

תרגיל 2 - חלק יבש

המתרגל האחראי על התרגיל: תומר כץ.

שאלותיכם במייל בעניינים מנהלתיים בלבד, יופנו רק אליו.

כתבו בתיבת **subject**: יבש 2 את"ם.

שאלות בעל-פה ייענו על ידי כל מתרגל.

הוראות הגשה:

- לכל שאלה יש לרשום את התשובה במקום המיועד לכך.
- יש לענות על גבי טופס התרגיל ולהגיש אותו באתר הקורס כקובץ PDF.
- על כל יום איחור או חלק ממנו, שאינו בתיאום עם המתרגל האחראי על התרגיל, יורדו 5 נקודות.
- הגשות באיחור יש לשלוח למייל של אחראי התרגיל בצירוף פרטים מלאים של המגישים (שם+ת.ז).
- שאלות הנוגעות לתרגיל יש לשאול דרך הפיאצה בלבד.
- ההגשה בזוגות.

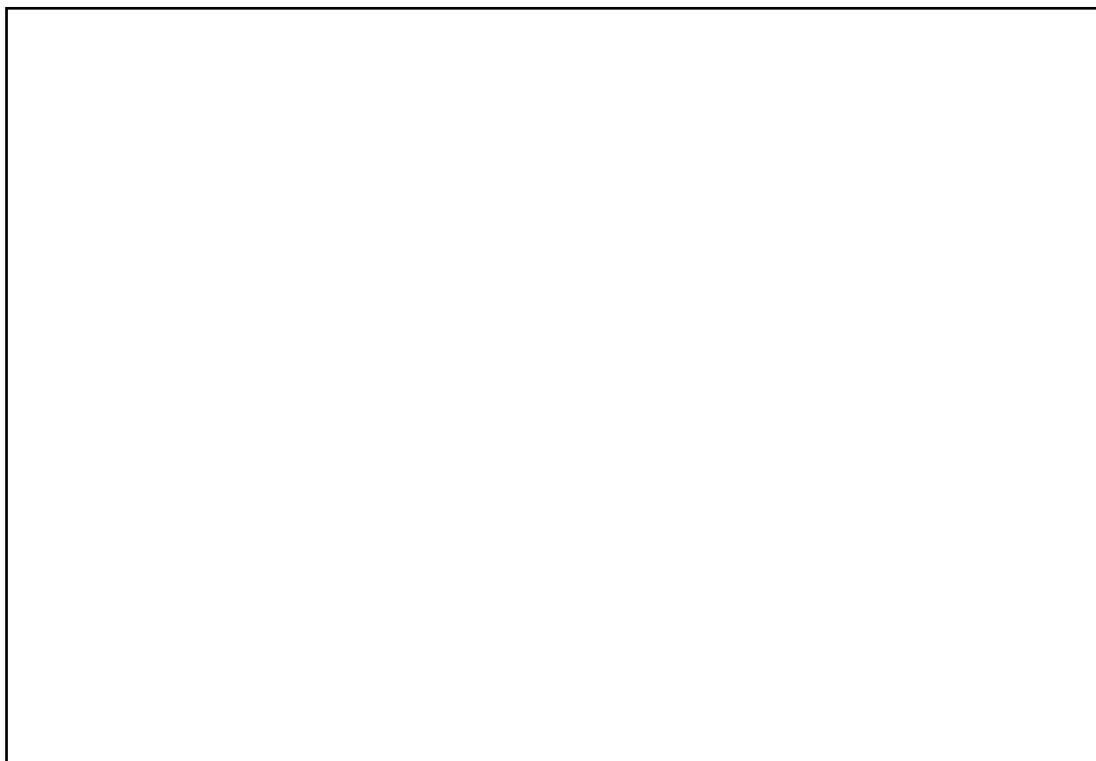
שאלה 1 (45 נק') – שגרות:

נועה המ"מ שמעה כי היא הולכת לקבל מחזור עתודאים. נועה לא יודעת מה עושים העתודאים בזמנם בחופשי אז היא החליטה לרשום להם תוכנית באסמבלי לשעות הפנאי. לפניכם מקטע הנתונים שנועה כתבה:

```
1 .section .data
2 A: .long 3
3 .quad B
4 .quad C
5 .quad D
6 .quad 0
7 B: .long 10
8 .quad E
9 .quad F
10 .quad 0
11 C: .long 22
12 .quad 0
13 D: .long 17
14 .quad G
15 .quad 0
```

```
16 E: .long 85
17 .quad 0
18 F: .long 2
19 .quad 0
20 G: .long 8
21 .quad 0
22 .
```

א. ציירו את הגרף המתקבל מפירוש מקטע הנתונים (מומלץ להסתכל בתרגול 3 תרגיל 1 ולהיזכר כיצד מפרשים את הזיכרון כרשימה מקושרת). בכל צומת בגרף ציינו את התווית המתאימה לו בלבד (אין צורך לציין ערכים נוספים) (3 נקודות)



הסמלת ספיר, שבאה לעזור לנועה, חשבה איך לשעשע את העתודאים הצעירים. לצורך כך, היא כתבה את הפונקציה הפשוטה func וקוד ששתמש בא:

```

23 .section .text
24 .global _start
25 _start:
26     mov $17, %esi
27     mov $A, %rdi
28     call func
29     movq $1, %rdi
30     sub %rax, %rdi
31     movq $60, %rax
32     syscall
33
34 func:
35     push %rbp
36     movq %rsp, %rbp
37     cmpl %esi, (%rdi)
38     jne next
39     mov $1, %rax
40     jmp end
41
42 next:
43     mov $0, %r10
44
45 test:
46     cmpq $0, 4(%rdi,%r10,8)
47     je fail
48     push %rdi
49     push %r10
50     mov 4(%rdi,%r10,8), %rdi
51     call func
52     pop %r10
53     pop %rdi
54     cmpq $0, %rax
55     jne finish
56     inc %r10
57     jmp test
58
59 finish:
60     mov $1, %rax
61     jmp end
62
63 fail:
64     mov $0, %rax
65
66 end:
67     leave
68     ret

```

ב. נתון שבתחילת התוכנית ערך של rsp הוא X. כאשר X הוא מספר הקסדצימלי. מה הוא הערך המקסימלי ומה הערך המינימלי ש-rsp יכול לאורך ריצת התוכנית? הביעו את התוצאה באמצעות נוסחה שהמספרים בה הם בבסיס הקסדצימלי (בטאו את התשובה באמצעות X). (7 נקודות)



ג. רשמו מה יהיה פלט הפונקציה עבור קטע הקוד הנוכחי (5 נקודות) _____.

ד. המירו את הפונקציה לשפת C על ידי כך שתשלימו את המקומות החסרים בקוד. היעזרו בהגדרת structn שנתונה לכם (10 נקודות):

```

typedef struct _Node{
    int data;
    struct _Node** sons;
}Node;

```

הערות:

- מבנה structn בזיכרון אילו הייתם מקמפלים את הקוד היה שונה מהצורה שבו הוא מופיע במקטע datan לעיל. הסיבה תובהר לכם בהערה הבאה.
- הניחו שהכוונה ב-Node** היא שרשימת המצביעים לבנים נמצאת בתוך ה struct ומיוצגת כמערך באורך לא קבוע (ולכן גם ה-struct בגודל לא קבוע. דבר זה אינו חוקי בשפת C. struct של שפת C תופס מקום קבוע בזיכרון. לשם התרגיל אנחנו מניחים משהו חריג, שניתן להשיג רק בזכות העובדה שאנו כותבים באסמבלי)
- מותר להשלים יותר ממילה אחת בכל קו אך לא יותר מפקודה אחת!

```

_____ func ( Node *root, _____ x){

    if (root->data == _____)

        _____;

    Node *son = root->sons;

    while(son != null)

        if (_____)

            return _____;

    son += _____ .

}

return _____;

}

```

הערה: בסעיפים הבאים יש כל מיני שינויים בקוד. כל שינוי מתקיים רק בסעיף בו מופיע. זאת אומרת שהסעיפים לא תלויים אחד בשני.

ה. צליל המ"כית מאמינה שהכול צריך להיות אחיד ומסודר. היא מחליטה לקחת את מקטע הנתונים של נועה ולשנות בכל struct את long בquad. כלומר מקטע הנתונים ישתנה כך:

```

1  .section .data
2  A:  .quad 3
3      .quad B
4      .quad C
5      .quad D
6      .quad 0
7  B:  .quad 10
8      .quad E
9      .quad F
10     .quad 0

```

ובאופן דומה כל שאר האותיות יחליפו את הנתון הראשון במקום long בquad. רשמו את השינויים שצריכים להיות בקוד על מנת שיעבוד בצורה תקינה עם מקטע הנתונים החדש (5 נקודות)

1. יוגב הסמב"צ אוהב לעזור לנועה ולכן החליט לשנות את מבנה הנתונים באופן הבא:

```
13 D: .long 17
14 .quad A
15 .quad 0
```

מה יהיה פלט התוכנית? יש לסמן תשובה מבין התשובות הבאות ולנמק במשפט אחד: (5 נקודות)

a. התוכנית תסתיים ופלט הפונקציה יהיה 1

b. התוכנית תסתיים ופלט הפונקציה יהיה b

c. התוכנית תכנס ללולאה אנסופית

d. התוכנית תקרוס במהלך ריצה

e. התוכנית כלל לא תבנה

נימוק:

2. הקוד הגיע למב"סית ובגלל קוצר הזמן שלה היא החליטה לקצר את הקוד. לפניכם מספר שינויים שהמב"סית הציעה. עליכם לכתוב עבור כל אחת מההצעות האם נכונות השגרה תיפגע (האם יש קלט

עבורו השגרה לאחר השינוי שונה מהשגרה לפני השינוי). הסיברו **בקצרה** את תשובתכם! (10

נקודות)

a. מחיקת הפקודת push ו pop שבשורות 52 ו 47.

b. מחיקת הפקודה pop **בשורה 51**

c. הוספת פקודה push %rdi אחרי test בשורה 44

d. הוספת הפקודה push %rdi אחרי test בשורה 44, הוספת הפקודה: mov (%rsp), %rdi לפני jmp בשורה 56.

שאלה 2 (30 נק') – קריאות מערכת:

ג'ואי מרגיש מתוסכל מכך שחבריו חושבים שהוא פחות חכם מהם. לכן, הוא מחליט להרשים אותם בעזרת כתיבת קוד באסמבלי. הקוד שג'ואי מתכנן לכתוב קוד שיקרא קלט מהמשתמש שבו הוא יתאר אילו מאכלים הוא מעוניין לקבל והקוד יחזיר לו מה ג'ואי מוכן לתת לו.

א. לפניכם מקטע הנתונים שג'ואי כתב מבלי ערכי הנתונים עצמם:

```
.section .data
msg1: .ascii ???????
msg2: .ascii ???????
msg1_len: .quad ____
msg2_len: .quad ____
all_msg_len: .quad ____
```

ג'ואי לא יודע עדיין אילו מחרוזות הוא יכתוב. עליכם להשלים את המקומות הריקים שקשורים לאורכי המחרוזות כך שמשתנה msg1_len יהיה האורך של msg1, msg2_len יהיה האורך של msg2 ובמשתנה all_msg_len יהיה שווה לסכום אורכי המחרוזות msg1 וmsg2. שימו לב עליכם לעשות זאת בצורה כזו שהאורכים יהיו נכונים בעת ריצת התוכנית ללא קשר לאילו מחרוזות ג'ואי יאתחל כערכים של msg1 ו-msg2.

ב. לפני ביצוע קריאת מערכת מתבצעים גיבויים של ערכים מסוימים בתוכנית. נרצה להבדיל בין האחריות של מערכת ההפעלה, אחריות המעבד ואחריות של קוד המשתמש, בביצוע גיבויים אלו.

a. מה באחריות קוד המשתמש לגבות?

b. מה באחריות מערכת ההפעלה לגבות?

c. מה באחריות המעבד לגבות?

ג. ג'ואי רצה לחסוך בקוד והחליט שבמקום להשתמש ב syscall הוא יקרא ישירות לפונקציות sys_read וsys_write שמערכת ההפעלה מממשת ('יבצע את הפקודה call sys_write לדוגמה). האם קריאה ישירה כזו תעבוד? אם כן הסיבירו לג'ואי מה נדרש לעשות כדי שזה יעבוד והאם יש בכך סיכון. אם לא, רשמו באיזה אחד משלבי התוכנית (קמפול, ריצה, טעינה, קישור וכו') יקרה הכישלון ומדוע.

ד. חברה טובה של ג'ואי, פיבי, טוענת שאין בכלל צורך בשתי פקודות return שונות. ואמרה לג'ואי לבטל לחלוטין את פקודת sysret ולהשתמש רק בret. האם ההצעה של פיבי טובה וישימה?

ה. רוס שמע על הקוד שג'ואי כותב לו ורצה להצטרף לחגיגה. הוא נסע לכנס מערכות ההפעלה השנתי וביקש אישור להוסיף קריאת מערכת חדשה sys_pivot. קריאת המערכת הזו תיצור 3 תיקיות עם השם "pivot1", "pivot2", "pivot3" (הרשאות התיקייה לא משנות). האם הקוד של רוס (שייקרא על ידי entry_syscall כמו כל קריאת מערכת) צריך להמשיך לשמור על קונבנציות system V? נמקו.

ו. הסבירו מה על רוס לעשות/להוסיף/לשנות לקוד מערכת ההפעלה על מנת שהקריאה שלו תעבוד (רק לפי מה שלמדתם בקורס)

ז. גונטר, מנהל בית הקפה, שמע על כל המשחקים במערכת ההפעלה שהחברים עושים וביקש מהם לכתוב עבורו גם קריאת מערכת חדשה. הוא מעוניין בקריאת מערכת בשם order_coffee. היא תקבל בתוך קלט את הארגומנטים הבאים: סוג קפה (מספר שלם), גודל הכוס (תו), לקחת או לשבת (bool), חם או קר (bool), שם המזמין (מחרוזת), האם להוסיף מאפה (bool), האם התשלום באשראי או במזומן (bool). ומחזירה את מספר ההזמנה בתור פלט. האם ניתן להוסיף קריאת מערכת שכזו? נמקו.

שאלה 3 (25 נק') – רמות הרשאה ואוגר הדגלים:

א. הפקודה `pushfq` דוחפת את הערך של אוגר הדגלים למחסנית. והפקודה `popfq` מוציאה את אוגר הדגלים מהמחסנית. הסבירו כיצד באמצעות שילוב של שתי פקודות אלו ניתן להדליק את הדגלים `CF` `OF`. שימו לב במידה ואחד הדגלים כבר דלוק יש להשאירו דלוק כלומר, בסיום התהליך על שני הדגלים להיות דולקים. אין לשנות את שאר הביטים בריגסטר הדגלים. בנוסף, אין לשנות אף רגיסטר שהוא לא `rflags`, `rip`, `rsp` (גם לא באופן זמני).
הערה: במידה ובדקתם את עצמכם באמצעות דיבאגר וראיתם שנדלק גם דגל `TF` זה בסדר תלמדו בהמשך מדוע הוא נדלק תוך כדי דיבוג.

ב. הולי התחמנית רוצה לאפשר לעצמה גישה ישירה אל התקני הקלט פלט ללא צורך בקריאות מערכת. איזה שינוי **באוגר הדגלים** יכול לעזור להולי במטרתה?
הערה: לא צריך לציין פקודה ספציפית, רק להגיד מה צריך לעשות ברמה התיאורטית

ג. הולי מחליטה לנסות את התעלול מסעיף א' רק שבמקום לשנות את `CF` `OF` היא רוצה לשנות את `IOPL`. להפתעתה, היא לא מצליחה לשנות את הביטים הללו. הסבירו מה ההיגיון בכך שהיא לא מצליחה לשנות את `IOPL`? התייחסו לצורך בקריאות מערכת.

ד. הולי לא מתייאשת ומנסה לגשת בלעיה באופן אחר. היא תכתוב בעצמה קריאת מערכת שתעזור לה. הקריאה תאפשר לכל משתמש לקרוא לה ולאחר שהיא תסתיים המשתמש יוכל לגשת ישירות להתקני הקלט פלט ללא צורך בקריאת מערכת. הסבירו מה על הולי לעשות בקריאת מערכת שהיא כותבת על מנת שהתוכנית שלה תצליח.

הערה: הסעיפים הבאים קשורים לפסיקות מומלץ לענות עליהם לאחר תרגול 6.

ה. וולי החבר המבולבל של הולי מתלבט כיצד ניתן לחסום פסיקות תוכנה לכן הוא שואל את הולי. אילו מבין התשובות הבאות על הולי לענות לו? יש לסמן את האפשרות הנכונה.

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. שינוי CPL ל00
4. לא ניתן לחסום פסיקות תוכנה.

ו. כעת נתון שוולי הצליח להגיע למצב שבו CPL שווה ל0. וולי מעוניין לחסום פסיקות חומרה שאינן מועברות דרך כניסת NMI. כיצד הוא יכול לעשות זאת? (5 נקודות)

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. עליו לחבר את הפסיקות לכניסת NMI ואז לכבות את דגל IF
4. לא ניתן לחסום פסיקות חומרה ולכן לא יצליח.