

Programming and Laboratory - 2

2. Tools

Giulio Ermanno Pibiri — giulioermanno.pibiri@unive.it

Nicola Prezza — nicola.prezza@unive.it

Department of Environmental Sciences, Informatics and Statistics

Overview

- C++ project directory layout
- Makefiles
- Setting up a project step-by-step
- Debugging — Part 1: asserts and Valgrind
- Debugging — Part 2: compiler warnings and sanitizers

C++ project directory layout

- A C++ project is a collection of header + source files.
- Header files:
 - define class interfaces / function signatures
 - hpp extension
 - put into `include/`
- Source files:
 - contain the implementation of the signatures defined in the corresponding `.hpp` files
 - cpp extension
 - put into `src/`

```
parent_project_folder/  
|  
|— include/  
|  
|— src/  
|  
|— build/  
|  
|— tools/
```

Other sub-directories are `test` and `external`, for example.

See here for a more detailed overview: <https://api.csswg.org/bikeshed/?force=1&url=https://raw.githubusercontent.com/vector-of-bool/pitchfork/develop/data/spec.bs#tld>.

Header and source files

- Header files (extension `.hpp`) are used to declare just the prototypes (also known as, “signatures” or “declarations”) of the functions whose body is defined elsewhere (in a `.cpp` file).

For example, this is a function’s prototype defined in the header file `"include/myfunction.hpp"`:

```
int myfunction(int x, double y);
```

- Header files are then included in the `cpp` files that need to use those functions (because the compiler requires that at least the prototype of a function is defined in the `cpp` file using that function).

The file `"src/myfunction.cpp"` will begin with

```
#include "myfunction.hpp"
```

This is exactly like writing

```
int myfunction(int x, double y);
```

directly in the `.cpp` file.

- The object files (`.o`) defining the function’s body have to be **linked** at compile time.

Make

<https://www.gnu.org/software/make/manual/make.html>

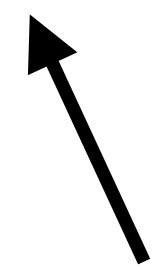
- The program make can be used to **automatize a pipeline** of tasks, each of which may depend on the output of other tasks.
- Example: a task t_1 produces file f_1 . Task t_2 requires f_1 and produces file f_2 . Hence, task t_2 cannot be run if file f_1 has not been created (i.e. if task t_1 is not run first)!
- Typically used to **compile code** (many intermediate object files).
- The pipeline of tasks is specified in a “special” file, called **Makefile**.

Makefiles

- A Makefile is composed by many rules.
- A rule is made up of:
 - **target**: name of a file we want to generate or name of an action (e.g., `clean`, `debug`, `release`, etc.)
 - **prerequisites**: file(s) needed as input to generate the target or name(s) of action needed to be executed before
 - **recipe**: an action to be performed (e.g., one or more compilation commands)

`<target>: <prerequisites>`

`<TAB><recipe>`



A TAB character (`'\t'`) is required here!

Makefiles

- Behaviour of make <target>:
 1. If any prerequisite *changed* (timestamps are used) execute *recursively* the recipe of the prerequisite.
 2. Execute the recipe of the target.
- If no target specified (you just typed make): take the first one.

FOLDERS

▼ myfunction-example-project

▼ build

mytool

▼ include

/* myfunction.hpp

▼ src

/* myfunction.cpp

► tools

/* Makefile

Makefile

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

OPTIONS=-O3

all: build/mytool

debug: OPTIONS=-O0 -g

debug: build/mytool

build/mytool: build/myfunction.o tools/main.cpp

g++ \${OPTIONS} tools/main.cpp -o build/mytool -I ./include/ build/myfunction.o

build/myfunction.o: src/myfunction.cpp include/myfunction.hpp

g++ \${OPTIONS} -c src/myfunction.cpp -I ./include/ -o build/myfunction.o

clean:

rm -rf build/*.o build/mytool

Makefiles

Not just for compiling code!

- What does the following Makefile do?

```
final.txt: text1.txt text2.txt
    cat text1.txt text2.txt > final.txt

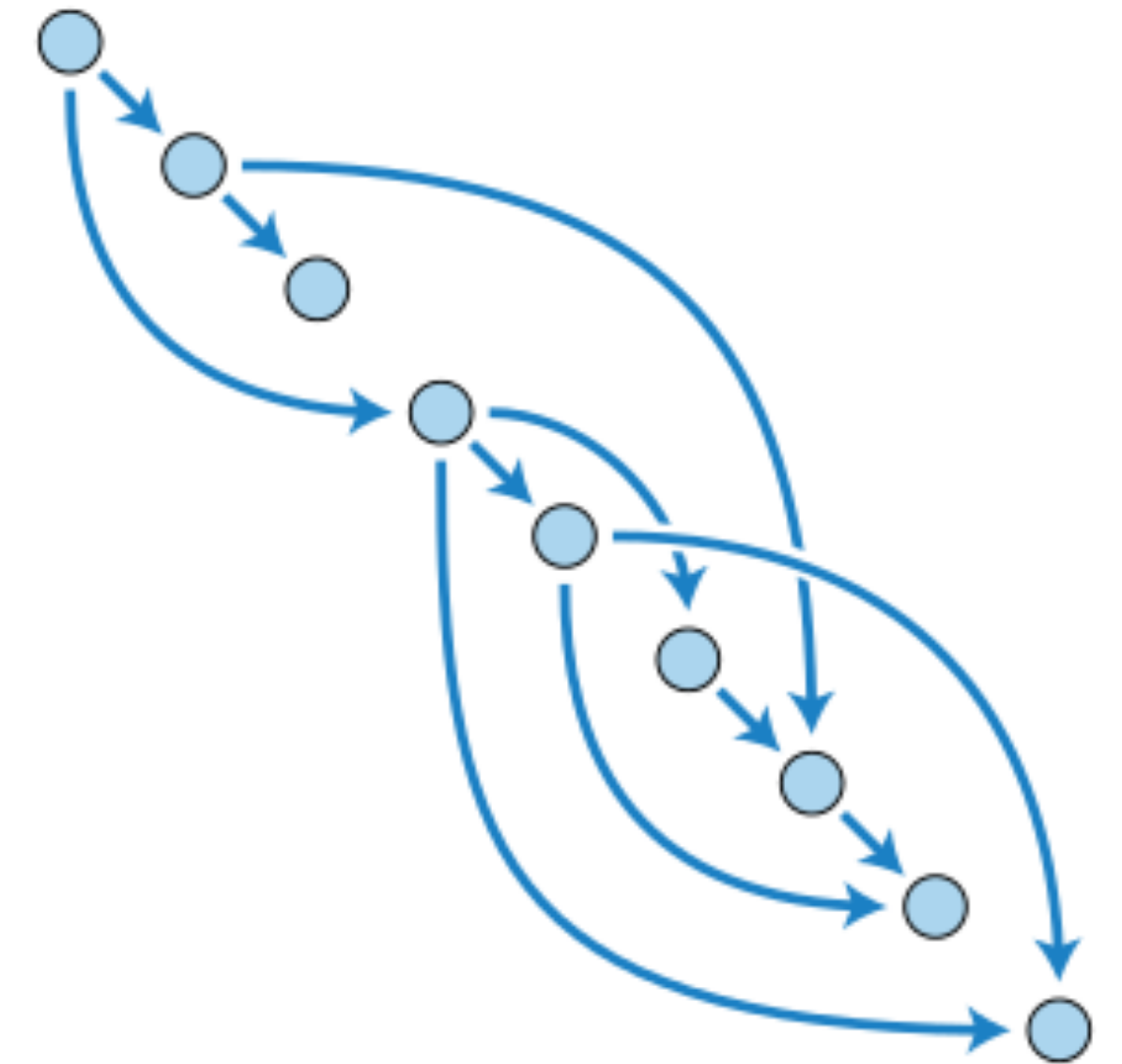
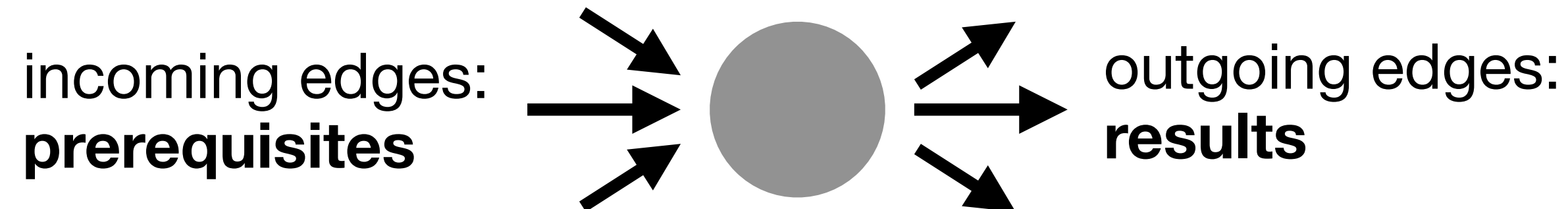
text1.txt:
    echo "text 1" > text1.txt

text2.txt:
    echo "text 2" > text2.txt
```

- What happens if I run make two times?
- What happens if I delete text1.txt and then run make?
- What if I just touch (changes timestamp – check with `ls --full-time`) the file text1.txt?

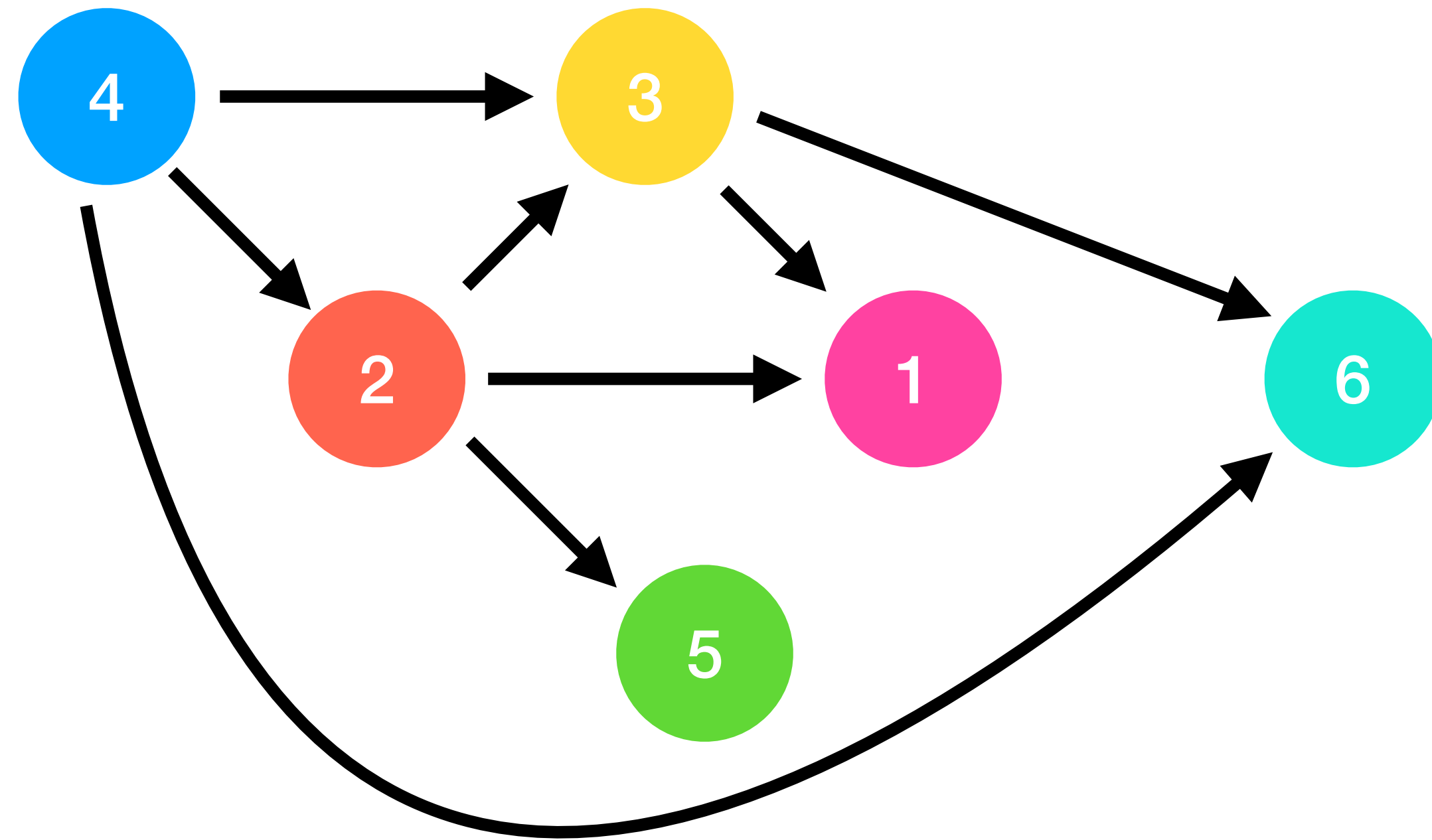
Makefiles as directed acyclic graphs (DAGs)

- The dependencies in Makefiles can be specified as **directed acyclic graphs** (or DAGs).
- Basic model:



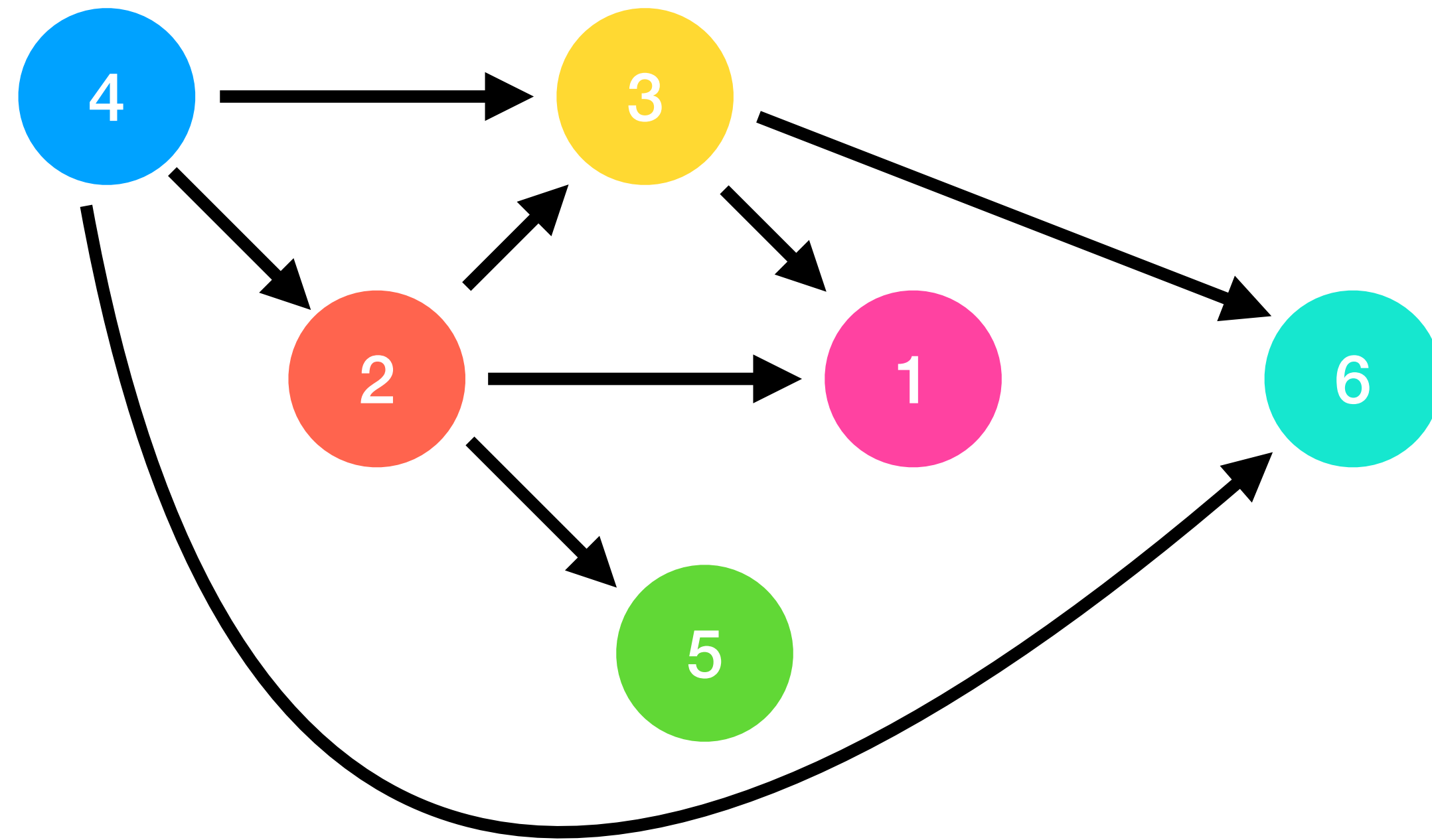
- To determine the order of execution of the targets, make sorts this graph so that arrows (dependencies) only go in one direction.
- This is called **topological sorting** (more details in CT0371) and is always possible on **acyclic** graphs.

DAG example



- Possible orders?

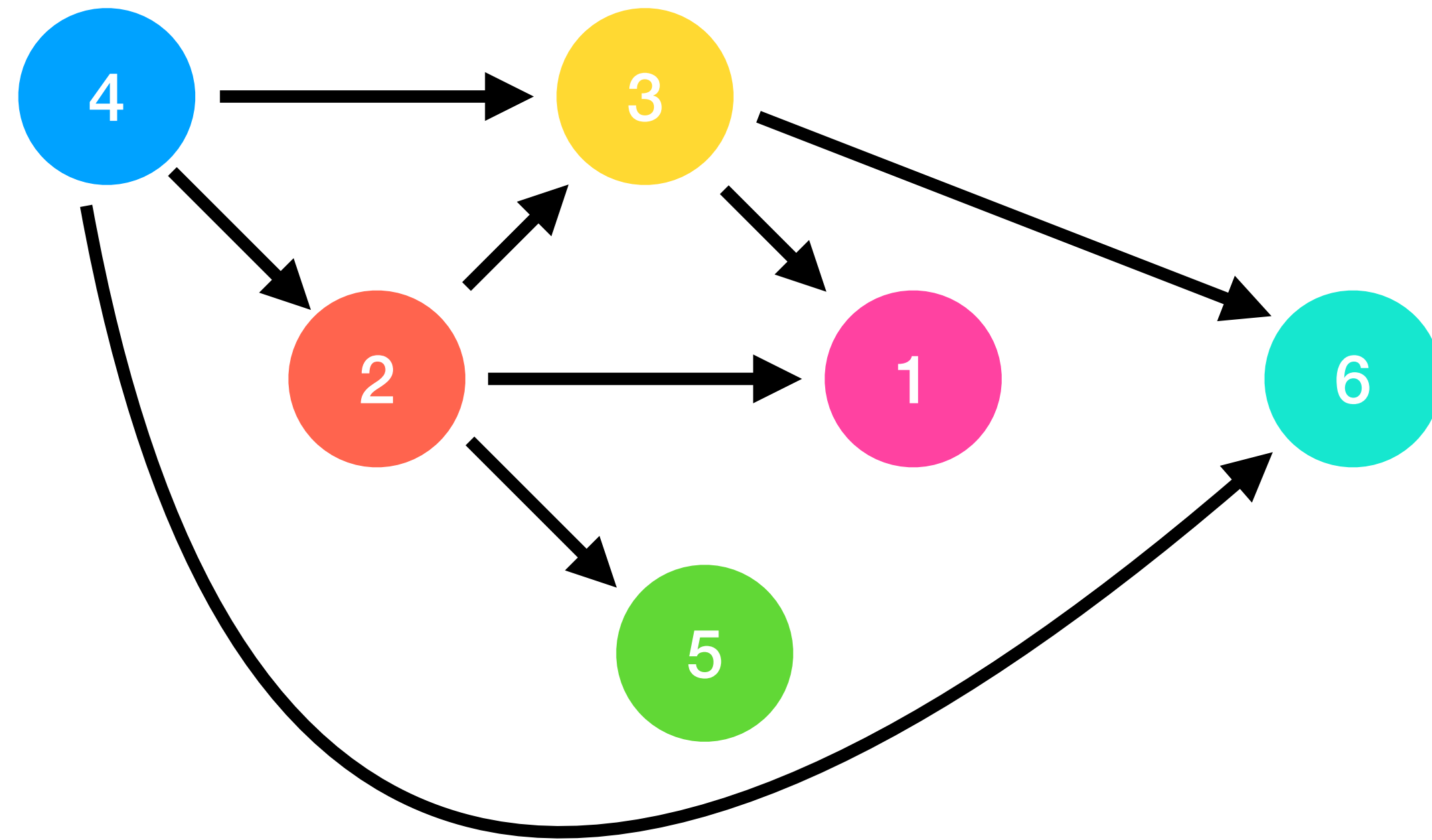
DAG example



- Possible orders?



DAG example



- Possible orders?



Q. Can you describe an algorithm to output one of these orders?

Exercise

Consider the following Makefile and draw the corresponding DAG.

```
project: main.o utils.o command.o
    cc -o project main.o utils.o command.o
main.o: main.c defs.h
    cc -c main.c
utils.o: utils.c defs.h command.h
    cc -c utils.c
command.o: command.c defs.h command.h
    cc -c command.c
```

Setting-up a project step-by-step

Example step-by-step

1. In your home folder, create a folder `power-root-example-project/` and enter it.
2. Create the project directory layout (sub-directories: `include/`, `src/`, `tools/`, `build/`).
3. Create a header `include/myfunctions.hpp` declaring the prototypes of these functions:

```
int power(int, int);  
int root(int, int);
```

4. Create a source code file `src/power.cpp` defining the body of `int power(int x, int y)`, which returns x^y (use a for loop).
5. Create a source code file `src/root.cpp` defining the body of `int root(int x, int y)` which returns the largest integer z such that $z^y \leq x$ (use function `power` and a while loop).
6. Create a source code file `tools/main.cpp` containing the main function which computes the 3-rd root of 74088. The result has to be printed on the screen as "The answer is" followed by the result of `root(74088,3)`.
7. Create a Makefile that compiles everything in an executable called `theanswer`:
 - Specify the path of the includes using option `-I`.
 - Use optimization level 3.
 - Create a separate object file and a separate Makefile's target for each `.cpp` file.
 - Add also a `clean` target that removes all object files.
 - Optional: add other targets (e.g., `debug`) to compile with different options.
8. Compile and run the project.

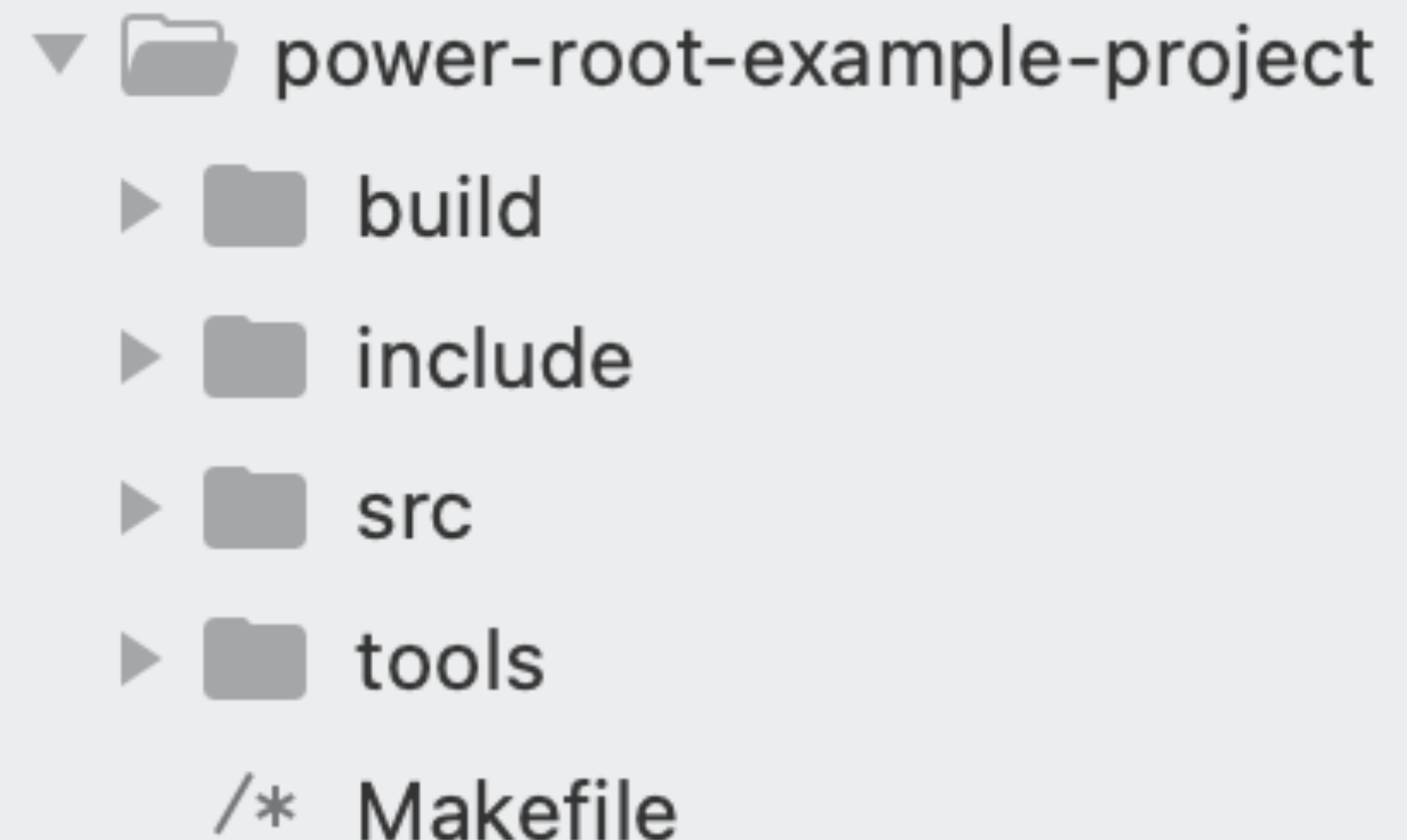
Step 1 and 2

In your home folder, create a folder `power-root-example-project/` and enter it.

Create the project directory layout (sub-directories: `include/`, `src/`, `tools/`, `build/`).

```
$ mkdir power-root-example-project; cd power-root-example-project  
$ mkdir include src tools build  
$ touch Makefile
```

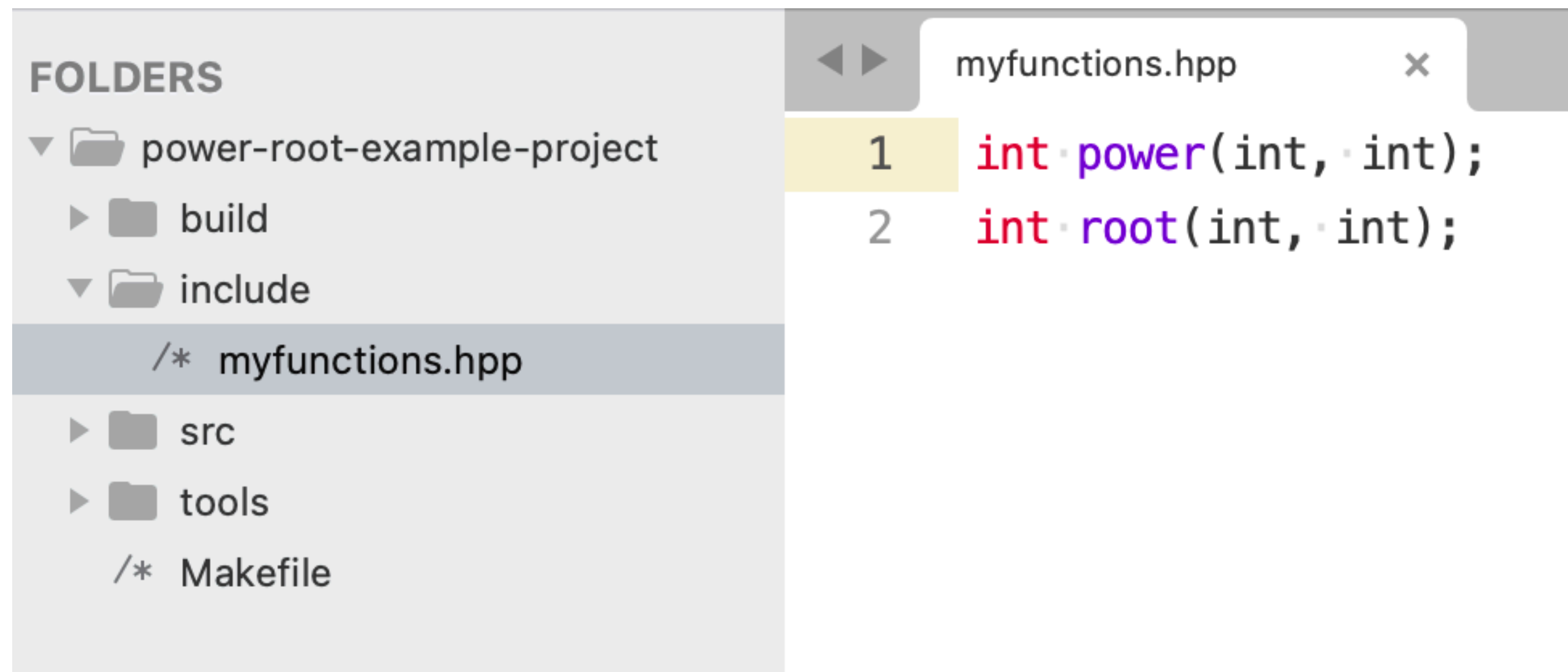
FOLDERS



Step 3

Create a header `include/myfunctions.hpp` declaring the prototypes of these functions:

```
int power(int, int);  
int root(int, int);
```



Step 4 and 5

Create a source code file `src/power.cpp` defining the body of `int power(int x, int y)`, which returns x^y (use a for loop).

Create a source code file `src/root.cpp` defining the body of `int root(int x, int y)` which returns the largest integer z such that $z^y \leq x$ (use function `power` and a while loop).

The screenshot shows a code editor with two tabs: `power.cpp` and `root.cpp`. On the left, a 'FOLDERS' panel shows the project structure: `power-root-example-project` containing `build`, `include` (with `myfunctions.hpp`), `src` (containing `power.cpp` and `root.cpp`), `tools`, and a `Makefile`.

power.cpp

```
1  #include "myfunctions.hpp"
2
3  int power(int x, int y) {
4      int result = 1;
5      for (int i = 0; i < y; ++i) result *= x;
6      return result;
7  }
8
```

root.cpp

```
1  #include "myfunctions.hpp"
2
3  /* return the largest z such that z^y <= x */
4  int root(int x, int y) {
5      int z = 0;
6      while (power(z + 1, y) <= x) z++;
7      return z;
8  }
9
```

Step 6

Create a source code file `tools/main.cpp` containing the main function which computes the 3-rd root of 74088. The result has to be printed on the screen as "The answer is" followed by the result of `root(74088,3)`.

FOLDERS

▼ power-root-example-project

▶ build

▼ include

/* myfunctions.hpp

▼ src

/* power.cpp

/* root.cpp

▼ tools

/* main.cpp

/* Makefile

◀ ▶

main.cpp

×

1

`#include <iostream>`

2

3

`#include "myfunctions.hpp"`

4

5

`int main() {`

6

`int ans = root(74088, 3);`

7

`std::cout << "The answer is " << ans << std::endl;`

8

`return 0;`

9

`}`

10

Step 7

Create a Makefile that compiles everything in an executable called theanswer:

- Specify the path of the includes using option `-I`.
- Use optimization level 3.
- Create a separate object file and a separate Makefile's target for each `.cpp` file.
- Add also a `clean` target that removes all object files.
- Optional: add other targets (e.g., `debug`) to compile with different options.

FOLDERS

- ▼ power-root-example-project
 - ▶ build
 - ▼ include
 - /* myfunctions.hpp
 - ▼ src
 - /* power.cpp
 - /* root.cpp
 - ▶ tools
- /* Makefile

```
Makefile
1  OPTIONS=-O3
2
3  all: build/theanswer
4
5  debug: OPTIONS=-O0 -g
6  debug: build/theanswer
7
8  build/theanswer: build/root.o build/power.o tools/main.cpp
9  g++ ${OPTIONS} tools/main.cpp -o build/theanswer -I include/ build/root.o build/power.o
10
11 build/root.o: src/root.cpp include/myfunctions.hpp
12 g++ ${OPTIONS} -c src/root.cpp -o build/root.o -I include/
13
14 build/power.o: src/power.cpp include/myfunctions.hpp
15 g++ ${OPTIONS} -c src/power.cpp -o build/power.o -I include/
16
17 clean:
18 rm -rf build/*.o build/theanswer
```

Step 8

- Compile and run the project.
- From the parent project folder:

```
$ make  
$ ./build/theanswer
```

or

```
$ make debug  
$ ./build/theanswer
```

Debugging — Part 1: asserts and Valgrind

The “art” of debugging

What kind of errors can we run into when programming?

- **Linking-time** errors
- **Compilation-time** errors
- **Run-time** errors – solutions:
 - debugging
 - pre/post conditions (asserts)
 - exceptions



The art of debugging

Debugging means finding **logical** errors in your program.

- Sometimes very hard to find: the program links, compiles, and runs but the **output is wrong!**
- Even worse, on some inputs the program works but on other input it does not work: hard to **reproduce** the bug.

“Reproducible bugs are candies.” — cit.

- To find bugs, we need to inspect the program at **run-time** (while it is executing).

How?

- Plan you algorithms carefully!
- Ensure pre/post conditions (asserts)
- Throw exceptions (next lectures)
- Use a debugger (Linux has **gdb**, but we will not cover this.)

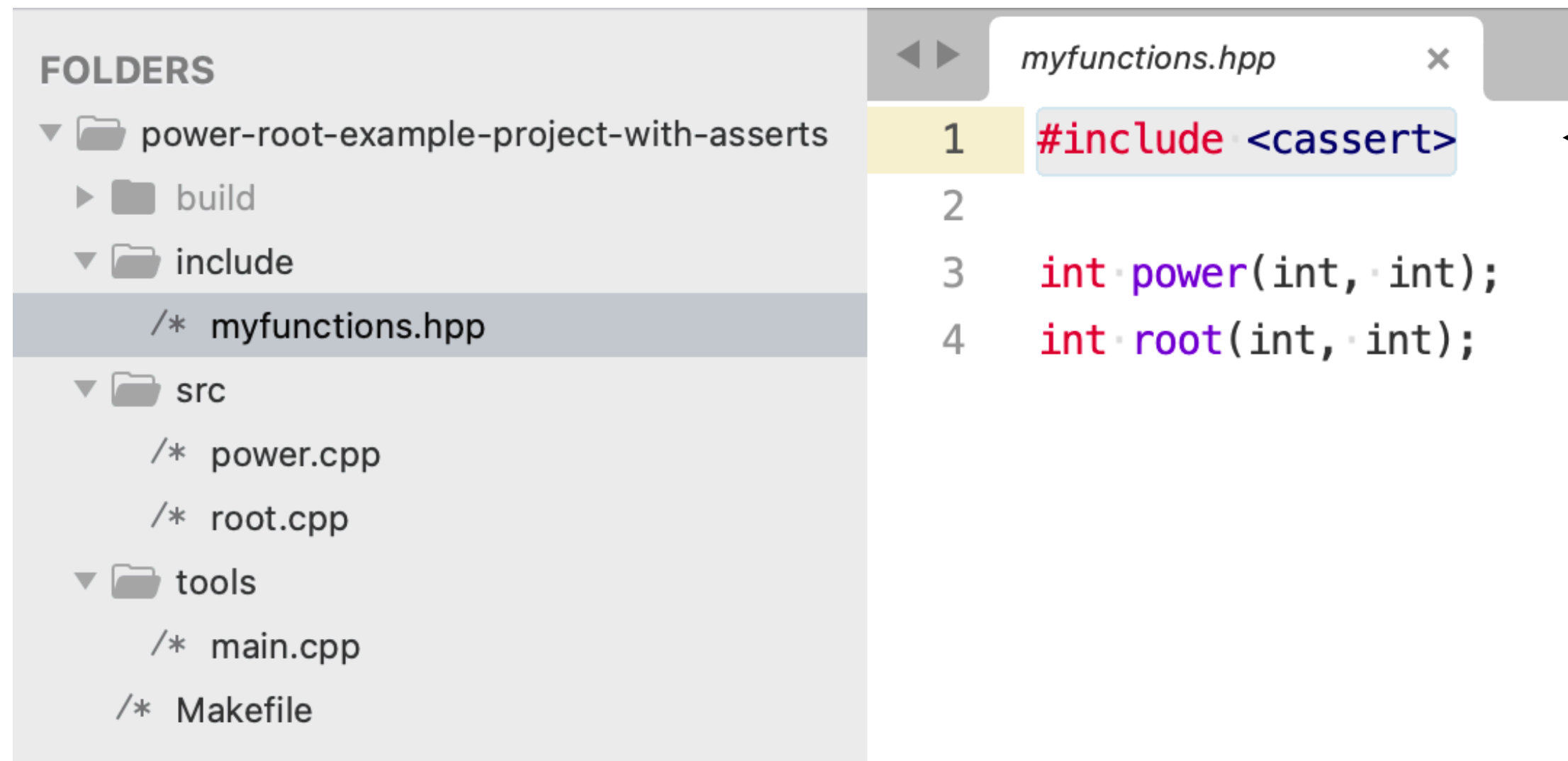
Asserts — a minimalist example

```
#include <cassert>
```

```
int main() {  
    assert(3 != 3); /* throws a failed assertion */  
}
```

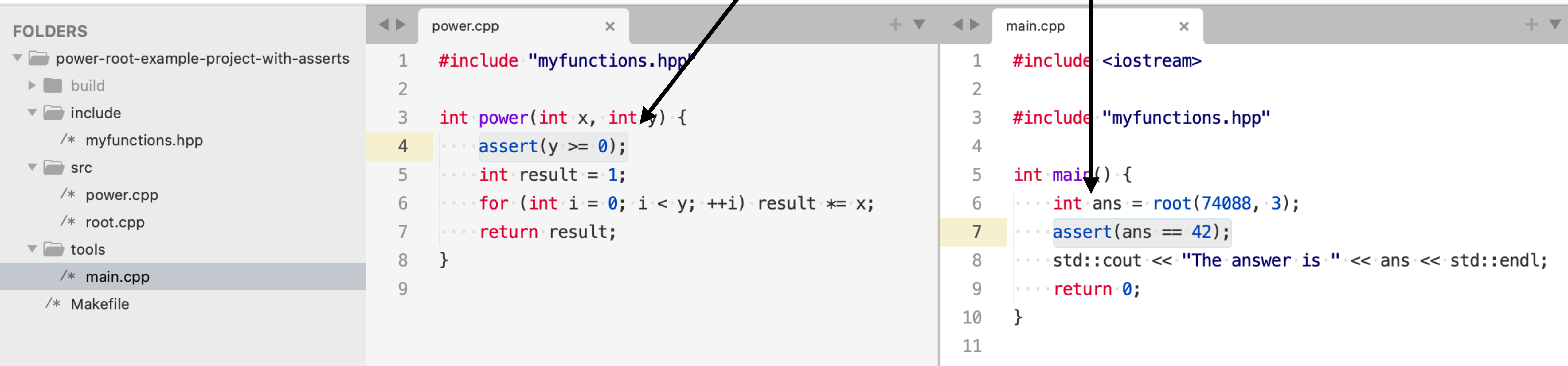
- `assert` is a macro (with a functional form) that takes as input a boolean condition and halts the program when the condition is not satisfied.
- **The best way to document your code.**
- Use it to check pre/post conditions for your functions.
- Compile with `g++ -DNDEBUG` (option `-D`, argument `NDEBUG`) to disable asserts (they are enabled by default): this way, they do not affect performance!
- Good idea to leave them enabled only in debug mode.

Back to our example



include the header "cassert"

use asserts to document your code



Back to our example

disable/enable asserts

The screenshot shows a code editor with a file explorer on the left and a Makefile editor on the right. The file explorer shows a project structure with folders 'build', 'include', 'src', and 'tools'. The Makefile editor shows the following content:

```
1  OPTIONS=-O3 -DNDEBUG -Wall -Wextra
2
3  all: build/theanswer
4
5  debug: OPTIONS=-O0 -g -DDEBUG -Wall -Wextra
6  debug: build/theanswer
7
8  build/theanswer: build/root.o build/power.o tools/main.cpp
9  g++ ${OPTIONS} tools/main.cpp -o build/theanswer -I include/ build/root.o build/power.o
10
11 build/root.o: src/root.cpp include/myfunctions.hpp
12 g++ ${OPTIONS} -c src/root.cpp -o build/root.o -I include/
13
14 build/power.o: src/power.cpp include/myfunctions.hpp
15 g++ ${OPTIONS} -c src/power.cpp -o build/power.o -I include/
16
17 clean:
18 rm -rf build/*.o build/theanswer
```

Two arrows point from the text 'disable/enable asserts' to the Makefile. One arrow points to the `-DNDEBUG` flag on line 1, and the other points to the `-DDEBUG` flag on line 5.

Memory debugging

Most of C++ errors you will encounter in your code are related to (bad) **memory management**.

For example:

- Runtime errors often **abort** the program with (a rather uninformative):

segmentation fault

Often these are caused by:

- **out-of-bounds** memory accesses
 - **invalid** memory **allocation** requests
- Incorrect memory handling could result in the RAM filling up quickly (**memory leaks**).

Memory debugging

- **Warning: g++ does not find these problems.**
- **Q. Why?**
 - Because memory monitoring can only be done at execution time.
 - In general, the problem is **undecidable** (we can only detect it while the program is running, and only if the problem occurs).
 - A memory debugger simulates a complete machine and flags uninitialized/unallocated memory locations.
- We will solve these problems with **Valgrind**: a programming tool for memory debugging, memory leak detection, and profiling.

Valgrind

<https://valgrind.org/>

```
prog2021@prog2021-pc: ~  
VALGRIND(1)                                Release 3.15.0                                VALGRIND(1)  
  
NAME  
    valgrind - a suite of tools for debugging and profiling programs  
  
SYNOPSIS  
    valgrind [valgrind-options] [your-program] [your-program-options]  
  
DESCRIPTION  
    Valgrind is a flexible program for debugging and profiling Linux  
    executables. It consists of a core, which provides a synthetic CPU in  
    software, and a series of debugging and profiling tools. The  
    architecture is modular, so that new tools can be created easily and  
    without disturbing the existing structure.  
  
    Some of the options described below work with all Valgrind tools, and  
    some only work with a few or one. The section MEMCHECK OPTIONS and  
    those below it describe tool-specific options.  
  
    This manual page covers only basic usage and options. For more  
    comprehensive information, please see the HTML documentation on your  
    system: $INSTALL/share/doc/valgrind/html/index.html, or online:  
    http://www.valgrind.org/docs/manual/index.html.  
Manual page valgrind(1) line 1 (press h for help or q to quit)
```


Compilation in debug mode

- In order to use Valgrind, we need to compile with `g++ -g`.
- **Q.** What does this option do?
 - It includes the names of functions, variables, etc., in the generated machine code.

This is needed because the debugger needs to tell us where the flow of execution was when the error was generated. Without these names, all the debugger could tell us would be something like:

“I’m running function 0x28fef4 and the value of variable 0x10dd12 is 42.”

- When not running in debug mode, the computer does not really care what the name of a function is (an address is enough).

Memory debugging — memcheck

We will use Valgrind's tool memcheck to detect memory bugs:

1. Use of **uninitialized memory**
2. Reading/writing memory **after** it has been freed
3. **Out-of-range**: reading/writing off the end of malloc'd blocks
4. **Memory leaks**

Uninitialized memory

```
#include <iostream>

int main() {
    int x;
    int y = x * 7;
    std::cout << y << std::endl;
}
```

This causes **undefined** behaviour. **Very dangerous!**

In terminal:

```
$ g++ -g hello.cpp -o hello
$ valgrind --track-origins=yes ./hello
```

Uninitialized memory

Valgrind detects the line (10) using the uninitialized value and the scope (5) containing it.

```
launch.json hello.cpp x
hello.cpp > ...
1  #include <iostream>
2
3  using namespace std;
4
5  int main(){
6
7      int x;
8      int y = x*7;
9
10     cout << y << endl;
11
12 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: bash

```
prog2021@prog2021-pc:~/hello$ valgrind --track-origins=yes ./hello
==8575== Memcheck, a memory error detector
==8575== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==8575== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==8575== Command: ./hello
==8575==
==8575== Conditional jump or move depends on uninitialised value(s)
==8575==    at 0x4981162: std::ostreambuf_iterator<char, std::char_traits<char> > std::num_put<char, std::ostreambuf_iterator<char, s
td::char_traits<char> > >::_M_insert_int<long>(std::ostreambuf_iterator<char, std::char_traits<char> >, std::ios_base&, char, long) c
onst (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.28)
==8575==    by 0x498FED9: std::ostream& std::ostream::_M_insert<long>(long) (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.28)
==8575==    by 0x1091D2: main (hello.cpp:10)
==8575== Uninitialised value was created by a stack allocation
==8575==    at 0x1091A9: main (hello.cpp:5)
```

Reading freed memory

```
#include <iostream>

int main() {
    int* a = new int[10];
    delete[] a;
    std::cout << a[5] << std::endl;
}
```

Often (but now always) this causes a **segmentation fault**.

In terminal:

```
$ g++ -g hello.cpp -o hello
$ valgrind ./hello
```


Reading freed memory

Valgrind detects: where the invalid **read** is performed (11), where memory was **allocated** (7) and where it was **freed** (9).

```
hello.cpp > main()
1  #include <iostream>
2
3  using namespace std;
4
5  int main(){
6
7      int* a = new int[10];
8
9      delete [] a;
10
11     cout << a[5] << endl;
12
13 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

1: bash

```
prog2021@prog2021-pc:~/hello$ valgrind ./hello
==8636== Memcheck, a memory error detector
==8636== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==8636== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==8636== Command: ./hello
==8636==
==8636== Invalid read of size 4
==8636==    at 0x10921E: main (hello.cpp:11)
==8636== Address 0x4dafc94 is 20 bytes inside a block of size 40 free'd
==8636==    at 0x483D74F: operator delete[](void*) (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==8636==    by 0x109215: main (hello.cpp:9)
==8636== Block was alloc'd at
==8636==    at 0x483C583: operator new[](unsigned long) (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==8636==    by 0x1091FE: main (hello.cpp:7)
```

Out-of-range errors

```
#include <iostream>

int main(){
    int* a = new int[10];
    std::cout << a[10] << std::endl;
    delete[] a;
}
```

Often (but now always) this causes a **segmentation fault**.

In terminal:

```
$ g++ -g hello.cpp -o hello
$ valgrind ./hello
```


Out-of-range errors

```
hello.cpp > main()
1  #include <iostream>
2
3  using namespace std;
4
5  int main(){
6
7      int* a = new int[10];
8      cout << a[10] << endl;
9      delete [] a;
10
11 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: bash

```
prog2021@prog2021-pc:~/hello$ valgrind ./hello
==8703== Memcheck, a memory error detector
==8703== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==8703== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==8703== Command: ./hello
==8703==
==8703== Invalid read of size 4
==8703==    at 0x10920B: main (hello.cpp:8)
==8703== Address 0x4dafca8 is 0 bytes after a block of size 40 alloc'd
==8703==    at 0x483C583: operator new[](unsigned long) (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==8703==    by 0x1091FE: main (hello.cpp:7)
==8703==
0
==8703==
==8703== HEAP SUMMARY:
==8703==    in use at exit: 0 bytes in 0 blocks
==8703==   total heap usage: 3 allocs, 3 frees, 73,768 bytes allocated
==8703==
==8703== All heap blocks were freed -- no leaks are possible
==8703==
==8703== For lists of detected and suppressed errors, rerun with: -s
==8703== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

Memory leaks

```
#include <iostream>

int main(){

    int* a = new int[10];

}
```

Be careful with **memory leaks**! If you repeatedly allocate memory and don't free it, you can easily fill your RAM and freeze your PC.

In terminal:

```
$ g++ -g hello.cpp -o hello
$ valgrind --leak-check=full ./hello
```


Memory leaks

```
hello.cpp > main()
1  #include <iostream>
2
3  using namespace std;
4
5  int main(){
6
7      int* a = new int[10];
8
9  }
10
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
==8731== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==8731== Command: ./hello
==8731==
==8731== HEAP SUMMARY:
==8731==    in use at exit: 40 bytes in 1 blocks
==8731==    total heap usage: 2 allocs, 1 frees, 72,744 bytes allocated
==8731==
==8731== 40 bytes in 1 blocks are definitely lost in loss record 1 of 1
==8731==    at 0x483C583: operator new[](unsigned long) (in /usr/lib/x86_64-linux-g
==8731==    by 0x10919E: main (hello.cpp:7)
==8731==
==8731== LEAK SUMMARY:
==8731==    definitely lost: 40 bytes in 1 blocks
==8731==    indirectly lost: 0 bytes in 0 blocks
==8731==    possibly lost: 0 bytes in 0 blocks
==8731==    still reachable: 0 bytes in 0 blocks
==8731==    suppressed: 0 bytes in 0 blocks
==8731==
==8731== For lists of detected and suppressed errors, rerun with: -s
==8731== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```


Memory leaks

Gold rule to avoid memory leaks:

- For each **new**, you have to write a corresponding **delete**.

In general: for each heap allocation, there should be a heap de-allocation (similarly, in C: for each `malloc`, you should have a `free`).

Memory leaks

- In general, don't call `delete` if you haven't called `new`.
- **Q.** Why is not (a manual) `delete` necessary instead in the following piece of code?

```
#include <vector>
```

```
int main() {
```

```
    auto v = std::vector<int>(100);
```

```
}
```

- Because `v` is on the stack (not on the heap). The object's destructor is automatically called when `v` is removed from the stack (i.e., when exiting `v`' scope).

Memory debugging

To sum up, one command for everything (note the compilation option `-g`):

```
$ g++ -g hello.cpp -o hello  
$ valgrind --leak-check=full --track-origins=yes ./hello
```

What you want is that the output of Valgrind ends with:

```
ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

Q. But why should you really care about memory bugs?

Exam project

You



me finding a
memory leak
in your project

teaching
assistants

Debugging — Part 2: compiler warnings and sanitizers

Compiler warnings

- The compiler can be instructed to report **warnings**.
- A warning is not an error but a suggestion that something is probably missing in your code or might go wrong...
- Comprehensive list of compiler flags to enable warnings:
<https://gcc.gnu.org/onlinedocs/gcc/Warning-Options.html>
- We will use two of them: `-Wall` `-Wextra`

`-Wall`

`-Wextra`

`-Wclobbered`
`-Wcast-function-type`
`-Wdeprecated-copy`
`-Wempty-body`
`-Wenum-conversion`
`-Wignored-qualifiers`
`-Wimplicit-fallthrough=3`
`-Wmissing-field-initializers`
`-Wmissing-parameter-type`
`-Wold-style-declaration`
`-Woverride-init`
`-Wsign-compare`
`-Wstring-compare`
`-Wredundant-move`
`-Wtype-limits`
`-Wuninitialized`
`-Wshift-negative-value`
`-Wunused-parameter`
`-Wunused-but-set-parameter`

`-Waddress`
`-Warray-bounds=1`
`-Warray-compare`
`-Warray-parameter=2`
`-Wbool-compare`
`-Wbool-operation`
`-Wc++11-compat-Wc++14-compat`
`-Wcatch-value`
`-Wchar-subscripts`
`-Wcomment`
`-Wdangling-pointer=2`
`-Wduplicate-decl-specifier`
`-Wenum-compare`
`-Wenum-int-mismatch`
`-Wformat`
`-Wformat-overflow`
`-Wformat-truncation`
`-Wint-in-bool-context`
`-Wimplicit`
`-Wimplicit-int`
`-Wimplicit-function-declaration`
`-Winit-self`
`-Wlogical-not-parentheses`
`-Wmain`
`-Wmaybe-uninitialized`
`-Wmemset-elt-size`
`-Wmemset-transposed-args`
`-Wmisleading-indentation`
`-Wmismatched-dealloc`
`-Wmismatched-new-delete`
`-Wmissing-attributes`
`-Wmissing-braces`
`-Wmultistatement-macros`
`-Wnarrowing`
`-Wnonnull`
`-Wnonnull-compare`
`-Wopenmp-simd`
`-Wparentheses`
`-Wpessimizing-move`
`-Wpointer-sign`
`-Wrange-loop-construct`
`-Wreorder`
`-Wrestrict`
`-Wreturn-type`
`-Wself-move`
`-Wsequence-point`
`-Wsign-compare`
`-Wsizeof-array-div`
`-Wsizeof-pointer-div`
`-Wsizeof-pointer-memaccess`
`-Wstrict-aliasing`
`-Wstrict-overflow=1`
`-Wswitch`
`-Wtautological-compare`
`-Wtrigraphs`
`-Wuninitialized`
`-Wunknown-pragmas`
`-Wunused-function`
`-Wunused-label`
`-Wunused-value`
`-Wunused-variable`
`-Wuse-after-free=3`
`-Wvla-parameter`
`-Wvolatile-register-var`
`-Wzero-length-bounds`

Compiler warnings — Example

```
1  #include <iostream>
2
3  int main() {
4      int x;
5      int y = x * 7;
6      std::cout << y << std::endl;
7  }
```

```
→ Desktop g++ test.cpp -o test -Wall -Wextra
test.cpp:5:11: warning: variable 'x' is uninitialized when used here [-Wuninitialized]
    int y = x * 7;
            ^
test.cpp:4:8: note: initialize the variable 'x' to silence this warning
    int x;
        ^
        = 0
1 warning generated.
→ Desktop █
```

Always add these two flags in your Makefile

FOLDERS

▼ power-root-example-project-with-asserts

▶ build

▶ include

▶ src

▶ tools

/* Makefile

Makefile

1 OPTIONS=-O3 -DNDEBUG -Wall -Wextra

2

3 all: build/theanswer

4

5 debug: OPTIONS=-O0 -g -DDEBUG -Wall -Wextra

6 debug: build/theanswer

7

8 build/theanswer: build/root.o build/power.o tools/main.cpp

9 g++ \${OPTIONS} tools/main.cpp -o build/theanswer -I include/ build/root.o build/power.o

10

11 build/root.o: src/root.cpp

12 g++ -c src/root.cpp -o build/root.o -I include/

13

14 build/power.o: src/power.cpp

15 g++ -c src/power.cpp -o build/power.o -I include/

16

17 clean:

18 rm -rf build/*.o build/theanswer

Compiler sanitizers

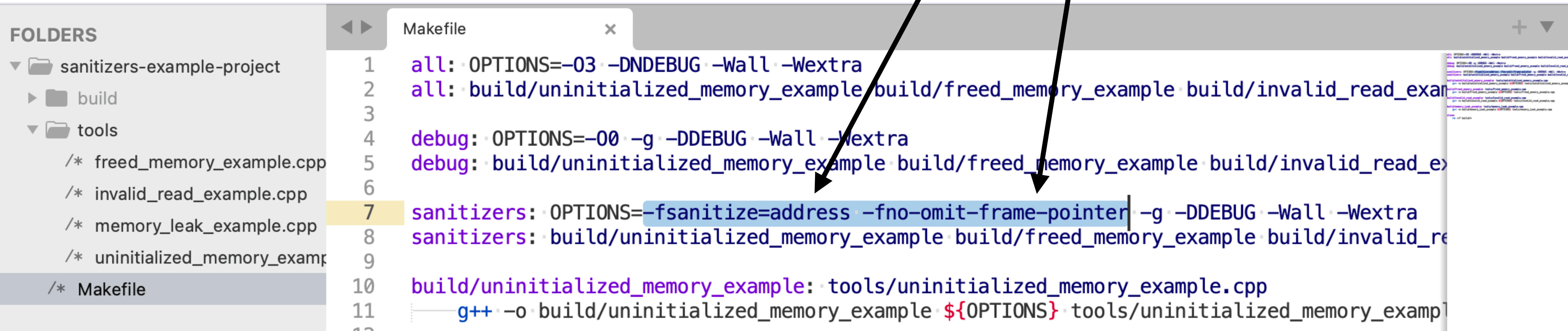
- Valgrind is a great tool to hunt memory bugs down. **Use it!**
- But Valgrind is a **simulator**: there could be some subtle problems in the code that look fine for Valgrind.
- Valgrind **does not scale**. If you are working on a large project and with some large datasets (large memory allocations), it will slow down program execution by (typically) one order to magnitude (10 times slower).
- Thus, it is fine for developing/debugging small-medium size projects.
- Here is a more precise alternative: **compiler sanitizers**.
- Two more compiler flags: `-fsanitize=address` and `-fno-omit-frame-pointer`.

<https://clang.llvm.org/docs/AddressSanitizer.html>

Compiler sanitizers

- Create a new target “sanitizers” in your Makefile with these two flags.
- You can enable/disable sanitizers at compile time:

```
$ make clean; make  
$ make clean; make sanitizers
```



Example 1: invalid read

FOLDERS

▼ sanitizers-example-project

▶ build

▼ tools

/* freed_memory_example.cpp

/* invalid_read_example.cpp

/* memory_leak_example.cpp

/* uninitialized_memory_example.

/* Makefile

invalid_read_example.cpp x

1 **#include** <iostream>

2

3 **int** main() {

4 **int** *a = **new** **int**[10];

5 std::cout << a[10] << std::endl;

6 **delete**[] a;

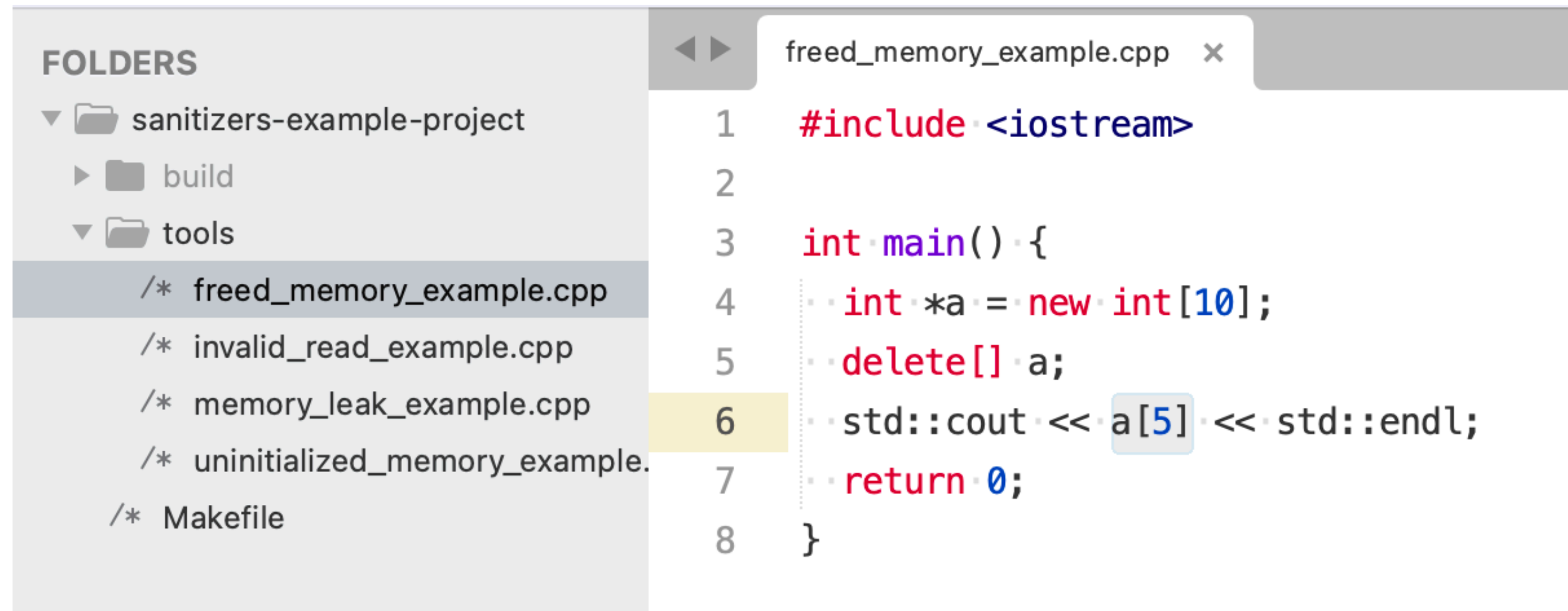
7 **return** 0;

8 }

```
==654763==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000000038 at pc 0x562d9e833322 bp 0x7ffe3a665210 sp 0x7ffe3a665200
READ of size 4 at 0x604000000038 thread T0
#0 0x562d9e833321 in main tools/invalid_read_example.cpp:5
#1 0x7f30277a6fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
#2 0x7f30277a707c in __libc_start_main_impl ../csu/libc-start.c:409
#3 0x562d9e833204 in _start (/home/giulio/pel/slides/1-introduction/code/sanitizers-example-project/build/invalid_read_example+0x1204)

0x604000000038 is located 0 bytes to the right of 40-byte region [0x604000000010,0x604000000038)
allocated by thread T0 here:
#0 0x7f3027d72337 in operator new[](unsigned long) ../../../../src/libsanitizer/asan/asan_new_delete.cpp:102
#1 0x562d9e8332de in main tools/invalid_read_example.cpp:4
#2 0x7f30277a6fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
```


Example 2: accessing freed memory



```
FOLDERS
▼ sanitizers-example-project
  ► build
  ▼ tools
    /* freed_memory_example.cpp
    /* invalid_read_example.cpp
    /* memory_leak_example.cpp
    /* uninitialized_memory_example.cpp
    /* Makefile

freed_memory_example.cpp x
1  #include <iostream>
2
3  int main() {
4      int *a = new int[10];
5      delete[] a;
6      std::cout << a[5] << std::endl;
7      return 0;
8  }
```

```
==654728==ERROR: AddressSanitizer: heap-use-after-free on address 0x604000000024 at pc 0x55f6d70a6335 bp 0x7fff3f1671e0 sp 0x7fff3f1671d0
READ of size 4 at 0x604000000024 thread T0
```

```
#0 0x55f6d70a6334 in main tools/freed_memory_example.cpp:6
#1 0x7faeb0877fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
#2 0x7faeb087807c in __libc_start_main_impl ../csu/libc-start.c:409
#3 0x55f6d70a6204 in _start (/home/giulio/pel/slides/1-introduction/code/sanitizers-example-project/build/freed_memory_example+0x1204)
```

```
0x604000000024 is located 20 bytes inside of 40-byte region [0x604000000010,0x604000000038)
```

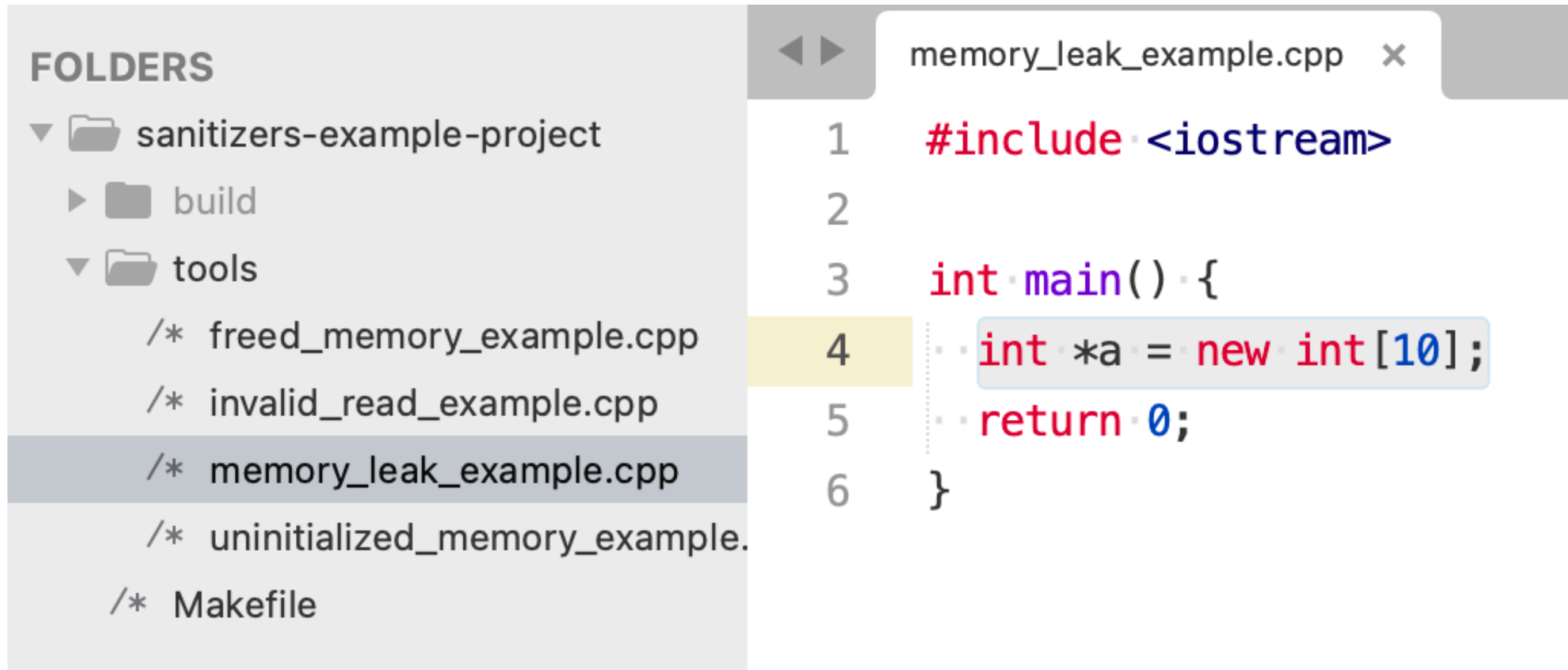
```
freed by thread T0 here:
```

```
#0 0x7faeb0e43e37 in operator delete[](void*) ../../../../src/libsanitizer/asan/asan_new_delete.cpp:163
#1 0x55f6d70a62f5 in main tools/freed_memory_example.cpp:5
#2 0x7faeb0877fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
```

```
previously allocated by thread T0 here:
```

```
#0 0x7faeb0e43337 in operator new[](unsigned long) ../../../../src/libsanitizer/asan/asan_new_delete.cpp:102
#1 0x55f6d70a62de in main tools/freed_memory_example.cpp:4
#2 0x7faeb0877fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
```

Example 3: memory leaks



FOLDERS

- ▼ sanitizers-example-project
 - ▶ build
 - ▼ tools
 - /* freed_memory_example.cpp
 - /* invalid_read_example.cpp
 - /* memory_leak_example.cpp
 - /* uninitialized_memory_example.
 - /* Makefile

```
memory_leak_example.cpp x
1  #include <iostream>
2
3  int main() {
4      int *a = new int[10];
5      return 0;
6  }
```

==657730==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 40 byte(s) in 1 object(s) allocated from:

```
#0 0x7f9af29e6337 in operator new[](unsigned long) ../../../../src/libsanitizer/asan/asan_new_delete.cpp:102
#1 0x56106d87225e in main tools/memory_leak_example.cpp:4
#2 0x7f9af241afcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
```

Sanitizers vs. Valgrind

- **Make your code safer by compiling with sanitizers when developing.**
- Sanitizers work at the **compilation** level: you need the source code. Valgrind is a simulator and you would only need the compiled object code.
- Valgrind is an external tool; not shipped with your compiler.
- This also means that to disable sanitizers, you have to compile it again. With Valgrind: compile once and use it only when needed.
- Sanitizers are more precise and can detect more errors.
- Sanitizers do not slow down your program by one order of magnitude; Valgrind does.
- Unfortunately, sanitizers are not well supported on Mac (hopefully, support will come in the close future).
- For your projects: **use both.**