



计算机科学导论

孙晓明

中国科学院计算技术研究所

2022-3-18

孙晓明

中国科学院计算技术研究所

邮编: 100190

电子邮件: sunxiaoming@ict.ac.cn

<http://theory.ict.ac.cn/en/>



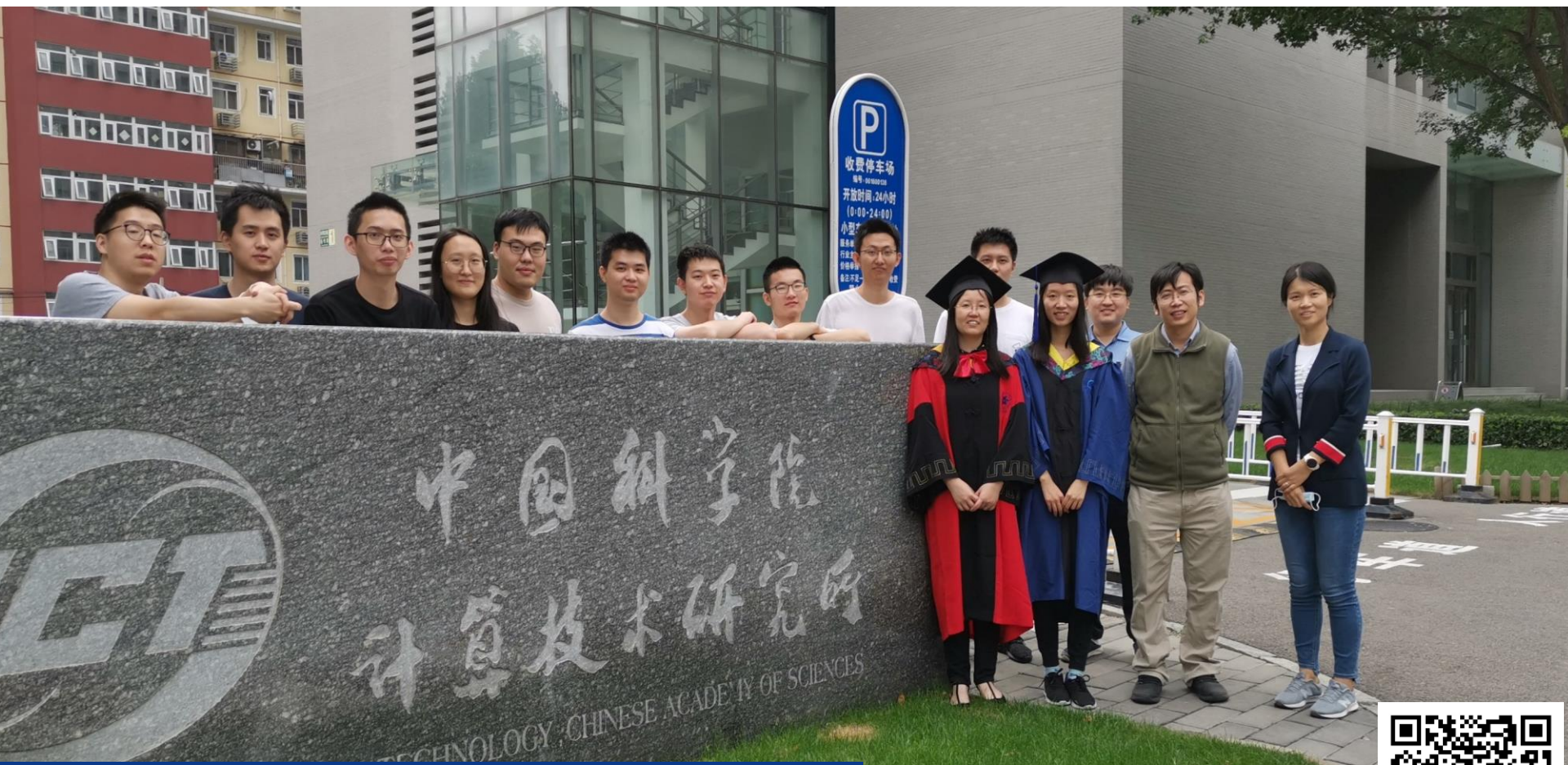
教育

- 1997. 9-2001. 7 清华大学计算机系, 学士
- 2001. 9-2005. 7 清华大学计算机系, 博士

工作经历

- 2005. 8-2008. 12 清华大学高等研究院, 助理研究员
- 2008. 12-2011. 9 清华大学高等研究院, 副研究员
- 2011. 9至今 中国科学院计算技术研究所, 研究员

主要研究领域为算法与计算复杂性、量子计算、组合数学等。曾获基金委首批优青资助, 入选中组部首批万人计划青年拔尖人才, 中国密码学会优秀青年奖、密码创新二等奖、王选杰出青年学者奖。目前担任中国计算机学会理论专委会主任, 全国量子计算与测量标准化技术委员会委员, 还担任《软件学报》《计算机研究与发展》《中国科学:信息科学》《Information and Computation》《JCST》《FCS》等杂志编委或青年编委。



中科院计算所量子计算与算法理论实验室
Laboratory for Quantum Computation and Theoretical Computer Science, ICT, CAS

<http://theory.ict.ac.cn/en/>





思考题

- 一位探险者在奥斯仙境旅行，他想要去翡翠城，但路上必须经过说谎国。说谎国的人永远说谎话，而诚实国的人永远讲真话。他走到了一个岔路口，两条路分别通向诚实国和说谎国。他不知道哪一条路是去说谎国的路。正在他犹豫不决的时候，路上来了两个人，已知其中一个是诚实国的，另一个是说谎国的。探险者需要问这两个人哪一条是去往说谎国的路，请问他应该怎么问？
- 要求：他只能问一次，而且答案只能是“是”或者“否”。



解答

- 两个人分别记做A和B，两条路分别记做S和T。
- 用0, 1表示来自诚实国和说谎国，因此 $A=1$, $B=0$ ；或者 $A=0$, $B=1$
- 用 $S=1$ 表示走路S可以到说谎国， $S=0$ 表示走路S不能够到说谎国（i.e. 走路T可以到说谎国）。
- 注意到：无论问A还是问B“你来自诚实国吗？”回答你对于“你来自诚实国”和“路S通往说谎国”这两个问题的回答是一样的吗？
- 问A：如果 $A=0$ ，则走路S，否则走路T。



逻辑思维

- 逻辑——①思维的规律、规则：这个想法似乎不合逻辑。 ②研究思维规律的科学，即逻辑学。 ③客观事物的规律：历史的逻辑。 ④观点，主张。多用于贬义：霸权主义的逻辑。（新华字典）
- 广义：泛指规律、道理
- 狭义：逻辑学
 - 哲学（古希腊）、数学（19世纪）
 - 计算机科学、语言学、心理学……



问题

- A, B, C, D, E五人参加百米比赛，请根据下面的叙述写出第1-5名：A不是第一名；B既不是第一名，也不是最后一名；C的名次仅次于A；D不是第二名；E比D低两个名次；没有两人并列。





布尔逻辑

- 真 T (true), 假 F (false)
 - 今天下雪。
 - $a^2 \geq 0$ 。
 - 国王和大臣的生死签
- 合取, 与 $\wedge$ (conjunction, and)
 - $x \wedge y = 1$ (T) *iff* $x = y = 1$ (T)
- 析取, 或 $\vee$ (disjunction, or)
 - $x \vee y = 0$ (F) *iff* $x = y = 0$ (F)

- 非 $\neg$ (negation, not)

- $\neg x = 1 \text{ (T) iff } x = 0 \text{ (F)}$

- 蕴含 $\rightarrow$ (material implication)

- $(x \rightarrow y) = 1 \text{ (T) iff } x = 0 \text{ (F) or } y = 1 \text{ (T)}$

- 山无陵，江水为竭，冬雷震震，夏雨雪，天地合，乃敢与君绝。

- 异或 $\oplus$ (exclusive or)

- $x \oplus y = 1 \text{ (T) iff } x \neq y$

- $x + y \bmod 2$



真值表

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0



■ 性质:

- $x \vee 0 = x, x \vee 1 = 1, x \wedge 0 = 0, x \wedge 1 = x$
- $x \vee \neg x = 1, x \wedge \neg x = 0$
- $x \wedge y = y \wedge x, x \vee y = y \vee x, x \oplus y = y \oplus x$
(交换律)
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$
(结合律)
- $(x \vee y) \vee z = x \vee (y \vee z)$
- $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$
(分配律)
- $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$
- more ??



■ 性质:

- $\neg(x \vee y) = \neg x \wedge \neg y$

- $\neg(x \wedge y) = \neg x \vee \neg y$

- $x \rightarrow y = \neg x \vee y$

- $x \oplus y = (\neg x \wedge y) \vee (x \wedge \neg y)$

- $x \oplus y = (x \vee y) \wedge (\neg x \vee \neg y)$

$$x \vee y = \neg(\neg x \wedge \neg y)$$

(**De Morgan律**)

- $(x \rightarrow y) \rightarrow z = ?$

- $(x \wedge \neg y) \vee z$

- 合取范式(conjunctive normal form, CNF)

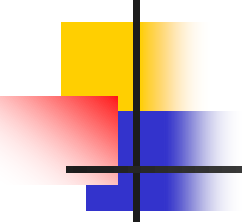
- $f(x_1, \dots, x_n) = Q_1 \wedge Q_2 \wedge Q_3 \dots \wedge Q_m$

- 其中: $Q_i = l_1 \vee l_2 \vee \dots \vee l_n$, $l_j = x_j$ 或 $\neg x_j$

- 析取范式(disjunctive normal form, DNF)

- $f(x_1, \dots, x_n) = Q_1 \vee Q_2 \vee Q_3 \dots \vee Q_m$

- 其中: $Q_i = l_1 \wedge l_2 \wedge \dots \wedge l_n$, $l_j = x_j$ 或 $\neg x_j$

- 
- 例: $x \rightarrow (y \rightarrow z) = ?$

- $(\neg x \vee \neg y \vee z)$

- $(\neg x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee (\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge z)$

x	y	z	f
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1



思考题

- 根据De Morgan律和合取范式（或析取范式），使用 $\neg$ 和 $\wedge$ （或 $\vee$ ）可以表示出所有的函数（？）。
- 问题：能否只用 $\wedge, \vee$ 表示出所有的函数？
 - 不能！
 - 单调性: $f(x) \leq f(x')$ if $x \leq x'$



思考题

- n 个变量的布尔函数有多少个？
 - $n=0$, 2个 (0和1)
 - $n=1$, 4个 (1, 0, x 和 $\neg x$)
 - $n=2$, ?
 - 2^{2^n}

思考题

■ n 个变量的单调布尔函数有多少个？

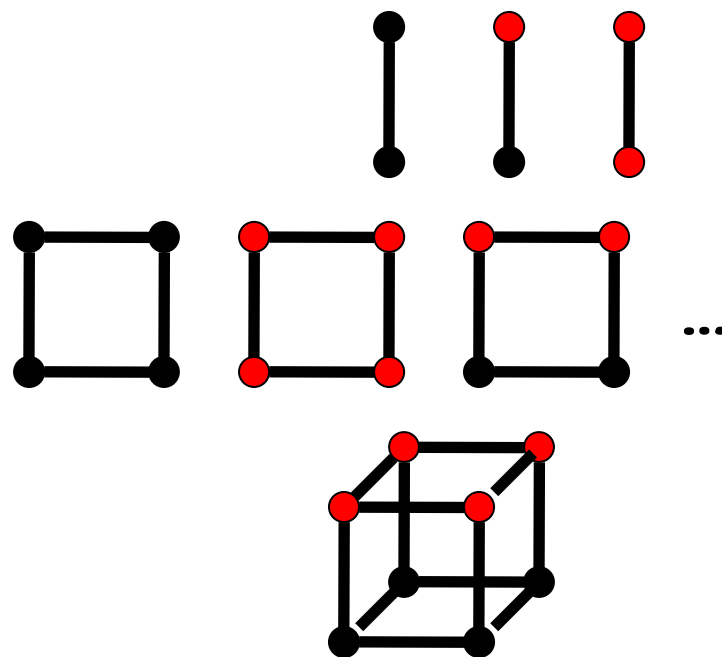
■ $n=0$, 2个

■ $n=1$, 3个

■ $n=2$, 6个

■ $n=3$, 20个

■ $n=4$, ?





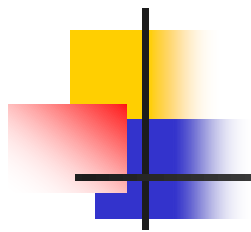
思考题

- 问题：能否只用 $\oplus$ ？（允许使用0，1）
 - 不能！
 - 只能写出 $x_{i1} \oplus \dots \oplus x_{ik} \oplus c$
- 如果只用 $\rightarrow$ 呢？
 - 可以！
 - $x \rightarrow 0 = \neg x$
 - $(x \rightarrow 0) \rightarrow y = x \vee y$

思考题

- 问题： n 名同学围成一圈，每个人随机的分配一顶红色或者蓝色的帽子，要求所有人同时猜出自己帽子的颜色。请设计一种策略，使得同时猜对的概率最高。





谢谢！