

גירסאות מיוחדות של הפקודה CALL

השימושים בפקודה CALL שראינו עד כה היו מהסוג של CALL לנקודה בזכרון הנמצאת בסגמנט קוד - יותר נכון label המצביע על פקודה. בגירסה הזו אוגר ה-IP או זוג האוגרים CS ו-IP משנים את ערכם להצביע על הנקודה הזו (תוך שימור כתובת החזרה במחסנית). זו אכן הגירסה הנפוצה ביותר של הפקודה CALL. אבל ישנם גירסאות נוספות.

קיימת גירסה של CALL עם אוגר 16 ביט. המשמעות שלו היא להציב את ערך האוגר לתוך IP. לדוגמא, הפקודה

CALL BX

גורמת לשימור IP והצבת הערך של האוגר BX לתוך IP, מעין השמה $IP = BX$.

שימוש בפקודה CALL להסתעפות עקיפה - מימוש פוינטר לפונקציה

אחד הגירסאות של הפקודה CALL היא הסתעפות עקיפה דרך משתנה בזכרון. במקרה הזה האופרנד של הפקודה CALL הוא לא כתובת של פקודה אלא כתובת של משתנה. במקרה הזה, הכתובת בזכרון איננו מגדיר את הערך החדש של CS:IP אלא היכן נמצא הערך החדש הזה. לסוג הזה של פקודת CALL יש גירסת NEAR וגירסת FAR. לדוגמא, נניח ששטח ה-DATA של תוכנית מכילה את ההגדרות הבאות:

```
f_ptr1 DW 100h
f_ptr2 DD 20003000h
```

אזי הפקודה

CALL f_ptr1

תגרום להסתעפות מסוג NEAR כאשר מלבד שימור הערך הנוכחי של IP, IP יקבל את הערך 100h. לעומת זאת, הפקודה

CALL f_ptr2

תגרום להסתעפות מסוג FAR כאשר מלבד שימור הערכים הנוכחיים של IP ושל CS, CS יקבל את הערך 2000h ו-IP יקבל את הערך 3000h.

אפשר גם פקודות מהצורה הבאה:

```
CALL WORD PTR [BP+6]  
CALL DWORD PTR [BX-4]
```

הסוג הזה של פקודות CALL משמש למימוש המושג ב-C הנקרא פונקציה.

אגב, במחשבים רבים יש גם גירסאות עקיפות לפקודה המקבילה MOV. אין גירסה כזו במחשב הזה, אבל יש פקודות הסתעפות עקיפות.

386 ואילך.

בנוסף לפקודות המצוינות לעיל יש ב-386 גירסאות נוספות של הפקודה CALL התומכות בהיסטים 32 ביט.

קיימות פקודות מהסוג

```
CALL ECX
```

שהמשמעות שלה היא שימור EIP והצבת הערך של ECX לתוך EIP.

כמו כן ישנן פקודות הסתעפות עקיפה NEAR 32 ביט (שינוי EIP בלבד) וכן הסתעפיות עקיפות 48 ביט. משתנים אלו נקראים Full Pointer או FWORD. להגדרת משתנים בשטח המידע משתמשים בהנחיה DF או DP. לפיכך ניתן לראות ב-386 פקודות כמו

```
f_ptr1 DF 605040302010h
```

.....

```
CALL f_ptr1
```

יגרום לשמירת CS ו-EIP והצבת

CS = 6050h ו-EIP = 40302010h.

```

/* p f.c - Use pointer to function */

int sqr(int x)
{
    return x*x;
} /* sqr */

int neg(int x)
{
    return -x;
} /* neg */

void main()
{
    int x,y, z;

    int (*fp)(int);

    x = 5;

    fp = sqr;

    y = (*fp)(x);

    fp = neg;

    z = (*fp)(x);

    printf("\nx = %d, y = %d, z = %d\n", x, y, z);
} /* main */

```

E:\>pf

x = 5, y = 25, z = -5

E:\>

מודלים של זיכרון של Turbo C

בעידן של ה-8086 יעילות אלקטרונית היה עניין חשוב. כאשר מימשו קומפילרים באותה תקופה הדבר הביא, בין השאר, להתלבטות בכל הקשור לשימוש בהסתעפויות מסוג NEAR או FAR (ופוינטרים לפונקציה 32 ביט) על מנת להסתעף לחתי תוכניות וכן בזמן מימוש פוינטרים למידע האם להשתמש בפוינטרים מלאים 32 ביט (16 להיסט ו-16 לסגמנט) או לעבוד בפוינטרים 16 ביט (היסטים בלבד). יש כאן tradeoff בין מהירות לבין כלליות: בחירה באפשרויות המהירות יותר (הסתעפיות NEAR או פוינטרים 16 ביט) מגבילה את הקוד המשתמש בהם לסגמנט יחיד לכל סוג שימוש (קוד או מידע). על כך נרחיב בהמשך.

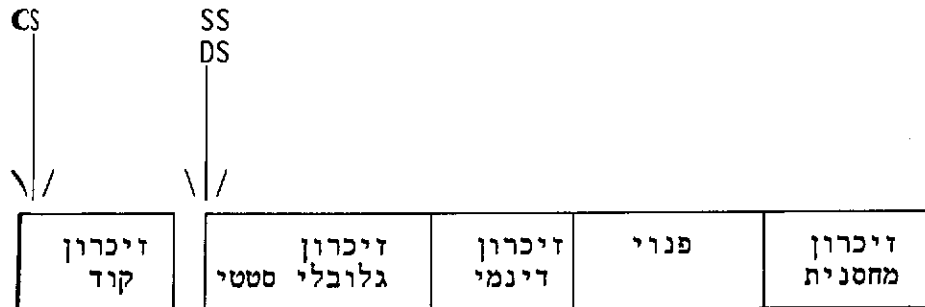
בקוד אסמבלי טהור, המתכנת יכול לממש רוטינות שלו כך שחלק מהרוטינות יהיו NEAR כשאפשר והאחרות FAR כשצריך. אבל כאן המתכנת לוקח על עצמו את האחריות. כאשר מנסים לממש מדיניות כזו בקומפילר הדבר הרבה יותר קשה, כי קשה לחזות מראש את כל התסריטים, ובפועל לא עשו את זה. מיקרוסופט ובעקבותם בורלנד מימשו מדיניות אחידה בכל הקשור למימוש קוד של קובצי המקור בכל פעולת קומפילציה מסוימת. יחד עם זאת, לפחות עבור C הם השאירו את האופציות פתוחות, כלומר המתכנת יכול לבחור איזה משתי האופציות בשתי הקטגוריות הוא צריך. הם קראו לאפשרויות הללו מודלים של זיכרון (Memory Models). המתכנת יכול לבחור האם הוא לממש את ההסתעפויות ב-NEAR או ב-FAR ובאופן בלתי תלוי אם הפוינטרי למידע יהיו מלאים 32 ביט ע"י בחירה באופצית מודל הזיכרון המתאים.

תוכנית שנטענת לזיכרון מקצה זיכרון ל-4 סוגי שימושים:

- שטח זיכרון לפקודות התוכנית - הקוד של התוכנית. השטח הזה נקבע בדיוק בזמן קומפילציה והוא תוצר של מספר הפקודות של התוכנית ואופיים.
- שטח זיכרון למשתנים גלובליים / סטטיים. גם השטח הזה נקבע בדיוק בזמן קומפילציה והוא תוצר של מספר המשתנים הגלובליים / סטטיים המוכרזים מראש בתוכנית.

- שטח זיכרון להקצאות דינמיות. הגודל המירבי של השטח הזה שתוכנית צריכה נקבע בפועל בזמן ריצה ואינו חייב להיות אחיד לכל הריצות של התוכנית. הוא נקבע על ידי בקשות ההקצאה (והשחרור) שיוזמת התוכנית.
- שטח המחסנית. כמו שטח ההקצאה הדינמי, הגודל המירבי של השטח הזה שתוכנית צריכה נקבע בפועל בזמן ריצה ואינו חייב להיות אחיד לכל הריצות של התוכנית. הוא נקבע על ידי עומק הקריאות לפרוצדורות, הפרמטרים והמשתנים האוטומטיים שמוכרזות ע"י הפרוצדורות הללו.

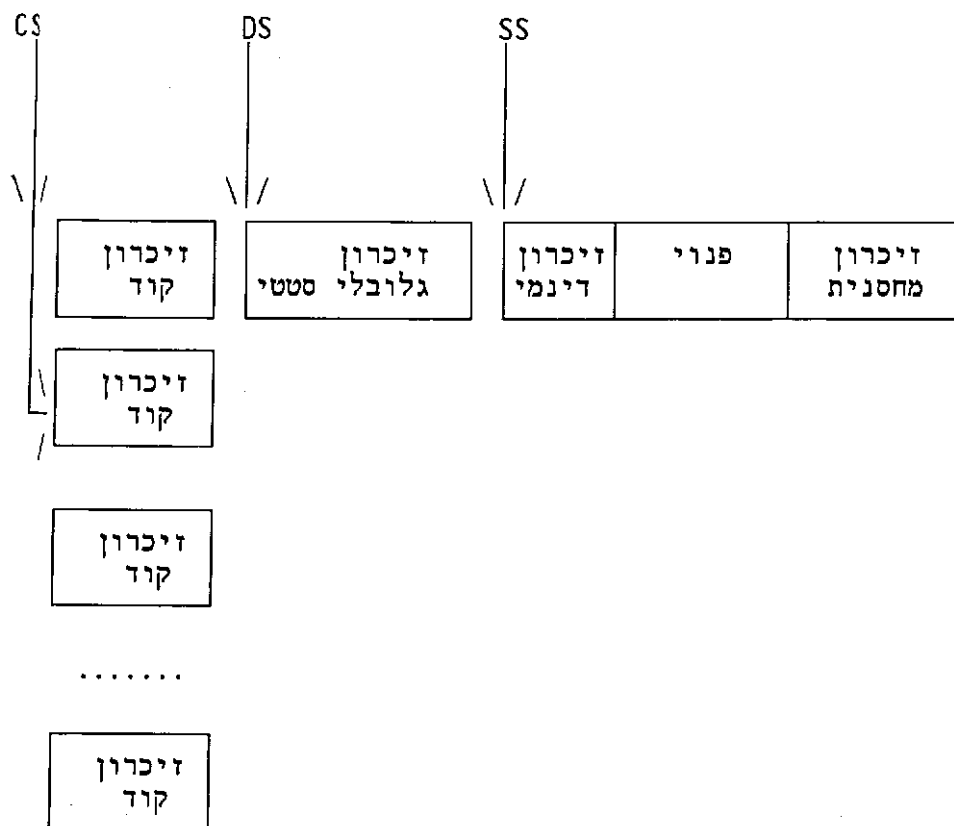
השניה. תמונת אוגרי הסגמנטים במודל Small נראית כך:



מודל Large

כמעט בקצה השני של האפשרויות הוא מודל Large. כאן מותרים לחלוטין על נושא המהירות לטובת גודל או "כלליות" של התוכנית. במודל הזה הקוד ינרל לתפוס כמה סגמנטים לפי הצורך (המגבלה היחידה היא ה-640K של כלל מערכת ה-DOS), ואילו לשטח הגלובלי / סטטי יש סגמנט יחיד משלו ולשטח הדינמי + מחסנית סגמנט יחיד משלו. במהלך ריצה של תוכנית במודל Large, אוגר ה-CS עשוי להשתנות בכל רגע, אך אוגרי ה-SS וה-DS שומרים על ערכם במהלך הריצה של התוכנית, אם כי DS ו-SS אינם שווים. כאן כל ההסתעפויות לפרצדורות הם FAR וכל הפוינטרים 32 ביט. הפוינטרים למידע חייבים להיות 32 ביט משום שכל פוינטר עשוי בהזדמנות אחת להצביע על שטח גלובלי/סטטי ובהזדמנות אחרית על שטח מחסנית או דינמי. תוכנית המקומפלת במודל Large היא כמעט ולא מוגבלת בגודל השטח המוקצה לקוד, אך שטח המידע של התוכנית מוגבל ל-128K כאשר 64K מתוכם יכולים להיות מנוצלים אך ורק למשתנים גלובליים/סטטיים ואילו רק עד 64K יכולים להיות מנוצלים לשטח דינמי + מחסנית. אי אפשר להגדיל את שטח המחסנית למעבר ל-64K על חשבון השטח הגלובלי/סטטי או להיפך. אך מתכנת המודע למגבלות הללו יכול לכתוב את התוכנית כך שיהיה למעשה חסכון באחד מסוגי השימוש לטובת השני. המקרה הנפוץ הוא ששטחי משתנים של פרוצדורות ימומשו גלובלית או סטטית, דבר שיקטין את הביקוש לשטח מחסנית על חשבון הסגמנט הגלובלי/סטטי. אגב, שיקולים מהסוג הזה קיימים גם במסגרות אחרות כמו Unix.

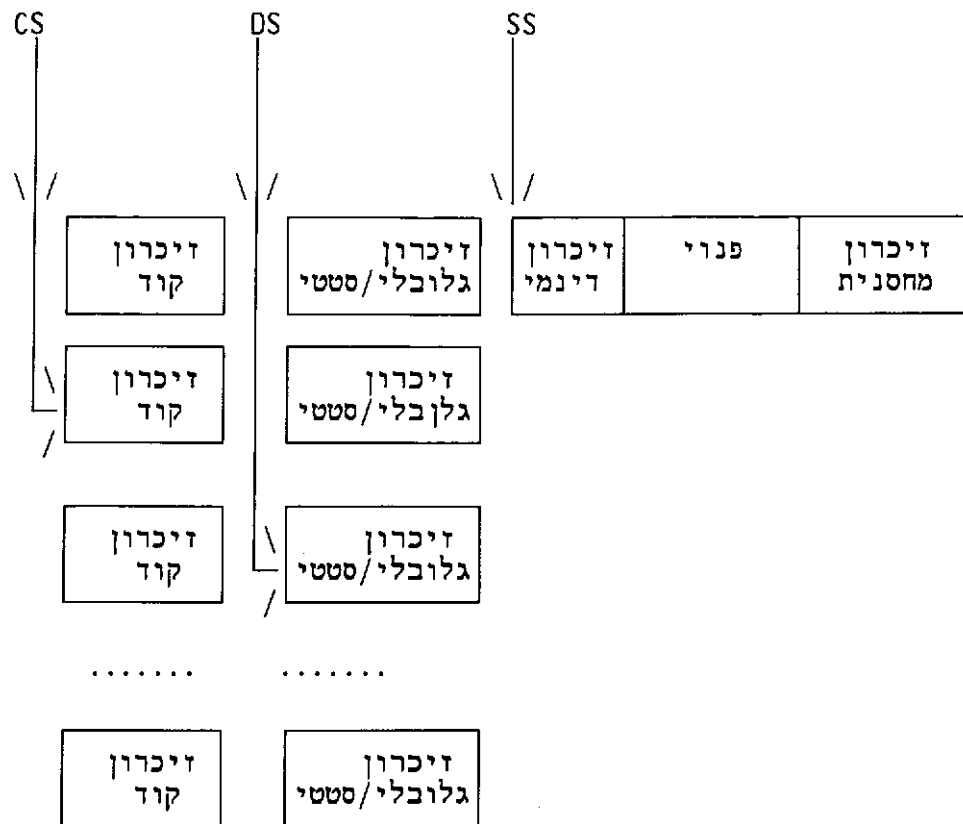
תמונת הזיכרון של מודל Large נראה עקרונית כך:



מודל Huge

מודל Huge הוא המודל הכללי או החזק ביותר, ועקרונית דומה למודל Large למעט שהשטח הגלובלי/סטטי אינו מוגבל לסגמנט יחיד. המחסנית לעומת זאת ממשיכה להיות מוגבלת לסגמנט אחד. לפיכך תוכנית המקומפלת במודל Huge היא כאילו לא מוגבלת הן בקוד והן במידע (שוב עד למגבלה הכוללת של 640K של ה-DOS). אולם ככל שמדובר בשימוש בזיכרון למידע, היכולת לנצל שטחי זיכרון גדולים מותנית בכך שהם יוכרזו כמשתנים גלובליים/סטטיים. תוכניתן הרוצה לכתוב תוכנית המנצלת שטחי זיכרון שהסה"כ שלהם עולה על 64K חייב את השטח העודף לתכנת כמשתנים גלובליים/סטטיים.

תמונת הזיכרון של תוכנית המקומפלת במודל Huge נראית כך:



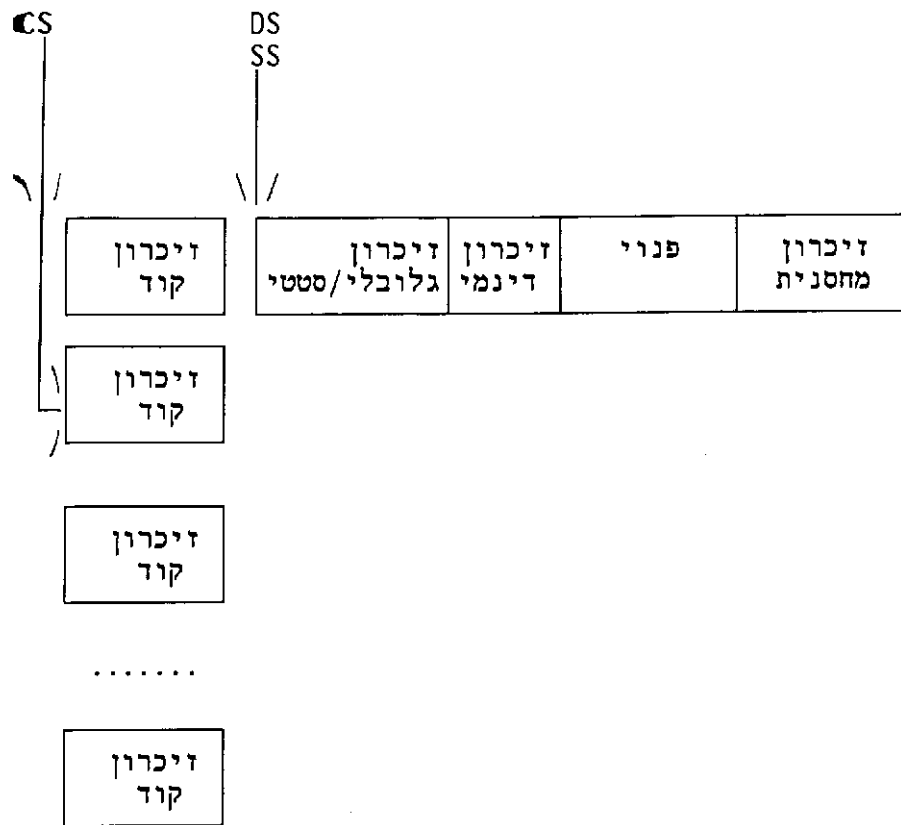
המודלים הנותרים

המודלים האחרים הם פשוט מודלי ביניים בין Small ל-Large. משום כך התעכבות עליהם לא תחכים אותנו בהרבה, אבל בקצרה:

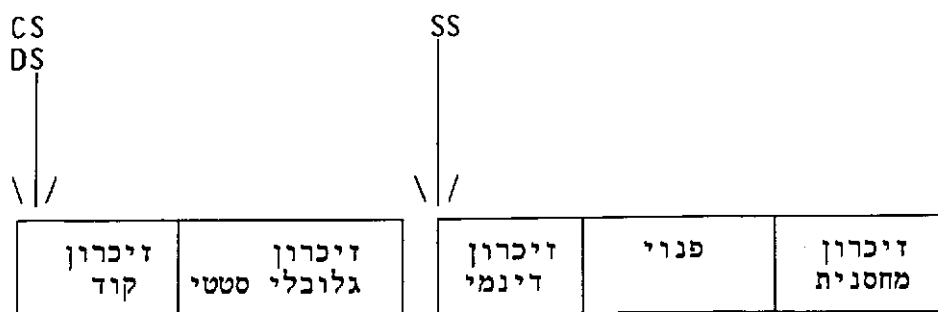
מודל Medium - שטח הקוד יכול להתפרס על מספר רצוי של סגמנטים כמו במודל Large אבל שטח המידע כולו (גלובלי/סטטי, דינמי, מחסנית) נכנס לסגמנט אחד כמו במודל Small. לפיכך כאן כל ההסתעפויות הם FAR, פוינטרים לפונקציה הם 32 ביט אבל הפוינטרים למידע הם 16 ביט.

מודל Compact - שטח הקוד והשטח הגלובלי/סטטי הם יחד בסגמנט אחד ואילו השטח הדינמי והמחסנית נמצאים בסגמנט נפרד. לפיכך גודל הקוד של התוכנית מגביל את גודל השטח הדינמי/סטטי ולהיפך אבל גודל השטח הגלובלי/סטטי לא מגביל את השטח הדינמי והמחסנית. במודל הזה כל ההסתעפויות הם NEAR, הפוינטרים לפונקציה הם 16 ביט. לעטמת זאת פוינטרים למידע הם 32 ביט.

תמונת הזיכרון של מודל Medium:



מודל הזיכרון של מודל Compact:



כתיבת תוכניות באסמבלי - ההבדלים בין המודלים

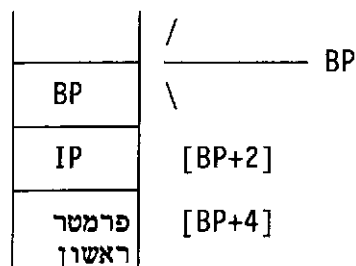
תוכניתן הכותב תוכנית אסמבלי הנקרא מתוכנית טורבו C חייב להיות מודע לאיזה מודל הוא כותב את התוכנית, גם אם למען האמת הוא לא צריך להבין לעומק את תמונת הזיכרון של המודל. תוכנית אסמבלי שנכתבת למודל Small לא תעבוד למודל Large. העובדות שתוכניתן האסמבלי צריך להיות מודע לן הן רק סוגי ההסתעפויות של המודל (FAR, NEAR) וגודל הפוינטרים למידע (16 או 32 ביט).

סוג ההסתעפויות - אם המודל משתמש בהסתעפויות NEAR בכדי להסתעף לפרוצדורה (מודלים Tiny, Small, Compact) אזי הרוטינה הנקראית מ-C חייבת להיות מוגדרת גם היא NEAR, ובהנחה שהפקודות הראשונות של הרוטינה הם

```
PUSH BP
MOV BP,SP
```

אזי הפרמטר הראשון המועבר אל הרוטינה נמצא בכתובת [BP+4].

זאת משום שתמונת המחסנית היא



אם לעומת זאת המודל משתמש בהסתעפויות מסוג FAR (מודלים Medium, Large, Huge), הפרמטר הראשון יהיה ב-[BP+6] משום שתמונת המחסנית עכשיו תהיה

	/	
BP	—	BP
	\	
IP		[BP+2]
CS		[BP+4]
פרמטר ראשון		[BP+6]

בנוסף לכך, גודל הפוינטרים לפונקציה בתוכנית (נניח שהם מועברים כפרמטרים, או משתנים גלובליים) תלויים רק בסוגי ההסתעפויות של המודל. אם סוג ההסתעפויות היו NEAR אז הפוינטר לפונקציה ממומש 16 ביט בלבד (ערך חדש ל-IP) ואם סוג ההסתעפויות היא FAR אזי הפוינטר לפונקציה היא 32 ביט (ערך חדש ל-IP בכתובות הנמוכות, ערך חדש ל-CS בכתובות המרוחקות יותר). לדוגמא, נניח שכתובת [BP+10] נמצא פוינטר לפונקציה, אם מדובר במודל שמשתמש בהסתעפויות NEAR אז הפוינטר לפונקציה יתפוס 2 בתים שהם ערך חדש ל-IP והסתעפויות דרכו יעשו בפקודה נוסף

CALL WORD PTR [BP+10]

לעומת זאת, אם מדובר במודל המשתמש בהסתעפויות FAR אזי בכתובות [BP+10] - [BP+11] ישב ערך חדש ל-IP ובכתובות [BP+12] - [BP+13] ישב ערך חדש ל-CS. הסתעפות דרך הפוינטר יהיה דרך פקודה נוסף

CALL DWORD PTR [BP+10]

סוג הפוינטרים למידע - במידה ופרוצדורת האסמבלי נקראית מתוכנית C המקומפלת במודל המממש פוינטרים למידע 16 ביט (מודלים Tiny, Small ו-Medium) כל פוינטר למידע הוא 16 ביט ומכיל היסט בלבד אם למשל בכתובת [BP+10] יש פוינטר כזה, שימוש בו יעשה ע"י פקודות נוסף

MOV BX,[BP+10]

MOV AX,[BX]

לעומת זאת, במידה ופרוצדורת האסמבלי נקראית מתוכנית C המקומפלת במודל המממש פוינטרים 32 ביט (מודלים Compact, Large ו-Huge) כל פוינטר למידע

הוא 32 ביט. אם למשל בכתובת [BP+10] יש פוינטר כזה, הוא מכיל היסט בכתובת
[BP+11] - [BP+10] ומספר סגמנט בכתובות [BP+12] - [BP+13]. השימוש בו
יעשה ע"י פקודות נוסף

```
MOV BX,[BP+10]  
MOV ES,[BP+12]  
MOV AX,ES:[BX]
```

כלומר שימוש אופיני של פוינטר כזה יכול להשמה לאוגר סגמנט ושימוש ב-
Segment Override.

התייחסות לזיכרון המחסנית דרך ה-BP

בכל המודלים האוגר SS לא משנה את ערכו, המחסנית הוא תמיד סגמנט אחד,
ולפיכך המתכנת אינו צורך לדאוג לכך שתוכן אוגר ה-SS יצביע לסגמנט "הנכון".
מהסיבה הזו בהתייחסות לזיכרון המחסנית יכולות להעשות תמיד בעזרת האוגר ה-BP
ללא צורך ב-Segment Override נוסח SS: וללא צורך בעדכון של תוכן אוגר ה-SS
לפני כן.

הכרזת משתנים בסגמנט ה-DATA

בכל המודלים למעט מודל Huge ערך ה-DS לא משנה את ערכו במהלך התוכנית.
לפיכך בכל תוכנית אסמבלי המשתלבת בקוד C והמקומפלת בכל המודלים למעט
מודל Huge ניתן להכריז על משתנים (סטטיים) תחת ה-DATA. או ה-DATA_
ולהתייחס בהם בתוכנית ללא חשש שה-DS לא בהכרח מצביע לסגמנט הנכון. אין צורך
לעדכן את ערכו של ה-DS ואין צורך ב-Segment Override. יוצא דופן הוא מודל
ה-Huge, תוכנית אסמבלי הנקראת מקוד C במקומפל במודל Huge כן צריכה
להתייחס לנושא הזה, נניח באמצעות האופרטור SEG.

חשוב לזכור: כאשר פוינטר (למידע או לפונקציה) מועבר כפרמטר, הגודל שלו
קובע את מיקומו של הפרמטר הבא אם ישנו כזה. במידה ופוינטר מועבר במחסנית
בכתובת [BP+10] והפוינטר הוא 16 ביט, הפרמטר הבא נמצא בכתובת [BP+12].
לעומת זאת אם הוא פוינטר ל-32 ביט הפרמטר הבא נמצא בכתובת [BP+14].
לפיכך יש כאן השפעה נוספת של המודל על מיקום הפרמטרים, שצריך להביא
בחשבון. במודלים Compact ו-Medium יש הבדל בהשפעה אם מדובר בפוינטר
לפונקציה או למידע. במודלים האחרים זה פשוט יותר: ב-Tiny ו-Small
הפונטרים מכל סוג הם 16 ביט, ב-Large ו-Huge הפוינטרים מכל סוג 32 ביט.

תוכניות דוגמא call_id1.c, idiv_mo7.asm

בתוכנית המשולבת call_id1.c, idiv_mo1.asm ההנחה ב-idiv_mo1.asm היתה שהקימפול הוא במודל Small. בקובץ idiv_mo7.asm הפונקציה idiv_mod ממומשת עבור קימפול במודל Large. תמונת המחסנית היא עכשיו כזו:

BP ישן	← BP
IP	[BP+2]
CS	[BP+4]
תוכן Num	[BP+6]
תוכן Denum	[BP+8]
כתובת Q	[BP+10]
כתובת Rem	[BP+14]

מבנה המחסנית השתנה בשני הקשרים: הפרמטר הראשון הוא ב-[BP+6] במקום ב-[BP+4] ומאחר והפוינטרים עכשיו 32 ביט, הפרמטר "כתובת Rem" נמצא במרחק 4 בתים מתחילת הפרמטר "כתובת Q". בנוסף לכך כל שימוש בפוינטרים מחייב מוערבות של אוגר סגמנט. כתור אוגר סגמנט נעשה שימוש ב-ES, והוא נטען בחצי המרוחק של שני הפוינטרים (BP+12 ו-BP+16). בפוינטר מלא ההיסט תמיד מקדים את מספר הסגמנט.

```

/* call_id1.c - call assembler subroutine idiv_mod.asm from C program */
#include <stdio.h>

extern int idiv_mod(int Num, int Denom, int *Q, int *Rem);

void main()
{
    int Num, Denom, Q, Rem, No_Zero_Divide;

    printf("\nEnter Numerator, Denominator\n:");
    scanf("%d %d",&Num, &Denom);
    No_Zero_Divide = idiv_mod(Num,Denom,&Q,&Rem);
    if (No_Zero_Divide)
        printf("\n %d div %d = %d, mod(%d,%d) = %d\n",
            Num, Denom, Q, Num, Denom, Rem);
    else
        printf("\nError: Zero Divide.\n");
} /* main */

```

```

E:\>tcc -ml call_id1.c idiv_mo7.asm
Turbo C++ Version 3.00 Copyright (c) 1992 Borland International
call_id1.c:
idiv_mo7.asm:
Turbo Assembler Version 3.1 Copyright (c) 1988, 1992 Borland
International

```

```

Assembling file:    idiv_mo7.ASM
Error messages:     None
Warning messages:   None
Passes:             1
Remaining memory:   398k

```

```

Turbo Link Version 5.0 Copyright (c) 1992 Borland International

```

```

    Available memory 4115728

```

```

E:\>CALL_ID1.EXE
Enter Numerator, Denominator
:7000    666

```

```

    7000 div 666 = 10, mod(7000,666) = 340

```

```

E:\>

```

```

; idiv_mo7.asm - MODEL LARGE assembler implementation of
;               C-callable function idiv_mod.
;
.MODEL LARGE
.CODE
; Implementation of C callable function ...
; ... int idiv_mod(int Num, int Denom, int *Q, int *Rem)
;               [BP+6]    [BP+8]    [BP+10]    [BP+14]
; Compute Q := |_ Num / Denom _| ,Rem := MOD(Num, Denom)
; function idiv_mod returns 0 if Denom = 0 (illegal ..
; ... division by zero), 1 otherwise
;
PUBLIC _idiv_mod
_idiv_mod PROC FAR
    PUSH BP          ; Preserve BP
    MOV BP,SP        ; Set BP to point to Parameter area
    PUSH SI          ; Preserve register variables
    PUSH DI          ;
    PUSH ES          ;

;
    MOV SI,[BP+8]    ; SI := Denom
    CMP SI,0        ; Denom = 0 ?
    JNE Cont        ; No, continue regular operation
                    ; Yes, Denom = 0
    MOV AX,0        ; Return value := 0
    JMP Done        ; Skip following code
Cont:              ; Denom <> 0
    MOV AX,[BP+6]    ; AX := Num
    CWD             ; DX:AX := AX
    IDIV SI         ; AX := DX:AX / SI, DX := MOD(AX,SI)
    MOV DI,[BP+10]   ; DI := Offset Q
    MOV ES,[BP+12]   ; ES := Seg Q
    MOV ES:[DI],AX   ; *Q := AX
    MOV DI,[BP+14]   ; DI := Offset Rem
    MOV ES,[BP+16]   ; ES := Seg Q
    MOV ES:[DI],DX   ; *Rem := DX
    MOV AX,1        ; Ensure return value := 1
Done:
;
    POP ES          ;
    POP DI          ; Restore register variables
    POP SI          ;
    POP BP          ; Restore BP register
    RET
_idiv_mod ENDP
END

```

תוכניות דוגמא call_id2.c, idiv_m10.asm

בתוכנית המשולבת call_id2.c, idiv_m06.asm ההנחה ב-idiv_m06.asm היתה שהקימפול הוא במודל Small. בקובץ idiv_m10.asm הפונקציה idiv_mod32 ממומשת עבור קימפול במודל Large. תמונת המחסנית היא עכשיו כזו:

BP ישן	← BP
IP	[BP+2]
CS	[BP+4]
Num תוכן	[BP+6]
Denum תוכן	[BP+10]
Q כתובת	[BP+14]
Rem כתובת	[BP+18]

מבנה המחסנית השתנה בשני הקשרים: הפרמטר הראשון הוא ב-[BP+6] במקום ב-[BP+4] ומאחר והפוינטרים עכשיו 32 ביט, הפרמטר "Rem כתובת" נמצא במרחק 4 בתים מתחילת הפרמטר "כתובת Q". בנוסף לכך כל שימוש בפוינטרים מחייב מוערבות של אוגר סגמנט. בתור אוגר סגמנט נעשה שימוש ב-ES, והוא נטען בחצי המרוחק של שני הפונטרים (BP+16 ו-BP+20). בפוינטר מלא ההיסט תמיד מקדים את מספר הסגמנט.


```

/* call_id2.c - call assembler subroutine idiv_mod32.asm from C program */

#include <stdio.h>

extern int idiv_mod32(long int Num, long int Denom,
                     long int *Q, long int *Rem);

void main()
{
    long int Num, Denom, Q, Rem;
    int No_Zero_Divide;

    printf("\nEnter Numerator, Denominator\n:");
    scanf("%ld %ld",&Num, &Denom);
    No_Zero_Divide = idiv_mod32(Num,Denom,&Q,&Rem);
    if (No_Zero_Divide)
        printf("\n %ld div %ld = %ld, mod(%ld,%ld) = %ld\n",
              Num, Denom, Q, Num, Denom, Rem);
    else
        printf("\nError: Zero Divide.\n");
} /* main */

```

```

E:\asm>tcc -ml call_id2.c idiv_m10.asm
Turbo C++ Version 3.00 Copyright (c) 1992 Borland International
call_id2.c:
idiv_m10.asm:
Turbo Assembler Version 3.1 Copyright (c) 1988, 1992 Borland
International

```

```

Assembling file:    idiv_m10.ASM
Error messages:     None
Warning messages:   None
Passes:             1
Remaining memory:   431k

```

```

Turbo Link Version 5.0 Copyright (c) 1992 Borland International

    Available memory 4149984

```

```

E:\asm>call_id2.exe
Enter Numerator, Denominator
:700000 111110

```

```

    700000 div 111110 = 6, mod(700000,111110) = 33340

```

```

E:\asm>

```

```

; idiv_m10.asm - Assembler implementation of
;                                     C-callable function idiv_mod32.
;

.MODEL LARGE
.CODE
.386
; Implementation of C callable function ...
; ... int idiv_mod32(long int Num, long int Denom,
;                   [BP+6]           [BP+10]
; long int *Q,      long int *Rem)
;   [BP+14]         [BP+18]
; Compute Q := |_ Num / Denom _| , Rem := MOD(Num, Denom)
; function idiv_mod32 returns 0 if Denom = 0 (illegal ..
; ... division by zero), 1 otherwise
;
PUBLIC _idiv_mod32
_idiv_mod32 PROC FAR
    PUSH BP          ; Preserve BP
    MOV BP,SP        ; Set BP to point to Parameter area
    PUSH SI          ; Preserve register variables
    PUSH DI
    PUSH ES

;
    MOV ESI,[BP+10]  ; ESI := Denom
    CMP ESI,0        ; Denom = 0 ?
    JNE Cont         ; No, continue regular operation
                    ; Yes, Denom = 0
    MOV AX,0         ; Return value := 0
    JMP Done         ; Skip following code
Cont:                ; Denom <> 0
    MOV EAX,[BP+6]   ; EAX := Num
    CDQ              ; EDX:EAX := EAX
    IDIV ESI         ; EAX := EDX:EAX / ESI, EDX := MOD(EAX,ESI)
    MOV DI,[BP+14]   ; DI := Offset Q
    MOV ES,[BP+16]   ; ES := Seg Q
    MOV ES:[DI],EAX  ; *Q := AX
    MOV DI,[BP+18]   ; DI := Offset Rem
    MOV ES,[BP+20]   ; ES := Seg Rem
    MOV ES:[DI],EDX  ; *Rem := DX
    MOV AX,1        ; Ensure return value := 1
Done:
;
    POP ES          ;
    POP DI          ; Restore register variables
    POP SI          ;
    POP BP          ; Restore BP register
    RET
_idiv_mod32 ENDP
END

```

תוכניות דוגמא runswap1.c, swaps.asm, swap11.asm, swap12.asm

תוכניות הדוגמא המצוינות ממחישות את עיקרי ההבדלים בתכנות באסמבלי במודלים Small ו-Large. תתי התוכניות swap16, swap32 ו-swap_n מבצעות החלפה של ערכי משתנים (בגדלים שונים) של התוכנית הקוראת לפי פוינטרים שהוכנית הקוראת מעבירה.

ההבדלים הבאים לידי ביטוי בדוגמאות הללו הן:
- בעוד ששני הפוינטרים המועברים כפוינטרים במודל Small נמצאים בכתובות [BP+4] ו-[BP+6] בתוכניות במודל Large הם נמצאים בכתובות [BP+6] ו-[BP+10].

- בעוד שכאשר משתמשים בפוינטרים במודל Small מתיחסים להיסט כאילו הוא כל הכתובות, בתוכניות במודל Large יש לדאוג לטעון לאוגר סגמנט את מרכיב הסגמנט של הפוינטר בטרם נעשה בו שימוש.

התוכנית swap11.asm נכתבה בסגנון 8086 כאשר אוגר הסגמנט ES היה בבחינת אוגר הסגמנט הפנוי היחיד למטרות מהסוג של שימוש בפוינטר מלא. התוכנית swap12.asm מנצלת את העובדה שהחל מה-386 קיימים למטרות מסוג זה 2 אוגרי סגמנט נוספים: FS ו-GS.

```

/* runswap1.c - run swaps */

extern void swap16( int *x, int *y);
extern void swap32(long int *x, long int *y);
extern void swap_n( void *x, void *y, int n);

int main ()
{
    int x=10, y=99;
    long int u=333333, v=777777;
    char str1[10]="Hello", str2[10]="World!";

    printf("x = %d, y = %d\n", x, y);
    swap16(&x, &y);
    printf("x = %d, y = %d\n", x, y);

    printf("u = %ld, v = %ld\n", u, v);
    swap32(&u, &v);
    printf("u = %ld, v = %ld\n", u, v);

    printf("str1 = %s, y = %s\n", str1, str2);
    swap_n(str1, str2, 10);
    printf("str1 = %s, str2 = %s\n", str1, str2);

    return 0;
} /* main */

```

```

E:\>tcc runswap1.c swaps.asm
Turbo C++ Version 3.00 Copyright (c) 1992 Borland International
runswap1.c:
swaps.asm:
Turbo Assembler Version 3.1 Copyright (c) 1988, 1992 Borland
International

```

```

Assembling file:    swaps.ASM
Error messages:     None
Warning messages:   None
Passes:             1
Remaining memory:   398k

```

```

Turbo Link Version 5.0 Copyright (c) 1992 Borland International

    Available memory 4129872

```

```

E:\ACADEMIC\ASM>runswap1.exe
x = 10, y = 99
x = 99, y = 10
u = 333333, v = 777777
u = 777777, v = 333333
str1 = Hello, y = World!
str1 = World!, str2 = Hello

E:\>

```

170

```

;
;  swaps.asm - swap program model small
;
.MODEL SMALL
.CODE
.386
;
;  extern void swap16( int *x, int *y);
;                      [BP+4]  [BP+6]
;
_swap16 PROC NEAR
    PUBLIC _swap16
    PUSH BP
    MOV BP,SP
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+4]
    MOV DI,[BP+6]
    MOV AX,[SI]
    XCHG AX,[DI]
    MOV [SI],AX
;
    POP DI
    POP SI
    POP BP
    RET
_swap16 ENDP
;
;  extern void swap32( long int *x, long int *y);
;                      [BP+4]          [BP+6]
;
_swap32 PROC NEAR
    PUBLIC _swap32
    PUSH BP
    MOV BP,SP
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+4]
    MOV DI,[BP+6]
    MOV EAX,[SI]
    XCHG EAX,[DI]
    MOV [SI],EAX
;
    POP DI
    POP SI
    POP BP
    RET
_swap32 ENDP

```

```

;
; extern void swap_n( void *x, void *y, int n);
;                      [BP+4]    [BP+6]    [BP+8]
;
;
__swap_n PROC NEAR
    PUBLIC __swap_n
    PUSH BP
    MOV BP,SP
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+4]
    MOV DI,[BP+6]
    MOV CX,[BP+8]
    JCXZ ToRet1
Aloop1:
    MOV AL,[SI]
    XCHG AL,[DI]
    MOV [SI],AL
    INC SI
    INC DI
;
    LOOP Aloop1
;
ToRet1:
    POP DI
    POP SI
    POP BP
    RET
__swap_n ENDP
    END

```

```

/* runswap1.c - run swaps */

extern void swap16( int *x, int *y);
extern void swap32(long int *x, long int *y);
extern void swap_n( void *x, void *y, int n);

int main ()
{
    int x=10, y=99;
    long int u=333333, v=777777;
    char str1[10]="Hello", str2[10]="World!";

    printf("x = %d, y = %d\n", x, y);
    swap16(&x, &y);
    printf("x = %d, y = %d\n", x, y);

    printf("u = %ld, v = %ld\n", u, v);
    swap32(&u, &v);
    printf("u = %ld, v = %ld\n", u, v);

    printf("str1 = %s, y = %s\n", str1, str2);
    swap_n(str1, str2, 10);
    printf("str1 = %s, str2 = %s\n", str1, str2);

    return 0;
} /* main */

```

```

E:\>tcc -ml runswap1.c swap11.asm
Turbo C++ Version 3.00 Copyright (c) 1992 Borland International
runswap1.c:
swap11.asm:
Turbo Assembler Version 3.1 Copyright (c) 1988, 1992 Borland
International

```

```

Assembling file:    swap11.ASM
Error messages:     None
Warning messages:   None
Passes:             1
Remaining memory:   397k

```

```

Turbo Link Version 5.0 Copyright (c) 1992 Borland International

    Available memory 4129616

```

```

E:\ACADEMIC\ASM>runswap1.exe
x = 10, y = 99
x = 99, y = 10
u = 333333, v = 777777
u = 777777, v = 333333
str1 = Hello, y = World!
str1 = World!, str2 = Hello

```

```

E:\>

```

173

```

;
; swap11.asm - swap program model large
;
.MODEL LARGE
.CODE
.386
;
; extern void swap16( int *x, int *y);
;                      [BP+6]  [BP+10]
;
_swap16 PROC FAR
PUBLIC _swap16
    PUSH BP
    MOV BP,SP
    PUSH ES
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+6]
    MOV DI,[BP+10]
;
    MOV ES,[BP+8]
    MOV AX,ES:[SI]
    MOV ES,[BP+12]
    XCHG AX,ES:[DI]
    MOV ES,[BP+8]
    MOV ES:[SI],AX
;
    POP DI
    POP SI
    POP ES
    POP BP
    RET
_swap16 ENDP
;
; extern void swap32( long int *x, long int *y);
;                      [BP+6]      [BP+10]
;
_swap32 PROC FAR
PUBLIC _swap32
    PUSH BP
    MOV BP,SP
    PUSH ES
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+6]
    MOV DI,[BP+10]
;
    MOV ES,[BP+8]
    MOV EAX,ES:[SI]
    MOV ES,[BP+12]
    XCHG EAX,ES:[DI]
    MOV ES,[BP+8]
    MOV ES:[SI],EAX
;
    POP DI
    POP SI
    POP ES
    POP BP
    RET
_swap32 ENDP

```



```

;
; extern void swap_n( void *x, void *y, int n);
;                      [BP+6]    [BP+10]  [BP+14]
;
;
_swap_n PROC FAR
    PUBLIC _swap_n
    PUSH BP
    MOV BP, SP
    PUSH ES
    PUSH SI
    PUSH DI
;
    MOV SI, [BP+6]
    MOV DI, [BP+10]
    MOV CX, [BP+14]
;
    JCXZ ToRet1
Aloop1:
    MOV ES, [BP+8]
    MOV AL, ES:[SI]
    MOV ES, [BP+12]
    XCHG AL, ES:[DI]
    MOV ES, [BP+8]
    MOV ES:[SI], AL
    INC SI
    INC DI
;
    LOOP Aloop1
;
ToRet1:
    POP DI
    POP SI
    POP ES
    POP BP
    RET
_swap_n ENDP
    END

```

```

;
;  swap12.asm - swap program model large
;
.MODEL LARGE
.CODE
.386
;
;  extern void swap16( int *x, int *y);
;                      [BP+6]  [BP+10]
;
_swap16 PROC FAR
PUBLIC _swap16
    PUSH BP
    MOV BP,SP
    PUSH GS
    PUSH FS
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+6]
    MOV GS,[BP+8]
    MOV DI,[BP+10]
    MOV FS,[BP+12]
;
    MOV AX,GS:[SI]
    XCHG AX,FS:[DI]
    MOV GS:[SI],AX
;
    POP DI
    POP SI
    POP FS
    POP GS
    POP BP
    RET
_swap16 ENDP
;
;  extern void swap32( long int *x, long int *y);
;                      [BP+6]      [BP+10]
;
_swap32 PROC FAR
PUBLIC _swap32
    PUSH BP
    MOV BP,SP
    PUSH GS
    PUSH FS
    PUSH SI
    PUSH DI
;
    MOV SI,[BP+6]
    MOV GS,[BP+8]
    MOV DI,[BP+10]
    MOV FS,[BP+12]
    MOV EAX,GS:[SI]
    XCHG EAX,FS:[DI]
    MOV GS:[SI],EAX
;
    POP DI
    POP SI
    POP FS
    POP GS
    POP BP
    RET
_swap32 ENDP

```

```

;
; extern void swap_n( void *x, void *y, int n);
;                [BP+6]    [BP+10]  [BP+14]
;
;
_swap_n PROC FAR
    PUBL IC _swap_n
        PUSH BP
        MOV BP,SP
        PUSH GS
        PUSH FS
        PUSH SI
        PUSH DI
;
    MOV SI,[BP+6]
    MOV GS,[BP+8]
    MOV DI,[BP+10]
    MOV FS,[BP+12]
    MOV CX,[BP+14]
;
    JCXZ ToRet1
Aloop1:
    MOV AL,GS:[SI]
    XCHG AL,FS:[DI]
    MOV GS:[SI],AL
    INC SI
    INC DI
;
    LOOP Aloop1
;
ToRet1:
    POP DI
    POP SI
    POP FS
    POP GS
    POP BP
    RET
_swap_n ENDP
    END

```