

אלף - בית בבראיל

⠠⠠⠠⠠⠠⠠⠠⠠

א	ב	ב	ג	ד	ה	ו	ז	חולם חסר	ט
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
קבוץ	ז	ח	ט	י	יחידק	כ	כ	ל	מ
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
נ	ס	ע	פ	פ	צ	ק	ר	ש	ש
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠

סימני-פיסוק

⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
סימן מחיקה	,	:	:	.	?	!	{	}	"
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
סימן מספר	-	-	...	* *					
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠				

⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠

⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠

⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠

⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠
⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠	⠠⠠

צופנים בינאריים

מאת : פרופ' מ. ברוקהיימר
תרגום : אורי אמיתי ואבי זכטר

הקדמה

שימוש בצופנים נעשה כדי להעביר הודעות שלא בדרך הרגילה. לדוגמא, בצופן מורס מיוצגות אותיות האלף-בית על-ידי שילוב של נקודות וקווים (סיגנלים ארוכים וקצרים). עובד הטלגרף מעביר הודעה על-ידי הפיכת האותיות בהודעה לצירופים מתאימים של נקודות וקווים. צופן המורס אינו נמצא בשימוש רב כיום אך הוא משמש דוגמא לצופן בינארי, כלומר הוא בנוי כולו משני סימנים בסיסיים בלבד. במאמר זה נתאר שני צופנים בינאריים הנמצאים בשימוש רב כיום.

ברייל

השיטה הראשונה היא שיטת האלף-בית של ברייל עבור עוורים. הגירסה העברית של שיטת ברייל מוצגת בדף השער של מאמר זה. כל אות (מספר, נקודה, סימן קריאה, וכו') מיוצגת בדף ברייל על-ידי מלבן, אשר בתוכו נמצאות שש "נקודות". כל אחת משש הנקודות יכולה להיות בולטת מעל משטח הנייר. לדוגמא האות ה' מוצגת על-ידי מבנה



כאשר הנקודות הגסות על דף ברייל אמיתי יהיו בליטות והנקודות העדינות יהיו חלק ממשטח הנייר. הקורא העוור מעביר אצבעותיו על פני דף הברייל. הוא חש בצורת הבליטות וזה מאפשר לו לקרוא.

זהו צופן בינארי: שני הסימנים הבסיסיים הם הבליטה, או העדר בליטה, וצורת המלבן בעל ששה סימנים כאלה מייצגת אות אחת רגילה.

כמה צירופים ניתן ליצור במלבן כזה? נתבונן בנקודות המלבן בסדר מסויים. לנקודה הראשונה שתי אפשרויות: ● או •

בלי תלות בנקודה הראשונה יש גם לנקודה השנייה שתי אפשרויות; ביחד יש לנו $2 \times 2 = 2^2$ אפשרויות:

● • ; ● ● ; • ● ; • •

עם כל אחת מארבע צורות אלה, הנקודה השלישית יכולה אף היא להיות ● או • לכן יהיו לנו $2^2 \times 2 = 2^3$ אפשרויות לגבי 3 הנקודות, וכך הלאה. ברור אפוא שקיימות $2^6 = 64$ אפשרויות לסידור המלבן.

קיימת בעיה קטנה: אחד מתוך 64 הצירופים אינו נותן כל מידע לקורא העוור: הוא אינו יכול להרגיש בצירוף זה. כלומר קיימות 63 אפשרויות שונות לסידור המלבן. האם די בכך? הבה נראה מהם הצרכים שלנו. עבור האלף-בית העברי אנו זקוקים ל-22 אותיות בלבד ועוד שש תנועות. לאור מכן יש להוסיף עשר ספרות של השיטה העשרונית, סימני הפסיק, המרכאות וכו'. עתה יש להוסיף את הסימנים המתמטיים הפשוטים, לפחות את אלה של שיוון ופעולות חשבון. אם לא נוסיף את האלף-בית הלטיני נשאר מוגבלים מאוד באפשרויותינו ובזאת כבר עברנו את 63 האפשרויות שלרשותנו.

במבט ראשון נראה כאילו אנו צריכים יותר מאשר שש נקודות, אולם אנחנו יכולים להיות הרבה יותר חסכוניים בשימוש בצורות. לדוגמא, אנחנו יכולים להציג את עשר הספרות העשרוניות בעזרת אותם סימני אותיות ולאודיהן יבוא סימן ברייל מיוחד. סימן זה מבהיר לקורא העוור שלפניו מספר ולא אות. (ראה דף שער). אפשר גם להשתמש בהרכבת מלבנים כדי לייצג אינפורמציה מסויימת. ראה לדוגמא, הצגת מספר 10 בכתב ברייל.

קטע ביניים

הרבה מכשירים ומערכות סביבנו הם ביסודם בינאריים. אורות אחוריים של מכונית מהווים דוגמא נוספת למערכת הפועלת בעזרת צופן בינארי: מלבד השימוש המקובל באורות אלה, הוסיפו לאחרונה "צופן אור" והוא הפעלת שני אורות האיתות בבת אחת. צופן אור זה פירושו שהמכונית נעצרה בגלל קלקול כלשהו; במלים אחרות אלה הן אותות של אזהרה. באופן תיאורטי ניתן עם ארבעה אורות אחוריים לבנות $15 = 2^4 - 1$ הודעות שונות.

צופן המינג (The Hamming Code)

(א) הקדמה

הצופן הבינארי הבא אותו נתאר, מהווה הרבה יותר מאשר מערכת הצפנה בלבד, כפי שנראה להלן.

לכולם מוכר הרעיון המונח ביסוד המחשב האלקטרוני. באופן כללי עובר המחשב על-ידי פולסים קצרים של זרם חשמלי. יש רק שתי אפשרויות: פולס או העדר פולס, המייצגים בדרך כלל 1 ו-0. סוגים שונים של מכונות אלקטרוניות פועלים במערכת בינארית זו. אנו נתרכז במכונה המשמשת להעברת הודעות.

הבה נניח כי שש עשרה האותיות הראשונות של האלף-בית העברי מיוצגות, בהתאמה, על-ידי 16 המספרים הבינאריים בעלי ארבע ספרות:

0001, 0010, 0011 וכו'.

אין, כמובן, כל משמעות מספרית לאפסים שבצד שמאל של המספרים, אולם יש להם משמעות רבה בצופן משום שבשעת קריאת הצופן אנו יודעים שכל האותיות מיוצגות על-ידי מספרים בעלי אורך שווה (4 ספרות).

לדוגמא: 111010101010

אפשר לפענח רק בצורה אחת: יין.

(ב) שגיאות

מה יקרה כאשר שולח ההודעה טועה: הוא משדר 0 במקום 1 או להיפך. למשל, הוא עלול לשדר יין כ- 111010101011, ואז תפוענח המילה כ"כין" - מילה חסרת משמעות.

כדי להימנע משגיאות כאלו, פיתחו דרכים שעיקרן הכנסת ספרות ביקורת לשדר. נתבונן תחילה בדוגמא פשוטה. במקום לשדר 4 ספרות לכל אות נשדר 5. הספרה החמישית תיבחר כך שהספרה 1 תופיע בקבוצה בת 5 הספרות, מספר זוגי של פעמים. (הספרה החמישית היא הספרה הימנית, משום שאת המספרים עצמם אנו קוראים, כמו תמיד, משמאל לימין). בשיטה זו המלה "יין" תשודר כך:

111011010010100

ספרות הביקורת מודגשות על-ידי קו. בהנחת השגיאה לעיל, השדר השגוי יראה

111011010010110

כך:

אולם הפעם קולט ההודעה יבחין מיד כי הקבוצה האחרונה של חמש ספרות כוללת שגיאה כי הספרה 1 מופיעה מספר אי-זוגי של פעמים. ואז, עם קצת מזל, יוכל לתקן את השגיאה בעזרת התוכן של ההודעה כולה. למעשה אין צורך להמתין עד שקולט ההודעה יבדוק את השרד בעצמו. ניתן לבנות את המכונה כך שהיא תבדוק באופן אוטומטי ותתריע על השגיאה על-ידי עצירה או על-ידי הדפסת הודעת שגיאה מתאימה.

לבדיקה זו ישנן שלוש מגבלות עיקריות:

- (1) אם נפלזו שתי שגיאות בקבוצה אחת של 5 ספרות, לא יתגלה הדבר בבדיקה.
 - (2) השגיאה יכולה להיות בבדיקה עצמה ואז עלול להגרם בזבז זמן.
 - (3) הבדיקה מגלה את עובדת היות השגיאה אך לא את מקומה. השאלה באיזו מחמש הספרות נפלה טעות נשארת ענין לניחוש אינטליגנטי.
- קשה להתגבר בקלות על כל המגבלות הללו. ראשית נסכים לפטר את העובד המבצע יותר משגיאה אחת באות אחת (1) ונתרכז בתיאור שיטה להתגבר על מגבלות (2) ו-(3).

(ג) גילוי שגיאות ומיקומן

ספרת ביקורת בודדת:

הבה נפתח שוב עם אות בודדת המוצפנת על-ידי מספר בינארי בן ארבע ספרות. נוסיף עתה ספרת ביקורת בודדת. ניתן לעשות זאת בדרכים רבות. לדוגמא: אנו יכולים לבחור את הספרה החמישית כך שהספרה 1 תופיע מספר זוגי של פעמים במקומות 1, 2, ו-5.

כך:

11010	יהיה	1101
10011	יהיה	1001

מה גילינו, בהתחשב בעובדה שאנו עוסקים בשגיאה אחת? אילו היתה שגיאה באחד המקומות 1, 2 או 5 היינו מגלים בבדיקה את עובדת היות השגיאה והיינו יודעים שהיא באחד המקומות הללו. אך אילו נפלה שגיאה במקומות 3 או 4 לא היינו מגלים זאת. בדיקה זו אינה טובה דיה. מסתבר שספרת ביקורת בודדת אינה מכילה מספיק אינפורמציה.

שתי ספרות ביקורת:

ומה בדבר שתי ספרות ביקורת? הסיכוי לשגיאה גדל עתה, משום שיש שש ספרות המייצגות כל אות, אך יתכן שהגדלנו גם את הסיכוי לגילוי שגיאה. ושוב אפשר לערוך את הבדיקה בדרכים רבות: לדוגמא, כך שמקומות 1, 2, ו-5 וכן מקומות 3, 4, 6 יכילו את הספרה 1 מספר זוגי של פעמים. כך נגלה באיזו קבוצה של שלוש ספרות מופיעה השגיאה. אך בכך אין שיפור רב לעומת השרד המקורי ללא ספרת ביקורת, אם נתחשב בעובדה שהגדלנו את אורכו של השרד ב-50%.

הנוכל להשתמש בצורה טובה יותר בשתי ספרות ביקורת?

הבה נעשה נסיון אחר:

בדיקה (1): במקומות 1, 2, 3 ו-5 תופיע הספרה 1 מספר זוגי של פעמים.

בדיקה (2): במקומות 2, 3, 4 ו-6 תופיע הספרה 1 מספר זוגי של פעמים.

בשדר קיימות האפשרויות הבאות:

(זכור! מרשים רק שגיאה אחת בכל אות המיוצגת על-ידי 4 ספרות ועוד שתי ספרות ביקורת)

(א) בדיקה (1) זוגי וּבדיקה (2) זוגי

(ב) בדיקה (1) אי-זוגי וּבדיקה (2) זוגי

(ג) בדיקה (1) זוגי וּבדיקה (2) אי-זוגי

(ד) בדיקה (1) אי-זוגי וּבדיקה (2) אי-זוגי

אפשרויות אלו מצביעות על מיקום השגיאה כדלקמן (בהתאמה):

(א) אין שגיאה

(ב) השגיאה מופיעה במקום 1 או 5.

(ג) השגיאה מופיעה במקום 4 או 6.

(ד) השגיאה מופיעה במקום 2 או 3.

לא רע! רווח של 50% תמורת גידול של 50% באורך השדר.

האם נוכל לשפר את השיטה עוד יותר? מחשבה מועטה תשכנע אותנו שלא נוכל לעשות כן. מאחר ויש לנו שתי ספרות ביקורת הרי בכל דרך שנקבע את הבדיקות ישארו 4 צירופים אפשריים א-ד. צירוף א' אינו מצביע על שגיאה אלא על העדר שגיאה. נותרנו עם שלוש אפשרויות המצביעות על שגיאה ואין אפשרות לבדוק ששה מקומות עם שלוש יחידות אינפורמציה. שים לב שיש באפשרותנו להציג את הצירופים א, ב, ג, ד, על-ידי המספרים הבינאריים 00, 01, 10, 11. שלוש ספרות ביקורת:

האם ישתפר המצב או יורע עם שלוש ספרות ביקורת? כעת כולל השדר 7 ספרות. אם נמשיך בקו המחשבה מסוף הפיסקה הקודמת הרי עם שלוש ספרות בינאריות נוכל ליצור את 7 המספרים הראשונים (אם נתעלם מן האפס שהרי כפי שראינו הוא מצביע על העדר שגיאה). יש לנו שבע ספרות ושבעה צירופים שונים של תוצאות הבדיקה. נשמע מביטח, אך אילו בדיקות נערוך?

שבעה הצירופים האפשריים של שלוש הבדיקות (ללא תלות במהות הבדיקה) הם (אי-זוגי, זוגי, זוגי), (זוגי, אי-זוגי, זוגי), (זוגי, אי-זוגי, אי-זוגי), (אי-זוגי, אי-זוגי, אי-זוגי)

ואפשר להציג זאת על-ידי 001, 010, ... , 111

כלומר שבעת המספרים הראשונים הכתובים בצורה בינארית.

היה זה יפה אילו האפשרות הראשונה היתה אומרת כי הספרה הראשונה של האות המשודרת היא השגויה, וכך הלאה. כלומר שהערך הבינארי של שלוש הבדיקות יהיה שווה למקום השגיאה.

מה משמעות דרישה זו? נתבונן ב-111 לדוגמא. אנו רוצים שמספר זה יאמר שיש שגיאה בספרה השביעית. מכאן ששגיאה בספרה זו חייבת להשפיע על כל שלוש הבדיקות - או במלים אחרות ספרה זו חייבת להופיע בכל הבדיקות: היא אינה יכולה להשפיע עליהן בלי להשתתף בהן.

ועתה נתבונן ב-110. אנו רוצים שמספר זה יצביע על שגיאה במקום השישי. לכן, הספרה השישית חייבת להשתתף בשתי הבדיקות הראשונות אך לא בשלישית.

נמשיך בדרך זו ונמצא ששלוש הבדיקות צריכות להיות:

בדיקה (א) מספר ספרות 1 במקומות 4, 5, 6, 7, הוא זוגי

בדיקה (ב) מספר ספרות 1 במקומות 2, 3, 6, 7, הוא זוגי

בדיקה (ג) מספר ספרות 1 במקומות 1, 3, 5, 7, הוא זוגי

עד כאן הכל בסדר - אך כיצד ייקבעו ספרות הביקורת עצמן? אם השדר כלול בארבע הספרות הראשונות ושאר שלוש הספרות הן ספרות ביקורת הרי בפנינו בעיה חדשה. כל אחת משלוש הבדיקות כוללת שתי ספרות ביקורת או יותר, כך ש"קשה" לחשב אותן. לדוגמא ניקח את השדר 1011.

שימוש בחוקי הבדיקה יתן:

בדיקה (א) - מספר ספרות 1 במקומות 5, 6, ו-7 חייב להיות אי-זוגי.

בדיקה (ב) - מספר ספרות 1 במקומות 6 ו-7 חייב להיות אי-זוגי.

בדיקה (ג) - מספר ספרות 1 במקומות 5 ו-7 חייב להיות זוגי.

תנאים אלו יתקיימו אם נציב 1 במקום 6 ואפס במקומות 5 ו-7, כלומר השדר יהיה 1011010. דרך זו נכונה מבחינה טכנית, אך מסורבלת במקצת.

אפשר לעשות זאת בצורה פשוטה בהרבה, אם נשים לב שהמקומות 1, 2, ו-4 מופיעים רק פעם אחת בקבוצות הביקורת וכל אחד מהם בקבוצה שונה. לכן אם נכניס את השדר למקומות 3, 5, 6, 7, נוכל לקבוע מיד את הספרות שיש להכניס למקומות 1, 2, 4. לכן בדוגמא הקודמת במקום 1011010 נשדר 0110011 כאשר ספרות הביקורת מודגשות בקו מתחתיהן.

ההסבר היה ארוך למדי כיוון שניסינו לפתח את הנושא בשלבים, אך עתה יכולים
אנו לסכם בקצרה.

הצפנה:

- (1) קח שדר כל שהוא והצפן אותו על-ידי יחוס מספר בינארי בעל אורך קבוע
לכל סימן בשדר. (האורך הקבוע אינו חייב להיות 4 כמו בדוגמאות. ראה סעיף 2).
- (2) חלק את השדר המוצפן לקבוצות בנות ארבע ספרות. הוסף אפסים אם יש צורך
להשלים את אורך השדר לכפולה של ארבע.
- (3) הוסף לכל קבוצה של ארבע ספרות עוד שלוש ספרות כך שהמקומות 1, 2, 4
יהיו שמורים לספרות הביקורת (שיוגדרו בסעיף 4), והמקומות 3, 5, 6, 7 לארבע
הספרות של האינפורמציה. מיספור הספרות הוא משמאל לימין.
- (4) ספרת הביקורת במקום 4 היא כזאת שמספר ספרות 1 במקומות 4, 5, 6 ו-7
הוא זוגי.
- ספרת הביקורת במקום 2 היא כזאת שמספר ספרות 1 במקומות 2, 3, 6 ו-7
הוא זוגי.
- ספרת הביקורת במקום 1 היא כזאת שמספר ספרות 1 במקומות 1, 3, 5 ו-7
הוא זוגי.

פיענוח:

- (5) בהנחה שלכל היותר יכולה להיות שגיאה אחת בשידור קבוצה בת 7 ספרות של
השדר, הקולט (למעשה עושה כל זאת המכונה) מבצע את שלוש הביקורות כסדרן.
אם מתגלה מספר אי-זוגי של ספרות 1 הקולט רושם 1. עבור מספר זוגי של ספרות 1
הוא רושם 0. המספר הבינארי הנרשם מציין את מיקומה של השגיאה בבית
(אם אכן יש שגיאה) ואז הוא מתקן אותה.
- (6) לבסוף מורדות ספרות הביקורת מן השדר ה"מתוקן" והוא מפוענח.

(ה) שדר לקוראי "שבבים"

השדר הבא הוצפן בהתאם לחוקים הנ"ל, כאשר השתמשנו ב-22 המספרים הבינאריים
הראשונים בני חמש ספרות לייצוג אותיות האלף-בית העברי.
שים לב: השדר הוא בעברית כך שיש לקוראו מימין לשמאל, אך כל אות מיוצגת
על-ידי מספר בינארי הנקרא משמאל לימין.

0000000101011101001010001000111000001001010100101

הדרכה: חלק את השדר לקבוצות בנות שבע ספרות. בדוק כל קבוצה וקבוצה אם

יש בה שגיאות (ותקן במידה ויש) הורד את ספרות הביקורת. חלק את השדר הנותר לקבוצות בנות חמש ספרות. כל קבוצה כזאת היא מספר בינארי המייצג אות. וכעת אולי תבין מדוע עושה זאת המכונה.

הערה:

האריתמטיקה של מספרים בינאריים כלולה בתוכנית לימודים, אך כשלעצמה היא אינה חשובה ביותר. חשובה התפישה של ההצגה הבינארית אשר משמעותה לאו דוקא בצופנים שהצגנו לעיל. במילים אחרות, היכולת לבצע פעולות חשבון במספרים בינאריים אינה מטרה חשובה ביותר, חשובה יותר היכולת לחשוב במושגים בינאריים ולראות מצבים בינאריים.

חלק מן הרעיונות במאמר זה מבוססים על מאמר בעל אותה כותרת שהופיע בעיתון ההולנדי פיתגורס. שמו של הצופן מתקן השגיאות מעיד על ממציאו: אמריקאי ששמו המינג.

שבבים-עלון מורי מתמטיקה תיק מס' 2