合取/析取范式

2015年11月9日星期一

回忆...

- “如果今天星期二，而且陶老师出差，则由马老师上课”
  - P：今天星期二
  - Q：陶老师出差
  - R：马老师上课

$$P \wedge Q \longrightarrow R$$
$$\neg(P \wedge Q) \vee R$$
$$(\neg P \vee \neg Q) \vee R$$
$$\neg P \vee \neg Q \vee R$$
$$\ldots\ldots$$

合取范式
(Conjunctive normal form, CNF)

- In Boolean logic, a formula is in conjunctive normal form (CNF) or clausal normal form if
  - it is a conjunction of disjunction clauses, where a clause is a disjunction of ***literals***;
  - it is an AND of ORs

- $\neg A \wedge (B \vee C)$
- $(A \vee B) \wedge (\neg B \vee C \vee \neg D) \wedge (D \vee \neg E)$
- $A \vee B$
- $A \wedge B$

- $\neg(B \vee C)$
- $(A \wedge B) \vee C$
- $A \wedge (B \vee (D \wedge E))$.

- $\neg B \wedge \neg C$
- $(A \vee C) \wedge (B \vee C)$
- $A \wedge (B \vee D) \wedge (B \vee E)$

https://en.wikipedia.org/wiki/Conjunctive_normal_form

析取范式
(Disjunctive normal form,DNF)

- In Boolean logic, a disjunctive normal form (DNF) is a standardization (or normalization) of a logical formula
  - which is a disjunction of conjunctive clauses, where a clause is a conjunction of ***literals***;
  - it can also be described as an OR of ANDs

$(A \wedge \neg B \wedge \neg C) \vee (\neg D \wedge E \wedge F)$

$(A \wedge B) \vee C$

but and also

$A \wedge B$

A

However, the following formulas are **NOT** in DNF:

$\neg(A \vee B)$ — NOT is the outermost operator

$A \vee (B \wedge (C \vee D))$ — an OR is nested within an AND

https://en.wikipedia.org/wiki/Disjunctive_normal_form

Existence of CNF/DNF

- Every propositional formula can be converted into an equivalent formula that is in CNF or DNF
- Since all logical formulae can be converted into an equivalent formula in conjunctive normal form, proofs are often based on the assumption that all formulae are CNF

How to obtain CNF/DNF?

- This transformation is based on rules about logical equivalences:
  - double negative law
  - De Morgan's laws
  - distributive law
  - …

(DeMorgan's laws)	$\neg(P \vee Q) \leftrightarrow (\neg P \wedge \neg Q);$ $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q);$
(Distributive property)	$(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R));$ $(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R));$
(Double negation)	$\neg(\neg P) \leftrightarrow P;$
(Associative property)	$(P \wedge (Q \wedge R)) \leftrightarrow ((P \wedge Q) \wedge R);$ $(P \vee (Q \vee R)) \leftrightarrow ((P \vee Q) \vee R);$
(Commutative property)	$(P \wedge Q) \leftrightarrow (Q \wedge P);$ $(P \vee Q) \leftrightarrow (Q \vee P).$

How to obtain CNF/DNF? (con't)

- Handle "$\rightarrow$"/ "$\leftrightarrow$"
  - $A \rightarrow B \Leftrightarrow \neg A \vee B$
  - $A \leftrightarrow B \Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A)$
- Handle "$\neg$"
  - $\neg\neg A \Leftrightarrow A$
  - $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
  - $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
- Apply distributive law:
  - $(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R))$; **Obtain DNF**
  - $(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$; **Obtain CNF**

How to obtain CNF/DNF? (con't)

- Example： obtain the CNF/DNF of $\neg(A \rightarrow B) \vee \neg C$
  - $\neg(A \rightarrow B) \vee \neg C$
  - $\Leftrightarrow \neg(\neg A \vee B) \vee \neg C$
  - $\Leftrightarrow (A \wedge \neg B) \vee \neg C$ **DNF**
  - $\Leftrightarrow (A \vee \neg C) \wedge (\neg B \wedge \neg C)$ **CNF**

How to obtain CNF/DNF? (con't)

- However, in some cases this conversion to CNF can lead to an exponential explosion of the formula.
- For example, translating the following non-CNF formula into CNF produces a formula with 2^n clauses:

$$(X_1 \wedge Y_1) \vee (X_2 \wedge Y_2) \vee \ldots \vee (X_n \wedge Y_n).$$

- In particular, the generated formula is:

$$(X_1 \vee X_2 \vee \cdots \vee X_n) \wedge (Y_1 \vee X_2 \vee \cdots \vee X_n) \wedge (X_1 \vee Y_2 \vee \cdots \vee X_n) \wedge (Y_1 \vee Y_2 \vee \cdots \vee X_n) \wedge \cdots \wedge (Y_1 \vee Y_2 \vee \cdots \vee Y_n).$$

- This formula contains 2^n clauses; each clause contains either X_i or Y_i for each *i*.

https://en.wikipedia.org/wiki/Disjunctive_normal_form

Question?

- How many CNF/DNF can be obtained for a given formula?

简单合取式（析取式）

Literal(字)

- 仅有有限个**命题变项或其否定**构成的合取式(析取式)称为**简单合取式(析取式)**

例如：给定命题变项p, q, 则

p，q，¬ p，¬ q，p∧q，p∧¬ q，¬ p∧q，

¬ p∧¬ q

都是简单合取式

一个简单合取式是矛盾式，当且仅当它同时含一个命题变项及其否定。

$p \wedge \neg p \wedge q$

极小项与极大项

命题变元

- 在含有n个命题变项$(A_1, A_2, \ldots, A_n)$的**简单合取式（析取式）**中，假设所有命题变项可以全排序
  - E.g., 字典序或指定其它顺序
- 若以下两个条件都满足；
  - 每个命题变项**出现且仅出现一次(A_i或$\neg A_i$)**, 且
  - 每个变项出现顺序遵循全排序顺序
- 则称这样的简单合取式(析取式)为***极小项(极大项)***

n个命题变项共有多少个极大(小)项? 2^n个

2^n个极小项（极大项）均互不等值

极小项与极大项

- 可以对2^n个极小项或极大项进行编号
  - 用m_i表示第i个极小项
    - 其中i是该极小项为true赋值的十进制表示
  - 用M_i表示第i个极大项
    - 其中i是该极大项为false赋值的十进制表示

p,q形成的极小项与极大项

极小项			极大项		
公式	成真赋值	名称	公式	成假赋值	名称
$\neg p \wedge \neg q$	0 0	m_0	$p \vee q$	0 0	M_0
$\neg p \wedge q$	0 1	m_1	$p \vee \neg q$	0 1	M_1
$p \wedge \neg q$	1 0	m_2	$\neg p \vee q$	1 0	M_2
$p \wedge q$	1 1	m_3	$\neg p \vee \neg q$	1 1	M_3

主合取范式 与主析取范式

(Principal Conjunctive Normal Form VS Principal Disjunctive Normal Form)

- 主合取范式：
  - 由极大项构成的合取范式

例子：n=3, 三个命题变项A,B,C

$(\neg A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C)$ 为主析取范式

$(A \vee B \vee \neg C) \wedge (\neg A \vee B \vee C)$ 为主合取范式

- 主析取范式：
  - 由极小项构成的析取范式

任何命题公式都存在与之等值的主合取范式和主析取范式，并且唯一

求主析取范式

设公式A含命题变项$p_1,p_2,\ldots,p_n$

(1) 求A的析取范式$A'=B_1\vee B_2\vee\ldots\vee B_s$, 其中$B_j$是简单合取式$j=1,2,\ldots,s$

(2) 若某个B_j既不含p_i, 又不含$\neg p_i$, 则将B_j展开成

$$B_j\Leftrightarrow B_j\wedge(p_i\vee\neg p_i)\Leftrightarrow(B_j\wedge p_i)\vee(B_j\wedge\neg p_i)$$

重复这个过程, 直到所有简单合取式都是长度为n的极小项为止

(3) 消去重复出现的极小项, 即用m_i代替$m_i\vee m_i$

(4) 将极小项按下标从小到大排列

求主合取范式

设公式A含命题变项$p_1,p_2,\ldots,p_n$

(1) 求A的合取范式$A'=B_1\wedge B_2\wedge\ldots\wedge B_s$, 其中$B_j$是简单析取式$j=1,2,\ldots,s$

(2) 若某个B_j既不含p_i, 又不含$\neg p_i$, 则将B_j展开成

$$B_j \Leftrightarrow B_j\vee(p_i\wedge\neg p_i) \Leftrightarrow (B_j\vee p_i)\wedge(B_j\vee\neg p_i)$$

重复这个过程, 直到所有简单析取式都是长度为n的极大项为止

(3) 消去重复出现的极大项, 即用M_i代替$M_i\wedge M_i$

(4) 将极大项按下标从小到大排列

实例

- Example2：obtain the PDNF/PCNF of$\neg(p \rightarrow q) \vee \neg r$

解（1）$\neg(p \rightarrow q) \vee \neg r \Leftrightarrow (p \wedge \neg q) \vee \neg r$

$p \wedge \neg q \Leftrightarrow (p \wedge \neg q) \wedge 1$

$\Leftrightarrow (p \wedge \neg q) \wedge (\neg r \vee r)$

$\Leftrightarrow (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r)$

$\Leftrightarrow m_4 \vee m_5$

$\neg r \Leftrightarrow (\neg p \vee p) \wedge (\neg q \vee q) \wedge \neg r$

$\Leftrightarrow (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r)$

$\Leftrightarrow m_0 \vee m_2 \vee m_4 \vee m_6$

得 $\neg(p \rightarrow q) \vee \neg r \Leftrightarrow m_0 \vee m_2 \vee m_4 \vee m_5 \vee m_6$

可记作 $\Leftrightarrow \Sigma(0,2,4,5,6)$

实例

- Example2： obtain the PDNF/PCNF of$\neg(\boldsymbol{p} \rightarrow \boldsymbol{q}) \vee \neg \boldsymbol{r}$

$$(2)\ \neg(p\rightarrow q)\vee\neg r \Leftrightarrow (p\vee\neg r)\wedge(\neg q\vee\neg r)$$

$$p\vee\neg r \Leftrightarrow p\vee 0\vee\neg r$$

$$\Leftrightarrow p\vee(q\wedge\neg q)\vee\neg r$$

$$\Leftrightarrow (p\vee q\vee\neg r)\wedge(p\vee\neg q\vee\neg r)$$

$$\Leftrightarrow M_1\wedge M_3$$

$$\neg q\vee\neg r \Leftrightarrow (p\wedge\neg p)\vee\neg q\vee\neg r$$

$$\Leftrightarrow (p\vee\neg q\vee\neg r)\wedge(\neg p\vee\neg q\vee\neg r)$$

$$\Leftrightarrow M_3\wedge M_7$$

得 $\neg(p\rightarrow q)\vee\neg r \Leftrightarrow M_1\wedge M_3\wedge M_7$

可记作 $\Leftrightarrow \Pi(1,3,7)$

快速算法

设公式含有n个命题变项，则

长度为k的简单合取式可展开成2^{n-k}个极小项的析取

例如 公式含p,q,r

$$q \Leftrightarrow (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$$
$$\Leftrightarrow m_2 \vee m_3 \vee m_6 \vee m_7$$

长度为k的简单析取式可展开成2^{n-k}个极大项的合取

例如 $p \vee \neg r \Leftrightarrow (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r)$
$$\Leftrightarrow M_1 \wedge M_3$$

实例

例2 (1) 求 $A \Leftrightarrow (\neg p \wedge q) \vee (\neg p \wedge \neg q \wedge r) \vee r$ 的主析取范式

解 用快速求法

(1) $\neg p \wedge q \Leftrightarrow (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \Leftrightarrow m_2 \vee m_3$

$\neg p \wedge \neg q \wedge r \Leftrightarrow m_1$

$r \Leftrightarrow (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r)$

$\Leftrightarrow m_1 \vee m_3 \vee m_5 \vee m_7$

得 $A \Leftrightarrow m_1 \vee m_2 \vee m_3 \vee m_5 \vee m_7 \Leftrightarrow \Sigma(1,2,3,5,7)$

实例(续)

(2) 求 $B \Leftrightarrow \neg p \wedge (p \vee q \vee \neg r)$ 的主合取范式

解 $\neg p \Leftrightarrow$

$$(\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$$

$$\Leftrightarrow M_4 \wedge M_5 \wedge M_6 \wedge M_7$$

$$p \vee q \vee \neg r \Leftrightarrow M_1$$

得 $B \Leftrightarrow M_1 \wedge M_4 \wedge M_5 \wedge M_6 \wedge M_7 \Leftrightarrow \Pi(1,4,5,6,7)$

主析取范式的用途

- 求公式的成真赋值和成假赋值

设公式A含n个命题变项，A的主析取范式有s个极小项，则A有s个成真赋值，它们是极小项下标的二进制表示，其余2^n-s个赋值都是成假赋值

例如 $\neg(p\rightarrow q)\vee\neg r \Leftrightarrow m_0\vee m_2\vee m_4\vee m_5\vee m_6$

成真赋值：000,010,100,101,110
成假赋值：001,011,111

主析取范式的用途(续)

- 判断公式类型

设A含n个命题变项，则

A为重言式当且仅当A的主析取范式含2^n个极小项

$$(\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee p$$
$$\Leftrightarrow (\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge \neg q) \vee (p \wedge q)$$
$$\Leftrightarrow \mathrm{m}_0 \vee m_1 \vee m_2 \vee m_3$$

A为可满足式当且仅当A的主析取范式中至少含一个极小项

$$(p \vee q) \rightarrow r$$
$$\Leftrightarrow \neg(p \vee q) \vee r$$
$$\Leftrightarrow (\neg p \wedge \neg q) \vee r$$
$$\Leftrightarrow (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee r$$
$$\Leftrightarrow (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r)$$
$$\Leftrightarrow m_0 \vee m_1 \vee m_3 \vee m_5 \vee m_7$$

主析取范式的用途(续)

- 判断两个公式是否相等
  - 两个公式相等当且仅当两者具有相同的PDNF

(1) p 与 $(\neg p \vee q) \rightarrow (p \wedge q)$

解 $p \Leftrightarrow p \wedge (\neg q \vee q) \Leftrightarrow (p \wedge \neg q) \vee (p \wedge q) \Leftrightarrow m_2 \vee m_3$

$(\neg p \vee q) \rightarrow (p \wedge q) \Leftrightarrow \neg(\neg p \vee q) \vee (p \wedge q)$

$\Leftrightarrow (p \wedge \neg q) \vee (p \wedge q) \Leftrightarrow m_2 \vee m_3$

故 $p \Leftrightarrow (\neg p \vee q) \rightarrow (p \wedge q)$

主析取范式的用途(续)

- 判断两个公式是否相等
  - 两个公式相等当且仅当两者具有相同的PDNF

(2) $(p\wedge q)\vee r$ 与 $p\wedge(q\vee r)$

$$(p\wedge q)\vee r \Leftrightarrow (p\wedge q\wedge\neg r)\vee(p\wedge q\wedge r)$$
$$\vee(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(p\wedge q\wedge r)$$
$$\Leftrightarrow m_1\vee m_3\vee m_5\vee m_6\vee m_7$$

$$p\wedge(q\vee r) \Leftrightarrow (p\wedge q)\vee(p\wedge r)$$
$$\Leftrightarrow(p\wedge q\wedge\neg r)\vee(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(p\wedge q\wedge r)$$
$$\Leftrightarrow m_5\vee m_6\vee m_7$$

故 $(p\wedge q)\vee r \not\Leftrightarrow p\wedge(q\vee r)$

Boolean Satisfiability Problem

SAT is one of the first problems that was proven to be NP-complete[1].

- **Boolean Satisfiability Problem**
  - sometimes called **Propositional Satisfiability Problem** and abbreviated as **SATISFIABILITY** or **SAT**
  - Is the problem of determining if there exists an interpretation that satisfies a given Boolean formula.
  - In other words, it asks whether the variables of a given Boolean formula can be consistently replaced by the values **TRUE** or **FALSE** in such a way that the formula evaluates to **TRUE**.
    - If this is the case, the formula is called **satisfiable**.
    - On the other hand, the formula is **unsatisfiable**.

https://en.wikipedia.org/wiki/Boolean_satisfiability_problem

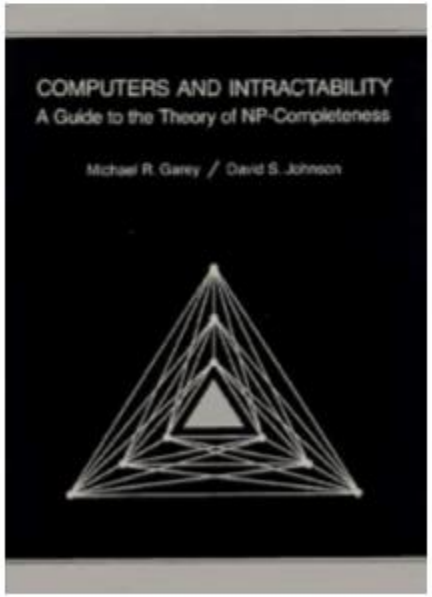
[1]*Cook, Stephen A. (1971). "The Complexity of Theorem-Proving Procedures" (PDF). Proceedings of the 3rd Annual ACM Symposium on Theory of Computing: 151–158. doi:10.1145/800157.805047.*

SAT问题

SATISFIABILITY

INSTANCE: A set U of variables and a collection C of clauses over U.
QUESTION: Is there a satisfying truth assignment for C?

For example, $U = \{u_1, u_2\}$ and $C = \{\{u_1, \bar{u}_2\}, \{\bar{u}_1, u_2\}\}$ provide an instance of SAT for which the answer is "yes." A satisfying truth assignment is given by $t(u_1) = t(u_2) = T$. On the other hand, replacing C by $C' = \{\{u_1, u_2\}, \{u_1, \bar{u}_2\}, \{\bar{u}_1\}\}$ yields an instance for which the answer is "no"; C' is not satisfiable.



2-SAT

- A 2-SAT problem may be described using a Boolean expression with a special restricted form:
  - a conjunction of disjunctions (and of ors), where each disjunction (or operation) has two arguments that may either be variables or the negations of variables

$$(x_0 \vee x_2) \wedge (x_0 \vee \neg x_3) \wedge (x_1 \vee \neg x_3) \wedge (x_1 \vee \neg x_4) \wedge (x_2 \vee \neg x_4) \wedge (x_0 \vee \neg x_5) \wedge (x_1 \vee \neg x_5) \wedge (x_2 \vee \neg x_5) \wedge (x_3 \vee x_6) \wedge (x_4 \vee x_6) \wedge (x_5 \vee x_6).$$

2-SAT can be solved efficiently
and the most efficient of them take linear time

https://en.wikipedia.org/wiki/2-satisfiability

3SAT问题 NPC

3-SATISFIABILITY (3SAT)

INSTANCE: Collection $C = \{c_1, c_2, \ldots, c_m\}$ of clauses on a finite set U of variables such that $|c_i| = 3$ for $1 \leqslant i \leqslant m$.

QUESTION: Is there a truth assignment for U that satisfies all the clauses in C?

- 1. 写一个程序，输入m, n(>=3);输出m个子 句，每个子句中有从 n个变量中随机取得的 三个。
- 例如m = 3,n = 5
  - (x1, ~x2, x3),(x2,x4,~x5),(~x3,x2,x5)

- 2. 扩展上面的程序，加入新的代码让程序 – 输出随机产生的合取范式 – 输出该合取范式是否是可满足的，如果是给出 相应的变量赋值