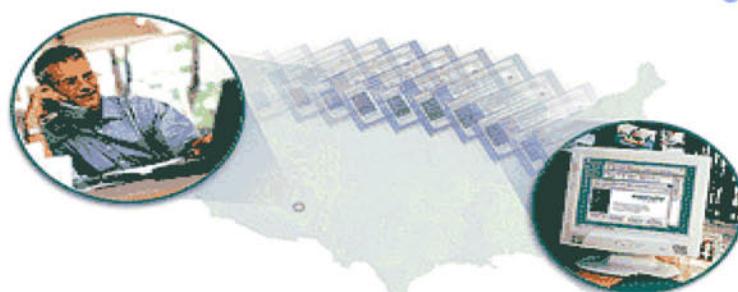




המכללה לטכנאים והנדסאים

עמל ב' – פתח תקווה

המחלקה להנדסת אלקטרוניקה



מערכות תקשורת תקשורת מחשבים

תקנים לגילוי ו/או תיקון שגיאות בתקשורת בין מחשבים

אפקט ריסויין

עריכה מקצועית:

© שאול קוּבָּל – SAUL COVAL®

עבור השיעורים של המרצה בלבד

מהדורה: Ver. 6.02 – 02/2009

כתובת המכללה: אמסטרדם 16 – פתח תקווה

גילוי/תיקון שגיאות בתקשורת מחשבים

ללאם הם מטור ויקיפדיה, האנציקלופדייה החופשית (wikipedia.org)

קוד תיקון שגיאות

קוד תיקון שגיאות הוא קוד בעל מספר תכונות שמאפשרות לשולח באמצעותו אוסף של מבחנים דרך עירוני תקשורת רושע, ולנטרל במידה מסוימת את השפעת רעש הדרק על המידע המתקבל. קוד התיקון פועלים על ידי הגדלת ההבדל בין המילים השונות בקוד, וכך הקטנת הסיכון שרעש היצוני יגרום לקליטת מילה השונה מהמילה שנשלחה. כאשר ההבדל בין מילות הקוד גדול במיוחד ניתן אפילו לתקן שגיאות, כל עוד מספר השגיאות קטן מספיק.

ניסוח פורמלי

קוד הוא קבוצת מילים, המורכבות ממספר קבוע של אותיות. כך, אם נסמן את קבוצת האותיות שהבחן אנו משתמשים ב- Ω , ואת אורך כל מילה בקוד ב- n , אז אפשר להסתכל על הקוד כתה קבוצה של הקבוצה Ω^n שנצטרצת על ידי מכללה קרוטזית של Ω בעצמה Ω^n פעמים (קבוצת ה- Ω -יות הסדרות של אברים מ- Ω). נתיחס לכל האותיות כסקולות, ונניח שככל הצליפות בין שתי אותיות שונות ב- Ω^n מתרחשות באותה תדרות.

קודים כללים הם בעלי יכולת לזהות שגיאות שהתרחשו בהם, ככל עוד מספר השגיאות שהתרחשו קטן ממספר האותיות השונות המוגIMALי בין שתי מילים בקוד (זוזו מרחק המוגIMAL של הקוד). לאחר מכן, נקבע מסר שהוא לכוונה תקן – מילה בקוד, אך למעשה הוא עיוות של המסר האמיתי. הקודים מתקני שגיאות יש את היכולת לזהות שהתרחששה שגיאת, יותר מזה – גם לזהות מה הייתה המילה המקורי. היכולת זו נובעת מרחק הקוד הגדל, שימושו לפי אותו רעיון כמו בזיהוי השגיאות – ניתן לתקן שגיאות במסר כל עד מספר השגיאות קטן ממש ממחצית המרחק של הקוד. אחרת יכולות להיות שתי מילים שונות בקוד שמרחיק מהמסר שהתקבלו הוא המוגIMAL מבין כל מילות הקוד, וכך ניתן להכיריעו איזו מילה נשלה במקור.

קוד תיקון שגיאות פשוט

הקוד פשוט ביותר לתקן שגיאות הוא פשוט קוד החזרה. חזרים על המסר המשודר מספר פעמים. אם בתחלת המרחק המוגIMAL שבין שתי מילים בקוד היה d אז בקוד שבו יש חזרה בונפה על המסר, המרחק המוגIMAL הוא כבר $2d$ וכן הלאה. קוד שמילוטי זה פשוט וזרה על מילות הקוד הוא קוד שהරחיק המוגIMAL בין מילוטיו הראן.

לדוגמה נניח שהקוד המוקורי הוא פשוט $\{0,1\}$ (הקוד הבינארי הפשוט), הקוד זה הוא בעל מרחק 1, וכן ניתן לזהות שגיאות. אם נחרור על כל דבר פשוט, נקבל את הקוד $\{0,0,1\}$. זה קוד עם מרחק 2, וכן ניתן לזהות שגיאת הסידור (תקבל המילה 01 או 10, שבוודאי לא שזרה), אבל לא לתקן אותה: אם התקבל 01 לא ניתן לדעת אם שוחר במקורה 00 או 11. אם נחרור על כל דבר שלוש פעמים, נקבל את הקוד החזרה $\{000,111\}$. זה קוד עם מרחק 3, וכן כבר ניתן לא רק לזהות, אלא גם לתקן טעות אחת: אם התקבל 001 אז ננראה שorder 000. קודי החזרה הם לא קודים ייעילים, כי בתפקיד הגדלת המרחק בין מילות הקוד נפתחו את אורך כל המילים. בדוגמה לעמלה, כדי להשיג קוד מרחק 3 נאלצנו לשדר מילים באורך 3, במקומות מסוימים גם גוטים לספוג יתר טערות. וכך אם נבנה קוד שבו ניתן לתקן טעות אחת, נציג רק $1/3$ (כלומר כמות האינפורמציה שהועברה הייתה $1/3$ מכמות הביטים ששודרו).

קוד נספה, יעיל במידה מפתיעה יחסית לפשטותו הוא הקוד שבו בונפה ספרה ביקורת. בזורה הוא מוגIMAL בקשרו של מילוטים אחד ו- q (כאשר q הוא מספר האותיות השונות). בזורה הוא ניתן להגדיר חיבור בין האותיות השונות. בהינתן קוד C נציג קוד חדש על ידי הוספה ספרה שמשלימה את סכום כל האותיות לאפס (מודולו q):

$$C^+ = \{(x_1, \dots, x_k, x_{k+1}) : x_1 + \dots + x_k + x_{k+1} = 0\}$$

ספרת הביקורת מעלה את המרחק בין שתי המילים הקשורות ביותר בקוד ב-1

קודים מורכבים

באמצעים אלגבריים מתוחכמים לבנות קודים מאוד חזקים מהבינהה של כמות המילים שליהם מול המרחק המוגIMAL בין מילות הקוד. לדוגמה, ניתן לזכור קוד תיקון שגיאות שישדר מידע של שלושה ביטים, A, B, C. הקוד יורכב משולש אותיות שהן פשוט הביטים עצם ואחריהם שלוש קומבינציות ה-XOR ביןיהם - AxB, AxC, BxC. קוד זה הוא בן 8 מילים שונות (מידע של שלושה ביטים), והוא 6 והマーク בין כל שתי מילים שונות בקוד גדול או שווה ל-3.

קיימים קודים חזקים כללים כמו קודי המיג'ר, LDPC, Trellis, קודי ריד סולומון ועוד. באופן כללי, קודי התיקון מתחלקים לשתי קבוצות: קוד בלוק וקוד קוונולוציה. את ה-"כח" של הקוד התיקון מודדים בדרך כלל בהගבר (לדוגמא 3 דזיבלים), כלומר שימוש בקוד הב"ל הוא אקוילנטי לשידור בהספק הגבואה באותו הגבר (הספק שידור הגבואה ב-3 דזיבלים לדוגמה).

גילוי שגיאות

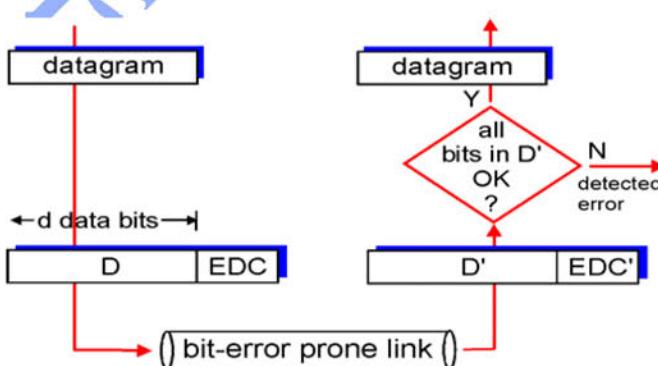
גילוי שגיאות ותיקון סיביות (יתירות).

EDC= Error Detection and Correction bits (redundancy)

הנתונים מוגנים על ידי בדיקת שגיאות הייבם לכלול שדות כותרות.

D = Data protected by error checking, may include header fields

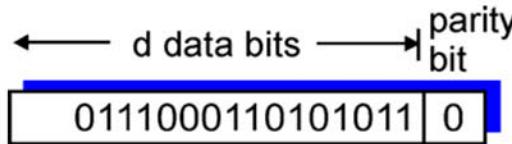
גילוי שגיאות הוא לא 100% אמין !



הפרוטוקולים יכולים להחמיר מספר שגיאות, אבל בדרך כלל שדות EDCA נוחנים גילוי טוב יותר וגם אפשרות לתקןם.

סיבית זוגיות

סיבית זוגיות היא קוד המוסיף סיבית בהזדמנות לאישר מציגת אם מספר הסיביות שערקן הוא 1 במידע הוא זוגי או אי-זוגי. אם סיבית אחת במידע המשוחרר השתבשה, הרי שהזוגיות של המידע השתנתה, ועל כן ניתן להזזה שארעה שגיאה (גם אם הסיבית שהשתבשה הינה סיבית הזוגיות עצמה!). ניתן אף להזזה כל סיבית הזוגיות שווה ל-0 הרו' שיבנו בהוג' להגדיר כי אם סיבית הזוגיות שווה ל-1 הרו' שיבנו מספר א' זוגי של סיביות האות-1 במידע, ואם סיבית הזוגיות שווה ל-0 הרו' שיבנו מספר זוגי של סיביות האות-1 במידע. מכאן נובע שבסכירה סיבית הזוגיות שהשתבשו הוא זוגי, הרו' שלא היה ניתן להזזה כי אירעה שגיאה, כיוון שככל שתי סיביות זוגיות אינה חסינה למגרי לשגיאות - אם מספר הסיביות שהשתבשו הוא זוגי, הרו' שלא היה ניתן להזזה כי אירעה שגיאה, לא ניתן להזזה סיביות משובשות מבטלת את ההשפעה ההדרית על סיבית הזוגיות. יותר מכך, גם כאשר בדיקת הזוגיות מזוהה כי אירעה שגיאה, לא ניתן להזזה באיזה סיבית או סיביות היא אירעה. על כן, יש להיפטר מכל המידע, ולשדרו מחדש מוחדר לחלוטן. בערוץ רועש, שידור מוצלח יכול לקחת זמן רב, או לא לזרות לעולם.

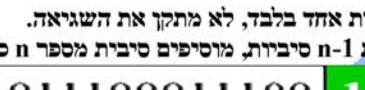


למרות ההסכנות מהם סובלת בדיקת הזוגיות, היא דורשת סיבית אחת בלבד עבור כל בלוק מידע, ועל כן התקורה בה היא נמוכה מאוד, והיא אפשרה שחזור של סיבית הסרה, כאשר ידוע איזו סיבית הסרה (אך כי בפועל הרבה לא ניתן לדעת זאת).

הוספת סיביות זוגיות: Single Bit Parity

מגלה שגיאות של סיביות בודדות. Detect single bit errors

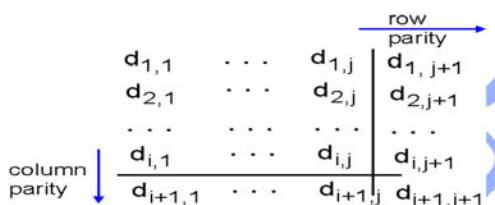
- גילוי: מחליט האם הייתה שגיאיה.
- תיקון: מתקן את השגיאות.
- דוגמה של סיבית זוגיות:



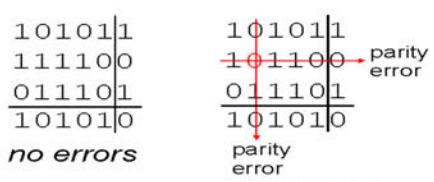
- אפשר לגלו'ת שגיאת של סיבית אחד בלבד, לא מתקן את השגיאת.
- מעבר נטען של מסגרת הכלולה-1-ה סיביות, מוסיפה סיבית מס' 8 כדי שהסהמota של "1" הוא זוגי (even parity).



השיטה לא מאפשרת גילוי של כמה שגיאות!!!

(LRC) Longitudinal Redundancy Check - בדיקת יתירות אורך

מגלה שגיאות של סיביות בודדות ומטתקן אוטם.
לא ניתן לגלו'ת שגיאות של ארבע סיביות צמודות זה לזה!!!!.



- פרוטוקולים רבים פועלם על ידי גילוי שגיאות ושידור מחדש.
- השניה עקב הדרך בשידור מחדש היא אורך מיידי לשימושים של מהירות גבוהה.

בשידור של מספיק יתירות של נתונים כדי לאפשר למקלט לתקן של שגיאות בודדות.

- דוגמה:
נתונים של $n \times m$ סיביות.

data (n-1)(m-1) bits	checksum $m + n - 1$ bits
-------------------------	------------------------------

				שורות parity
	$d_{1,1}$...	$d_{1,m-1}$	$d_{1,n}$
	$d_{2,1}$...	$d_{2,m-1}$	$d_{2,n}$

	$d_{n-1,1}$...	$d_{n-1,m-1}$	$d_{n-1,n}$
Parity	עمرודה	$d_{n,1}$...	$d_{n,m-1}$
				$d_{n,n}$

דרך חישובLAGILIOI שגיאהבчисלוב מושלב LRC

1	0	1	0	1	0	error	דוגמת גילוי שגיאה
1	1	1	1	0	0	ok	בתיקון מושלב LRC
0	1	1	1	0	1	ok	
1	0	1	0	1	1	ok	
error	ok	ok	ok	ok	ok		

קוד המיניג – מטריך ויקיפדיה, האנציקלופדייה החופשית

הוא קוד תיקון שגיאות ליניארי, הקרויה על שם של ריצ'רד המיניג אשר הגה את הקוד. קוד המיניג מסוגל לזהות ולתקן שגיאות בסיבית בודדת, וכן לזהות (אך לא לתקן) שגיאה בשתי סיביות. לשם השוואת, קוד הוגנות הפשטוט אותו מסוגל לזהות שגיאות כאשר שתי סיביות מתחפות, או לתקן את השגיאות שהחלה כן מסוגל לזהות.

מספר הסיבות הנוספות הדורשות עבור קוד המיניג הוא המינימאלי ההכרחי עבור כל קוד לתקן שגיאות המסוגל לתקן שגיאה בסיבית בודדת.

היסטוריה

בשנות ה-40 של המאה ה-20, ריצ'רד המיניג עבד ב厶בודות בול על המחשב האלקטרו-מכני "Bell Model V", אשר הקטל שלו הוזן בעזרת כרטיסים מנוקבים. עקב חוסר מהימנותו של קורא הכרטיסים, שגיאות הכרטיסים היו דבר שבסגרה, ולכן במאלה ימי השבעה, קוד מובנה מועוד ב厶בוד המיניג היה מזמין שגיאות ומدى נורחות כך שמעילי המחשב יכול לתקן ידנית את הבעיה, ובמהלך סופי השבעה, כאשר מפעלי המחשב לא היוโนוכחים, כל שהמבחן יכול לעשות היה לנטרש את המשימה שבה התגלו שגיאות ולהמשיך למשימה הבאה.

המיניג עבד במשך שבוע, והפק מותסכל יותר וייתר מהצורך להפעיל מחדש את התוכניות שלו עקב התקלות של קורא הכרטיסים. במהלך השנהו של לאחר מכן הוא שקד על עיבית תיקון-השגיאות, ופיתח שורה של אלגוריתמים רבי-יעצמה לטיפול בעיה. בשנת 1950 הוא פרסם את מה שידוע כ"קוד המיניג", אשר נשאר בשימוש במספר ישומים גם כיום.

צופן (קוד) המיניג – Hamming Codes היא אחת השיטות הראשונות לייצור קודים לתיקון שגיאות.

הקוד המיניג נקבע על-פי מספר סיביות הקוד, H , שאותם נרצה להוסיף לסדרת הנתונים. בקוד המיניג, אנו משדרים בולוקים באורך מרבי L , כאשר: $L = 2^H - 1$. הינו אורך הבלוק לאחר הקידוד – כולל סיביות הנוספות. ככלומר אם ברצאת להשתמש ב- $H=3$ סיביות תיקון שגיאות, נוכל לקודד עזורתן לא יותר מ- $2^{H-1} - H = 2^2 - 3 = 1$ סיביות נתוניות. סיביות המיניג ממוקמות בבלוק במקומות סידורי נקבעים על-ידי 2^H (דהיינו: 1, 2, 4, 8, וכו').



נתון למשולוח:



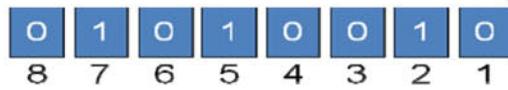
שידור:



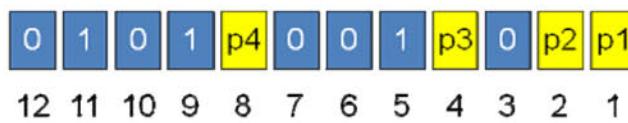
כאשר:

- p1 is even parity for 1, 3, 5, 7, 9, 11
- p2 is even parity for 2, 3, 6, 7, 10, 11
- p3 is even parity for 4, 5, 6, 7, 12
- p4 is even parity for 8, 9, 10, 11, 12

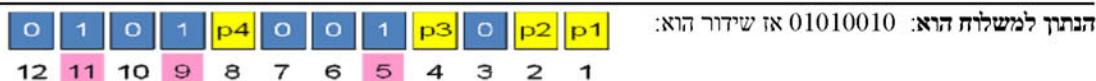
בנייה שהבנתו למשולוח הוא:



Transmitter: ◉



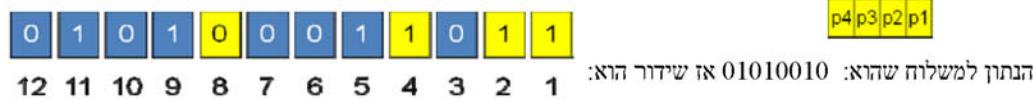
ערכון של סיביות המיניג מחושב על-ידי ביצוע פעולה XOR על ערך המספרי, המוצג בשיטה בינארית, של מקום סיביות הנתונים בעלות ערך "1" בבלוק המורחב. התוצאה המתקבלת (מספר בינארי בן 4 סיביות) היא ערך סיביות המיניג בבלוק.



$$\begin{array}{r} 5 = 0 \ 1 \ 0 \ 1 \\ 9 = 1 \ 0 \ 0 \ 1 \\ 11 = \underline{1 \ 0 \ 1 \ 1} \\ \hline 0 \ 1 \ 1 \ 1 \end{array}$$

מקומות בהם יש אחדים

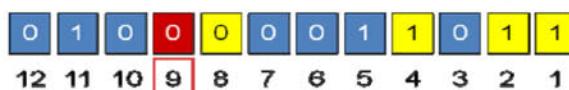
XOR



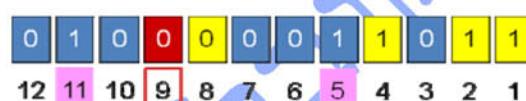
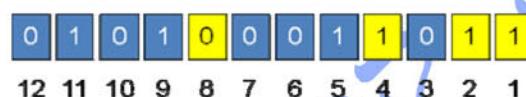
p4|p3|p2|p1

המקלט מבצע פעולה XOR על מספר המורכב מ-4 סיביות המויצג, ועל המספרים – המציגים את מקומן של הסיביות המדוע בעלות ערך "1". אם התוצאה היא אפס, הבלוק הגיע ללא שגיאות.

בכיס כנעת שנייה בסיבית מס' 9 (נכנים 0 במקום 1) ונבדוק את השפעתה. הבלוק השגוי:



דרך למציאת השגיאה:



או לצורך מציאת השגיאה:

קוד המיניג

$$\begin{array}{r} H = 0111 \\ 5 = 0101 \\ 11 = \underline{1011} \\ \hline 9 = 1001 \end{array}$$

מקומות בהם יש אחדים

מקום בו יש סיבית שגיאה

XOR

XOR

המשך קוד המיניג מתוך ויקיפדיה, האנציקלופדיה החופשית אם נסיף עוד סיביות לתיקון-שגיאות להודעה, ואם נתן לארגן שגיאות בסיביות מידע שונה שגיאה יפיקו תוצאות שונות שגיאה שונת, יהיה ניתן להוות את הביטים השגויים. בהודעה באורך 7 סיביות, ישן 7 שגיאות סיבית-בוחנת אפשריות, על כן 3 סיביות לתיקון-שגיאות יכולות פונציאלית גם לציג שאריעה שגיאה, וגם היכן היא אירעה.

המיניג לימד את שיטות הקידום והקימוט, כולל את שתיים-מתוך-חמש, והזלהה להכליל את רענוןתיהם. תחילה, הוא קבע סימונים כללים לתיאור המערכת, כולל סימון למספר סיביות המידע וסיביות לתיקון-שגיאות בכל בלוק. לדוגמה, קוד הזוגיות מכל סיבית בוחנת לכל 밀ת מידע, על כן בהנחה של מילים ASCII היו באורך 7 סיביות, המיניג תיאר את קוד הזוגיות כקוד (7,8), כיוון שככל מילת מידע הוא באורך 8 סיביות, מוחלט מהווים את המידע. באופן דומה, קוד ההישנות היה מוגדר כ(1,3) (כאשר קבוע ההישנות הוא 3). "שיעור האינפורמציה" הוא המספר השני מהולך בראשון - בקוד ההישנות, לדוגמה, שיעור האינפורמציה שווה ל-1/3.

כמו כן, המיניג שם לב לבעיות כאשר שתי סיביות או יותר מתחפכות, וכינה מצב זה "MRIAK" (כינוי מונח זה MRIAK המיניג, על שמו). עקרונית, "MRIAK המיניג" הוא מספר הסיביות המינימלי שדרוש לשנות במילת קוד וחוקית כדי לקבל מילת קוד וחוקית אחרת. קוד הזוגיות הוא בעל מרחק 2, שכן כל שתי סיביות מתחפכות אינן מתגלות. קוד ההישנות (3,1) הוא בעל מרחק 3, שכן יש זורק לשנות לפחות 3 סיביות (כולן בשלשה אחת) כדי לקבל מילת קוד וחוקית אחרת. באופן דומה, בקוד ההישנות (4,1) – כל סיבית משוכפלת 4 פעמים – יש מרחק 4, על כן שגיאה של התהפהכות שני ביטים ניתן לתיקון לגילוי.

המיניג התעניין בשתי בעיות בבת-אחת: הגדלת המרחק ככל האפשר, כאשר באותו זמן מגדילים את שיעור המידע כמו שבתhan. במהלך שנות ה-40, הוא פיתח מסגר סכימות קידוד, אשר היו שיפור דרמטי ביחס לקודים הקיימים. המפתח לכל המערכות שפיתחה בין סיביות הזוגיות. שון היי מוסגולה לבדוק תקין זו של זו, ולא רק של המידע עצמו.

תיאור תפקידן של סיביות הזוגיות בקוד המיניג הכללי הוא די פשוט:

כל הסיביות שנמצאות במקומות שונים חזקה של שתים-ממשות סיבית וזוגית. (אליה הסיביות שבמקומות 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216, 33554432, 67108864, 134217728, 268435456, 536870912, 1073741824, 2147483648, 4294967296, 8589934592, 17179869184, 34359738368, 68719476736, 137438953472, 274877906944, 549755813888, 1099511627776, 2199023255552, 4398046511104, 8796093022208, 17592186044416, 35184372088832, 70368744177664, 140737488355328, 281474976710656, 562949953421312, 112589990684264, 225179981368528, 450359962737056, 900719925474112, 180143985094824, 360287970189648, 720575940379296, 1441151880758592, 2882303761517184, 5764607523034368, 11529215046068736, 23058430092137472, 46116860184274944, 92233720368549888, 18446744073709976, 36893488147419952, 73786976294839904, 147573952589679808, 295147905179359616, 590295810358719232, 1180591620717438464, 2361183241434876928, 4722366482869753856, 9444732965739507712, 18889465931479015424, 37778931862958030848, 75557863725916061696, 15111572745823212332, 30223145491646424664, 60446290983292849328, 12089258196658569864, 24178516393317139728, 48357032786634279456, 96714065573268558912, 193428131146537117824, 386856262293074235648, 773712524586148471296, 1547425049172296942592, 3094850098344593885184, 6189700196689187770368, 12379400393378375540736, 24758800786756751081472, 49517601573513502162944, 99035203147027004325888, 198070406294054008651776, 396140812588108017303552, 792281625176216034607104, 1584563250352432069214208, 3169126500704864138428416, 6338253001409728276856832, 12676506002819456553713664, 25353012005638913107427328, 50706024011277826214854656, 10141204802255645242910932, 20282409604511290485821864, 40564819208522580971643728, 81129638417045161943287456, 16225927683409032388657412, 32451855366818064777314824, 64903710733636129554629648, 129807421467272259109259296, 259614842934544518218518592, 519229685869088536437037184, 1038459371738177072874074368, 2076918743476354145748148736, 4153837486952708291496297472, 8307674973905416582992594944, 16615349747810833165985989888, 33230699495621666331971979776, 66461398991243332663943959552, 132922797982486665327887919104, 265845595964973330655775838208, 531691191929946661311551676416, 1063382383859893322623023352832, 2126764767719786645246046705664, 4253529535439573290492093411328, 8507059070879146580984186822656, 17014118141758293161968373645312, 34028236283516586323936747290624, 68056472567033172647873494581248, 13611294513406634529574698916296, 27222589026813269059149397832592, 54445178053626538118298795665184, 108890356107253176236597911330368, 217780712214506352473195822660736, 435561424428752704946391645321472, 871122848857505409892783290642944, 1742245697715010819785566581284888, 3484491395430021639571133162569776, 696898279086004327914226632513952, 139379655817200865582845326502784, 278759311634401731165685653005568, 557518623268803462331371306011136, 1115037246537606924662742612022272, 2230074493075213849325485224044544, 4460148986150427698650970448089088, 8920297972300855397301940896178176, 17840595944601710794603881792356352, 35681191889203421589207763584712704, 71362383778406843178415527169425408, 14272476755681368635683055433885816, 28544953511362737271366110867771632, 57089857022725474542732221735543264, 114179714044500949855444443471065328, 228359428089001899710888886942130656, 456718856178003799421777773884261312, 913437712356007598843555547768522624, 1826875424712015197687111095337045248, 3653750849424030395374222190674085496, 7307501698848060790748444381348170992, 1461500339769612158148888762676341984, 2923000679539224316297777525352683968, 5846001359078448632595555050705367936, 1169200279155689726591110010140735972, 2338400558311379453182220020281471944, 4676801116622758906364440040562943888, 9353602233245517812728880081125887776, 1870720446649023562557776016225775552, 3741440893298047125115552032451551104, 7482881786596094250230774064903052208, 14965763573192188504461548129806104176, 29931527146384377008923096259612208352, 59863054292768754017846192519224416704, 11972610858553750803572384479844883408, 23945221717107501607144768959689766816, 47890443434215003214289537919379533632, 95780886868430006428579075838758667264, 191561773736860012857158151677573344528, 383123547473720025714316303355146689056, 766247094947440051428632606710293378112, 1532494189894800102857265213420586756224, 306498837978960020571453042684117351248, 61299767595792004014290608536823470496, 12259953519158400802857317107364684992, 2451990703831680160571463421472937984, 4903981407663360321142926842945875968, 9807962815326720642285853685891751936, 1961592563065440128571770737783503872, 3923185126130880257143541475567007744, 7846370252261760514287082951134015488, 1569274050452332028571416590226803096, 3138548100904664057142833180453606192, 6277096201809328114285666360907212384, 12554192403618656228571332721854246768, 25108384807237312457142665443708493536, 50216769614474624914285330887416987072, 10043353922894924982856661775833976144, 20086707845789849965713323551667952288, 40173415691579709931426647103335904576, 80346831383159419862853294206671809152, 16069366276631883972571588841334361831, 32138732553263767945143177682668732662, 64277465106527535890286355365337465324, 128554930213055071780572710730674930648, 257109860426110143561145421461349861296, 514219720852220287122290842922697725932, 102843944170444057424458168445339545184, 205687888340888114848916336886679090368, 411375776681776229697832673773358180736, 822751553363552459395665347546716361472, 164550310672710491879133069509343272352, 329100621345420983758266139018686545104, 658201242690841967516532278037373090208, 1316402445381683935331664556074745180416, 2632804890763367870663329112149490360832, 5265609781526735741326658224298980721664, 10531219563134671482653316484597614433328, 21062439126269342965306632969195228866656, 42124878252538685930613265938390457733312, 8424975650507737186122653187678091546624, 16849951301015474372245266375356182933248, 33699902602030948744490532750712365586496, 67399805204061897488981065501424731172992, 134799610408123794977962130028494462345984, 269599220816247589955924260056988924681968, 539198441632495179911848520013977849363936, 107839688326498535982369040027955578877872, 215679376652997071964738080055911555555644, 431358753305994143929476160011823111111288, 862717506611988287858952320023646222222576, 1725435013223976575778046400472924444445152, 345087002644795315155608880094584888888824, 690174005289590630311217760189169777777748, 1380348010579181260624355320378335555555596, 276069602115836252124871064075667111111192, 552139204231672504249742128151334222222384, 1104278408463345008494944256302668444444768, 2208556816926690016989888512605337688888136, 4417113633853380033979777025210675355555572, 8834227267706760067959554050421350711111144, 17668454535413520135919108008442707422222288, 3533690907082704027183821601688454044444456, 706738181416540805436764320337690888888812, 1413476362832704108673326460673581777777724, 2826952725665408217346652921347163555555548, 5653905451330816434693305842694327111111196, 11307810902616832683366116853886554555555592, 2261562180523366536673223337177311111111184, 4523124361046733073346446674354622222222368, 9046248722093466146692893348709244444444736, 180924974441869322933858669741848888888812, 361849948883738645867717339483697777777724, 723699897767477291735434678967395555555548, 1447399795535955823468683417934791111111196, 2894799591071911646937366835869582222222368, 5789599182143823293874733677739164444444736, 1157919364286764658774466755558232777777724, 2315838728573529317548933511518465555555548, 4631677457147058635097866702306931111111196, 9263354914294017270195733404613862222222368, 1852670982858034454039146680923731111111192, 3705341965716068908078293381847462222222364, 7410683931432137816156586763694924444444728, 148213678626642763323137333273894888888812, 29642735725328546664667466734778955555555456, 59285471450657093329335466739557911

במילים אחרות, סיבית זוגיות במקומות i , כאשר $2^k = n$, בדקה את הביטים אשר הסיבית k ביצוג הבינארי של המיקום שלהם שווה ל-1. במקרה, ביצוג ה-13, או 1101 ביצוג בינארי, נבדקת על ידי הסיבית 1 ($=0100$) ו-4 ($=1000$).

יעילות התקורה של קוד המנג

נמצא קודם מה מספר הסיביות המינימלי שיש להוסיף למילת מידע כדי להבטיח שבין שנייה בסיבית בודדת, ללא תלות בקוד התקון: נסמן את מספר הסיביות הנדרשת ב- t , ואת מספר הסיביות של המידע המקורי ב- n . על כן, אורך מילת הקוד המתבלת יהיה $n+t$. קיימות 2^n מיליםBINARIES שונות באורך n . כל מילה שכזו מקודדים במילה באורך $n+t$. עתה נשים לב שבדי לוחות שגיאה, אם נשנה את מילת הקוד בסיבית אחת כלשהי, עדין צריכה להתקבל מילת המידע המקורי. לכן בעצם לכל מילת מידע $n+t+1$ מילים שונת באורך $n+t$ (מילת הקוד וכל ריציאה שלה בשינוי סיבית בודדת). על כן מבחינה מתמטית חיב להתקים: $2^{n+t} \leq 2^n \cdot 2^{t+1}$.

כלומר, מספר מילות הקוד והוריאציות עליהן חיב להיות לפחות מאותו גודל כמו מספר מילות המידע, כדי שייהי ניתן לקוד כל מילת מידע. מיפויו אי השווון הזה אנו מקבלים: $n+t+1 \leq 2^{t+1}$

זה אומר חסם תחthon של קוד לתיקון שגיאה של סיבית בודדת חיב לקיים. נראה שקווד המנג מקיים את החסם המינימלי, ככלומר קווד המנג מקיים: $2^t + t + 1 = 2^{t+1}$

בקוד המנג מושפעים סיבית זוגיות על כל סיבית ביצוג הבינארי של מקום הסיביות. עם t ספרותBINARIES אפשר ליצג כל מספר עשרוני עד $-1 - 2^t$. מכאן שבזורה t סיבית זוגיות של קווד המנג אנו יכולים לקוד מילת מידע עד אורך t ($2^t - 1$) (כיוון שגם סיביות הזוגיות תופסות מקום במלת הקוד, הרישוט תמיד שמורות להן). עבור ה- t המקסימלי בהינתן t , מתקיים: $2^t - t - 1 = n$

לקחנו את ה- t המקסימלי לשם פשטות החישוב. אם היינו לוקחים כל t בתוכם האפשרי עברו t כלשהו, היינו מקבלים תוצאה דומה, אך היינו נאלצים לעבד עם פונקציית הערך השלם (כיון שאפשר להשתמש "בשברי" סיביות יתרות) על אי-שוויון המתאר את החסם. בכל מקרה אפשר (ובחילק מהקרים אף נהוג) לחתה כל הוחעה באורך הקטן מ- t המקסימלי, ולחותף לה אפסים לטופה כדי לקבל הductה באורך מקסימלי (כדי לשים לב שואוף פועלה כזה לא משנה אף סיבית מהמידע או הזוגיות).

נזכיר זאת בא-השוון של החסם: $2^t \leq 2^t \quad (2^t - t - 1) + t + 1 \leq 2^t \quad \text{כלומר קיבלנו} \quad 2^t = 2^t$

ומכאן, שעבור קווד המנג אכן מתקיים: $n + t + 1 = 2^t$ על כן, ראיינו כי קווד המנג הוא אופטימי מבחינת סיביות יתרות הדורות לזרוך תיקון שגיאה בסיבית בודדת.

דוגמה לשימוש בקווד המנג (11,7)

נסתכל על מילת המידע "0110101" (באורך 7 סיביות, בקרה משמאלי למן). לצורך הדגמה של קווד המנג, צורת חישבו והשימוש בו כדי לזהות שגיאות. ראו את הטבלה שלהלן. הסימן Δ מציין סיביות מידע, ו- Ξ מציין סיביות זוגיות. תחילת מציבים את סיביות המידע במקומות המיועדים להם (המקומות שמורים לסייעות הזוגיות), וסיביות הזוגיות מחושבות על פי המקובל (מספר אי זוגי של סיביות השווות ל-1 ית� סיבית הזוגות ל-1 גם כן).

d_7	d_6	d_5	p_4	d_4	d_3	d_2	p_3	d_1	p_2	p_1
1	0	1		0	1	1		0		
1		1		0		1		0		p_1
1	0			0	1			0	0	p_2
							0	1	1	p_3
1	0	1	0							p_4
1	0	1	0	0	1	1	0	0	0	1

הישוב סיביות הזוגיות של קווד המנג

밀ת הקוד המתבלת (עם סיביות הזוגיות) היא "10001100101". עתה נניח, לשם הדוגמה, כי הסיבית האחרון מתבלת באופן משובש, ככלומר הופכת ל-0, והמילה המשודרת היא "10001100100". כאשר אנו לנתח את המילה המתבלת, נסמן ב-1 כל סיבית זוגיות שגיאה (ביחות לחישוב זוגיות של הסיביות שהיא בודקת אותן).

	d_7	d_6	d_5	p_4	d_4	d_3	d_2	p_3	d_1	p_2	p_1	סיבית זוגיות	בדיקה הזוגות	밀ת המידע שהתקבלה:	
					1	0	0	1	0	0	1	1	0	0	10001100100
1					0	1	0		1	0	1			p_1	
1					0	0		0	1		0	0		p_2	
0								0	1	1	0			p_3	
1					0	0	1	0		0	1	0		p_4	

בדיקות סיביות הזוגיות (סיביות שגויות מודגשות)

השלב האחרון הוא לחשב את הערך המספרי של סיביות הזוגיות (ערך כל סיבית זוגיות נקבע על פי מיקומה). הערך המספרי של סיביות הזוגיות המוחשנות בבדיקה הוא 11, דבר שמצוין על קר שסתמיות ה-11 במלת המידע (כולל סיביות הזוגיות) היא השגיאה, ויש להפוך את ערכה.

	p_1	p_2	p_3	p_4	
בינארי	1	1	0	1	
$\Sigma = 11$	1	2		8	

כאשר נפרק את הסיבית ה-11, נקבל חזרה את המילה המקורית ששוחרה - "10001100101". אם נסיר את סיביות הזוגיות של קוד המינג, נזהור למלילה המקורית 0110101.

יש לשים לב כי אם רף סיבית זוגיות אחת נכשלת, אז בוחנות היא הסיבית השגויה (ואפשר לבדוק זאת גם לפני שיטת הבדיקה לעיל). בסום, נניח כי שתי סיביות התחלפו, במדויקות "x" ו"y". אם "x" ו"y" מוגנים על ידי אותה סיביות זוגיות, הרי שסיבית הזוגיות זו לא תגלה את השגיאה בשניהם. אולם, לפחות סיבית זוגיות אחת מתגלת שגויה, כיוון ש $x \neq y$ והם חיביכים להיות שונים לפחות במקרה אחד (כידוע), קיימת הצגה ביבינארית יחידה לכל מספר, וכל מספר מוצג על ידי הצגה אחרת). על כן קוד המינג מזהה שקיימת שגיאה, אולם הוא אינו יכול להבדיל שגיאת זו משגיאות של סיבית בודדת, ובפרט לתת אינדיקציה בוגרנו על מוקם הנacenן שבו אירעה השגיאה.

(עריכה) קוד המינג (7,4)

כימ, "קוד המינג" מתייחס למעשא לקוד המינג הספציפי (7,4), אשר הרוצג לראשונה בשנת 1950. קוד המינג זה מוסף 3 סיביות זוגיות על כל 4 סיביות מידע של ההזדעה. בדומה לקוד המינג הכללי, **האלגוריתם** של קוד המינג (7,4) מסוגל לתקן כל שגיאה בסיבית בודדת, ולהזות כל שגיאה בסיבית בהזדעת או בשתי סיביות. דבר זה אומר שעבורו שדריך שידור שבמקרה דרכך לא קוראים **פרצי שגאה**, קוד המינג (7,4) אפקטיבי למדי (שכן הסבירות לשתי שגיאות ב-7 סיביות היא נמוכה מאד, והערעור ציריך להיות רועש למדי כדי שמצב כזה יקרה).

על מנת להציג את אפשרות התקיןנו ניוט להשתמש בטכניקה הבאה: בחלק את המילים (כעת מילה היא רצף מקודד בקוד המינג של 7 אותיות)ishereshonu לקבוזות בננות 7 מיללים. כעת במקומות לשדר מילה אחר מילה, נשדר בכל פעם 7 סיביות ממיללים שונות. כך, אם יש פרץ שגאה, שבדרך הורס מספר גדול של סיביות, ניתן יהיה לתקן, כי ככל מילה תהרס רק סיבית אחת.

(עריכה) מטריצות המינג

באופן מעשי, קוד המינג משתמשים במכלול **מטריצות** מיוחדות הקרויה "מטריצות המינג" כדי למש את הפעולות של ייצור הקוד ובדיקה הזגויות. עבור קוד המינג (7,4), משתמשים בשתי מטריצות הקשורות זו לזו - מטריצת יצרת הקוד **G** ומטריצת בדיקת הזוגיות **H**:

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad G := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

ארבע השורות הראשונות של **G** מייצגות את **מטריצת הייחידה** I_4 . כאשר שלושת השורות האחרונות מהוות מיפוי של 3 סיביות המידיע ל-3 סיביות הזוגיות. וקטור הפעודה ב**G** מהווים בסיס **לגרען** של **H**. מטריצת הייחידה מעבירה את וקטור המידע אל מרכיב המכפלת (מטריצת הייחידה מהו **איבר ייחידה** ביחס למכפלה מטריצות). בזיגז לאמה שנאמר לעיל,igan סיביות הזוגיות מופיעות בסוף מילת הקוד (סדרן סיביות הזוגיות כפי שהציגו מוקדם נועד לנוחיות ההציג וההבנה, ואין לו ממשמעות עקרונית בקוד עצמו).

באופן דומה, שלוש העמודות האחרונות של **H** מייצגות את מטריצת הזאות I_3 , כאשר ארבע העמודות הראשונות מייצגות את המיפוי (זהזה למיפוי של מטריצה **G**) בין סיביות המידע לסיביות הזוגיות.

לאורך ביצוע האלגוריתם של ייצור הקוד והבדיקה, מייצגים את מילת המידע בתור וקטור עמו. לדוגמה, אם מילת המידע שלנו היא "1011", נקבל את הווקטור:

$$P = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

קידוד המידע

נניח כי ברצוננו לשדר את המידע מעל **ערן רועש**. על כן, ניקח את המכפלת של **G** ו-**P**, כאשר המכפלת מתבצעת במודולו-2, ונקבל את מילת הקוד α שיש לשדר (נשים לב שמילת הקוד אכן באורך 7 סיביות, וסיביות הזוגיות מופיעות בסוף המילה):

$$G \cdot P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = x$$

בדיקה זוגיות

אם שום שגיאה לא אירעה במהלך השידור, הרי שמילת הקוד המתבקשת r זהה למילת הקוד המשוחררת α : $X = r$. כדי לראות אם אירע שיבוש במילת הקוד, המქבל צריך להכפיל את **H** עם r . ביצוע המכפלת הוא (שוב במודולו-2) מביא את התוצאות:

$$H \cdot r = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

כיוון שקיבלו את וקטור האפס, המקבל יכול להסיק כי שם שגיאה לא אירעה. וקטור האפס מציין שלא ארבע שגיאות כיוון ששאשר וקטור המידע מוכפל עם G . הוקטור המתפרק מהמקפלת מהוות צירוף לינארי של הבסיס של H . לכן, כל עדיל לא מתחבא שום שגיאו בינו השינויים \mathbf{z} , משיר להזיהות בגרעין של H . והמקפלת המשנית להציג את וקטור האפס.

תיקון שגיאות

על כן, הביטוי $\text{ה}^{\text{ל}}$ מציין כי אירעה שגיאה בסיבית ה- i של המידע.

Hr = **H(x + ei)** = **Hx + Hei**. ה-**H** א-**x** ו-**e** ו-**H** ו-**e** ו-**H**.

כיוון שאנו מודע המשדר, הוא לא שגיאות, ולכן תוצאות המכפלת של H ו- α הרא אפס (כפי שראינו קודם). לכן:

$$\mathbf{H}\mathbf{x} + \mathbf{H}\mathbf{e}_i = \mathbf{0} + \mathbf{H}\mathbf{e}_i = \mathbf{H}\mathbf{e}_i$$

הכפלה **H** עם וקטור היחידה ה-**z** מוגבה בתרזאה את העמודה ה-**x** של **H**, ועל כן אנו יודעים כי השגיאה ארירעה בסיבית מספר סידורה הורא כמו העמודה שקיבלונו, ככלומר שהסיבית השגיאה היא הסיבית ה-**z**, ועל כן נוכל לתקן את השגיאה בעזרת מידע זה.

כשנברצע את המכפלת נקבל:

לדוגמה, **בנייה כי המידע המתkeletal הרוא:**

$$\mathbf{Hr} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\mathbf{r} = \mathbf{x} + \mathbf{e}_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

אשר מותאים לעמודה השניה לעמודה השניה של **H**. על כן, השגיאה אירעה בסיבית הנטיה, ולכן ניתן לתקן אותה כראוי בנסיבות הנטיה. פרט לכך, ניתן להשתמש בקוד המיגג כדי לזהות שגיאות בסיבית בודדת או בשתי סיביות, פשוט על ידי ביחסת המכפלה של **H** - קיימת שגיאה ואיתם המכפלה אינה שווה לוקטור האפס. עם זאת, כפי שנאמר, בלתי אפשר להבדיל בין שגיאות בסיבית בודדת לשגיאות בשתי סיביות בשימוש קוד המיגג בלבד.

קוד המיגג עם סיבית זוגיות נספת
ניתן להשתמש בסיבית זוגיות נוספת, כדי לשרף את יכולות הזיהוי שגאה של קוד המיגג. סיבית הזוגיות הנוספת בודקת את כל הסיביות של מילת הקוד הנוצרת בקוד המיגג (כלומר היא בודקת את סיביות המידע ואת סיביות הזוגיות של המיגג). פעולה כזו מגילה את מרחק המיגג מ-4.
בעקבות כך, ניתן להזות את כל השגיאות בסיבית בודדת, בשתי סיביות או בשלוש סיביות. כמו כן, ניתן להבדיל בין שניות בשתי סיביות לשגיאות בסיבית בחדמת או שלוש סיביות.

על כן, ניתן לפחות את השגיאות בשתי סיבות, ולטמןן כלא בגיןות לתיקון (ובכך לבקש שידור מחדש): כאשר מוצעים תיקון שגיאה, אם מוחים שגיאה בסיבית הוגייתה הנוספת וגם קוד המיגן מצין שישנה שגיאה, שגיאה זו ניתן להתקן. לעומת זאת, כאשר לא מוחים שגיאה בסיבית הוגיות, אולם קוד המיגן מזהה שקיימת שגיאה, ניתן להנעה כי הדבר נובע משגיאה בשתי סיבות, אולם לא ניתן לדעת בוודאות באיזה סיבות שגיאה אירעה.

קוד שתים-מטרד-חמש

בשנות ה-40 של המאה ה-20, מudyבדות בלב השתמשו בדק מתחכם מעט יותר הקרויה קוד שטיים-מטור-המש. קוד זה הבטיח כי כל בлок של חמש סיביות יכול לבדוק שתי סיביות עם הערך 1. המחשב יכול לוחות שארעה שגיאה, אם לא היה בדיקות שתי סיביות עם הערך 1 בכל בлок. עם זאת, גם קוד זה היה מסוגל לוחות בוודאות רק שגיאות בסיבית בודדת; אם סיבית אחת התהפקה ל-0 ואחרות התהפקה ל-1 באותה הבלוק, הכלל של שתיים מטור חמיש היה בשאר תקף, והשגיאה לא הייתה מוגלה.

הישברת

קו"ד נפרק נסרך באותו הזמן ביצוע שכפל של כל סיבית מידע מספר קבוע של פעמים, במטרה להבטיח שהוא ישורט באופן תקין. למשל, אם הסביבה הנשלהת היא 1, וקובע ההשנות המשורט היא "111". אם שלושת הביטים המתקבלים אינם והם, הרי שבוחנות אירעה שגיאה. אם ערכן השידור נקי מספיק מהפרעות, הרי שנטען לתגיה כי באופן סביר רק סיבית אחת לכל הייתור תשתנה בכל שלשה. על כן, 001, 010, וכן 100 הצביעו על כך ששודר 0, ואילו 110, 101, וכן 011 הצביעו על כך ששודר 1, על פי עקרון הרוב כאשר כל סיבית בשלשה מהוות "קול הצעה" בתגובה לערוכה המקורי של הסביבה המשוחררת.

אלה, אולם לא ניתן לזהות את כל השגיאות הכלולות שיבוש ב-3 סיבות.
אולם לא הינו מסוגל לתקן אותן בהינתן שגיאות בהודעה המשודרת נקראה קוד לתיקון שגיאות, אולם קודים כאלה אינן מסוגלים לתקן את כל השגיאות. בדוגמה שלנו ("שידור 1 כ"11"), אם בעקבות ריש עירוני שת סיוביית בשלשה היו מתחלה והוא מתබל לדוגמה "001", הרי שהמערכת לא הדימה מהזה את השגיאה כראוי, אף מסיקה באופן שני כי הסיבית המקורית הייתה 0. אם הינו מגדילים את קבוע ההישנות ל-4 (כלומר הינו משכפלים כל סיבית 4 פעם), הינו מסוגלים לזהות את כל השגיאות הכלולות שיבוש של לכל היותר 2 סיבות, אולם לא הינו מסוגל לתקן אותן (כי או שהיא נוצר מזב של "תיקו" בערכיו הסיביות המשודרת); אם קבוע ההישנות הוא 5, ניתן לתקן שגיאות

אף על הוכחת לתקן שגייאות עברו קבעוי הישנות הינו לא עיל באופן מובהק, שכן הוא מקטין את קצב העברה פי קבעו הישנות, על כן היעילות של הקוד יורדת דרסטית ככל שהוא מגדים את קבוע היחסנות במטרה להזות ולתקן שגייאות רבות יותר, והופך את הקוד ללא מעשי במערכות זמן אמת.

סיכום כל הנתונים - Internet checksum

משרה: גילי שגיאות (כדוגמה סיביות הפעולה) מקטע של נתונים משודרים. השיטה היא לשכבות הוהבל בלבד (transport layer).

בצד השולחן:

- מתייחס לתוך המקטע כסדרה רציפה של מספרים שלמים בעלי 16 סיביות.
- בדיקת הסיכום: סכום (סכום על פי משלים ל-1) של ערכי המקטע.
- המערכת המשדרת מוסיפה את ערך הסיכום בשדה של ביקורת UDP.

בצד המקלט:

- מחשב את סכום הביקורת של המקטע שהתקבל.
- משווה בין הערך שהיחס בין תוכן השדה UDP שהתקבל.
- אם לא שוים או קיימת שגיאה - NO - error detected.
- עם שווים או מקיימים שהגען הגיע שלם (אבל אולי יתגנו שגיאות).
- YES - no error detected. But maybe errors nonetheless?

- משתמש באורך $k = 16$ or 32 bits כסכום לביקורת:
- מתחילה אוחכל k bits לאפס.
- מוסיף כל בלוק של k סיביות מתוך המקטע לאורך הסיכומיים, כולל הוספה סיביות הנשא (carry).
- מוסיף את התוצאה ה- k bits (append) למבנה המקטע.
- המקלט מחשב את הסכום בזירה דומה, ומציע השוואה עם סכום הביקורת כפי שהוא הגיע.

דוגמת נתון לשידור: כותרת שלום אולם.

h	e	l	l	o	w	o	r	l	d	.	
48	65	6C	6C	6F	20	77	6F	72	6C	64	2E

חישוב הסיכומיים - Checksum calculation

$$4865 + 6C6C + 6F20 + 776F + 726C + 642E = 271FA$$

$$71FA + 2 = 71FC$$

carry check sum

SOH Data: "hello world." 71FC EOT

יתרונות / חסרונות:

- קל לחישוב.
- גודל קטן, 8 או 16 סיביות (1 or 2 octets overhead).
- חלק מהשגיאות לא ניתנות לגילוי, כמו בדוגמה שבמבחן:

0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
total	7	total	7

בדיקה יתרות מתחזרית [CRC] מתוק ויקיפדיה, האנציקלופדיה החופשית

בדיקה יתרות מתחזרית (או מעגלית) (באנגלית: redundancy check Cyclic, או בקיצור CRC) היא סוג של קוד לאיתור שגיאות או פונקציית גיבוב (hash function) המשמשת לאיתור שגיאות בהעברת נתונים.

לפני העברת המידע מחושב CRC ומתווסף למידע המועבר. לאחר העברת המידע, הצד מקבל מאשר באמצעות CRC שהמידע הועבר ללא שינויים.

השימוש ב-CRC נפוץ במיוחד בשל קלות המימוש שלו בחומרה בינארית, קלות החישוב המתמטית שלו, ובמיוחד הייעילות שלו בגילוי שגיאות נפוצות הנבעות כתוצאה מעורורי תקשורת רועשים.

CRC אופן הפעולה של הפרטוקול

פרוטוקול CRC מבוסס על האיזומורפיים שבין וקטוריים לפולינומים, כך שמשתיכלים על כל וקטור באורך n כפולינום שמקדשו הם קואורדינאטים הוווקטוריים.

פרוטוקול CRC משתמש בפולינום המוגדר בפולינום יוצר מדרגה r .
סוגים שונים של **CRC** משמשים בפולינומים יוצרים שונים.

בהתאם לוגון CRC מוגדרת כפונקציית שילוב בין הוראות CRC ו-[הוראות ביניים](#), עלינו לבצע את הפעולות הבאות:

- גנרי 2 אפסים מימין להגדעה.
 - בחלק בפוליטום (חורך שימוש בחילוק של השדה מחוזו 2) נחסר את השארית חורך שימוש ב-אפס במקום בחיסור רגיל.
 - בקרה את התוצאה שקיבלנו מימין להגדעה האנורית וגעשלה.

כמו בכל קידוד Checksum. הzd המקביל ייבצע את שלבים 1 ו-2 והוא ש-z הביטים האחוריים שבסלחו זהם לתרזאה שהתקבלה.

יכולת לגילוי של טעות (שגיאה)

CRC יכול, תוך שימוש בפוליגומרים (רבו איברים), לגלוות:

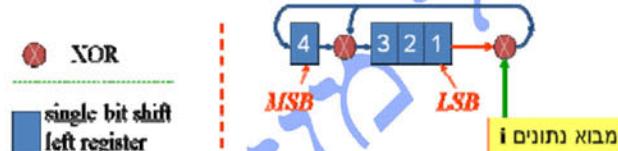
- כל השגיאות של סבירות בודדות.
 - כל השגיאות של זוגות סבירות.
 - כל כמהות זוגית של השגיאות.
 - כל חבילת שגיאות בתנאי שאורך זה הרבה יותר מאשר שגיאות.
 - רוב הבעיות גחלות של שגיאות.
 - מספר שגיאות אנכיות שישית ועוד.
 - תוך הפנה לשגרוב השגיאות הנו דוממים.

בדיקות יתרות מתחזורת

בשיטה CRC תור הבדיקה להבלוק של סיביות נתונים נוצר באג'ר ההזהה (shift register) עם משוב, אשר בו עוברות סיביות הנתונים באופן מהזורי.

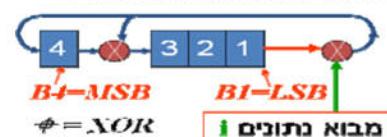
תהליך זה גורם לכם שתו הבדיקה הינו פונקציה מורכבת של סיביות הנתונים.

להרחיבת השיטה נתבונן בדוגמה הבאה. נבחר אוגר הוזה הכלול 4 סיביות, כמפורט באירור:

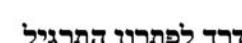


בכל יחידת זמן זותם הסבירות לפאי סטטוני החיצים באורו. בדוגמה שלנו נסמן ב- (n) את ערך הסבירות ה-k-ית באורו בזמן t. כמו כן, נסמן ב- (n)i את היחס מרוגז ברגע t. אנו רואים ש:

$$\begin{aligned} b_1(n) &= b_2(n-1) \\ b_2(n) &= b_3(n-1) \\ b_3(n) &= b_4(n-1) \oplus i(n) \oplus b_1(n-1) \\ b_4(n) &= b_1(n-1) \oplus i(n) \end{aligned}$$



בנניה שמצבו התחלה של האוגר הינו 0,0000, b1(0) = b2(0) = b3(0) = b4(0) = 0, כלומר: אם שתי הסיבוטות הראשונות הינם 11, הרי לאחר ייחידת זמן אחד ערכיו הסיבוטיים באוגר הינם 1100, ומאז אוגר אחר שמייחדתו נועזיה 1010.



$$\begin{aligned} b_1(0) &= 0 \\ b_2(0) &= 0 \\ b_3(0) &= 0 \\ b_4(0) &= 0 \end{aligned}$$



$$\begin{aligned} b1(1) &= b2(0) = 0 \\ b2(1) &= b3(0) = 0 \\ b3(1) &= b4(0) \neq i(n) \neq b1(0) = 0 \neq 1 \neq 0 = 1 \\ b4(1) &= b1(n-1) \neq i(n) = 0 \neq 1 = 1 \end{aligned}$$



$$\begin{aligned} b1(2) &= b2(1) = 0 \\ b2(2) &= b3(1) = 1 \\ b3(2) &= b4(1) \neq i(n) \neq b1(1) = 1 \neq 1 \neq 0 = 0 \\ b4(2) &= b1(1) \neq i(n) = 0 \neq 1 = 1 \end{aligned}$$



CRC computation - חישוב מתמטי

Uses shift and XOR registers to simulate long division, mod 2.

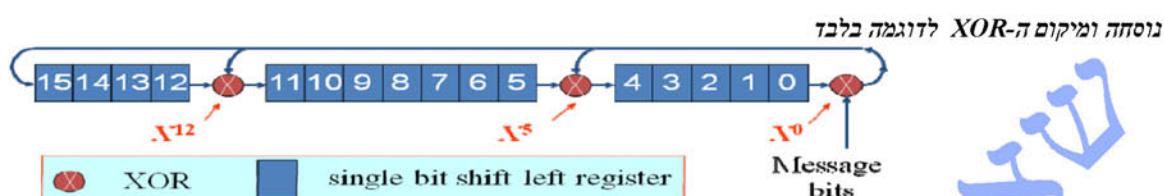
Input all message bits as shown.

Sender: Contents of complete register when message finished is CRC field.

Receiver: Contents of complete register when message finished should be 0.

Benefit: can be done quickly with hardware

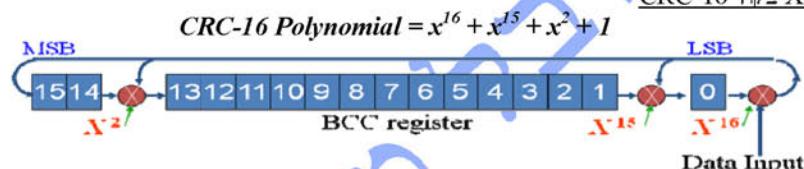
Example: $k = 16$ bit CRC, $P = X^{16} + X^{12} + X^5 + 1$



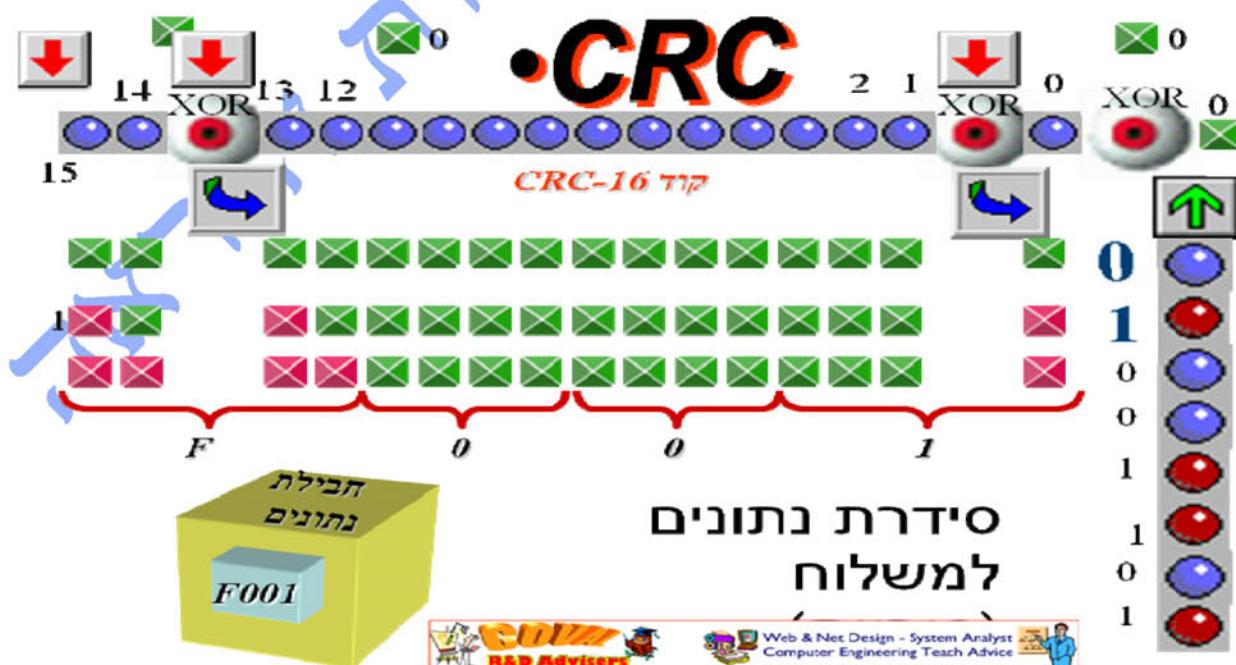
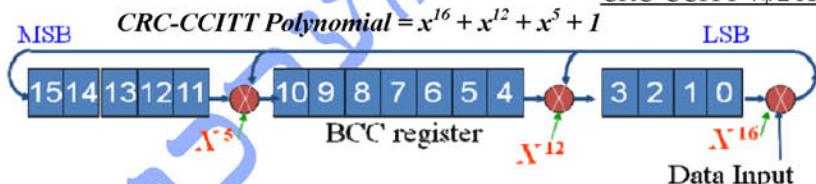
תאפשר האוגר לאחר מעבר סדרת הנתונים דרכו הינהתו המשלה למשדר, לאחר שידור סיביות הנתונים. המקלט מעביר את סדרת הנתונים המשודרת דרך אותו סוג של אוגר, ומשווה אתתו הבדיקה ששוחרר לתוכאה שהתקבלת אצל. אם התווים אינם זהים, הלה שגיאה בшибורה.

באופן כללי, גודלתו הבדיקה (או גודל האוגר) קובע את יכולת הבדיקה לנילוחות שגיאות. ככל שתו הבדיקה ארוך יותר, אנו משדרים בעצם מספר רב יותר של סיביות בבדיקה. ההסתברות שלא נגלה שגיאה הולכת וקטנה.

נוסחה ומיוקם ה-XOR בקוד CRC-16



נוסחה ומיוקם ה-XOR בקוד CRC-CCITT



עדכון: יום שלישי 10 פברואר 2009 - ט"ז שבט תשס"ט - קובץ שמירה: Error Detection Protocols.doc