קומפילציה tcc -S ותוכנית הדוגמא call_idl.asm

call_idl.asm הינו קובץ האסמבלי שמתקבל מקימפול התוכנית call_idl.c ע"י האופציות

```
tcc -S -r- call_idl.c
```

כאשר האופציה S- מנחה את הקומפילר לתרגם את התוכנית לקובץ אסמבלי (call_idl.asm) במקום לקבצי obj ו-exe שהקומפילר בדרך כלל מיצר. האופציה r- מנחה את הקומפילר לא להשתמש במשתני אוגר. האופציה הזו נבחרה בשביל להקל על הבנת התוכנית.

חלקי התוכן של call_idl.asm החשובים לנו נסקרו קודם לכן תחת הכותרת "סכמת ניהול המשתנים של TURBO C".

האופציה S- נתמכת ברוב הקומפילרים של C. יש לו מספר שימושים חשובים. תוכניתן אסמבלי שיש לו משימה מורכבת יכול בהחלט להסתיע בידיעת איך הקומפילר ממש אותו. בנוסף, תוכניתן בשפה C המפתח תוכנה שבו הוא מכיר את שפת האסמבלי יכול ע"י עיון בקובץ האסמבלי הנוצר לאתר בעיות הכרוכות בקימפול שונה מהצפוי של תוכנית המקור. זה יכול להוביל לאיתור שגיעות הנובעות מפרשנות שונה מהצפוי של הקוד ע"י הקומפילר או איתור סיבות לאיטיות של קוד איטי מהצפוי בקובץ ה-exe. אפשר אפילו "לשפר" את ה-exe הנוצר ע"י הכנסת שינויים בקובץ ה-asm והכללותו בקימפול במקום קובץ המקור ב-C.

call_id1.asm

tcc -S -r- call_id1.c

```
        ifndef  ??version
?debug  macro
        endm
$comm   macro   name,dist,size,count
        comm    dist name:BYTE:count*size
        endm
        else
$comm   macro   name,dist,size,count
        comm    dist name[size]:BYTE:count
        endm
        endif
        ?debug  S "call_id1.c"
        ?debug  C E9857A13270A63616C6C5F6964312E63
        ?debug  C E90018521815433A5C54435C494E434C5544455C737464696F2E68
        ?debug  C E90018521815433A5C54435C494E434C5544455C5F646566732E68
        ?debug  C E90018521815433A5C54435C494E434C5544455C5F6E756C6C2E68
_TEXT   segment byte public 'CODE'
_TEXT   ends
DGROUP  group   _DATA,_BSS
        assume  cs:_TEXT,ds:DGROUP
_DATA   segment word public 'DATA'
d@      label   byte
d@w     label   word
_DATA   ends
_BSS    segment word public 'BSS'
b@      label   byte
b@w     label   word
_BSS    ends
_TEXT   segment byte public 'CODE'
   ;
   ;     void main()
   ;
        assume  cs:_TEXT
_main   proc    near
        push    bp
        mov     bp,sp
        sub     sp,10
   ;
   ;        {
   ;          int Num, Denom, Q, Rem, No_Zero_Divide;
   ;
   ;          printf("\Enter Numerator, Denominator\n:");
   ;
        mov     ax,offset DGROUP:s@
        push    ax
        call    near ptr _printf
        pop     cx
```

```
;
;           scanf("%d %d",&Num, &Denom);
;
        lea     ax,word ptr [bp-4]
        push    ax
        lea     ax,word ptr [bp-2]
        push    ax
        mov     ax,offset DGROUP:s@+31
        push    ax
        call    near ptr _scanf
        add     sp,6
;
;           No_Zero_Divide = idiv_mod(Num,Denom,&Q,&Rem);
;
        lea     ax,word ptr [bp-8]
        push    ax
        lea     ax,word ptr [bp-6]
        push    ax
        push    word ptr [bp-4]
        push    word ptr [bp-2]
        call    near ptr _idiv_mod
        add     sp,8
        mov     word ptr [bp-10],ax
;
;           if  (No_Zero_Divide)
;
        cmp     word ptr [bp-10],0
        je      short @1@86
;
;             printf("\n %d div %d = %d, mod(%d,%d) = %d\n",
;
;
;                       Num, Denom, Q, Num, Denom, Rem);
;
        push    word ptr [bp-8]
        push    word ptr [bp-4]
        push    word ptr [bp-2]
        push    word ptr [bp-6]
        push    word ptr [bp-4]
        push    word ptr [bp-2]
        mov     ax,offset DGROUP:s@+37
        push    ax
        call    near ptr _printf
        add     sp,14
        jmp     short @1@114
```

```
@1@86:
   ;
   ;           else
   ;              printf("\nError: Zero Divide.\n");
   ;
        mov     ax,offset DGROUP:s@+72
        push    ax
        call    near ptr _printf
        pop     cx
@1@114:
   ;
   ;         } /* main */
   ;
        mov     sp,bp
        pop     bp
        ret
_main   endp
        ?debug  C E9
_TEXT   ends
_DATA   segment word public 'DATA'
s@      label   byte
        db      'Enter Numerator, Denominator'
        db      10
        db      ':'
        db      0
        db      '%d %d'
        db      0
        db      10
        db      ' %d div %d = %d, mod(%d,%d) = %d'
        db      10
        db      0
        db      10
        db      'Error: Zero Divide.'
        db      10
        db      0
_DATA   ends
_TEXT   segment byte public 'CODE'
_TEXT   ends
        public  _main
        extrn   _idiv_mod:near
        extrn   _scanf:near
        extrn   _printf:near
_s@     equ     s@
        end
```

רקורסיה ותוכנית הדוגמא fibo4.asm

fibo4.asm הינו קובץ האסמבלי שמתקבל מקימפול התוכנית fibo4.c ע"י האופציות

```
tcc -S -r- fibo4.c
```

כאשר האופציה S- מנחה את הקומפילר לתרגם את התוכנית לקובץ אסמבלי (fibo4.asm) במקום לקבצי obj ו-exe שהקומפילר בדרך כלל מיצר. האופציה r- מנחה את הקומפילר לא להשתמש במשתני אוגר. האופציה הזו נבחרה בשביל להקל על הבנת התוכנית.

תפקידה של הדוגמא למחיש את מימוש מושג הרקורסיה ברמת הקומפילציה.

החשיבות של הנושא הזה בפרק זה הוא להמחיש שכאשר ממשים משתנים / פרמטרים וכתובות חזרה דרך המחסנית כפי ש-Turbo C ורוב הקומפילרים של C עושים, מימוש קוד רקורסיבי הוא אופציה המתקבלת בחינם או שהצורך של התחשבות נוספת במימוש קוד רקורסיבי מינימלי ביותר. אם נעיין במימוש של הקוד שנפרש על מנת לממש את הקריאה

```
fibo(n-2)
```

המימוש שלו באסמבלי יהיה

```
mov ax,word ptr [bp+4]
sub ax,2
push ax
call near ptr _fibo
```

לפיכך הקריאה הרקורסיבית אינה שונה במאומה מקריאה לפונקציה חיצונית. יש הבדל לוגי בכך שההסתעפות היא לראשות הפונקציה עצמה ולא לכתובת שמחוץ לרוטינה אבל זה לא בא לידי ביטוי בטקסט של הקוד שנוצר. לשון אחר: מתכנת שהיה צריך לממש את הרקורסיה ידנית באסמבלי לא צריך לדעת יותר מהמוסכמות הרגילות של מימוש פונקציות ב-C.

העובדה שמימוש רקורסיה מתקבלת כתוספת חינם למוסכמות מימוש פונקציות ב-C לא היה, כנראה, הסיבה העיקרית להגדרת בצורתן מבוססת המחסנית. סביר להניח שהמניע העיקרי היה לקבל אפקט זהה (או כמעט זהה, תלוי בהשקפה) של הרצת קוד במקביל במימוש מושג התהליכים, נושא מתקדם שלא נכנס לו כאן. למעשה מושג "מחסנית מערכת" הקיימת בכל הארכיטקטורות של מחשבים מודרניים הומצאה על מנת לקבל את האפקט הזה, הנקרא Re-entrancy. אנחנו נומר שהסיבה שהאפקט מתקבל היא מאותה סיבה שהמוסכמות משרתות גם מימוש תהליכים.

הסיבה שמוסכמות הללו תומכות ברקורסיה (או ב-Re-entrancy באופן כללי) היא בכך שהם ממשות את מנגנוני המשתנים, הפרמטרים ושימור כתובות הסתעפות עתידיות בתוך שטחי זיכרון דינמיים שמשתחררים בסדר של "אחרון נכנס ראשון יוצא".

על מנת לממש קריאה רקורסבית צריך לממש רובד חדש של פרמטרים ומשתנים לוקליים תוך שימור הערכים הקודמים והסתעפות לראשית הרוטינה תוך שימור כתובת החזרה. על מנת לממש חזרה מרקוסיה צריך לחזור חזרה לפקודה שמעבר לקריאה הרקורסיבית האחרונה (או מעבר לקריאה המקורית) ולשחרר את רובד המשתנים הלוקליים והפרמטרים האחרון תוך שחזור הקודם לו. את כל אלה המוסכמות עושות ממילא מעצמם.

```
/* fibo4.c - implement Fibonacci numbers - naive recursion  */

#include <stdio.h>

unsigned long int fibo(unsigned int n)
{
  unsigned long int x, y, z;

  if  ( n <= 2 )
     return 1L;
  else
    x = fibo(n-1);
    y = fibo(n-2);
    z = x + y;
    return z;
}

 void main()
  {
    unsigned int n;
    printf("Enter an integer:\n");
    scanf("%d",&n);

    printf("Fibonacci(%u) = %lu\n", n, fibo(n));

  }
```

```
E:\>fibo4.exe
Enter an integer:
10
Fibonacci(10) = 55

E:\>
```

fibo4.asm

```
_TEXT   segment byte public 'CODE'
_TEXT   ends
DGROUP  group   _DATA,_BSS
        assume  cs:_TEXT,ds:DGROUP
_DATA   segment word public 'DATA'
d@      label   byte
d@w     label   word
_DATA   ends
_BSS    segment word public 'BSS'
b@      label   byte
b@w     label   word
_BSS    ends
_TEXT   segment byte public 'CODE'
   ;
   ;    unsigned long int fibo(unsigned int n)
   ;
        assume  cs:_TEXT
_fibo   proc    near
        push    bp
        mov     bp,sp
        sub     sp,12
   ;
   ;    {
   ;      unsigned long int x, y, z;
   ;
   ;      if  ( n <= 2 )
   ;
        cmp     word ptr [bp+4],2
        ja      short @1@142
   ;
   ;         return 1L;
   ;
        xor     dx,dx
        mov     ax,1
@1@86:
        jmp     short @1@198
        jmp     short @1@170
@1@142:
   ;
   ;      else
   ;        x = fibo(n-1);
   ;
        mov     ax,word ptr [bp+4]
        dec     ax
        push    ax
        call    near ptr _fibo
        pop     cx
        mov     word ptr [bp-2],dx
        mov     word ptr [bp-4],ax
@1@170:
   ;
   ;        y = fibo(n-2);
   ;
        mov     ax,word ptr [bp+4]
        sub     ax,2
        push    ax
        call    near ptr _fibo
        pop     cx
        mov     word ptr [bp-6],dx
        mov     word ptr [bp-8],ax
```

tcc -S -r- fibo4.asm

```
   ;
   ;        z = x + y;
   ;
        mov     ax,word ptr [bp-2]
        mov     dx,word ptr [bp-4]
        add     dx,word ptr [bp-8]
        adc     ax,word ptr [bp-6]
        mov     word ptr [bp-10],ax
        mov     word ptr [bp-12],dx
   ;
   ;        return z;
   ;
        mov     dx,word ptr [bp-10]
        mov     ax,word ptr [bp-12]
        jmp     short @1@86
@1@198:
   ;
   ;    }
   ;
        mov     sp,bp
        pop     bp
        ret
_fibo   endp
   ;
   ;     void main()
   ;
        assume  cs:_TEXT
_main   proc    near
        push    bp
        mov     bp,sp
        sub     sp,2
   ;
   ;      {
   ;        unsigned int n;
   ;        printf("Enter an integer:\n");
   ;
        mov     ax,offset DGROUP:s@
        push    ax
        call    near ptr _printf
        pop     cx
   ;
   ;        scanf("%d",&n);
   ;
        lea     ax,word ptr [bp-2]
        push    ax
        mov     ax,offset DGROUP:s@+19
        push    ax
        call    near ptr _scanf
        pop     cx
        pop     cx
```

```
    ;
    ;
    ;       printf("Fibonacci(%u) = %lu\n", n, fibo(n));
    ;
        push    word ptr [bp-2]
        call    near ptr _fibo
        pop     cx
        push    dx
        push    ax
        push    word ptr [bp-2]
        mov     ax,offset DGROUP:s@+22
        push    ax
        call    near ptr _printf
        add     sp,8
    ;
    ;
    ;     }
    ;
        mov     sp,bp
        pop     bp
        ret
_main   endp
        ?debug  C E9
_TEXT   ends
_DATA   segment word public 'DATA'
s@      label   byte
        db      'Enter an integer:'
        db      10
        db      0
        db      '%d'
        db      0
        db      'Fibonacci(%u) = %lu'
        db      10
        db      0
_DATA   ends
_TEXT   segment byte public 'CODE'
_TEXT   ends
        public  _main
        public  _fibo
        extrn   _scanf:near
        extrn   _printf:near
_s@     equ     s@
        end
```

גירסאות מיוחדות של הפקודה CALL

השימושים בפקודה CALL שראינו עד עכשיו היו מהסוג של CALL לנקודה בזיכרון הנמצא 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.

ב-8086 היה קיים גירסה של CALL עם אוגר 16 ביט. המשמעות שלו היא להציב את ערך האוגר לתוך IP. לדוגמא, הפקודה

```
CALL BX
```

היתה 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 בזיכרון. במקרה הזה האופרנד של הפקודה CALL הוא לא כתובת של פקודה אלא כתובת של משתנה. במקרה הזה, הכתובת בזיכרון איננו מגדיר את הערך החדש של CS:IP אלא היכן נמצא הערך החדש בזה. 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
```

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

```
CALL f_ptr2
```

יגרום להסתעפות מסוג FAR כאשר מלבד שימור הערכים הנוכחים של 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 פיונטר לפונקציה.

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 גירסות נוספות של הפקודה CALL התומכות בהיסטים 32 ביט.

קימות פקודות ההסוג

```
CALL ECX
```

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

כמו כן ישנם פקודות הסתעפות עקיפה NEAR 32 ביט (שינוי EIP בלבד) וכן הסתעפיות עקיפות 48 ביט. משתנים כאילו 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.

```
/* pf.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:\>
```