C++ devirtualization in clang

Piotr Padlewski, University of Warsaw,
intern at Google

Why devirtualization matters?

- Because we want to inline virtual functions!
- even if we will not inline, optimizer will take advantage of direct call
- we can make binaries smaller

Everything will lead to performance boost.

How virtual calls works

```
struct A {
  virtual void foo();
};
void g(A * a) {
  a->foo();
}
```

```
%vtable = load void (%struct.A*)**, void (%struct.A*)*** %a, align 8
%1 = load void (%struct.A*)*, void (%struct.A*)** %vtable, align 8
call void %1(%struct.A* %a)
```

Old devirtualization

```
struct A {
  virtual void foo();
};

void f() {
  A a;
  a.foo();
  a.foo();
}
```

Both will be direct call

Old devirtualization

```
struct A {
  virtual void foo();
};
void A::foo() { }
void g(A& a) {
  a.foo();
}

void f() {
  A a;
  g(a);
}
```

Works because g will be inlined

… and also because foo is defined in this TU.

Old devirtualization

```
struct A {
  A();
  virtual void foo();
};
void A::foo() { }
void g(A& a) {
  a.foo();
}
void f() {
  A a;
  g(a);
}
```

Constructor is now outline.

Won’t devirtualize because optimizer doesn’t know what is stored to vptr.

Old devirtualization

```
struct A {
  virtual void bar();
  virtual void foo();
};
void A::bar() { }
void g(A& a) {
  a.foo();
  a.foo();
}
void f() {
  A a;
  g(a);
}
```

Won’t devirtualize because optimizer doesn’t know that foo didn’t change vptr.

Old devirtualization

```
struct A {
  virtual void foo();
  virtual ~A() = default;
};
void g(A& a) {
  a.foo();
}
void f() {
  A a;
  g(a);
}
```

Won’t devirtualize because vtable is now external.

@vtable for A = external unnamed_addr constant [5 x i8*]

Calling the same virtual function

```
struct A {
  virtual void foo();
};
void g(A * a) {
  a->foo();
  a->foo();
}
```

```
%vtable = load  (…) %a
 %1 = load void (...) %vtable
 call void %1(%struct.A* %a)

%vtable2 = load  (…) %a
 %2 = load void (...) %vtable2
 call void %2(%struct.A* %a)
```

Placement new is evil

```
struct A {
  virtual void foo();
};
struct B : A {
  virtual void foo();
};
void A::foo() { new(this) B; } //in .cc
void g() {
  A *a = new A;
  a->foo();
  a->foo(); // Undefined behaviour
}
```

```
struct A {
  virtual A* foo();
};
struct B : A {
  virtual A* foo();
};
A* A::foo() { return new(this) B; }
void g() {
  A *a = new A;
  A *a2 = a->foo();
  a2->foo(); // this is fine
}
```

assuming type after ctor call

After calling the constructor, it would be very nice to know what is the vptr value.

```
call void @_ZN1AC1Ev(%struct.A* %a)

 %vtable = load i64*, i64** %a, align 8
 %cmp = icmp eq i64* %vtable, @vtable
 tail call void @llvm.assume(i1 %cmp)

 %vtable1 = load void (%struct.A*)**, void (%struct.A*)*** %a, align 8
```

available_externally vtables

```
@vtable for A = external unnamed_addr constant [6 x i8*]

@vtable for a = available_externally unnamed_addr constant [6 x i8*] (

    definition)
```

Unfortunately it is not safe to generate available_externally vtables in cases like:

- class has inline virtual functions
- class has hidden virtual functions - __attribute__((visibility("hidden")))

propagating “constness” of vptr

```
struct A {
  virtual void foo();
};
void g(A * a) {
  a->foo();
  a->foo();
}
```

```
%vtable = load  (…) %a
 %1 = load void (...) %vtable
 call void %1(%struct.A* %a)

%vtable2 = load  (…) %a
 %2 = load void (...) %vtable2
 call void %2(%struct.A* %a)
```

propagating “constness” of vptr

```
%vtable = load  (…) %a
 %1 = load void (...) %vtable
 call void %1(%struct.A* %a)

%vtable2 = load  (…) %a
 %2 = load void (...) %vtable2
 call void %2(%struct.A* %a)
```

```
%vtable = load  (…) %a
 %1 = load void (...) %vtable
 call void %1(%struct.A* %a)

 %2 = load void (...) %vtable
 call void %2(%struct.A* %a)
```

introducing !invariant.group

```
%vtable = load  (…) %a, !invariant.group !0
 %1 = load void (...) %vtable
 call void %1(%struct.A* %a)

%vtable2 = load  (…) %a, !invariant.group !0
 %2 = load void (...) %vtable2
 call void %2(%struct.A* %a)
```

Dealing with placement new

```
int main() {
  MyClass c;
  c.foo();
  auto c2 = new (&c) MyOtherClass();
  c2->foo();
  c2->~MyOtherClass();
  new (&c) MyClass();
}
```

introducing invariant.group.barrier

```
auto c2 = new (&c) MyOtherClass();
```

```
call void @_ZN7MyClassD1Ev(%struct.MyClass* nonnull %c) #1
%2 = bitcast %struct.MyClass* %c to %struct.MyOtherClass*
%3 = call @llvm.invariant.group.barrier(%2)
```

introducing -fstrict-vtable-pointers

For reasons like:

- LTO between code with **!invariant.group** and without is unsafe
- Optimizers don’t know how to deal with **invariant.group.barrier**
- **UBSan** doesn’t check for UBs from changing dynamic type
- Whole thing is still experimental.

Corner cases

```
void g() {
  A *a = new A;
  a->foo();
  A *b = new(a) B;
  assert(a == b);
  b->foo();
}
```

After assert llvm knows that a == b and can replace one with another.

Results

Unknown...

We know that devirtualization happen.

But the project is not yet done, there are so many things that we can still do, and the largest thing will come with !invariant. group.

Sources

Devirtualization paper:

https://goo.gl/r5dOxR

How devirtualization works in gcc (*Jan Hubička*)

http://hubicka.blogspot.com/2014/01/devirtualization-in-c-part-1.html

https://www.youtube.com/watch?v=oN15LjHX9xY

Thank you