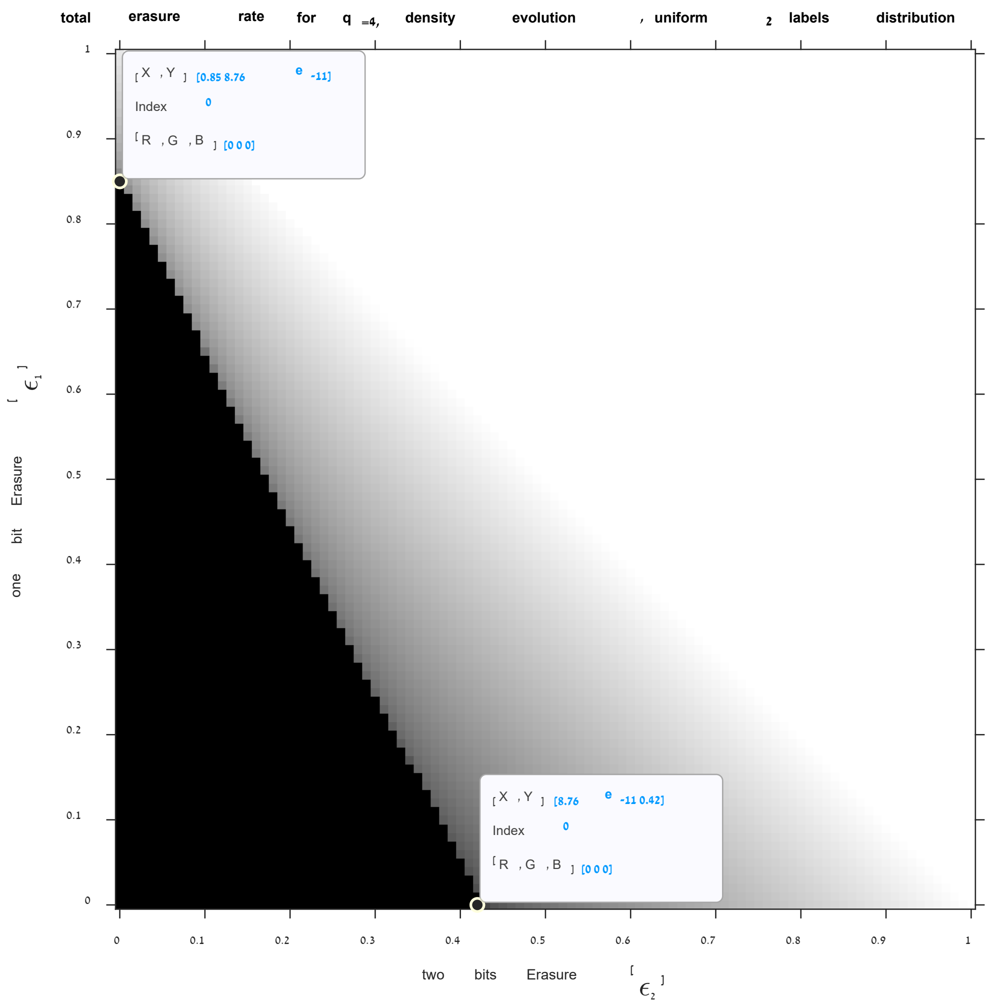


גרף 7 : שיעור השגיאה לאחר פענוח עבור $n=2004$ ו-$[dv,dc]=[3,6]$, הערכים 1,3 במטריצה H

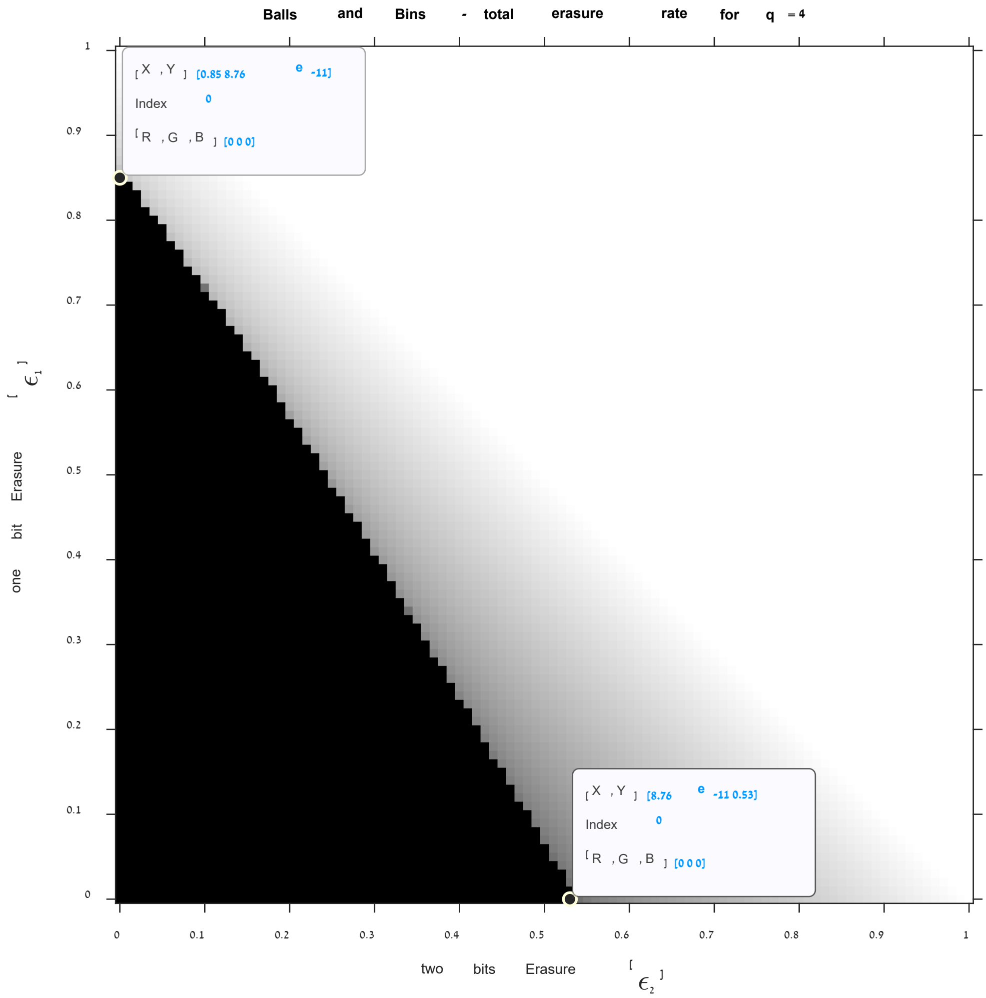
4.3 מימוש משוואות density evolution בצורה מדויקת עבור q=4



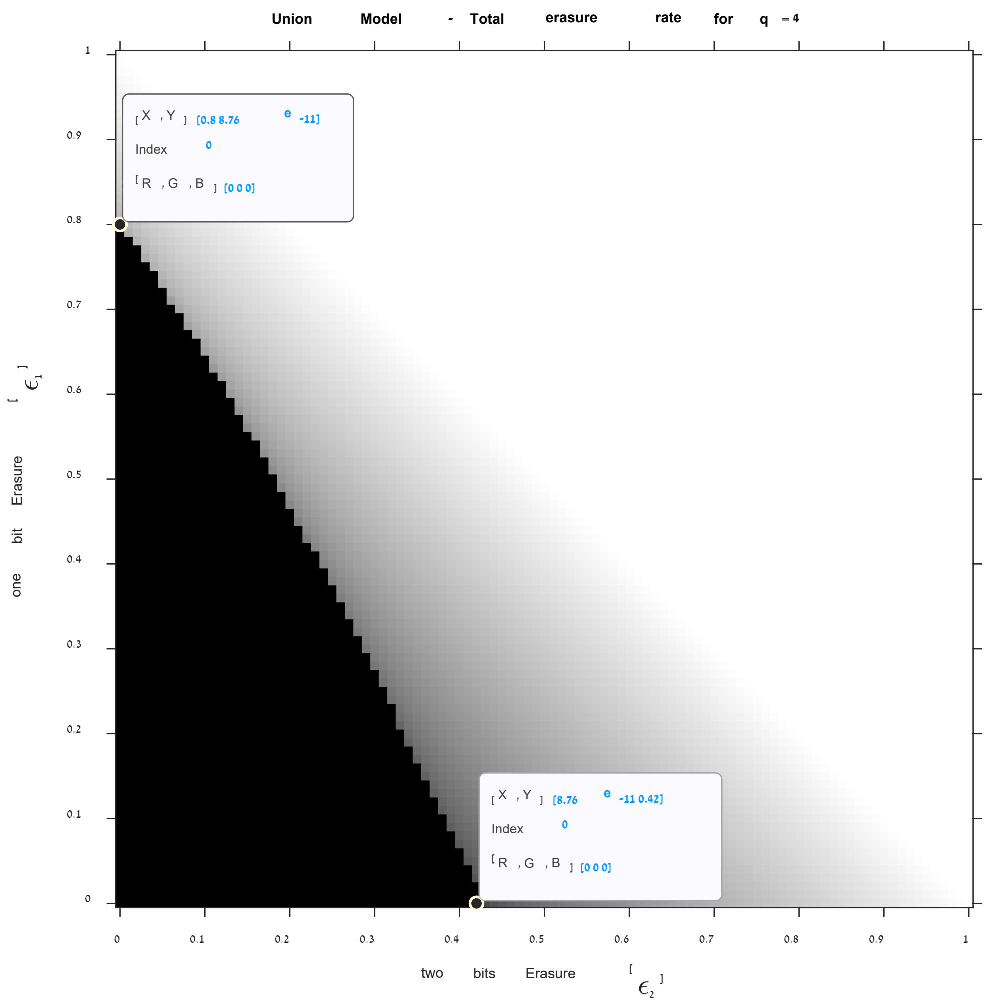
גרף 8: שיעור השגיאה לפי density evolution בחישוב מדויק עבור q=4, פילוג אחיד על כל התיוגים



גרף 9 : שיעור השגיאה לפי *density evolution* בחישוב מדויק עבור *q=4*, פילוג אחיד על שני תיוגים

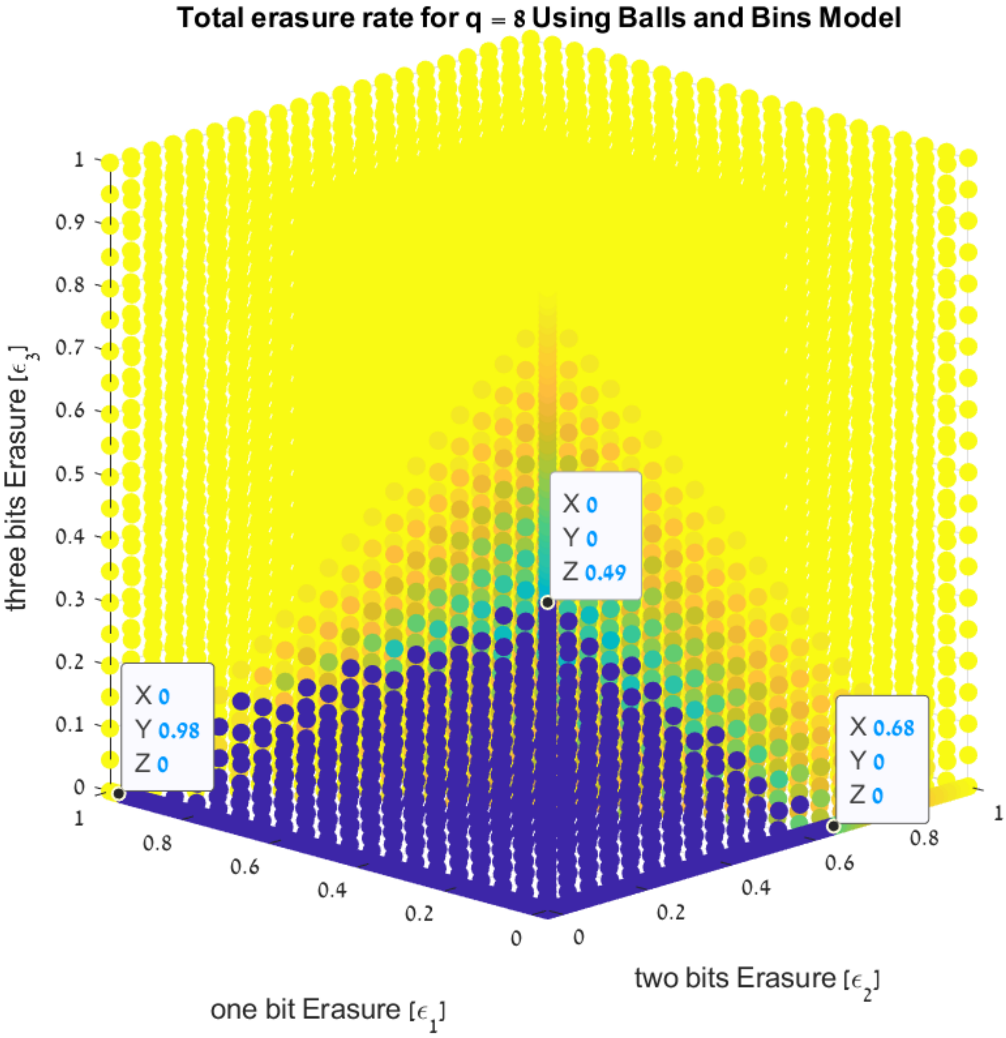


גרף 10 : שיעור השגיאה לפי density evolution בקירוב Balls and Bins עבור q=4

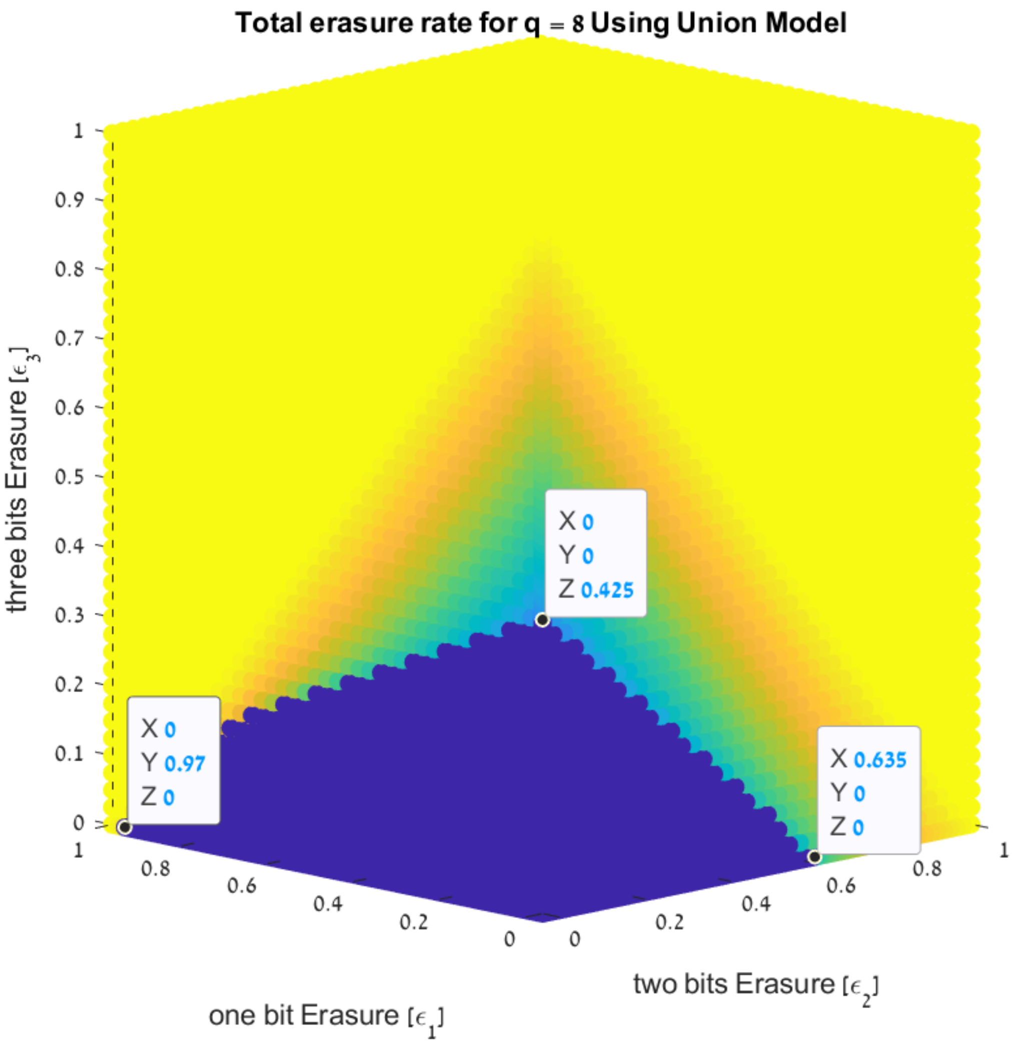


גרף 11 : שיעור השגיאה לפי density evolution בקירוב Union עבור q=4

4.5 מודל Balls and Bins ו-Union Model עבור q=8



גרף 12 : שיעור השגיאה לפי density evolution בקירוב Balls and Bins עבור q=8



גרף 13 : שיעור השגיאה לפי density evolution בקירוב Union עבור q=8

5 דיון בתוצאות

בפרויקט זה ראינו איך הפרמטרים של ה-QBMC ושל הערוץ LDPC משפיעים על יכולת השחזור של קוד תחת מודל QMBC, והשוונו תוצאות אלו לסף התאורטי ולסף מקורב לאחר שחישובים מדויקים התגלו כמסובכים מבחינת חישובית.

בהשוואה בין גרף 2 לגרף 3 ובין גרף 4 לגרף 5 ניתן לראות כי עבור אותם d_v, d_c יש שיפור בביצועים עבור אורכי קוד יותר גדולים. עבור אורך קוד 1002 יש שיעור שגיאה גדול יותר מעבור אורך קוד 2004. ישנו שיפור בסף השחזור האמפירי עבור אורכי קוד יותר גדולים, ועל ידי כך מתקרבים לסף התאורטי כפי שמתואר בטבלה 1. יש לציין שהסף התאורטי הוא סף המתקבל בצורה אסימפטוטית שמושג עבור אורך קוד אינסופי, ולכן התוצאות שקיבלנו הן רק קירוב. ראינו ניתן להבחין כי d_v ו-d_c משפיעים על הסף, ומתקבלים ביצועים וסף טוב יותר עבור $(d_v, d_c) = (3,6)$, כיוון ששיעור השגיאה עבור אותה הסתברות מחיקה גדול יותר עבור $(d_v, d_c) = (4,8)$.

לאחר מכן הכללו את המימוש ל-QBMC ועבור $q = 4$ קיבלנו תמונה דו ממדית שמתארת את אזור שיעור השגיאה לאחר פענוח עבור הגרלה של קודים שונים עם אותם ממדים. בגרף 7 רואים שעבור פילוג אחיד על 2 ערכים במטריצת בדיקת הזוגיות משיג ביצועים טובים יותר (ערכים כהים יותר בתמונה) מאשר בגרף 6 כאשר הפילוג הוא על כל הערכים. עבור אותה הסתברות מחיקה $\varepsilon_1 = 0.85$ מתקבל באחד שיעור שגיאה של 0.153 לעומת 0.7 באחר.
הרזולוציה הנמוכה של הגרף (0.05 בכל הסתברות מחיקה) היא בחירה נוחה כיוון שהסימולציה אורכת זמן רב והרצה שלה ברזולוציה גבוהה יותר לא הייתה ממשית.

ומה שעניין אותנו בעיקר היה חיתוך הסף בצירים (כלומר כאשר מאפסים את אחד מההסתברויות מחיקה, ורצים על ההסתברות השנייה כדי לראות איפה מתקבל הסף באותו הציר). כמו כן בחנו את השפעת הפילוג של הערכים במטריצת בדיקת הזוגיות על הסף.

שמנו לב שנדרש הרבה מאוד זמן לחישוב אמפירי של תוצאות הללו, ואפילו עבור $q = 4$ חישובים לא היו פשוטים, לכן עברנו מחישוב אמפירי של הסף, לחישוב אנליטי.
בעזרת אלגוריתם density evolution קיבלנו את הסף התאורטי שיצא מאוד דומה לתוצאה האמפירית.

בגרף 8 ובגרף 9 אפשר לאמוד את ההבדל בסף הפענוח עבור שתי ההתפלגויות על התיוגים.
ניתן לראות שעבור פילוג אחיד עבור שני ערכים משיג סף טוב יותר בפענוח עבור ε_1 (חיתוך ב-0.85 לעומת 0.82), יחד עם אותו סף ב-$\varepsilon_2 = 0.42$.

אך גם החישוב התאורטי התגלה ככרוך בהרבה חישובים מסובכים, לכן עדיין לא הגענו לסיבוכיות נורמלית, לכן ביצענו שני קירובים על הסף התאורטי על מנת שנוכל לקבל את אזורי סף הפיענוח גם

עבור $q = 8$ ובשביל זה השתמשנו במודל ההסתברותי Balls and Bins שנתן לנו תוצאות שהיו קרובות לסף התאורטי, ולאחר מכן שיפרנו את הקירוב על ידי שימוש במודל היותר טוב למקרה שלנו – Union Model שנתן לנו תוצאות מאוד קרובות למה שקיבלנו בחישוב התאורטי האמיתי, ולכן הקירוב שלו עבור $q = 8$ הינו יותר נכון.

עבור $q = 4$, כפי שניתן לראות בגרף 10 רואים כי מודל Balls and Bins לא נותן קירוב טוב (סיפים 0.53 ו-0.85) לעומת מודל Union בגרף 11 (סיפים 0.42 ו-0.85). הסף 0.42 יותר מהימן לתוצאה התאורטית המתוארת בטבלה 1. כמו כן, עבור $q = 8$ אנו מקבלים תוצאות טובות יותר בגרף 13 של מודל Union מאשר גרף 12 (מקבלים מעין תוצאה של overshoot עבור מודל ה BaB).

6 סיכום ומסקנות

קודי LDPC משיגים ביצועים טובים יחסית למגבלת הקיבול (טבלה 1). שיטת הפענוח האיטרטיבית של Message Passing יחסית מהירה, אך ניתוח הביצועים אמפירית ואנליטית זה משימה הכרוכה בחישובים מסובכים. עבור קודי LDPC מעל $GF(4)$ בחירת ערכי התיוגים במטריצה H משפיעה על הביצועים כך שדווקא הבחירה הטריוויאלית (פילוג אחיד על כל הערכים) היא לא הבחירה האופטימלית. ככל ששיש יותר רמות המתחים/זרמים בהתקני אחסון (q גדל) מושגים ביצועים יותר טובים (כך למשל, עבור q = 8(Triple level cell) מתקבלים סיפים טובים יותר בהסתברויות השגיאה מאשר $q = 4$. המודלים Balls and Bins ו-Union מקבעים אותנו לבחירת תיוגים אחידה ומונעים מאיתנו לבחון אופטימיזציה דומה עבור $q = 8$.

7 מחקר המשך

חלק ניכר מעבודתנו נעשה תוך כדי מגבלות סיבוכיות (עבור הפתרון המלא של ה-DE - $O(t_q^{dc-1} \cdot (q-1)^{dc})$, לעומת הפתרון המקורב – $O(\log(q)^{dc-1})$). ניתן למצוא אופטימיזציות שיאפשרו לנו ניתוח רחב יותר. ניתן להתמקד בלבחון את הביצועים עבור הסתברויות מחיקה חלקיות תוך איפוס של השאר ולהשיג בהן רזולוציה טובה יותר, כך לממש את המודלים שהשתמשנו בהם עבור $q = 16$ ועבור $q = 32$. ה-Balls and Bins וה-Union Model מניחים פילוג אחיד בתיוגים. ניתן לנסות למצוא קירובים אחרים שמתחשבים בתיוגים ובכך לנסות לאשש את ההשפעה של פילוג זה על הביצועים.

8 ביבליוגרפיה

[1] J. S. Sorcha Bennett, “The Characterisation of TLC NAND Flash Memory, Leading to a Definable Endurance/Retention Trade-Off,” *International Journal of Computer and Information Engineering*, כרך 10, מס' 4, 2016.

[2] T. R. a. R. Urbanke, Modern Coding Theory, Cambridge: Cambridge University Press, 2008.

[3] R. C. a. Y. Cassuto, “LDPC Codes for the q-ary Bit-Measurement Channel,” Technion - Israel Institute of Technology, Haifa, 2016.

[4] R. J. McEliece, “Finite Fields for Computer Scientists and Engineers,” Kluwer Academic Publishers, 1987.

[5] R. C. a. Y. Cassuto, “Iterative decoding of LDPC codes over the qary partial erasure channel,” *IEEE Transactions on Information Theory*, כרך 62, מס' 5, 2016.

[6] R. H. Morelos-Zaragoza, The art of error correcting coding, John Wiley & Sons, 2002.

[7] S. K. T. L. J. Nana Traore, “Message Passing Algortihm and Linear Programming Decoding for LDPC and Linear Block Codes,” Aalborg University, Aalborg, 2007.

[8] A. Shokrollahi, “LDPC Codes: An Introduction,” Digital Fountain, Inc., Fremont, 2003.

[9] J. L. a. H. Z. José M.F. Moura, “Structured Low-Density Parity-Check Codes,” *IEEE SIGNAL PROCESSING MAGAZINE*, 2004.