

C Home_assignment

207938903 יהונתן ארמא

:Part B

(1) ההבדל בין משתנים גלובליים ללוקאליים:

בשפת c, משתנים ניתן להגדיר בתוך פונקציות ומחוץ לפונקציות.

משתנים המוגדרים מחוץ לפונקציות נקראים 'משתנים גלובליים' ומשתנים המוגדרים בתוך פונקציות נקראים 'משתנים לוקאליים'.

ה-**"scope"** של המשתנים הגלובליים הוא כל התוכנית, כלומר כל פונקציה בתוכנית (יותר נכון ב-file כל עוד לא הגדרנו את המשתנה ב-extern) יכולה 'לראות' את המשתנה ולהשתמש בו.

ה-“scope” של המשתנים הלוקאליים הוא הפונקציה או “הסוגריים המסלולים” בהם הם הוגדרו, כלומר אם משתנה הוגדר בפונקציה מסוימת אז לא ניתן ‘לראות’ אותו בפונקציה אחרת, ואם משתנה הוגדר בתוך בלוק מסוים (לדוגמה “if”) אז לא ניתן ‘לראות’ אותו מחוץ לבלוק.

עוד הבדל בין השניים – משתנים לוקאליים שמורים במחסים (Stack frame) בעוד שמשתנים גלובליים שמורים מחוץ ל-Stack. (Data או BSS)

בתוכנית שהוצגה לנו:

דוגמה למשתנה גלובלי:

maxTrace (שורה 34) – חוץ מזה שסומן לנו בגדול שזה החלק של המשתנים הגלובליים, ניתן להבין שזה משתנה גלובלי מכיוון שהוא לא בתוך אף פונקציה (הוא לא חלק משום "scope") ולכן ה-"scope" שלו הוא כל התוכנית.

דוגמה למשתנה לוקאלי:

Trace (שורה 101) – משתנה זה הוגדר לנו בתוך פונקציה (ComputeTrace) ולכן ה-“scope” שלו הוא רק בתוך הפונקציה הזאת.

(2) ניתן לראות שכאשר עושים Debug לתוכנית מקבלים עליה נתונים בזמן אמת.

לדוגמה, בריצה זו קיבלנו שהערך של המשתנה Mat הוא "0x00d8fac8" שזה הכתובת של האיבר הראשון במערך.

Name	Value	Type
auxMat	0x00d8f930 {0x00d8f930, -858993460, -858993460, -858993460, -858993460, -858993460, ...}	int[10][10]
ch	-52	char
Mat	0x00d8fac8 {0x00d8fac8, -858993460, -858993460, -858993460, -858993460, -858993460, ...}	int[10][10]
matTrace	-858993460	int
maxDiag	-858993460	int
offset	0	int
Selector	-52	char
str	0x00d8fe8 <Invalid characters in string.>	char[3]

בנוסף, הכתובת האחרונה של המערך תהיה הכתובת שקבלנו ועוד 4 (שזה גודל int) כפול M (אורך המטריצה) כפול M (רוחב המטריצה) פחות 1 (כי התחלנו לספור מ-0). ומכיוון שבמקרה שלנו M=10 אז נקבל שהאיבר האחרון במערך שמור ב-offset של 396 מההתחלה של המערך כלומר במרחק הקסה של 18C. ולכן יהיה שמור בכתובת "0x00d8fc54".

נבחין שכתובות אלו ישתנו עם כל הרצה של התוכנית ולא ישארו קבועות.

(3) הפעם פתחנו את החלון של הרגיסטרים ב-Debug Mode, ושמו BreakPoint בדיוק בהגעה לפונקציה ComputeTrace. קיבלנו את הערך הבא:

```

99  //-----
100 int ComputeTrace(int Mat[M][M]) {
101     int Trace = 0, i;
102     for (i = 0; i < M; i++) Trace += Mat[i][i];
103     return Trace;
104 }
105 //-----
106 //-----
107 //-----
108 //-----
109 //-----
110 //-----
111 //-----
112 //-----
113 //-----
114 //-----
115 //-----
116 //-----
117 //-----
118 //-----
119 //-----
120 //-----
121 //-----
122 //-----
123 //-----
124 //-----
125 //-----
126 //-----
127 //-----
128 //-----
129 //-----
130 //-----
131 //-----
132 //-----
133 //-----
134 //-----
135 //-----
136 //-----
137 //-----
138 //-----
139 //-----
140 //-----
141 //-----
142 //-----
143 //-----
144 //-----
145 //-----
146 //-----
147 //-----
148 //-----
149 //-----
150 //-----
151 //-----
152 //-----
153 //-----
154 //-----
155 //-----
156 //-----
157 //-----
158 //-----
159 //-----
160 //-----
161 //-----
162 //-----
163 //-----
164 //-----
165 //-----
166 //-----
167 //-----
168 //-----
169 //-----
170 //-----
171 //-----
172 //-----
173 //-----
174 //-----
175 //-----
176 //-----
177 //-----
178 //-----
179 //-----
180 //-----
181 //-----
182 //-----
183 //-----
184 //-----
185 //-----
186 //-----
187 //-----
188 //-----
189 //-----
190 //-----
191 //-----
192 //-----
193 //-----
194 //-----
195 //-----
196 //-----
197 //-----
198 //-----
199 //-----
200 //-----
201 //-----
202 //-----
203 //-----
204 //-----
205 //-----
206 //-----
207 //-----
208 //-----
209 //-----
210 //-----
211 //-----
212 //-----
213 //-----
214 //-----
215 //-----
216 //-----
217 //-----
218 //-----
219 //-----
220 //-----
221 //-----
222 //-----
223 //-----
224 //-----
225 //-----
226 //-----
227 //-----
228 //-----
229 //-----
230 //-----
231 //-----
232 //-----
233 //-----
234 //-----
235 //-----
236 //-----
237 //-----
238 //-----
239 //-----
240 //-----
241 //-----
242 //-----
243 //-----
244 //-----
245 //-----
246 //-----
247 //-----
248 //-----
249 //-----
250 //-----
251 //-----
252 //-----
253 //-----
254 //-----
255 //-----
256 //-----
257 //-----
258 //-----
259 //-----
260 //-----
261 //-----
262 //-----
263 //-----
264 //-----
265 //-----
266 //-----
267 //-----
268 //-----
269 //-----
270 //-----
271 //-----
272 //-----
273 //-----
274 //-----
275 //-----
276 //-----
277 //-----
278 //-----
279 //-----
280 //-----
281 //-----
282 //-----
283 //-----
284 //-----
285 //-----
286 //-----
287 //-----
288 //-----
289 //-----
290 //-----
291 //-----
292 //-----
293 //-----
294 //-----
295 //-----
296 //-----
297 //-----
298 //-----
299 //-----
300 //-----
301 //-----
302 //-----
303 //-----
304 //-----
305 //-----
306 //-----
307 //-----
308 //-----
309 //-----
310 //-----
311 //-----
312 //-----
313 //-----
314 //-----
315 //-----
316 //-----
317 //-----
318 //-----
319 //-----
320 //-----
321 //-----
322 //-----
323 //-----
324 //-----
325 //-----
326 //-----
327 //-----
328 //-----
329 //-----
330 //-----
331 //-----
332 //-----
333 //-----
334 //-----
335 //-----
336 //-----
337 //-----
338 //-----
339 //-----
340 //-----
341 //-----
342 //-----
343 //-----
344 //-----
345 //-----
346 //-----
347 //-----
348 //-----
349 //-----
350 //-----
351 //-----
352 //-----
353 //-----
354 //-----
355 //-----
356 //-----
357 //-----
358 //-----
359 //-----
360 //-----
361 //-----
362 //-----
363 //-----
364 //-----
365 //-----
366 //-----
367 //-----
368 //-----
369 //-----
370 //-----
371 //-----
372 //-----
373 //-----
374 //-----
375 //-----
376 //-----
377 //-----
378 //-----
379 //-----
380 //-----
381 //-----
382 //-----
383 //-----
384 //-----
385 //-----
386 //-----
387 //-----
388 //-----
389 //-----
390 //-----
391 //-----
392 //-----
393 //-----
394 //-----
395 //-----
396 //-----
397 //-----
398 //-----
399 //-----
400 //-----
401 //-----
402 //-----
403 //-----
404 //-----
405 //-----
406 //-----
407 //-----
408 //-----
409 //-----
410 //-----
411 //-----
412 //-----
413 //-----
414 //-----
415 //-----
416 //-----
417 //-----
418 //-----
419 //-----
420 //-----
421 //-----
422 //-----
423 //-----
424 //-----
425 //-----
426 //-----
427 //-----
428 //-----
429 //-----
430 //-----
431 //-----
432 //-----
433 //-----
434 //-----
435 //-----
436 //-----
437 //-----
438 //-----
439 //-----
440 //-----
441 //-----
442 //-----
443 //-----
444 //-----
445 //-----
446 //-----
447 //-----
448 //-----
449 //-----
450 //-----
451 //-----
452 //-----
453 //-----
454 //-----
455 //-----
456 //-----
457 //-----
458 //-----
459 //-----
460 //-----
461 //-----
462 //-----
463 //-----
464 //-----
465 //-----
466 //-----
467 //-----
468 //-----
469 //-----
470 //-----
471 //-----
472 //-----
473 //-----
474 //-----
475 //-----
476 //-----
477 //-----
478 //-----
479 //-----
480 //-----
481 //-----
482 //-----
483 //-----
484 //-----
485 //-----
486 //-----
487 //-----
488 //-----
489 //-----
490 //-----
491 //-----
492 //-----
493 //-----
494 //-----
495 //-----
496 //-----
497 //-----
498 //-----
499 //-----
500 //-----
501 //-----
502 //-----
503 //-----
504 //-----
505 //-----
506 //-----
507 //-----
508 //-----
509 //-----
510 //-----
511 //-----
512 //-----
513 //-----
514 //-----
515 //-----
516 //-----
517 //-----
518 //-----
519 //-----
520 //-----
521 //-----
522 //-----
523 //-----
524 //-----
525 //-----
526 //-----
527 //-----
528 //-----
529 //-----
530 //-----
531 //-----
532 //-----
533 //-----
534 //-----
535 //-----
536 //-----
537 //-----
538 //-----
539 //-----
540 //-----
541 //-----
542 //-----
543 //-----
544 //-----
545 //-----
546 //-----
547 //-----
548 //-----
549 //-----
550 //-----
551 //-----
552 //-----
553 //-----
554 //-----
555 //-----
556 //-----
557 //-----
558 //-----
559 //-----
560 //-----
561 //-----
562 //-----
563 //-----
564 //-----
565 //-----
566 //-----
567 //-----
568 //-----
569 //-----
570 //-----
571 //-----
572 //-----
573 //-----
574 //-----
575 //-----
576 //-----
577 //-----
578 //-----
579 //-----
580 //-----
581 //-----
582 //-----
583 //-----
584 //-----
585 //-----
586 //-----
587 //-----
588 //-----
589 //-----
590 //-----
591 //-----
592 //-----
593 //-----
594 //-----
595 //-----
596 //-----
597 //-----
598 //-----
599 //-----
600 //-----
601 //-----
602 //-----
603 //-----
604 //-----
605 //-----
606 //-----
607 //-----
608 //-----
609 //-----
610 //-----
611 //-----
612 //-----
613 //-----
614 //-----
615 //-----
616 //-----
617 //-----
618 //-----
619 //-----
620 //-----
621 //-----
622 //-----
623 //-----
624 //-----
625 //-----
626 //-----
627 //-----
628 //-----
629 //-----
630 //-----
631 //-----
632 //-----
633 //-----
634 //-----
635 //-----
636 //-----
637 //-----
638 //-----
639 //-----
640 //-----
641 //-----
642 //-----
643 //-----
644 //-----
645 //-----
646 //-----
647 //-----
648 //-----
649 //-----
650 //-----
651 //-----
652 //-----
653 //-----
654 //-----
655 //-----
656 //-----
657 //-----
658 //-----
659 //-----
660 //-----
661 //-----
662 //-----
663 //-----
664 //-----
665 //-----
666 //-----
667 //-----
668 //-----
669 //-----
670 //-----
671 //-----
672 //-----
673 //-----
674 //-----
675 //-----
676 //-----
677 //-----
678 //-----
679 //-----
680 //-----
681 //-----
682 //-----
683 //-----
684 //-----
685 //-----
686 //-----
687 //-----
688 //-----
689 //-----
690 //-----
691 //-----
692 //-----
693 //-----
694 //-----
695 //-----
696 //-----
697 //-----
698 //-----
699 //-----
700 //-----
701 //-----
702 //-----
703 //-----
704 //-----
705 //-----
706 //-----
707 //-----
708 //-----
709 //-----
710 //-----
711 //-----
712 //-----
713 //-----
714 //-----
715 //-----
716 //-----
717 //-----
718 //-----
719 //-----
720 //-----
721 //-----
722 //-----
723 //-----
724 //-----
725 //-----
726 //-----
727 //-----
728 //-----
729 //-----
730 //-----
731 //-----
732 //-----
733 //-----
734 //-----
735 //-----
736 //-----
737 //-----
738 //-----
739 //-----
740 //-----
741 //-----
742 //-----
743 //-----
744 //-----
745 //-----
746 //-----
747 //-----
748 //-----
749 //-----
750 //-----
751 //-----
752 //-----
753 //-----
754 //-----
755 //-----
756 //-----
757 //-----
758 //-----
759 //-----
760 //-----
761 //-----
762 //-----
763 //-----
764 //-----
765 //-----
766 //-----
767 //-----
768 //-----
769 //-----
770 //-----
771 //-----
772 //-----
773 //-----
774 //-----
775 //-----
776 //-----
777 //-----
778 //-----
779 //-----
780 //-----
781 //-----
782 //-----
783 //-----
784 //-----
785 //-----
786 //-----
787 //-----
788 //-----
789 //-----
790 //-----
791 //-----
792 //-----
793 //-----
794 //-----
795 //-----
796 //-----
797 //-----
798 //-----
799 //-----
800 //-----
801 //-----
802 //-----
803 //-----
804 //-----
805 //-----
806 //-----
807 //-----
808 //-----
809 //-----
810 //-----
811 //-----
812 //-----
813 //-----
814 //-----
815 //-----
816 //-----
817 //-----
818 //-----
819 //-----
820 //-----
821 //-----
822 //-----
823 //-----
824 //-----
825 //-----
826 //-----
827 //-----
828 //-----
829 //-----
830 //-----
831 //-----
832 //-----
833 //-----
834 //-----
835 //-----
836 //-----
837 //-----
838 //-----
839 //-----
840 //-----
841 //-----
842 //-----
843 //-----
844 //-----
845 //-----
846 //-----
847 //-----
848 //-----
849 //-----
850 //-----
851 //-----
852 //-----
853 //-----
854 //-----
855 //-----
856 //-----
857 //-----
858 //-----
859 //-----
860 //-----
861 //-----
862 //-----
863 //-----
864 //-----
865 //-----
866 //-----
867 //-----
868 //-----
869 //-----
870 //-----
871 //-----
872 //-----
873 //-----
874 //-----
875 //-----
876 //-----
877 //-----
878 //-----
879 //-----
880 //-----
881 //-----
882 //-----
883 //-----
884 //-----
885 //-----
886 //-----
887 //-----
888 //-----
889 //-----
890 //-----
891 //-----
892 //-----
893 //-----
894 //-----
895 //-----
896 //-----
897 //-----
898 //-----
899 //-----
900 //-----
901 //-----
902 //-----
903 //-----
904 //-----
905 //-----
906 //-----
907 //-----
908 //-----
909 //-----
910 //-----
911 //-----
912 //-----
913 //-----
914 //-----
915 //-----
916 //-----
917 //-----
918 //-----
919 //-----
920 //-----
921 //-----
922 //-----
923 //-----
924 //-----
925 //-----
926 //-----
927 //-----
928 //-----
929 //-----
930 //-----
931 //-----
932 //-----
933 //-----
934 //-----
935 //-----
936 //-----
937 //-----
938 //-----
939 //-----
940 //-----
941 //-----
942 //-----
943 //-----
944 //-----
945 //-----
946 //-----
947 //-----
948 //-----
949 //-----
950 //-----
951 //-----
952 //-----
953 //-----
954 //-----
955 //-----
956 //-----
957 //-----
958 //-----
959 //-----
960 //-----
961 //-----
962 //-----
963 //-----
964 //-----
965 //-----
966 //-----
967 //-----
968 //-----
969 //-----
970 //-----
971 //-----
972 //-----
973 //-----
974 //-----
975 //-----
976 //-----
977 //-----
978 //-----
979 //-----
980 //-----
981 //-----
982 //-----
983 //-----
984 //-----
985 //-----
986 //-----
987 //-----
988 //-----
989 //-----
990 //-----
991 //-----
992 //-----
993 //-----
994 //-----
995 //-----
996 //-----
997 //-----
998 //-----
999 //-----
1000 //-----

```

ניתן לראות שערך הרגיסטר ה-EIP (כלומר PC) הוא 00181780.

(4) נבחין שזוהי הפונקציה FillMatrix ב-DisAssembly:

```

//-----
void FillMatrix(unsigned int Mat[M][M], int offset) {
00181930 push     ebp
00181931 mov     ebp,esp
00181933 sub     esp,0D8h
00181939 push     ebx
0018193A push     esi
0018193B push     edi
0018193C lea     edi,[ebp-0D8h]
00181942 mov     ecx,36h
00181947 mov     eax,0CCCCCCCCh
0018194C rep stos dword ptr es:[edi]
0018194E mov     ecx,offset _AF62F785_source@c (018C003h)
00181953 call    @_CheckForDebuggerJustMyCode@4 (018122Bh)
    int i, j;
    for (i = 0; i < M; i++) {
00181958 mov     dword ptr [i],0
0018195F jmp     FillMatrix+3Ah (018196Ah)
00181961 mov     eax,dword ptr [i]
00181964 add     eax,1
00181967 mov     dword ptr [i],eax
0018196A cmp     dword ptr [i],0Ah
0018196E jge     FillMatrix+7Bh (01819ABh)
        for (j = 0; j < M; j++) {
00181970 mov     dword ptr [j],0
00181977 jmp     FillMatrix+52h (0181982h)
00181979 mov     eax,dword ptr [j]
0018197C add     eax,1
0018197F mov     dword ptr [j],eax
00181982 cmp     dword ptr [j],0Ah
00181986 jge     FillMatrix+79h (01819A9h)
            Mat[i][j]
            = (offset + i * M + j) % CEIL;
00181988 imul    eax,dword ptr [i],0Ah
0018198C add     eax,dword ptr [offset]
0018198F add     eax,dword ptr [j]
00181992 cdq
00181993 mov     ecx,64h
00181998 idiv    eax,ecx
0018199A imul    eax,dword ptr [i],28h
0018199E add     eax,dword ptr [Mat]
001819A1 mov     ecx,dword ptr [j]
001819A4 mov     dword ptr [eax+ecx*4],edx
        }
001819A7 jmp     FillMatrix+49h (0181979h)
    }
001819A9 jmp     FillMatrix+31h (0181961h)
}
001819AB pop     edi
001819AC pop     esi
001819AD pop     ebx
001819AE add     esp,0D8h
001819B4 cmp     ebp,esp
001819B6 call    __RTC_CheckEsp (018123Ah)
001819BB mov     esp,ebp
001819BD pop     ebp
001819BE ret

```

ניתן להבחין כי:
 הכתובת הראשונה היא 00181930
 זוהי כתובת הפונקציה.

שם הפונקציה FillMatrix מרמז על כך שזאת הפונקציה שממלאת לנו את המטריצה ואכן הפונקציה הזאת מקבלת מטריצה (תאכלס עושה שימוש בכתובת של המטריצה וממלאת שם ערכים) וממלאת את הכניסות במטריצה בערכים לפי נוסחה.

גודל הפונקציה:
 ניתן לראות שהפונקציה מתחילה בכתובת 00181930 ונגמרת בכתובת 001819BE.
 סה"כ לאחר חיסור בהקסא:
 8E כלומר 142 בייטים.

הפונקציה נשמרת ב-RAM באזור שנקרא Code segment או בשם אחר Text Segment.
 שזהו מיקום Read Only ב-Ram שנמצא בתחילתו.

- (5) נבחין שמשנתה auxMat הוא משנתה לוקאלי שמוגדר בתוך פונקציית ה-main. כלומר ניתן לגשת אליו בכל פונקציית ה-main ורק בתוכה. יש לשים לב שהוא נשלח לפונקציה אחרת מה-main, וזה אולי יכול לבלבל, אבל בעצם מה שנשלח זה הכתובת של המערך (כי ערך של משנתה מסוג מערך הוא בעצם הכתובת בה הוא שמור) ובגלל שב-C השימוש הוא ב- Call By Value אז הכתובת מגיעה לפונקציה הנקראת והיא יכול לערוך את המערך. אבל, לא בגלל שניתן לגשת למשתנה דרכה.

כתובתו בפונקציית ה-main:

Name	Value
auxMat	0x00b7f974 { -858993460, -858993460, -858993460, -858993460, -858993460, -858993460, -858993460, ... }
ch	52 'c'
Mat	0x00b7fb0c { 0x00b7fb0c, -858993460, -858993460, -858993460, -858993460, -858993460, -858993460, ... }
matTrace	-858993460
maxDiag	-858993460
offset	0
Selector	52 'c'
str	0x00b7f92c <Invalid characters in string.>

והוא שמור על ה-stack.

- (6) לפי Disassembly:

```

a = a > b ? a : b;
00221D07 mov     eax,dword ptr [a]
00221D0D cmp     eax,dword ptr [b]
00221D13 jle     main+73h (0221D23h)
00221D15 mov     ecx,dword ptr [a]
00221D18 mov     dword ptr [ebp-518h],ecx
00221D21 jmp     main+7Fh (0221D2Fh)
a = a > b ? a : b;
00221D23 mov     edx,dword ptr [b]
00221D29 mov     dword ptr [ebp-518h],edx
00221D2F mov     eax,dword ptr [ebp-518h]
00221D35 mov     dword ptr [a],eax

```