פרק -3
קודים (צפנים)

<u>הגדרה</u>: קוד או צופן הוא צורת הצגת מידע. לא תמיד משתמשים בצופן כדי לשמור על סודיות. במערכות מחשבים למשל , מטרת הצפנת (או קידוד) המידע הינה התאמה ליכולת העיבוד של המחשב.
הצופן המתאים ביותר למחשב הוא הצופן הבינרי.

3.2 <u>קוד BCD</u> . <u>(BINARY CODED DECIMAL)</u> (הכוונה לספרה עשרונית מוצפנת בקוד בינרי).

כיוון שמערכות ספרתיות (לדוגמא מחשבים) בנויות בטכנולוגיות הפועלות לפי 2 מצבים מוגדרים , (בדרך כלל רמות מתח שונות) ניתן לסמן מצב אחד – 0 ומצב שני – 1. ולכן נח לייצג באמצעותן מספרים בינריים.
בחיי היום יום אנו משתמשים בדרך כלל במספרים עשרוניים ולא פעם היינו מעדיפים להשתמש בהם גם במערכות הספרתיות. שימוש <u>ישיר</u> כזה אינו בר-ביצוע כיוון שהבסיס במערכות סיפרתיות הינו בינרי וברור שחוקי אריתמטיקה בינרית שונים מחוקי אריתמטיקה עשרוניים. אולם ניתן למצוא דרך ביניים שבה נצפין (נקודד) מספרים עשרוניים בצופן בינרי, כפי שנראה בהמשך. צופן כזה נקרא BCD.
צופן מסוג זה מנצל את היתרונות של המספרים העשרוניים (שאליהם התרגלנו בחיי היום יום) וגם את יתרונותיהם של המספרים הבינריים.

<u>צורת הקידוד בקוד BCD</u> : בצופן BCD כל <u>ספרה</u> עשרונית תוצפן <u>בנפרד</u> בקוד בינרי באורך 4 סיביות (מספיק 4 סיביות כי ערך מכסימלי (בבסיס 10) הוא 9, ובייצוג בינרי זה 1001).

אם נתון קוד BCD : $x_3\ x_2\ x_1\ x_0$ (x_3 - סיבית ה- M.S.B.) אזי ערך עשרוני של הקוד כפי שלמדנו

$$N = x_3 \times 2^3 + x_2 \cdot 2^2 + x_1 \cdot 2^1 + x_0 \cdot 2^0$$
$$= x_3 \times \underline{8} + x_2 \cdot \underline{4} + x_1 \cdot \underline{2} + x_0 \cdot \underline{1}$$

ולכן קוד BCD נקרא גם קוד 8421. אם נרצה להצפין את המספר העשרוני 15 בצופן BCD, אזי נקודד כל ספרה לקוד ה-BCD שלה . לדוגמא :

$$\underbrace{0001}_{1}\ \underbrace{0101}_{5}$$

דוגמא :

נתון קוד BCD הבא : 010101001001. תרגם אותו למספר עשרוני.

<u>פתרון</u> : נחלק את הקוד מימין לשמאל לרביעיות,וכל רביעיה נתיחס אליה כספרה עשרונית אחת.

$\underbrace{1001}_{9}\ \underbrace{0100}_{4}\ \underbrace{0101}_{5}$ כלומר קוד העשרות שקיבלנו הוא 549.

<u>יתרון הבולט של קוד BCD הוא</u> : הפשטות במעבר למספר עשרוני ולהפך. (כפי שראינו בדוגמאות לעיל).

חסרון של קוד BCD הוא : שחוקי האריתמטיקה לא מתאימים תמיד.

<u>משפט</u> .(ללא הוכחה)

כאשר מחברים 2 ספרות בקוד BCD אזי :

א. אם תוצאת חיבור <u>קטנה</u> מ-10 אזי תוצאה נכונה.

ב. אם תוצאת חיבור <u>גדולה</u> מ-9 אזי מוסיפים 6 לתוצאת החיבור, ואזי מקבלים תוצאה נכונה בקוד BCD.

<u>דוגמא א'</u> : חבר 5+3 בקוד BCD

$$\begin{array}{r} 0101 \\ + \\ \underline{0011} \\ (1000)_2 = 8 \end{array}$$

תוצאה שהתקבלה נכונה (מתאים למשפט).

<u>דוגמא ב'</u> : חבר 5+6 בקוד BCD

$$\begin{array}{r} 0101 \\ + \\ \underline{0110} \\ 1011 \end{array}$$

לפי משפט נוסיף 6 לתוצאה ונקבל :

$$\begin{array}{r} 1011 \\ + \\ \underline{0110} \\ 00010001 \end{array}$$

נתרגם תוצאה לקוד עשרוני

$\underbrace{0001}_{1}$ $\underbrace{0001}_{1}$ וקיבלנו 11 בבסיס 10.

3.2 <u>קודים שונים לספרות עשרוניות</u>

3.2.1 <u>קודים משקליים</u>

כל ספרה עשרונית מיוצגת ע"י 4 סיביות (כי ערך מכסימלי 9 ומספיק 4 סיביות לקודד ערך זה)

$x_4\ x_3\ x_2\ x_1$. לכל סיבית i משקל W_i.

ערך הספרה המיוצגת הינו :

$$N = \sum_{i=1}^{4} W_i \cdot x_i = W_1 \cdot x_1 + W_2 x_2 + W_3 \cdot x_3 + W_4 \cdot x_4$$

דוגמאות לקודים משקליים :

ספרה עשרונית	קוד BCD $w_4\ w_3\ w_2\ w_1 = 8421$	קוד 2421 $w_4\ w_3\ w_2\ w_1 = 2421$
0	0000	0000
1	0001	0001
2	0010	0010
3	0011	0011
4	0100	0100
5	0101	1011
6	0110	1100
7	0111	1101
8	1000	1110
9	1001	1111

3.2.2 <u>קודים לא משקליים</u>

בקודם אלו אין אפשרות לתרגם לערך עשרוני ע"י הכפלה במשקלים.

למשל : קוד EXCESS-3 מתקבל מ-BCD ע"י תוספת 0011 לכל מילת קוד של הקוד BCD.

למשל: הספרה עשרונית 0 בקוד BCD: 0000

הספרה עשרונית 0 בקוד EXCESS-3: 0011

3.2.3 <u>קודים ציקליים</u>

הגדרה: קוד שבו מילת קוד של ספרה כלשהי שונה ממילת הקוד של הספרה שלפניה ואחריה בסיבית אחת בלבד נקרא קוד ציקלי .

מקרה פרטי של קוד ציקלי : קוד GRAY (קוד משוקף).

<u>הגדרה</u>: קוד GRAY הינו קוד ציקלי שבו המילה ראשונה כולה אפסים. קוד זה מאד שימושי וישמש אותו בהמשך בנושא של מינימיזציה של פונקציות .

<u>דוגמאות של קוד GRAY בגודל n סיביות :</u>

n = 1 הקוד : 0

1

n = 2 הקוד 00 ← קוד של ערך עשרוני 0

01 ← קוד של ערך עשרוני 1

11 ← קוד של ערך עשרוני 2

10 ← קוד של ערך עשרוני 3

n = 3 הקוד :

000 ← קוד של ערך 0
001 קוד של ערך 1
011 קוד של ערך 2
010 .
110 .
111 .
101 .
100 ← קוד של ערך 7

3.2.3.1 השיטה לבניית קוד GRAY (משוקף)

<u>משפט</u>: קוד משוקף (GRAY) בעל n סיביות מתקבל מקוד משוקף בעל (n-1) באופן הבא:

רשום את הקוד של (n-1) סיביות בצורה אנכית. בתחתית הקוד העבר ציר סימטריה. שקף את הקוד סביב ציר הסימטריה. לאחר שקוף מקבלים 2^n מילות קוד. (2^{n-1} מילות קוד מעל ציר ו- 2^{n-1} מילות קוד מתחת לציר).

ל- $2^{(n-1)}$ המילים שמעל לציר הוסף 0 בתור סיבית M.S.B.

ל- $2^{(n-1)}$ המילים שמתחת לציר הוסף 1 בתור סיבית M.S.B.

<u>דוגמאות:</u> נבנה קוד GRAY של 2 סיביות, באמצעות קוד של סיבית אחת

עבור n =1 הקוד הינו :

0
1

עבור n = 2 הקוד הינו :

00
01
11
10

3.2.3.2 <u>המרה מקוד GRAY לקוד בינרי והפוך</u>

נניח ש- $g_n g_{(n-1)} ... g_o$ הינה מילה בקוד GRAY.

נניח ש- $b_n b_{(n-1)} ... b_o$ המספר הבינרי <u>המתאים</u>.

נגדיר פעולה שנקראת XOR בין 2 משתנים בינריים B, A ונסמן $A \oplus B$.

טבלת האמת של XOR :

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

3.2.3.3 **המרה מקוד בינרי ל- GRAY** (ללא הוכחה)

$$g_n = b_n$$

עבור : i<n $\quad g_i = b_i \oplus b_{i+1}$

דוגמא :

קוד GRAY	**קוד בינרי**

$$b_3 = 1 \longrightarrow g_3 = 1$$

$$b_2 = 0 \xrightarrow{1 \oplus 0} g_2 = 1$$

$$b_1 = 0 \xrightarrow{0 \oplus 0} g_1 = 0$$

$$b_0 = 1 \xrightarrow{0 \oplus 1} g_0 = 1$$

3.2.3.4 **המרה מקוד GRAY לבינרי** (ללא הוכחה)

אלגוריתם : התבונן בקוד GRAY.

- אם מספר ה-1 משמאל לסיבית i הוא זוגי אזי $b_i = g_i$
- אם מספר ה-1 משמאל לסיבית i הוא אי זוגי אזי $b_i = g_i'$

(כמובן תמיד $b_n = g_n$)

דוגמא : נתון קוד GRAY : 1101

הקוד הבינרי שמתקבל : 1001

3.3 קודים (צפנים) אלפא-נומריים

3.3.1 כללי

קיימים 2 סוגי עיבוד נתונים במערכות ספרתיות ובעיקר במחשבים :

- עיבוד נתונים מספריים (נומריים), בד"כ עיבוד זה כולל חישובים אריתמטיים שונים וכדומה.
- קיימים נתונים שאינם מספריים כגון : שם וכתובת של פלוני. נתונים כאלו כמובן אינם משמשים לביצוע חישובים. נתונים מסוג זה מבוטאים ע"י 3 קבוצות תווים : ספרות, אותיות ותווים מיוחדים. נתונים כאלו נקראים אלפא-נומריים.

3.3.2 קוד ASCII

קוד זה מורכב ממילים בגודל 7 סיביות, כלומר ניתן להצפין בו 128 נתונים אלפא-נומריים.

קוד זה הינו נפוץ מאד ראשי תיבות של הקוד :

AMERICAN STANDART CODE INFORMATION INTERCHANGE

בעמ' הבא מפורט הקוד ה- ASCII בצורת טבלה של שורות ועמודות. כאמור לעיל הקוד בנוי מ-7 סיביות נסמנם :

$b_6 \ b_5 \ b_4$	$b_3 \ b_2 \ b_1 \ b_0$

4 הסיביות $b_3 \ b_2 \ b_1 \ b_0$ מציינות את השורה של התו (יש כאלו 16).

3 הסיביות $b_6 \ b_5 \ b_4$ מציינות את העמודה של התו (יש 8 כאלו).

הצטלבות של שורה ועמודה יוצרת התיחסות לתו מסוים בטבלה.

בהתיחס לטבלת הקוד ה- ASCII שמופיע בעמ' הבא נראה דוגמא של קידוד תו אלפא נומרי.

נתון קוד ASCII : 1000101. עפ"י מבנה הקוד שתואר לעיל התו נמצא בשורה 5 ובעמודה 4 בטבלה. מן הטבלה מתברר כי זה קוד של אות E.

קוד ASCII

b_6 b_5 b_4 (column)									
b_3 b_2 b_1 b_0	ROW (hex)	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
0000	0	NUL	DLE	SP	0	@	P	'	P
0001	1	SOH	DC1	!	1	A	Q	a	q
0010	2	STX	DC2	"	2	B	R	b	r
0011	3	ETX	DC3	#	3	C	S	c	s
0100	4	EOT	DC4	$	4	D	T	d	t
0101	5	ENQ	NAK	%	5	E	U	e	u
0110	6	ACK	SYN	&	6	F	V	f	v
0111	7	BEL	ETB	,	7	G	W	g	w
1000	8	BS	CAN	(	8	H	X	h	x
1001	9	HT	EM	)	9	I	Y	i	y
1010	A	LF	SUB	*	:	J	Z	j	z
1011	B	VT	ESC	+	;	K	[	k	{
1100	C	FF	FS	,	<	L	\	l	|
1101	D	CR	GS	-	=	M	]	m	}
1110	E	SO	RS	.	>	N	^	n	~
1111	F	SI	US	/	?	O	-	o	DEL

Control codes			
NUL	Null	DLE	Data link escape
SOH	Start of heading	DC1	Device control 1
STX	Start of text	DC2	Device control 2
ETX	End of text	DC3	Device control 3
EOT	End of transmission	DC4	Device control 4
ENQ	Enquiry	NAK	Negative acknowledge
ACK	Acknowledge	SYN	Synchronize
BEL	Bell	ETB	End transmitted block
BS	Backspace	CAN	Cancel
HT	Horizontal tab	EM	End of medium
LF	Line feed	SUB	Substitute
VT	Vertical tab	ESC	Escape
FF	Form feed	FS	File separator
CR	Carriage return	GS	Group separator
SO	Shift out	RS	Record separator
SI	Shift in	US	Unit separator
SP	Space	DEL	Delete or rubout

3.4 קודים לגילוי ותיקון שגיאות

מטרה : גילוי ותיקון שגיאות במידע עקב שיבושים, למשל : עקב רעש.

3.4.1 **הקדמה** : ניקח סדרה של n ספרות בינריות. כפי שלמדנו הן יכולות לייצג 2^n צירופים שונים. אם יש לנו קוד אשר בו מנוצלים כל 2^n הצירופים. אנו אומרים שאין בו (בקוד) יתרות. פרושו : אין כל צרוף בקוד שאיננו מנוצל (שאין משתמשים בו).

אם בקוד זה תארע שגיאה באחת הסיביות אזי נקבל מילת קוד אחרת.

דוגמא : בקוד BCD כל ספרה הינה בתחום 0 עד 9 וקוד זה כפי שלמדנו גודלו 4 סיביות. נתבונן בקוד של $6 \leftarrow 0110$. נניח שאירעה שגיאה בסיבית שלישית מימין (1 הפך ל-0) נקבל 0010. צרוף זה הוא חוקי בקוד BCD וערכו 2, לכן במקרה זה לא נגלה שאירעה שגיאה.

לעומת זאת, בקוד BCD, יש פעמים בהן שגיאה באחת הסיביות תתן צרוף לא חוקי בקוד, ואזי נוכל לגלות שאירעה שגיאה לדוגמא : אם בצרוף 0110 (6) אירעה שגיאה בסיבית M.S.B $(0 \leftarrow 1)$ אזי נקבל צרוף 1110 (ערך 14). צרוף זה אינו חוקי בקוד BCD (ערך מכסימלי -1001 9) ולכן נוכל לגלות שאירעה שגיאה.

מסקנה : בקוד BCD פעמים נגלה שאירעה שגיאה, ופעמים לא נגלה שאירעה שגיאה.

הערות : א. יש קודים שבהם נגלה כל שגיאה שתקרה.

ב. יש קודים שבהם לא נגלה אף שגיאה (ראה הקדמה).

3.4.2 **מקורות השגיאות** :

א. בקו ההעברה בין יחידות השונות במחשב. פירושו : כאשר מעבירים מידע מיחידה ליחידה יש סכנה שרעש אקראי ישנה את אחת הסיביות (או יותר). שגיאות מסוג זה הינן חמורות כי הן אקראיות דהיינו לא צפויות מראש וקשה לגלות אימתי אירעו (לא כמו חוט קרוע – דבר שניתן לגלות ולתקן).

ב. שריטות אבק וכו' על גבי מקורות מידע (דיסקים וכו').

3.4.3 **הגדרות שונות לגבי קודים לתיקון/גילוי שגיאות**

3.4.3.1 2 מושגים חשובים : גילוי שגיאה (ERROR DETECTION)

תיקון שגיאה (ERROR CORRECTION)

ההבדל בין המושגים : במונח "גילוי שגיאה" אנו מתכוונים לגילוי המילה שבה קרתה השגיאה. במונח "תיקון שגיאה" אנו מתכוונים לגילוי הסיביות אשר בם אירעה השגיאה. דבר זה מאפשר לתקן את השגיאות.

3.4.3.2 **מרחק בין 2 מילים בינריות:**

הגדרה : נתונות לנו 2 מילים בינריות בגודל n סיביות כל אחת : $A \leftrightarrow a_{(n-1)}...a_0$

$B \leftrightarrow b_{(n-1)}...b_0$

המרחק בין המילים מוגדר כמספר הסיביות שיש לשנות, כדי לקבל מילה אחת מן השניה.

סימון d (A, B) – מרחק בין מילה A ל-B.

דוגמא: $A = a_4\, a_3\, a_2\, a_1\, a_0 = 10110$ $\quad B = b_4\, b_3\, b_2\, b_1\, b_0 = 10000$

שים לב: $a_1 \neq b_1 \quad a_2 \neq b_2$ ולכן $d(A,B) = 2$.

כללית: עבור 2 מילים בגודל n סיביות: המרחק בין 2 המילים הוא בין 0 (אם 2 מילים זהות) ל-n (אם כל הסיביות שונות) כלומר $0 \le d(A,B) \le n$

3.4.3.3 מרחק של קוד

הגדרה: מרחק של קוד הינו המרחק המינימלי בין 2 מילים כלשהן בקוד.

הערה: אם בקוד בינרי רגיל שהוא קוד במרחק 1 תיפול טעות באחת המילים הרי שנקבל מילה אחת ששייכת לקוד.

מסקנה: אם אנו רוצים לגלות שגיאה אחת, צריכים שמרחק הקוד יהיה לפחות 2.

3.4.4 נוסחה לגילוי ותיקון שגיאות (ללא הוכחה)

$$m = 2c + d + 1$$

m - מרחק הקוד

d - (DETECT) שגיאות שניתן לגלות (בנוסף לשגיאות שתוקנו).

הסבר: אם שגיאה תוקנה הרי ברור שהיא שהתגלתה.

c - (CORRECT) שגיאות שניתן לתקן.

הערה : מספר השגיאות שניתן לגלות הינו c+d .

דוגמאות לשימוש בנוסחה:

$$m = 1 \Rightarrow c = 0 \quad d = 0$$

$$m = 2 \Rightarrow c = 0 \quad d = 1$$

$$m = 3 \Rightarrow \begin{cases} c = 0 \quad d = 2 \\ \text{או} \\ c = 1 \quad d = 0 \end{cases}$$

(באפשרות השנייה c=1 d=0 כלומר : ניתן לתקן שגיאה אחת וכמובן שניתן לגלות שגיאה אחת) .

$$m = 4 \Rightarrow \begin{cases} c = 1 \quad d = 1 \\ \text{או} \\ c = 0 \quad d = 3 \end{cases}$$

3.4.5 בדיקת שגיאות בשיטת הזוגיות . (PARITY-CHECK)

הקדמה : בשיטה זו (שמאד מקובלת) ניתן לגלות שגיאה בודדת (בלבד) אך לא לתקן שגיאה ולא לגלות שגיאה כפולה.

3.4.5.1 קוד משלים לזוגי (EVEN PARITY)

דוגמא : נבנה קוד זוגיות בגודל 3 סיביות. סיבית M.S.B תיקרא סיבית זוגיות.

שיטה לבניית קוד : נבנה קוד בינרי רגיל עבור 2 סיביות. קיימים 4 צירופים :

ערך	צרוף בינרי
0	00
1	01
2	10
3	11

לכל צרוף בינרי נוסיף סיבית נוספת בשיטה הבאה : אם מספר ה-'1' בצרוף הבינרי הוא זוגי אזי סיבית PARITIY היא 0 . אם מס' ה-'1' בצרוף בינרי הוא אי זוגי אזי PARITY = 1 ונקבל :

ערך	צרוף בינרי	PARITY
0	00	0
1	01	1
2	10	1
3	11	0

קבלנו 4 מילות קוד ←000 (קוד של ערך 0)

101 (קוד של ערך 1)

110 (קוד של ערך 2)

011 (קוד של ערך 3)

מרחק הקוד הוא 2.

הערה : שים לב שמס' ה-'1' בכל מילת קוד הוא זוגי.

מסקנה: אם חלה שגיאה בודדת באחת ממילות הקוד (כלומר סיבית אחת של 1 נהפכה ל-0 או הפוך) אזי מס' ה-1 במילה יהיה אי זוגי ולכן נוכל לגלות שגיאה בודדת. לא נוכל לתקן את השגיאה הבודדת כי לא נדע את מיקום השגיאה.

לדוגמא: נניח קיבלנו 001 וזה שגיאה (כי מס' '1' הוא אי זוגי) יתכן שמילת קוד לפני שגיאה היתה 000 או 011 או 101. כמו כן, אם חלו 2 שגיאות לא נגלה זאת כי מס' ה-'1' במילה ישאר זוגי. אם חל מס' אי זוגי של שגיאות נגלה שגיאה אבל לא נדע כמה שגיאות חלו.

סיכום: בנית קוד משלים לזוגי (EVEN PARITY) בגודל n סיביות

באותה צורה שפתחנו את קוד זוגיות לקוד בעל 3 סיביות אפשר לפתח קוד עבור n סיביות $n \geq 3$.

תאור השיטה:

א. קבל את $2^{(n-1)}$ צירופים בינריים שונים לגבי $(n-1)$ סיביות ה-L.S.B.

ב. לגבי כל צרוף מצא את סיבית ה- PARITY:

אם מס' ה-'1' בצרוף הוא זוגי אזי PARITY = 0.

אם מס' ה-'1' בצרוף הוא אי זוגי אזי PARITY = 1.

ג. הוסף את סיבית ה-PARITY לצרוף בינרי כסיבית M.S.B.

הערה: שים לב, נגלה גם שגיאה בסיבית ה-: PARITY.

3.4.5.2 קוד משלים לאי זוגי (ODD PARITY)

בשיטה זו מוסיפים סיבית PARITY בשיטה הבאה:

לכל צרוף בינרי נוסיף סיבית PARITY באופן הבא:

אם מס' ה-'1' בצרוף הוא אי זוגי אזי PARITY = '0'.

אם מס' ה-'1' בצרוף הוא זוגי אזי PARITY = 1.

כלומר סכום ה-'1' במילת הקוד הוא אי זוגי. גם כאן מרחק הקוד הוא 2.

תרגיל בנושא תקון שגיאות ע"י קוד לבדיקת זוגיות.

נתונות 9 סיביות אינפורמציה במערך 3x3. סיביות V_{ij} אלו סיביות אינפורמציה .

P_{ij} - סיבית PARITY.

V_{11}	V_{12}	V_{13}	P_{14}
V_{21}	V_{22}	V_{23}	P_{24}
V_{31}	V_{32}	V_{33}	P_{34}
P_{41}	P_{42}	P_{43}	P_{44}

נוסיף לכל שורה ועמודה סיבית זוגיות.

ניתן להוכיח כי P_{44} הינה סיבית זוגיות של העמודה האחרונה והשורה האחרונה.

נראה שהצופן מתקן שגיאה בודדת:

אם נפלה שגיאה במקום ij כלשהו אזי נקבל שגיאות בבדיקת זוגיות של: שורה i ועמודה j.

3.4.6 קוד : **X OUT OF Y**

הגדרת הקוד : כל מילות הקוד באורך Y מכילות בדיוק מספר של X סיביות בערך 1

למשל $(2)OUT-OF(5)$.

קוד זה מכיל מכיל 10 מילים שבכל אחת 5 סיביות. כל מילה מכילה 2 פעמים '1'.

מילות הקוד הינן : 00011,00101,00110 11000

ניתן להוכיח: מרחק קוד = 2 $\Leftarrow$ ניתן לגלות שגיאה אחת.

3.4.7 קוד המינג: קוד במרחק 3

עד עתה ראינו שכדי לגלות ולתקן שגיאה בודדת חייב הקוד להיות במרחק 3. נשאלת השאלה כיצד מגלים ומתקנים שגיאה בודדת.

אנו נסביר את הטכניקה מבלי להכנס להוכחות. (יש קורס תורת הצפינה שבו עוסקים בזאת בהרחבה).

נניח שבקוד יש לנו 2^m מילות קוד שונות, לכן נצטרך m סיביות מידע .

ל-m סיביות הללו נוסיף k סיביות בדיקה. לכן מילת קוד תכיל n סיביות כאשר: $n=m+k$.

מציאת k (ללא הוכחה): לפי הנוסחא $2^k \geq n+1$

מסקנה: אם יש לנו מילה באורך n ורוצים לקבוע קוד במרחק 3 אזי צריך למצוא k מינימלי שמקיים את האי-שוויון . אחר שמוצאים את k אזי: $m=n-k$.

אנו נדבר על מקרה שבו n=7 (כלומר קוד המינג באורך 7) .

מציאת k :

$2^k \geq 7+1=8$. k מינימלי שמקיים את האי שוויון הינו 3 . ולכן $m=4$.

נניח שלא אירעה יותר משגיאה אחת.

שידור .

לסיביות אינפורמציה נקרא: $M_1\ M_2\ M_3\ M_4$

לסיביות הבדיקה נקרא: $P_1\ P_2\ P_3$

המילה תשודר בצורה כזו:

סיבית מס' →	1	2	3	4	5	6	7
	P_1	P_2	M_1	P_3	M_2	M_3	M_4

P_1 ייבחר כך שסיביות (P_1,M_1,M_2,M_4) יתנו PARITY זוגי (כלומר משלים לזוגי).

P_2 ייבחר כך שסיביות (P_2,M_1,M_3,M_4) יתנו PARITY זוגי.

P_3 ייבחר כך שסיביות (P_3,M_2,M_3,M_4) יתנו PARITY זוגי.

קליטה .

נניח כי במקלט (תחנת קליטה) קיבלנו את המילה הבאה :

וקטור W = | W_1 | W_2 | W_3 | W_4 | W_5 | W_6 | W_7 |

בצע את הפעולות הבאות :

$C_3= P(W_4, W_5 ,W_6 , W_7)$. P הינו משלים לזוגי .

$C_2= P(W_2, W_3 ,W_6 , W_7)$

$C_1= P(W_1, W_3 ,W_5 , W_7)$

תוצאה : אם $C_3C_2C_1=000$ אזי לא קרתה שגיאה.

אם אחד מה-C שונה מ-0 אזי קרתה שגיאה . **מקום השגיאה הוא** : $(C_3C_2C_1)_2$.

בתרגול נראה דוגמאות .