ISCAS 中国科学院软件研究所学术年会’2022
暨计算机科学国家重点实验室开放周
学术论文

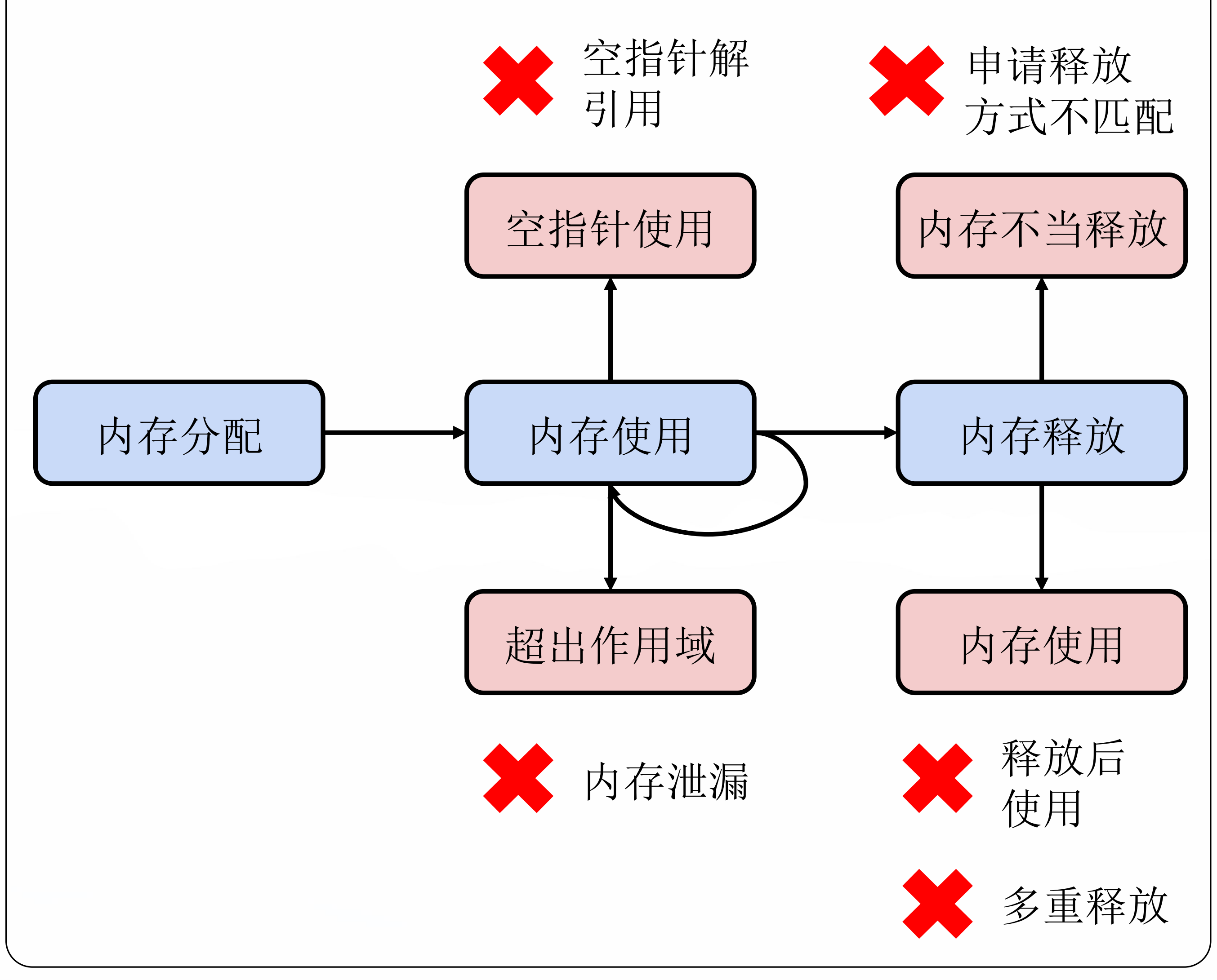
通过追踪 C++ 智能指针的堆内存管理机制进行内存相关错误的检测
Detecting Memory-Related Bugs by Tracking Heap Memory Management of C++ Smart Pointers

马旭桐[1]、燕季薇、王伟、严俊[2]、张健[3]、裘宗燕

发表会议：*2021 36th IEEE/ACM International Conference on Automated Software Engineering*, pp. 880-891

联系方式：maxt@ios.ac.cn[1], yanjun@ios.ac.cn[2], zj@ios.ac.cn[3]

一般程序的内存管理及常见内存错误



基于 C++ 智能指针机制的自动化内存管理

- 分配内存后立即赋值给智能指针对象
- 使用**析构函数**机制**自动释放**指向的堆内存块
- 智能指针用于**管理**内存，普通指针用于**使用**内存

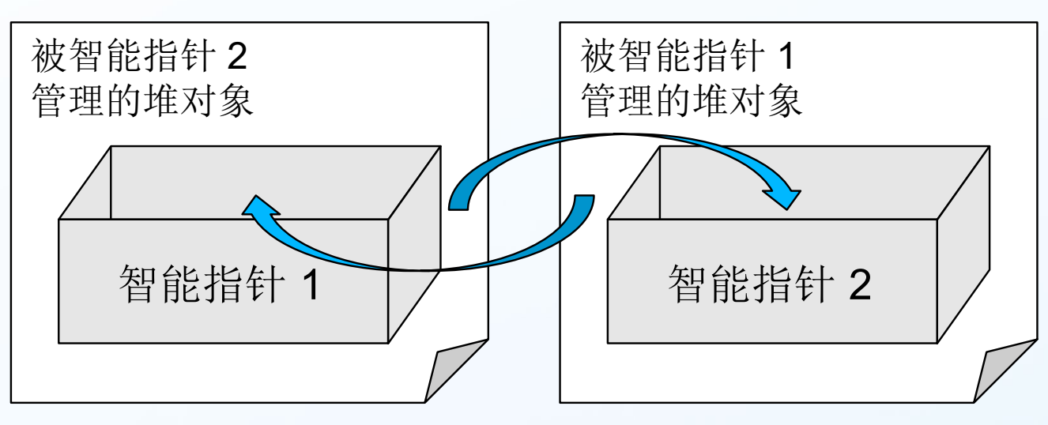
```
void ManualBark() {
  Dog *dog = new Dog;
  dog->bark();
  delete dog;
}
```

```
void AutoBark() {
  unique_ptr<Dog> dog(new Dog);
  dog->bark();
  // 无需手动进行内存释放操作
}
```

使用智能指针无法避免所有内存相关错误

- 类似于普通指针使用时的**空指针解引用**等指针使用问题
- 智能指针使用时特有的**不当赋值**、**循环引用**问题
- 智能指针种类选择不当导致的**运行效率**问题

内存不当释放



被智能指针管理对象间的循环引用

内存泄漏

智能指针方法中的动作提取 → 智能指针动作的操作语义建模 → 对象生命周期状态的扩展 → 针对特定缺陷的检查器设计

检测工具 *Spelton*

手工构造的代码片段的检查结果

工具名称	*CSA*	*Infer*	*CppCheck*	*SPrinter*	*Spelton*
正确报告数	72	0	172	206	1,016
正确未报数	1,656	1,656	1,656	1,656	1,656
误报数	0	0	4	10	0
漏报数	946	1,018	846	812	2
准确率	100.00%	无效	97,73	95.37%	100.00%
召回率	7.07%	无效	16.90%	20.24%	99.80%
F1 值	13.21%	无效	28.81%	33.39%	99.90%

本工具

- 本研究开发的 *Spelton* 工具可以在无误报的情况下找到几乎全部问题
- 对比的知名开源静态分析工具都仅能找到其中的一部分，但准确率也都比较高

其他工具共产生 3 个正确的智能指针误用报告

中大型开源项目的检查结果

项目名称	千行代码	*CSA*	*Infer*	*CppCheck*	*SPrinter*	*Spelton*
Aquila	15.92	0	8	17	0	7/7
Aria2	125.19	4(1)	12	0	2(2)	20/35
Celero	8.37	0	3	0	0	3/6
Evpp	60.13	47(9)	14(6)	12	1	14/18
Osrm	746.33	14	12	20	0	6/7
Restbed	22.86	2	254(18)	34	0	3/7
Spdlog	32.55	0	1	3	0	3/3
MySQL	3,633.72	1637(14)	1668(2)	工具崩溃	89(37)	59/79
LLVM	5,842.38	657(35)	5567(18)	326	59(9)	326/486
合计	-	2361(59)	7539(44)	412	151(48)	441/648

括号中为路径中包含智能指针的报告数量

有良好维护的大型开源项目中发现大量问题

共提交 14 项修改建议，其中 7 项已合并，涉及 76 个缺陷报告