简单数理逻辑及其应用

清华大学 计算机科学与技术系
李恺威
chnlkw@gmail.com

概述

- 数理逻辑
  - 命题
  - 联结词
  - 合式公式
  - 等值公式、定理
  - 范式
- SAT 问题
  - 2-SAT
  - DPLL 算法
- SMT 问题
  - 分类
  - 应用

命题

- 定义

  一个非真即假的陈述句

- 例子

  李恺威是学霸

  郭家宝太牛啦！

  我在说的是假话

命题变项

- 命题符号化
- P表示“李恺威是学霸”
- 命题变项P：表示任意命题

简单命题和复合命题

- P: 雪是白的且“ 1+1=2”
- 可分割为
  - R: 雪是白的
  - S:1+1=2

命题联结词

- 非 ¬
- 与 ∧　合取
- 或 ∨　析取

p	$\neg p$
0	1
1	0

p	q	$p \wedge q$	$p \vee q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

- **推断**
  - **因果关系**

- **等价**

P	Q	$P \rightarrow Q$	$P \leftrightarrow Q$
F	F	T	T
F	T	T	F
T	F	F	F
T	T	T	T

合式公式
Well-formed formula

- 命题变项和连接词的组合
- 定义

1. 简单命题是合式公式
2. 如果 A 是合式公式，那么 ¬A 也是合式公式
3. 如果 A, B 是合式公式，那么 (A ∧ B), (A ∨ B), (A → B) 和 (A ↔ B) 是合式公式
4. 当且仅当经过有限次地使用 1,2,3 所组成的符号串才是合式公式

合式公式

- 合式公式简称公式
- 例子

  $p \wedge (p \rightarrow q) \rightarrow q$

- If A then B else C 能用合式公式表示吗？

合式公式分类

- 永真式：在任何解释 I 下都为真 (T)
- 可满足式：在某个解释 I_0 下为真 (T)
- 矛盾式：在任何解释 I 下都为假 (F)
- 例
  1. $P \vee \neg P$ $\quad$ I_0=(T) I_1=(F)
  2. $P \wedge \neg Q$ $\quad$ I_0=(T, F)
  3. $P \vee \neg P$ $\quad$ 矛盾

三种公式关系

- A 永真，当且仅当 ¬A 永假
- A 可满足，当且仅当 ¬A 非永真
- A 不可满足，当且仅当 A 永假

等值公式

- 两个公式 A 和 B，
- $P_1,\ldots,P_n$ 是所有 A 和 B 中的命题变项
- A 和 B 有 2^n 个不同的解释
- 在任何解释下， A 和 B 的真值都相等
- 称 A 和 B 等值，记 A=B

等值定理

- 对公式 A 和 B， A=B 的充分必要条件是 A↔B 是永真式
- 不要将“ =” 视作连结词
- A=B 表示公式 A 与 B 的一种关系

1. 自反性： A=A
2. 对称性：若 A=B，则 B=A
3. 传递性：若 A=B， B=C，则 A=C

等值公式

1. **双重否定律**

$$\neg\neg P = P$$

2. **结合律**

$$(P \vee Q) \vee R = P \vee (Q \vee R)$$

$$(P \wedge Q) \wedge R = P \wedge (Q \wedge R)$$

$$(P \leftrightarrow Q) \leftrightarrow R = P \leftrightarrow (Q \leftrightarrow R)$$

3. **交换律**

$$P \vee Q = Q \vee P$$

$$P \wedge Q = Q \wedge P$$

$$P \leftrightarrow Q = Q \leftrightarrow P$$

4. 分配律

$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$

$$P \rightarrow (Q \rightarrow R) = (P \rightarrow Q) \rightarrow (P \rightarrow R)$$

5. 等幂律

$$P \vee P = P$$

$$P \wedge P = P$$

$$P \rightarrow P = T$$

$$P \leftrightarrow P = T$$

6. 吸收律

$$P \vee (P \wedge Q) = P$$

$$P \wedge (P \vee Q) = P$$

7. 摩根（ De Morgan ）律:

$$\neg (P \vee Q) = \neg P \wedge \neg Q$$

$$\neg (P \wedge Q) = \neg P \vee \neg Q$$

命题公式与真值表

- 给出公式，列写真值表很容易
- 反过来呢？

P	Q	A	B
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	F

- 尝试写出 A， B 由 P， Q 表达的公式

从 T 列写

- $A=(\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge Q)$
- $B=(\neg P \wedge \neg Q) \vee (\neg P \wedge Q)$

P	Q	A	B
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	F

从 F 列写

- $A=(\neg P \vee Q)$
- $B=(\neg P \vee Q) \wedge (\neg P \vee \neg Q)$

P	Q	A	B
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	F

范式

- 列写方法多样，是否有标准形式？
- 定义：
  - 文字：简单命题 P 及其否定式 ¬P
  - 合取式：一些文字的合取
  - 析取式：一些文字的析取
  - 析取范式：形如 $A_1 \vee A_2 \vee \ldots\ldots \vee A_n$(其中 A_i 为合取式)
  - 合取范式：形如 $A_1 \wedge A_2 \wedge \ldots\ldots \wedge A_n$(其中 A_i 为析取式)

范式

- 范式定理：任意命题公式都存在有与其等值的合取范式和析取范式
- 求范式
- A □ B = $\neg A \vee B$
- $A \leftrightarrow B \quad = (\neg A \vee B) \wedge (A \vee \neg B)$

  $= (A \wedge B) \vee (\neg A \wedge \neg B)$

小结

- 命题
- 联结词
- 合式公式
- 等值公式、定理
- 范式

SAT 问题
Boolean satisfiability problem

- 给出一个合式公式，判断其是否可满足
- 将合式公式化成合取范式
- $A_1 \wedge A_2 \wedge \ldots\ldots \wedge A_n$
- $A_i=(P_{i1} \vee P_{i2} \vee \ldots P_{im})$
- 求解办法？

2-SAT

- 特殊情况
- 合取式的每一项 A_i 最多只有 2 个变量析取 (m<=2)
- $(X_0 \vee X_2) \wedge (\neg X_0 \vee X_3) \wedge (X_1 \vee \neg X_3)$

  T T T

  T T T

构图法

- N 个变项， 2N 个节点（ A_i 与 ¬ A_i 为对偶点）
- A ∨ B = ¬A □ B
- 对每一项 (A ∨ B)
- 从 ¬A 向 B 连一条边
- 从 ¬B 向 A 连一条边
- 如果取了 ¬A 则必须取 B
- 若存在 A 到 ¬A 存在路径，则无解

寻找可行解

- 有向图
- 强连通分量缩环
- 给个对偶分支取一条

3-SAT

- 析取式中某些项包含的变量为 3 个
- 上述算法不成立
- 第一个所知的 NP 完全问题
- 1971 年由史提芬 ·A· 古克 (Stephen A. Cook) 提出的古克定理证明
- 一般 SAT 问题，搜索！

DPLL 算法

- Davis-Putnam-Logemann-Loveland
- 它在 1962 年由 Martin Davis, Hilary Putnam, George Logemann 和 Donald W. Loveland 提出 , 作为早期 Davis-Putnam 算法的一种改进。 Davis-Putnam 算法是 Davis 与 Putnam 在 1960 年发展的一种算法
- 50 年来最有效的算法

- Φ： 一系列析取式的集合（表示它们合取）
- Function DPLL(Φ)

  if Φ 为空集 then

  return true

  if Φ 只含一个析取式 then

  return true

  for Φ 中的每个析取式 l do

  如果析取式 l 只含有一个变量，直接确定其值使析取结果为 True

  for Φ 中每个未定变量 x do

  如果 x 出现的形式相同，确定其值使结果为 True

  选择 Φ 中一个未定变量 y

  return DPLL(Φ ∧ y) or DPLL(Φ ∧ not y) // 搜索

SAT 问题扩展？

- 一系列约束条件取并
- 判断是否可满足
- SAT：约束条件为布尔变量的析取
- 布尔 □ 整数、实数？
- 析取 □ 数学运算？

SMT

- 可满足模块理论
- Satisfiability Modulo Theories
- 在不同论域上的约束判定问题
- 论域举例
  - Boolean (SAT 问题)
  - Integers
  - Real numbers
  - Arrays
  - Bit vectors

解线性比特向量算法

(3 位宽)

$3x + 4y + 2z = 0$

$2x + 2y + 2 = 0$

$4y + 2x + 2z = 0$

X 在第一个方程中的解

$3^{-1} \bmod 8 = 3,$

$x = 4y + 2z$

带入 x

(3 位宽)

$2y + 4z + 2 = 0$

$4y + 6z = 0$

解线性比特向量算法

(3 位宽)

$2y + 4z + 2 = 0$

$4y + 6z \quad = 0$

所有系数为偶数

除以 2

忽略最高位高位比特

(2 位宽)

$y[1:0] + 2z[1:0] + 1 = 0$

$2y[1:0] + 3z[1:0] = 0$

解线性比特向量算法

(2 位宽)
y[1:0] + 2z[1:0] + 1 = 0
2y[1:0] + 3z[1:0] = 0

求解 y[1:0]

(2 位宽)
y[1:0]=2z + 3

带入 y[1:0]

(2 位宽)
3z[1:0] + 2 = 0

解线性比特向量算法

(2 位宽)
3z[1:0] + 2 = 0

求解 z[1:0]

(2 位宽)
z[1:0]=2

结果 (3 位宽):
z[1:0] = 2
y[1:0] = 2z[1:0] + 3 = 3
y = y’ @ 2
z = z’ @ 3
x = 4y + 2z

研究两大方向

- 数学计算
  - 整数域、实数域
  - 线性、非线性
- 计算机运算
  - 比特向量
  - 数组

应用场景 (1)

- 方程求解

$$(\sin(x)^3 = \cos(\log(y) \cdot x) \vee b \vee -x^2 \geq 2.3y)$$
$$\wedge \left(\neg b \vee y < -34.4 \vee \exp(x) > \frac{y}{x}\right)$$

$b \in \mathbb{B}, x, y \in \mathbb{R}$

应用场景 (2)

- 程序 bug 扫描
- int two-hop(int x)
- {
- int a[4] = {3, 0, 2, 1};
- if(x < 0 or x > 3) return -1;
- return a[a[x]-1]; //out of range while x = 1 !
- }

Reference

- 《数理逻辑与集合论》清华大学出版社 石纯一 2000
- 《 2-SAT 解法浅析》 赵爽
- http://en.wikipedia.org/wiki/Boolean_satisfiability_problem
- http://en.wikipedia.org/wiki/DPLL_algorithm
- http://en.wikipedia.org/wiki/Satisfiability_Modulo_Theories
- Cristian Cadar, Vijay Ganesh, Peter Pawlowski, David Dill, and Dawson Engler.EXE: Automatically generating inputs of death. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, October-November 2006.
- DECISION PROCEDURES FOR BIT-VECTORS, ARRAYS AND INTEGERS. Vijay Ganesh.September 2007

谢谢大家！