Lecture1

Topic	备注	书上页数	PPT页数
P与NP问题的定义			5
对象的表达方式		14	26
计算任务		15	29
复杂性：时间，空间，电路			30-32
搜索问题和判定问题		15	35-36
算法A作为问题的解决者			40
一致性问题（图灵机）和非一致性计算模型（电路）		16-17	41-46

Lecture 2 计算模型

Topic	备注	书上页数	PPT页数
一致性模型	图灵机	16	2
非一致性模型	电路和接受建议的机器		2

|图灵机的简单描述||17| 5 |图灵机的正式描述|||6 |图灵机的高级描述||18|7-10 |有限自动机和图灵机的区别|||11| |图灵机函数计算的例子|||12| |多带图灵机|能被多带图灵机计算 iff 能被单带图灵机计算||13-14| |确定及非确定性图灵机|确定：每一步都只有一个可能的转移值。非确定：每一步可能有多个选择||15-20 |合理的计算模型的三个条件|||22| |丘奇-图灵论题||19|23| |不可计算的函数|例子：图灵机不可计算问题||24-26| |图灵归约（理解为函数调用）||22|27| |通用算法||23|28-29| |oracle machine（预言机）|其实也是图灵归约和函数调用|27-28|30-33|

Lecture 3 计算模型

Topic	备注	书上页数	PPT页数
非一致性计算模型	对于不同长度的输入 使用不同图灵机	28	3
# 布尔电路及定义	布尔变量：输入0-1 布尔函数:输出0-1	29-30	4-9
# 布尔电路与布尔函数、扇入与扇出、电路簇	一个布尔电路计算一个布尔函数	30	10-12
# 电路复杂性	研究布尔电路大小及深度的界限	31	13-18
# 布尔电路模拟图灵机	输入t时刻array，输出t+1时刻array		20-25
一致性类	多项式规模的电路簇可被认为是一致的，如果	31	26
接受建议的机器	每个问题需要额外l(n)长度的建议	32	27
受限的计算模型：布尔公式，CNF（合取）DNF（析取）范式，常数深度电路，单调线路	布尔电路模型引出的自然子类	33	27-31

Lecture 4 P与NP问题

Topic	备注	书上页数	PPT页数
P与NP	P代表可被有效求解的问题，NP代表解可被有效验证的问题	35	4
	NP 完全性理论的基础是归约，一个问题归约到另一个问题，如果在给定解后者的高效算法时，前者也可被高效解决，因此NP类（是否等于P）归结到每个单独的NP完全问题。	35	4
搜索版本：求解与检验	搜索问题的定义；多项式界关系（能否在多项式时间内求解）；搜索问题的两类问题：PF与PC：多项式时间内可寻找和多项式时间内可验证	37-38	6-7
作为自然搜索问题的P类	多项式时间内P=PF	38	8-9
作为自然搜索问题的NP类		38	10-11
搜索形式的P-vs-NP问题	若PC=PF则P=NP	39	12
判定版本:证明与验证	对搜索问题的研究可以简化为对判定问题的研究，PC中所有搜索问题都可以看作是寻找证明的问题，寻找属于解的实例集的NP-witness,寻找y，证明V(x,y)=1	39-40	14
判定版本的P问题		39	16
NP类及NP-证明系统及其定义	NP问题时具有可高效验证证明系统的判定问题，验证程序性质：完备性（生存能力）：正确断言有有效证明，y为NP-witness(证据）。合理性（安全性）：错误断言没有有效证明。	40-42	17-20
两种表示的等价性	PC IN PF 当且仅当P=NP	43	21-24
NP问题的传统定义	证明传统定义与上面的定义等价	43-44	25-28

Lecture 5 多项式时间规约

Topic	备注	书上页数	PPT页数
NP完全问题的大致定义	NPC问题代表如果这一类问题如果存在多项式时间算法，那么所有NP问题多项式时间内可解	46	4
规约定义	图灵归约，神谕机，计算等价性。根据预言机，把解决一个问题通过调用函数规约到解决另一个问题。计算等价性：两个问题可以彼此归约	46	8-11
cook归约	搜索判定都可用，每个PC中的搜索问题都可以cook规约到np中一个判定问题，定义和性质	47	12-13
Karp归约	判定到判定问题归约，cook归约的特例	47	14
Levin归约	搜索问题到搜索问题归约	47	15
优化问题到搜索问题的归约		48	16-18
搜索问题自归约性	自归约：如果搜索问题和对应判定问题计算等价。搜索：找到解，判定：解是否存在	50	19-23
- 可满足性问题	布尔电路可满足性问题（CSAT），布尔公式可满足性问题（SAT），合取范式可满足性问题（CNF-SAT），3SAT定义	51	21-22
NPC问题的自归约性	与任意一个NP-完全判定问题相关的求np-witness的搜索问题都是自归约的	52-53	24
研究NP完全问题的思路	1.给出NPC的定义并且证明其存在 2. 按照定义给出一个具体的NPC问题，实际上就是CSAT。3. 利用归约定理证明更多的NPC，如果A是NPC，B是NP，如果调用B可解A，则B是NPC。如果任何一个NPC问题可多项式时间内解决，则P=NP		27

Lecture 6 NP完全问题

Topic	备注	书上页数	PPT页数
NP完全问题的定义	搜索和判定问题的NPC问题。判定：所有NP Karp归约。搜索：所有NP levin归约。	53-54	3
NP完全问题存在性		54	5
一些NP完全问题			
CSAT与SAT的NPC	CSAT是NPC问题以及证明	57-58	7-11
证明一个问题是NPC问题的方法			12
SAT	SAT也是NP完全，证明可以在多项式时间内，将CSAT归约到SAT，则SAT NPC	59-60	13-18
kSAT	合取范式的每个子句刚好包含k个变量		19-20
3SAT的NPC	3SAT是NPC问题，若扩展到每个变量恰好只出现3次，也是NPC问题（证明：添加辅助变量）	61	21-23

Lecture 7 NP完全问题

Topic	备注	书上页数	PPT页数
一些自然的NPC问题			3
集合覆盖问题	集合覆盖是NP完全的	62	4
顶点覆盖问题	顶点覆盖问题是NP完全的	63	6-7
团问题	定义和证明	63	7-13
图着色问题以及01INT问题	图着色问题也是NPC问题	64	14
NP集合中那些既不是NPC也不是P的问题（NPI）			
承诺问题	要求放宽的问题：只需要对特定集合的问题示例求解，这个集合称作承诺	69-72	19-26
最优化搜索问题		74	27
coNP类及其与NP类的交集	co表示是复杂类的补集 https://en.wikipedia.org/wiki/Co-NP	74-77	28-34

Lecture 8 P与NP的变形

Topic	备注	书上页数	PPT页数
非一致多项式时间(P/poly)	多项式规模电路解决，只能处理固定输入长度的的机器的高效计算，P属于P/poly,反之不一定。判定问题属于p/poly当且仅当可以用多项式规模电路求解	86-89	
多项式时间层级（PH）	一种量化布尔公式，交替使用固定数量的存在量词和全称量词	90	
非一致多项式时间	例子：布尔电路和接受建议的机器 研究动机：其在计算上的限制蕴涵了对多项式时间算法的限制	87	3-4
布尔电路	用电路规模作为复杂性量度：能计算n长度输入的最小电路复杂度。一致性类。能用多项式规模电路解决的问题也能在多项式时间内解决	87-88	5-9
接受建议的机器	输入长度n，解决问题需要长度为l(n)的建议	88-90	10-12
P/poly和电路复杂性的关系	P/poly的两类含义。多项式规模电路可解决，以及可以被多项式长度建议序列多项式时间内可解。二者等价	89	13-15
多项式时间层级	https://en.wikipedia.org/wiki/Polynomial_hierarchy	91-92	17-20
PH以及P vs NP问题	PH=P成立当且仅当P=NP	92	22-23

Lecture 9 More resource more power?

Topic	备注	书上页数	PPT页数
非一致性复杂度层级	P/l 多项式时间内用长为l的建议可解的判定问题类	103	4
时间层级	DTIME用于定义复杂度类	104-107	9-16
时间缝隙和加速		109	17-20

Lecture 10-11 空间复杂度

Topic	备注	书上页数	PPT页数
前提	DSPACE(s)一类可在空间复杂度s内解决的判定问题(确定图灵机）；NSPACE(s)可以在空间复杂度s内内被非确定图灵机解决的判定问题；空间复杂度用对数空间复杂度-L		2
	对数空间类：L,NL;NSPACE(s) \in DSPACE(s2); NL = co-NL;		3
	空间复杂度定义	116	4
时间复杂度类	DSPACE NSPACE	117	6-7
时间与空间	和时间不同，空间可被重用。考虑组合引理:简单组合和仿生组合	117-118	8-9
DTIME与SPACE关系	在SPACE(t(n))空间内解决的一定能在对应时间内解决，反之则不成立*由空间复杂度定义了时间复杂度的上界。因此，能在L或者NL空间内解决的问题一定是多项式时间内可解决的。	119	10
在线与离线模型	不确定性模型需要付出额外空间代价	130	12
对数空间	L类：可以用对数空间复杂度求解的判定问题类；L=DSPACE(logn) NL=NSPACE(logn)，且NL=coNL	123	14-15
图的联通性	CONN 两个顶点之间是否有通路，UCONN:无向图联通性（属于L）；st-CONN:有向联通性，且是NLC问题；CONN是NLC	125-126，131	17-20,25
对数空间归约及NL完全性			21-22
Savitch's 定理及其证明	NSPACE(s)\in DSPACE(O(s^2))	132	23-37
NL属于P证明	对数空间归约等价于多项式时间归约，根据P10 时空转换定理		29
PSPACE与NPSPACE		139	49
Immerman定理	证明coNL = NL		50-57
TQBF	SAT的量词版本		58-62
PSPACE完全性	1.归约 2.定义 3.TQBF是PSPACE完全的		

Lec 12 随机性与计数

Topic	备注	书上页数	PPT页数
通信复杂度	通信至少需要n+1 bit。提高效率：使用随机策略提高到O(logn) bit	148	3-9
离散对数问题以及例子			10-14
概率图灵机		149-150	15
错误类型	双边错误：可能在两个方向都出错(对->错，错->对），单边错误：只会在单方向出错。零边错误：不给出错误解，但会输出无解	150-151	17
随机化归约		151	18
概率多项式时间	PP是可以在多项式时间内用概率图灵机解决的判定问题全体，并且错误概率小于1/2	149	19
BPP定义以及错误归约	错误概率小于1/3	152-153	20-23
Adleman's 定理	BPP是P/poly的真子集	153	24
BPP以及布尔电路			25-27
单边错误 RP & coRP	RP:判定对正确概率大于1/2，错的不会误判。 co-RP相反，对的不会错判，错误正确判定概率大于1/2	157	29-30
BPP与coRP,RP关系	BPP可以被归约到coRP	156-157	31
零边错误 ZPP	RP与coRP的交集（证明：书本160）	159-160	32
不同类之间的关系	P,RP,CORP,CONP,NP,BPP,PSPACE		36-38
polynomial identity testing			39-44
randomized log-space	RL & BPL		46
计数问题			47-49

Lecture 13-14 交互式证明系统

Topic	备注	书上页数	PPT页数
单向函数	很容易evaluate（x->f(x)）但是很难invert(f(x)->x)		2-3
交互式证明系统 IP	合理性 完备性 效率，与NP系统的关系	289-291	8-23
图同构问题的交互式证明系统	假设图不同构，验证者每次发一个与1或者2同构的图给证明者，证明者要告诉它发来的图和哪个同构，每次都对，则证明	292-293	24-27
IP与NP关系	coNP属于IP，NP属于IP，IP=PSPACE	295-296	28-30
零知识证明	完全零知识，零知识定义以及证明	300-302	32-37
零知识证明的功能	图同构问题的零知识证明，证明思路很有用	303-304	36-37
图三色的零知识证明	图三色问题有零知识证明系统，图三色是NPC问题，所有NP都有零知识证明系统	305-306	38-49
零知识证明协议分析			45-47

Lecture 15 PCP

Topic	备注	书上页数	PPT页数
PCP(概率可检验证明系统）的定义	只选取一部分位置进行验证，来评估断言正确性	310	4-5，12
PCP定理以及和NP的关系	NP=PCP(log,O(1)) 可以根据常数个测试比特对证明进行有意义的评估	311-312	13-17