Andrew login ID: ______________________
Full Name: _______________________
Problem 1. (16 points):

This problem tests your understanding of how integers and floating point numbers are stored in memory. For Parts A-D, indicate what the output of the program would be, assuming that there are no errors during the compilation and execution of the program. Assume standard Linux alignment policies.

Consider the following C data structures.

```c
struct point { int x, y; }

struct MyStruct
{
    int i;
    union
    {
        struct point p;
        double d;
    } u;
    int j;
    double e;
};
```

Part A:

```c
int funA(struct MyStruct *m)
{
    m->u.p.x = 5;
    m->u.p.y = 10;
}

int main()
{
    struct MyStruct m;

    memset(&m, 0, sizeof(struct MyStruct));
    funA(&m);
    printf("%d, %d \n", m.u.p.x, m.u.p.y);
}
```

Output: ____________
Part B:

```c
int funB(struct MyStruct m)
{
  m.u.p.x = 5;
  m.u.p.y = 10;
}

int main()
{
  struct MyStruct m;

  memset( &m, 0, sizeof(struct MyStruct) );
  funB(m);
  printf("%d, %d \n", m.u.p.x, m.u.p.y);
}

Output: ___________
```

Part C:

```c
int funC(struct MyStruct *m)
{
  int *ptr = (int*)m;
  ptr = ptr + 2;
  *ptr = 5;
  ptr++;
  *ptr = 10;
}

int main()
{
  struct MyStruct m;

  memset( &m, 0, sizeof(struct MyStruct) );
  funC(&m);
  printf("%d, %d \n", m.u.p.x, m.u.p.y);
}

Output: ___________
```
Part D:

```
int funD(struct MyStruct *m)
{
    *(int*) &m->u.d = 5;
    *(int*) (&m->u.d + 1) = 10;
}

int main()
{
    struct MyStruct m;
    memset(&m, 0, sizeof(struct MyStruct));
    funD(&m);
    printf("%d, %d \n", m.u.p.x, m.u.p.y);
}
```

Output: ____________

Part E: Recall that a float is a 32-bit floating point number. It is divided into a 23 bit frac field, an 8 bit exp field, and a single-bit sign field.

```
void main()
{
    union hack /* struct that lets us XOR floats */
    {
        float f;
        unsigned u;
    } max, temp; /* 2 hack unions */

    float x = 1.0;
    float y = 0.5;

    do /* find the largest fp-number < 2.0 */
    {
        max.f = x;
        x += y;
        y *= 0.5;
    } while (x != max.f && x < 2.0);

    /* Assume now that max.f stores largest fp-number < 2.0 */
    temp.f = 1.0;
    temp.u = temp.u ^ max.u;
}
```

At the end of this program, how many bits in temp.u are set to 1? ____________.
Problem 2. (15 points):

This problem tests your understanding of Unix system I/O.

Part 1 (10 pts):
Examine the following C code, and answer the questions below. You may assume that there are neither compilation nor execution errors.

```c
1: int main(int argc, char * argv[])  
2: {                                      
3:     int fd1, fd2, fd3;               
4:     char c;                          
5:                                             
6:     fd1 = open("foo", O_RDONLY);       
7:     if (fork() == 0) {                
8:         fd2 = open("foo", O_RDONLY);   
9:         read(fd2, &c, 1);             
10:        ...                           
11:     } else {                         
12:         wait(NULL);                 
13:         fd3 = open("bar", O_RDONLY); 
14:         dup2(fd3, fd1);             
15:        ...                           
16:     }                               
17:     ...                              
18: }
```
The figure above represents some of the kernel data structures used to manage files. We use \([x]\) to denote file \(x\)’s descriptor table entry, which points to file \(x\)’s open file table. For example, in the above figure, \([foo]\) denotes descriptor table entry created in line 6 by the program on the previous page, which points to file \(foo\)’s open file table. Correspondingly, \([foo].pos\) and \([foo].refcnt\) denote the “File pos” and “refcnt” entry in its open file table.

Using the notation described in the previous paragraph and the program on the previous page, please complete the following tables. When filling out a row, indicate the state of the system immediately after the line indicated has executed. Ignore table entries marked with a “——-”.

### Parent process:

<table>
<thead>
<tr>
<th>line #</th>
<th>fd1</th>
<th>fd2</th>
<th>fd3</th>
<th>[foo].pos</th>
<th>[foo].refcnt</th>
<th>[bar].pos</th>
<th>[bar].refcnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>line 6</td>
<td>[foo]</td>
<td>———</td>
<td>———</td>
<td>0</td>
<td>1</td>
<td>———</td>
<td>———</td>
</tr>
<tr>
<td>line 13</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
</tr>
<tr>
<td>line 14</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
</tr>
</tbody>
</table>

### Child process:

<table>
<thead>
<tr>
<th>line #</th>
<th>fd1</th>
<th>fd2</th>
<th>fd3</th>
<th>[foo].pos</th>
<th>[foo].refcnt</th>
<th>[bar].pos</th>
<th>[bar].refcnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>line 8</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
</tr>
<tr>
<td>line 9</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
<td>———</td>
</tr>
</tbody>
</table>
Part 2 (5 pts):

This problem is concerned with a simple client-server application. The server is called dump. It waits for a client connection request on port 3304, and then outputs to stdout every character that it receives from the client. The client is called msger. Its source code is listed below. The header files and the variable declarations are omitted in this source, but you can assume that the code compiles and runs without any errors.

```c
int main(int argc, char * argv[]) {
    /* the variable declarations are omitted here */
    sock = socket(AF_INET, SOCK_STREAM, 0);
    client.sin_add.s_addr = htonl(INADDR_ANY);
    client.sin_family = AF_INET;
    client.sin_port = 0;
    server.sin_add.s_addr = inet_addr("192.168.0.1");
    server.sin_family = AF_INET;
    server.sin_port = htons(3304);
    connect(sock, (struct sockaddr *)&server, sizeof(server));
    if (fork() == 0) {
        dup2(STDOUT_FILENO, sock);
    }
    strcpy(msg_buf, "hello world\n");
    rio_writen(sock, msg_buf, strlen(msg_buf));
    close(sock);
}
```

A. This client uses rio_writen(), what is the main reason for using rio_writen() instead of the standard unix system call write()? Limit your answer to no more than one sentence.

B. Suppose dump is running on a computer with IP address ”192.168.0.1”. You launch msger on a computer with IP address ”192.168.0.2”, please fill in the following table with the output on stdout from both computers. Write ”Nothing” if there is no output.

<table>
<thead>
<tr>
<th>192.168.0.1</th>
<th>192.168.0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Problem 3. (10 points):

Consider the source code below, where M and N are constants declared with \texttt{#define}.

```c
int array1[M][N];
int array2[N][M];

void copy(int i, int j)
{
    array1[i][j] = array2[j][i];
}
```

Suppose the above code generates the following assembly code:

```asm
copy:
    push %ebp
    mov %esp,%ebp
    mov 0xc(%ebp),%edx
    push %ebx
    lea (%edx,%edx,2),%eax
    mov 0x8(%ebp),%ebx
    lea 0x0(,%ebx,8),%ecx
    lea (%edx,%eax,4),%eax
    sub %ebx,%ecx
    add %ebx,%eax
    mov array2(,%eax,4),%eax
    add %edx,%ecx
    mov %eax,array1(,%ecx,4)
    mov (%esp,1),%ebx
    pop %ebx
    ret
```

What are the values of M and N?

M = ____________

N = ____________
Problem 4. (9 points):

This problem tests your understanding of exceptional control flow. Consider the following program. You may assume that printf is unbuffered and executes atomically. The program /bin/echo prints its command line argument to stdout.

```c
1 sigset_t s1;
2 static int count = 0;
3 char *argv[] = {"/bin/echo", "Hello", NULL};
4 pid_t pid;
5
6 void handler () {
7   printf ("Bye\n");
8 }
9
10 int main () {
11   int i = 0;
12    signal (SIGCHLD, handler);
13    sigemptyset (&s1);
14    sigaddset (&s1, SIGCHLD);
15    sigprocmask (SIG_BLOCK, &s1, NULL);
16    for (i = 0; i < 3; i++) {
17      if (fork() == 0) {
18        count++;
19        execve ("/bin/echo", argv, NULL);
20      }
21      wait(NULL);
22    }
23    sigprocmask (SIG_UNBLOCK, &s1, NULL);
24 }
25
```
1. What are the possible outputs of the program?

2. When the program reaches line 31, what are the possible values that `count` may have?

3. Consider the same code, without blocking `SIGCHLD`, i.e. with lines 20, and 30 removed. Would the output be similar? If you answered no, list one possible output.
Problem 5. (12 points):

The code samples below are designed to test your understanding of multithreading, semaphores, and the effects of multiple threads modifying the same data. For each section, you will be asked to specify how many different outputs the given code can have. Since there may be many possible outputs, you will not be asked to provide the outputs themselves. You may assume, for the purposes of this problem, that printf executes atomically.

```c
sem_t sem;

int main()
{
    int j;
    pthread_t tids[3];
    sem_init(&sem, 0, 1);
    for (j=0; j<3; j++) {
        pthread_create(&tids[j], NULL, doit, NULL);
    }
    for (j=0; j<3; j++) {
        pthread_join(&tids[j], NULL);
    }
    return 0;
}
```

This is the main function for all three problems below. The only differences in the problems are the details of the thread function, `doit` listed on the next page.
part A:

```c
int i = 0;

void *doit(void *arg)
{
    P(&sem);
    i = i + 1;
    printf("%d\n", i);
    V(&sem);
}
```

How many different outputs are possible on executing the code above? ______________

part B:

```c
int i = 0;

void *doit(void *arg)
{
    P(&sem);
    i = i + 1;
    V(&sem);
    printf("%d\n", i);
}
```

How many different outputs are possible on executing the code above? ______________

part C:

```c
int i = 0;

void *doit(void *arg)
{
    i = i + 1;
    printf("%d\n", i);
}
```

When the above code runs, at least one of the four outputs listed below are not possible.

<table>
<thead>
<tr>
<th></th>
<th>(a)</th>
<th>(b)</th>
<th>(c)</th>
<th>(d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

List the letters identifying the illegal outputs here: ______________
**Problem 6. (18 points):**

When attempting to debug a program, it is often helpful to look at the stack to determine what functions have been called and with what arguments. This is called a backtrace and can be performed in gdb with the `bt` command. Your task for this section of the exam is to harness your knowledge of the x86 calling conventions, combined with your understanding of different data representations to perform a manual backtrace. To facilitate this, we have provided you with the contents of the stack in hexadecimal format. We have also provided you with a table mapping certain addresses to strings. Additionally, we have given you the address ranges for the machine code of the various functions. Finally, when the `bt` is executed you are inside the `bar()` function and the value of `ebp` is 0xbffff988.

Your backtrace should terminate at the `main()` function (and should also include any arguments to `main`).

You may assume that all arrays of strings are terminated with a NULL pointer.

When providing your answers, please specify the name of the argument and use the following conventions:

- characters should be written in single quotes (e.g. `character='c'`).
- integers should be written in decimal format (e.g. `integer=23`).
- strings should be in double quotes (e.g. `string="This is a string"`).
- string arrays should be written in square brackets and be comma delimited (e.g. `array=["This", "is", "an", "array", (NULL)]`)
- pointers should be written as hexadecimal numbers (e.g. `pointer=0xbffffffa84`)

For example: `main(argc=2, argv=["/bin/foo", "Word", (NULL)])`
The stack is as follows:

<table>
<thead>
<tr>
<th>Address</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xbff988</td>
<td>0xbff9b8</td>
</tr>
<tr>
<td>0xbff98c</td>
<td>0x8048401</td>
</tr>
<tr>
<td>0xbff990</td>
<td>0xbfffb28</td>
</tr>
<tr>
<td>0xbff994</td>
<td>0xdeadbeef</td>
</tr>
<tr>
<td>0xbff998</td>
<td>0xbff9a8</td>
</tr>
<tr>
<td>0xbff99c</td>
<td>0x4002c4ed</td>
</tr>
<tr>
<td>0xbff9a0</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbff9a4</td>
<td>0x804833a</td>
</tr>
<tr>
<td>0xbff9a8</td>
<td>0x000000a0</td>
</tr>
<tr>
<td>0xbff9ac</td>
<td>0x80483e9</td>
</tr>
<tr>
<td>0xbff9b0</td>
<td>0xbff9d0</td>
</tr>
<tr>
<td>0xbff9b4</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbff9b8</td>
<td>0xbff9d8</td>
</tr>
<tr>
<td>0xbff9bc</td>
<td>0x8048378</td>
</tr>
<tr>
<td>0xbff9c0</td>
<td>0x0000000f</td>
</tr>
<tr>
<td>0xbff9c4</td>
<td>0x0000002d</td>
</tr>
<tr>
<td>0xbff9c8</td>
<td>0x000000d5</td>
</tr>
<tr>
<td>0xbff9cc</td>
<td>0x80483e9</td>
</tr>
<tr>
<td>0xbff9d0</td>
<td>0xbff9d0</td>
</tr>
<tr>
<td>0xbff9d4</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbff9d8</td>
<td>0xbff9f8</td>
</tr>
<tr>
<td>0xbff9dc</td>
<td>0x4002c4ed</td>
</tr>
<tr>
<td>0xbff9e0</td>
<td>0x00000002</td>
</tr>
<tr>
<td>0xbff9e4</td>
<td>0xbfffa2c</td>
</tr>
<tr>
<td>0xbff9e8</td>
<td>0x00000004</td>
</tr>
<tr>
<td>0xbff9ec</td>
<td>0x80483e9</td>
</tr>
<tr>
<td>0xbff9f0</td>
<td>0xbff9d0</td>
</tr>
<tr>
<td>0xbff9f4</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbff9f8</td>
<td>0xbfffa48</td>
</tr>
<tr>
<td>0xbff9fc</td>
<td>0x00000002</td>
</tr>
<tr>
<td>0xbfffa00</td>
<td>0x75656869</td>
</tr>
<tr>
<td>0xbfffa04</td>
<td>0x4002c3ac</td>
</tr>
<tr>
<td>0xbfffa08</td>
<td>0xbfffb08</td>
</tr>
<tr>
<td>0xbfffa0c</td>
<td>0xbfffb28</td>
</tr>
<tr>
<td>0xbfffa10</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbfffa14</td>
<td>0xbfffb38</td>
</tr>
<tr>
<td>0xbfffa18</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbfffa1c</td>
<td>0x80483e9</td>
</tr>
<tr>
<td>0xbfffa20</td>
<td>0xbff9d0</td>
</tr>
<tr>
<td>0xbfffa24</td>
<td>0x00000002</td>
</tr>
<tr>
<td>0xbfffa28</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbfffa2c</td>
<td>0xbfffb08</td>
</tr>
<tr>
<td>0xbfffa30</td>
<td>0xbfffb88</td>
</tr>
<tr>
<td>0xbfffa34</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0xbfffa38</td>
<td>0x000d5213</td>
</tr>
<tr>
<td>0xbfffa3c</td>
<td>0x80483e9</td>
</tr>
<tr>
<td>0xbfffa40</td>
<td>0xbff9d0</td>
</tr>
<tr>
<td>0xbfffa44</td>
<td>0x0000003b</td>
</tr>
</tbody>
</table>

The following table lists a few selected characters and their associated ASCII values.

<table>
<thead>
<tr>
<th>Hex</th>
<th>Char</th>
<th>Hex</th>
<th>Char</th>
<th>Hex</th>
<th>Char</th>
<th>Hex</th>
<th>Char</th>
</tr>
</thead>
<tbody>
<tr>
<td>2b</td>
<td>'+'</td>
<td>2c</td>
<td>','</td>
<td>2d</td>
<td>'-'</td>
<td>2e</td>
<td>'.'</td>
</tr>
<tr>
<td>2f</td>
<td>'/'</td>
<td>30</td>
<td>'0'</td>
<td>65</td>
<td>'A'</td>
<td>97</td>
<td>'a'</td>
</tr>
</tbody>
</table>
The following table lists the addresses at which certain strings are found in the executable.

<table>
<thead>
<tr>
<th>Address</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xbffffb08</td>
<td>&quot;/bin/foo&quot;</td>
</tr>
<tr>
<td>0xbffffb28</td>
<td>“Walrus”</td>
</tr>
<tr>
<td>0xbffffb48</td>
<td>“Game”</td>
</tr>
<tr>
<td>0xbffffb68</td>
<td>“Dawg”</td>
</tr>
<tr>
<td>0xbffffb88</td>
<td>“Lock”</td>
</tr>
<tr>
<td>0xbffffba8</td>
<td>“Worst”</td>
</tr>
<tr>
<td>0xbffffbc8</td>
<td>“Wiz”</td>
</tr>
<tr>
<td>0xbffffbe8</td>
<td>“Mack”</td>
</tr>
</tbody>
</table>

The following table lists the addresses at which certain functions begin in the executable. You should assume that each function immediately follows the function listed above it in the executable.

<table>
<thead>
<tr>
<th>Address</th>
<th>Prototype</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0804835c</td>
<td>int main(int argc, char *argv[]);</td>
</tr>
<tr>
<td>0x08048388</td>
<td>int foo(void *addr);</td>
</tr>
<tr>
<td>0x08048392</td>
<td>void fancy(int i, char *str);</td>
</tr>
<tr>
<td>0x08048398</td>
<td>int hammer(int a, char c, int i);</td>
</tr>
<tr>
<td>0x08048404</td>
<td>char bar(char *str, double *dp);</td>
</tr>
<tr>
<td>0x0804840e</td>
<td>double chouse(int i);</td>
</tr>
</tbody>
</table>

Please fill in the following fields as per the guidelines given above. Note that you might not need all of the space provided.

1. bar ( ____________________________________________________________________________
__________________________________________________________________________ )

2. ____________________________________________________________________________
__________________________________________________________________________

3. ____________________________________________________________________________
__________________________________________________________________________

4. ____________________________________________________________________________
__________________________________________________________________________
Problem 7. (9 points):

This problem deals with dynamic memory allocators.

Part A: Suppose that you have been asked to implement a dynamic memory allocator for a real-time system with strict bounds on the amount of time for an operation (a malloc, a free, etc). In order to combat false fragmentation, you have decided to use some sort of coalescing. Which type of coalescing (immediate or deferred) should you use, and why? Use at most two sentences for your answer.

Part B: Assume a minimum block size of 32 bytes for this part of the problem. Do implicit free lists or explicit free lists use more memory. That is, will one of these strategies necessarily use more space than the other, assuming that everything else in the allocators are identical, and why? Use at most two sentences for your answer.

Part C: Assume you are designing a special purpose dynamic memory allocator. One of the interesting properties of this system is that only 8 different sizes, all of which you know in advance and all of which are small relative to the page size of the system, will be requested by the user (though there are no guarantees how many times each of these will be requested). What are the most important ways in which your design for this allocator would differ from your design of a general purpose allocator? Use at most 2 sentences for your answer.
Problem 8. (24 points):

You are working for a company that is developing a new processor and the compiler team is way behind schedule. In order to sell your product you need to show high performance on certain kernels important to your potential users. You have been asked to optimize the following kernel. You can’t use assembly because the ISA of the processor may change.

You can assume that $N$ and $M$ are large and that $M$ is always even. The processor will have a cache, it won’t be large compared to $N*M$. $a$, $b$, and $e$ are all 2-D $N\times M$ arrays. $e$ may have values other than 0 in it before the call to kernel.

```c
void
kernel(int N, int M, int* a, int *b, int *e)
{
    int i, j, k;

    for (i=0; i<M; i++)
        for (j=0; j<N; j++)
            if (isodd(a[j*M+i])) {
                for (k=0; k<M; k++)
                    e[j*M+i] += a[j*M+i]*b[j*M+k];
            }

    int
    isodd(int val)
    {
        return ((val % 2) == 1);
    }
}
```

Use this space for your work. Nothing on this page will be used in the grading of this question. This is a two part question. Put your final answer on the next two pages.
For your reference here is the original code again:

```c
void kernel(int N, int M, int* a, int *b, int *e) {
    int i, j, k;
    for (i=0; i<M; i++)
        for (j=0; j<N; j++)
            if (isodd(a[j*M+i])) {
                for (k=0; k<M; k++)
                    e[j*M+i] += a[j*M+i]*b[j*M+k];
            }
}

int isodd(int val) {
    return ((val % 2) == 1);
}
```

**Part 1:** Provide an optimized version of `kernel` here. Please be neat as illegible answers will receive no credit.
void kernel(int N, int M, int* a, int *b, int *e) {
    int i, j, k;
    for (i=0; i<M; i++)
        for (j=0; j<N; j++)
            if (isodd(a[j*M+i])) {
                for (k=0; k<M; k++)
                    e[j*M+i] += a[j*M+i]*b[j*M+k];
            }
}

int isodd(int val) {
    return ((val % 2) == 1);
}

Part 2: List the optimizations you performed and, in no more than one short sentence (a sentence fragment is ok too), the rationale behind each one.
Problem 9. (10 points):

Imagine that you are given two computers (A and B) that operate at the same processor clock rate, but that use different cache structures. The manufacturers did not provide you with any information on how kind of cache organizations are used in these machines. Instead you ran a test program that measures how fast one memory read operation is for sequentially reading one array of a given size. You get the following result:

![Graph showing the average read time in cycles for different working set sizes between Computer A and Computer B.](image)

On the vertical axis is the number of cycles for one memory read instruction. The horizontal axis is the size of the test array in bytes.

1. How many levels of caching is used by computer A and how large are these caches?

2. How many levels of caching is used by computer B and how large are these caches?

3. A database program is run on these computers. The most time consuming part of this particular database uses a hash table of 250,000 entries of 8 bytes each. Which computer is faster?

4. Does the answer to part 3 changes if the hash table size is increased? If yes, at what size?

5. Based on this data, is it possible to tell how these caches are organized?