CS 485
Advanced Object Oriented Design

In Memory Objects and RTTI

Spring 2019

14_InMemoryObjects

References

Stroustrup, The C++ Programming Language, 4th Edition

Meyers, More Effective C++, 3rd Edition

http://www.openrce.org/articles/full_view/23

http://blog.quarkslab.com/visual-c-rtti-inspection.html

https://ofekshilon.com/2010/11/07/d1reportallclasslayout-dumping-object-memory-layout/
https://ofekshilon.com/2012/04/11/viewing-types-part-2-the-manual-way/

https://blogs.msdn.microsoft.com/vcblog/2007/05/17/diagnosing-hidden-odr-violations-in-visual-c-and-fixing-lnk2022/

https://blogs.msdn.microsoft.com/zhanli/2010/07/01/c-tips-adjustor-thunk-what-is-it-why-and-how-it-works/

https://pigworlds.wordpress.com/2009/01/17/msvc-compiler-d1reportsingleclasslayout-d1reportallclasslayout/

https://www.hex-rays.com/products/ida/support/download.shtml

http://stackoverflow.com/questions/36954679/confusion-on-assembly-output-of-virtual-table-in-visual-c-2015

https://shaharmike.com/cpp/vtable-part1/

https://alschwalm.com/blog/static/2017/01/24/reversing-c-virtual-functions-part-2-2/

Notes

Object In Memory Layout

- Data Members
  - one set of data members per *object*
  - includes data members from parent classes

- Member Functions
  - non-virtual functions
  - Virtual Function Table (vtbl)
    - one vtbl per *class*
    - one vtbl ptr (vfptr) per *object*
    - not a bad job interview question

In Memory Layout

- Developer Command Prompt for VS17

cl.exe /c /d1reportSingleClassLayoutanimal animal.cpp > animal_single.out

```
class animal
{
  public:
    animal() ;
    animal(int w);
    int getWeight() ;
    void setWeight (int *w);

    virtual int eat(animal &pA);
    virtual void makeSound () = 0;
    virtual int getWeight2 () = 0;
    virtual void hi ();

private:
  int mWeight;
  int mHeight;

  static int mSTATIC;
  static const int mSTATIC_CONST = 1 ;
};
```

```
class animal  size(12):
  +---
 0  | {vfptr}
 4  | mWeight
 8  | mHeight
  +---

animal::$vftable@:
  | &animal_meta
  |  0
 0  | &animal::eat
 1  | &animal::makeSound
 2  | &animal::getWeight2
 3  | &animal::hi

animal::eat this adjustor: 0
animal::makeSound this adjustor: 0
animal::getWeight2 this adjustor: 0
animal::hi this adjustor: 0
```

In Memory Layout

- Developer Command Prompt for VS17

cl.exe /c /d1reportSingleClassLayoutcat cat.cpp > cat_single.out

```
class cat : public animal
{
  public:
    cat(int w);

    void makeSound();
    int getWeight2();
    void bye();
    void boggle();
    void boggle(int x);
    void hi();

    virtual int getTeeth ();

    int nonVirtualFunction ();
private:
  int mWeight;
  int mTeeth;
};
```

```
class cat size(20):
  +---
 0  | +--- (base class animal)
 0  | | {vfptr}
 4  | | mWeight
 8  | | mHeight
   | +---
12  | mWeight
16  | mTeeth
  +---

cat::$vftable@:
  | &cat_meta
  |  0
 0  | &animal::eat
 1  | &cat::makeSound
 2  | &cat::getWeight2
 3  | &cat::hi
 4  | &cat::getTeeth

cat::makeSound this adjustor: 0
cat::getWeight2 this adjustor: 0
cat::hi this adjustor: 0
cat::getTeeth this adjustor: 0
```

- describe how the following works

```
animal otherAnimal;
animal *pA = new cat(3);
pA->hi();
pA->eat(otherAnimal);
```

http://www.openrce.org/articles/full_view/23

Overloaded Functions

Name mangling/decorating

cl.exe /c /FAcs main.cpp

```
?foo@@YAHH@Z                    ; foo

?foo@@YAHXZ                   ; foo

?foo@@YAHM@Z                    ; foo
```

```
int foo (int x)
{
  return 42;
}

int foo ()
{
  return 42;
}

int foo (float z)
{
  return 42;
}
```

http://www.kegel.com/mangle.html

https://en.wikiversity.org/wiki/Visual_C%2B%2B_name_mangling

http://mearie.org/documents/mscmangle/

https://msdn.microsoft.com/en-us/library/56h2zst2.aspx

http://www.agner.org/optimize/calling_conventions.pdf

Sub-Sub-Class

```
class tiger : public cat
{
public:
  tiger (int w);

  int getWeight2 ();
  void hi ();

  int nonVirtualFunction ();
private:
  int mStripes;
};
```

```
class tiger size(24):
  +---
 0  | +--- (base class cat)
 0  | | +--- (base class animal)
 0  | | | {vfptr}
 4  | | | mWeight
 8  | | | mHeight
  | | +---
12  | | mWeight
16  | | mTeeth
  | +---
20  | mStripes
  +---

tiger::$vftable@:
  | &tiger_meta
  |  0
 0  | &cat::makeSound
 1  | &tiger::getWeight2
 2  | &tiger::hi
 3  | &animal::eat
 4  | &cat::getTeeth

tiger::getWeight2 this adjustor: 0
tiger::hi this adjustor: 0
```

Multiple Inheritance

```
class SpaceTiger : public tiger, public SpaceCreature
{
public:
  SpaceTiger (int w, int oxygen);

  void useOxygen ();

  void hi ();


private:

  int mSpaceStripes;

};
```

```
class SpaceTiger  size(36):
  +---
 0  | +--- (base class tiger)
 0  | | +--- (base class cat)
 0  | | | +--- (base class animal)
 0  | | | | {vfptr}
 4  | | | | mWeight
 8  | | | | mHeight
  | | | +---
12  | | | mWeight
16  | | | mTeeth
  | | +---
20  | | mStripes
  | +---
24  | +--- (base class SpaceCreature)
24  | | {vfptr}
28  | | mOxygen
  | +---
32  | mSpaceStripes
  +---

SpaceTiger::$vftable@tiger@:
  | &SpaceTiger_meta
  |  0
 0  | &cat::makeSound
 1  | &tiger::getWeight2
 2  | &SpaceTiger::hi
 3  | &animal::eat
 4  | &cat::getTeeth

SpaceTiger::$vftable@SpaceCreature@:
  | -24
 0  | &SpaceTiger::useOxygen

SpaceTiger::useOxygen this adjustor: 24
SpaceTiger::hi this adjustor: 0
```

Runtime Type Information

```
animal *pcAnimal = new cat(9);
cat *pcCat = new cat(8);

// up cast
// which hi() is called?
(dynamic_cast<animal*>(pcCat))->hi();

// down cast
std::cout << (dynamic_cast<cat *>(pcAnimal))->getTeeth();

std::cout << typeid(*pcAnimal).name() << std::endl;

std::cout << typeid(*pcAnimal).raw_name() << std::endl;

std::cout << (dynamic_cast<tiger *>(pcAnimal))->getStripes ();
```

https://docs.microsoft.com/en-us/windows/desktop/Debug/pe-format

https://docs.microsoft.com/en-us/cpp/cpp/run-time-type-information?view=vs-2017

https://docs.microsoft.com/en-us/cpp/cpp/type-info-class?view=vs-2017

https://blog.quarkslab.com/visual-c-rtti-inspection.html

RTTI

```
class _s__RTTICompleteObjectLocator size(20):
  +---
 0  | signature
 4  | offset
 8  | cdOffset
12  | pTypeDescriptor
16  | pClassDescriptor
  +---
```

```
typedef const struct _s__RTTICompleteObjectLocator {
  unsigned long signature;
  unsigned long offset;
  unsigned long cdOffset;
  _TypeDescriptor *pTypeDescriptor;
  __RTTIClassHierarchyDescriptor *pClassDescriptor;
} __RTTICompleteObjectLocator;
```

```
typedef const struct _s__RTTIClassHierarchyDescriptor {
  unsigned long signature;
  unsigned long attributes;
  unsigned long numBaseClasses;
  __RTTIBaseClassArray *pBaseClassArray;
} __RTTIClassHierarchyDescriptor;
```

```
typedef const struct _s__RTTIBaseClassArray {
  __RTTIBaseClassDescriptor *arrayOfBaseClassDescriptors [];
} __RTTIBaseClassArray;
```

```
typedef const struct _s__RTTIBaseClassDescriptor {
  _TypeDescriptor *pTypeDescriptor;
  unsigned long numContainedBases;
  _PMD where;
  unsigned long attributes;
} __RTTIBaseClassDescriptor;
```

http://www.geoffchappell.com/studies/msvc/language/predefined/

http://blog.quarkslab.com/visual-c-rtti-inspection.html

http://blog.quarkslab.com/visual-c-rtti-inspection.html