目录

总结

最开始可以看南京大学《软件分析》和北京大学《程序分析》，燕云直播上可以看到课程视频。学完一次之后也可以回来反复看。南京大学的课程深入讲解了数据流分析和基于抽象解释的指针分析，北大的课程涵盖较广，还包含了 类 C 语言的指针分析、符号执行、program synthesis 等内容。

随着学习的深入，也经常会发现自己之前的视角，对相关领域的理解过于狭隘，这一点在学习资源上也是如此，经常会有很好的学习资源，学习路线我不知道，错失很好的学习材料，增加学习难度。因此这里分享的资源也会一定程度上受限于我自己的水平，反映我自身水平的不足。只能自己希望这些链接对大家有用吧。所以有什么好的资料也欢迎推荐给我。

我目前学习了南大和北大这两门课，目前也还没有找到下一步比较系统的学习资料，在复习之前学忘了的基础知识和零散地看一些 C/C++语言上的分析。目前的下一步考虑是看《Types and Programming Languages》、《Software Foundations》(https://softwarefoundations.cis.upenn.edu/)、《The Formal Semantics of Programming Languages: An Introduction》。

如果你们看到了一些（觉得不错的、一般的、不好的）学习资料都可以推荐给我。

为什么分享这个

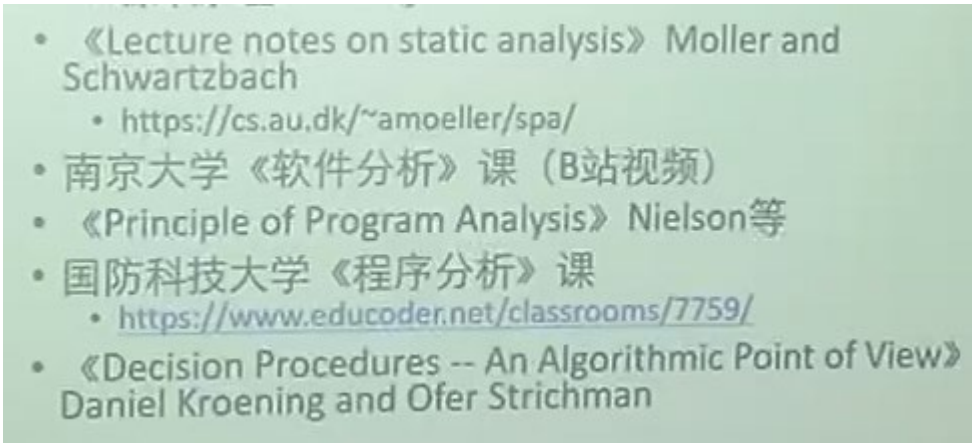
主要原因是，碰巧自己记录的学习资源是比较容易分享的形式。

之前想找相关的国外大学的网课，（毕竟对国外大学有哪些也不是很熟）一直很难搜索到，有时候在知乎上零零散散看到一两个。但是有一次我搜索一些数据流分析的一个术语 Meet-Over-All-Path 的时候发现谷歌搜出来好多网课的课件。因此得以顺着找到很多相关大学的课程，记录下来。我还没来得及看，所以说不出哪个课程比较容易跟上，希望对大家有用吧。

1. 程序分析

熊英飞老师的课：https://xiongyingfei.github.io/SA/2020/main.htm 涉及指针分析，数据流分析等等。

老师的其他推荐：Denmark 大学 Michael Schwatzbach 的 Lecture Notes on Static Analysis 和 CMU Jo Aldrich 的 Program Analysis 课程上的 Lecture Notes。前者比较简短，后者比较深入。两者的内容都已经在我的课上覆盖。



https://github.com/RangerNJU/Static-Program-Analysis-Book#课程视频和阅读资料 这里还有很多资源。

国际课程

MIT 6.820 fundamentals-of-program-analysis 程序分析入门课。没有视频

https://learning-modules.mit.edu/materials/index.html?uuid=/course/6/fa17/6.820#materials 课程的一堆资料

https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-820-fundamentals-of-program-analysis-fall-2015/syllabus/ 列举了一些教材（Textbook）根据名字可以在 http://libgen.is/ 上找到

https://www.cs.cornell.edu/courses/cs711/2005fa/ Cornell CS711 专讲各种分析，有很多不错的 PDF

https://homepages.dcc.ufmg.br/~fernando/classes/dcc888/ UFMG 的 DCC 888

https://www.cs.cmu.edu/~aldrich/courses/17-355-19sp/ CMU 程序分析

http://www.cs.toronto.edu/~chechik/courses06/csc2125/ Toronto CSC2125 Topics in Software Engineering: Static Analysis of Programs

包含程序分析的编译器课程

Data Flow Analysis and Optimizations：

http://www.cs.cmu.edu/afs/cs/academic/class/15745-s06/web/syllabus.html CMU 15-745 Optimizing Compilers

https://cseweb.ucsd.edu/classes/fa12/cse231-a/ UCSD CSE 231 Advanced Compilers

http://pages.cs.wisc.edu/~horwitz/CS704-NOTES/ https://github.com/barghouthi/cs704 WISC CS704 Programming Languages and Compilers

https://groups.seas.harvard.edu/courses/cs252/2020sp/ Harvard cs252 Advanced Topics in PL

https://www.cs.purdue.edu/homes/hosking/502/ purdue CS502 Compiling and Programming Systems

这些课程资料里面找到的书

http://www.cs.toronto.edu/~chechik/courses06/csc2125/readings.html Toronto CSC2125 的 reading list

Principles of Program Analysis，作者 Flemming Nielson, Hanne Riis Nielson, Chris Hankin. 2nd edition, 2005. Springer.

The Formal Semantics of Programming Languages: An Introduction

Types and Programming Languages

其他资料

https://people.cs.ksu.edu/~schmidt/papers/schmidt/Escuela03/ Abstract interpretation and static analysis - International Winter School on Semantics and Applications

2. 抽象解释-程序分析

https://www.di.ens.fr/~cousot/AI/IntroAbsInt.html Abstract Interpretation in a Nutshell 介绍了程序分析的各种分支，https://www.di.ens.fr/~cousot/AI/ 抽象解释的入门介绍。清楚说明了抽象解释的应用。

MIT 16.399 http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/ 一门抽象解释的课。似乎没有视频

https://courses.cs.washington.edu/courses/cse501/15sp/papers/hind.pdf Pointer Analysis: Haven't We Solved This Problem Yet 指针分析的综述性文章

https://yanniss.github.io/points-to-tutorial15.pdf Foundations and Trends in Programming Languages 一个 72 页的入门教程

2.1.1. 南大《软件分析》那边的资料

https://pascal-group.bitbucket.io/teaching.html 课程主页，下载课件

https://github.com/RangerNJU/Static-Program-Analysis-Book 有人对应做出来的 gitbook，一般复习、想要粗略浏览整个课程我会看这个

浅谈 编程语言研究 与 程序分析 李樾 https://zhuanlan.zhihu.com/p/45208498 分析了静态分析会议的历史，研究方向等。

沉浸式《程序分析》教材 https://zhuanlan.zhihu.com/p/417187798 不错的入门材料

其他：

https://www.zhihu.com/people/tree-big-77/posts 知乎的文章列表 https://www.zhihu.com/people/silverbullettt/posts

https://www.zhihu.com/column/pl-research 知乎专栏

其他人的笔记

很多人在网上发表这个课程的笔记，一搜可以找到一大堆。

https://www.jianshu.com/p/1ca6e11b1e72 研究 reflection、Native code。

2.1.2. 指针分析

Dagstuhl Seminar 13162. 2013 研讨会总结分析技术

Vini Kanvar, Uday P. Khedker, “Heap Abstractions for Static Analysis”. ACM CSUR 2016 堆抽象的论文

2.2. PL 理论

软件理论基础与实践 熊英飞、胡振江老师的课：https://xiongyingfei.github.io/SF/2021/lectures.html 编程语言与形式化基础

编程语言设计原理 课程 熊英飞等 https://xiongyingfei.github.io/DPPL/2021/main.htm 较深入，编程语言设计

3. 符号执行项目

6.858 Spring 2018 Lab 3: Symbolic execution

TODO