

CSC 347 - Concepts of Programming Languages

Undefined Behavior

Instructor: Stefan Mitsch



Learning Objectives

- ❓ What should happen if the language does not specify the meaning of some construct?
- ❓ What should happen when `x` is holding 8 bits, `x=7` and then `x = x+1` ?
 - Understand examples of undefined behavior in C



Under and Overflow

```
1 #include <stdio.h>
2
3 int isMinValue (int x) {
4     return (x-1) > x;
5 }
6 int main () {
7     int i = -2000000000;
8     while (!isMinValue(i))
9         i--;
10    printf ("Min value is %d\n", i);
11 }
```

```
1 $ gcc -O1 undefined.c && ./a.out
2 Min value is -2147483648
```

```
1 $ gcc -O2 undefined.c && ./a.out
2 ^C #infinite loop
3
```



Order of Operations

```
1 #include <stdio.h>
2 int count = 0;
3 int f () {
4     count += 1;
5     return count;
6 }
7 int main () {
8     int z = f() + f();
9     printf ("%d\n", z);
10    z = (z += 1) + (z = z*z);
11    printf ("%d\n", z);
12 }
```

```
1 $ clang -Wall undefined3.c
2 undefined3.c:11:21: warning: unsequenced modification and access to 'z'
3   z = (z += 1) + (z = z*z);
4             ~~~ ^
5 1 warning generated.
6 $ ./a.out
7 3
8 20
```

- `z=z+1; z=z+z*z`



Order of Operations

```
1 #include <stdio.h>
2 int count = 0;
3 int f () {
4     count += 1;
5     return count;
6 }
7 int main () {
8     int z = f() + f();
9     printf ("%d\n", z);
10    z = (z += 1) + (z = z*z);
11    printf ("%d\n", z);
12 }
```

```
1 $ gcc -Wall -O3 undefined3.c
2 undefined3.c: In function 'main':
3 undefined3.c:11:5: warning: operation on 'z' may be undefined
4     z = (z += 1) + (z = z*z);
5         ^
6 $ ./a.out
7 3
8 32
```

- `z=z+1; z=z*z; z=z+z;`



Compiler Optimizations

- For undefined executions, the compiler can do what it likes
- This can lead to some surprising compiler optimizations
- [C null pointer optimization 1](#)



Dangling Pointers

- See the worksheet for this week.
- [More examples of undefined behavior](#)
- [More undefined behavior](#)



Summary

- Undefined behavior resolved in the compiler (compiler decides what is the meaning of undefined programs)
- Undefined behavior often presents security risks