软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(11):2553−2563 [doi: 10.3724/SP.J.1001.2011.03957]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

鸽巢公式的一些性质*

许道云+, 韦 立, 王晓峰

(贵州大学 计算机科学系,贵州 贵阳 550025)

Some Properties of Pigeon-Hole Formulas

XU Dao-Yun+, WEI Li, WANG Xiao-Feng

(Department of Computer Science, Guizhou University, Guiyang 550025, China)

+ Corresponding author: E-mail: dyxu@gzu.edu.cn

Xu DY, Wei L, Wang XF. Some properties of pigeon-hole formulas. *Journal of Software*, 2011,22(11): 2553−2563. http://www.jos.org.cn/1000-9825/3957.htm

Abstract: The pigeon-hole formula PH_n^{n+1}, defined from the pigeon hole principles, is one of the hardest examples on resolution. The research of the formula's constructions and properties is helpful for constructing other hard examples. It is shown that PH_n^{n+1} is a minimal unsatisfiable formula. The two normal forms of maximal satisfiable truth assignments for PH_n^{n+1} are presented by the minimal unsatisfiability of PH_n^{n+1}, which one of normal forms is used in Haken's proof of hardness for PH_n^{n+1}. The formula PH_n^{n+1} has well isomorphics properties on substructures. For the modified DPLL algorithm introduced by the isomorphism rule, the complexity of refutation proof of PH_n^{n+1} can be reduced to $O(n^3)$.

Key words: pigeon-hole formula; minimal unsatisfiability; maximal satisfiable assignment; normal form; substructure isomorphism

摘 要: 由鸽巢原理定义的鸽巢公式 PH_n^{n+1} 是著名的消解难例之一,研究该公式的结构和性质有助于其他难例的构造.证明了 PH_n^{n+1} 是一个极小不可满足公式,根据其极小不可满足性,给出了最大可满足真值指派的两种标准形式,Haken 关于 PH_n^{n+1} 的难解证明用到了其中一种标准形式.公式 PH_n^{n+1} 具有良好的子结构同构性质,如果 DPLL 算法中允许使用同构规则,则存在 PH_n^{n+1} 的反驳证明,其复杂性可以降至 $O(n^3)$.

关键词: 鸽巢公式;极小不可满足;最大可满足指派;标准形式;子结构同构

中图法分类号: TP301 **文献标识码**: A

在组合学和人工智能中,许多原理和问题可以用命题公式表示.通过适当变形构造的公式具有很多有趣的性质,如消解难例、对称性质、子结构同构性质、极小不可满足性等[1−5].著名的消解难例——鸽巢公式——来自于组合学中的鸽巢原理.鸽巢原理是指:n+1 只鸽子进入 n 个巢,必有一个巢至少有 2 只鸽子[6].通过引入变元 $x_{i,j}$ 表示 i 号鸽子进入 j 号巢,则鸽巢原理可用如下公式表示:

$$\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\rightarrow\vee_{1\leqslant i<i'\leqslant n+1}(\vee_{1\leqslant j\leqslant n}(x_{i,j}\wedge x_{i',j})).$$

* 基金项目: 国家自然科学基金(60863005, 61111130186)
收稿时间: 2010-07-07; 定稿时间: 2010-11-03

由鸽巢原理,考虑一对矛盾:n+1 只鸽子进入 n 个巢,要求每只鸽子都进巢,且每个巢中不允许有两只鸽子.改写鸽巢原理的表示公式得到鸽巢公式: $PH_n^{n+1} := \wedge_{1\le i\le n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\le i<i'\le n+1}(\wedge_{1\le j\le n}(\neg x_{i,j}\vee\neg x_{i',j}))$.

容易验证,鸽巢公式 PH_n^{n+1} 是一个不可满足公式.Haken 首先证明了鸽巢公式在通常的树消解下,其反驳证明树的节点数至少在指数级[4].换言之,如果以消解证明中出现的子句个数度量其证明的复杂性,则公式 PH_n^{n+1} 的任何反驳证明的复杂性至少在指数级.难例在算法测试及密码学中的应用具有极其重要的地位,难例的寻找以及结构性质的研究与分析受到广泛关注[1−5,7].鸽巢公式在难例构造中具有重要的参照作用.如,团与补团公式 $CLIQUE_k^n$ 是鸽巢公式的一种推广.公式 $CLIQUE_k^n$ 来源于团与补团原理:给定一个 n 节点集 V,以 V 作为结点集考虑两个图 G 和 H.如果 G 是一个 k 团图,并且 H 是一个 k–1 补团图,则 G 中必有一条边不在 H 中出现(注:一个图称为 k 团图,如果存在一个具有 k 个节点的子集,任意两个不同点之间均有一条边;一个图称为 k 补团图,如果其节点集可以划分为 k 个不同部分,使得图中任意两个在不同划分部分中的节点之间没有边相连).有关公式 $CLIQUE_k^n$ 的定义以及与 PH_{k-1}^k 之间的联系,可参见文献[7].直观上,图 G 指示其中有一个带有 k 个节点的团,其节点集设为 V_0,V_0 任意两个不同节点之间有一条边相连;而图 H 指示节点集 V 可以划分成 k–1 个互不相交的节点集簇 $V_1,\ldots,V_{k-1}$,并且不同节点子集之间在 H 中无边相连.因此,由 $V_0\subseteq V=V_1\cup\ldots\cup V_{k-1}$ 并根据鸽巢原理,必有 $u,v\in V_0$ 在不同划分块 $V_i,V_j(1\le i\ne j\le k-1)$中.即 G 中有一条边不在 H 中出现.

在 DPLL 算法应用中,往往会出现不同节点上标记公式(在同构意义下)结构上相同.对称规则是指:当两个公式同构时,用空子句取代其中之一标记节点.对称规则也称为同构规则.两个公式同构是指:存在变元集上一个双射,将其作用在公式之一,并对部分变元对应的文字符号作适当对换后,得到同一个公式.双射的作用相当于对变元进行改名,变元对应的文字符号对换等操作不影响公式的可满足性.于是,如果两个公式同构,则它们具有相同的可满足性.在 DPLL 算法中引入同构规则后得到的改进算法,可使某些难例的计算复杂性产生本质改变.在消解证明中也有类似情况发生.对于有些难例,消解证明本身困难,但公式的子结构上可能具有良好的同构性质.如果扩充通常消解规则,允许使用对称规则,则消解难度或算法的复杂性可以降至多项式量级[1,2,8].

一个 CNF 公式是极小不可满足的是指:公式本身不可满足,但从中任意删去一个子句后得到的公式可满足.极小不可满足公式这种临界现象可以应用到可满足性(satisfiability,简称 SAT)问题研究的许多地方[9−13].DPLL 算法作为求解 SAT 问题的一种基础方法[12,13],各种改进策略的目的是使计算复杂性有所改善.对于某些特定限制下的公式类,引进的改进策略会对复杂性有本质改进.

从公式的结构研究 SAT 问题及其算法具有其特殊性,公式的特殊结构有助于设计有效算法求解问题.本文研究鸽巢公式的一些结构性质,基于鸽巢公式的极小不可满足性,找到了公式 PH_n^{n+1} 最大可满足真值指派的两种标准形式.Haken 关于 PH_n^{n+1} 消解困难的证明用到了其中一种标准形式[4].本文进一步分析了 PH_n^{n+1} 的子结构具有的良好同构性质.基于子结构的同构性质,如果在 DPLL 算法中引入同构规则,分枝点上两个同构公式只处理其中之一,以空子句取代同构公式进行剪枝,则证明树的节点数可以降至 $O(n^3)$.

本文所得到的 PH_n^{n+1} 最大可满足真值指派的标准形式以及有关的同构性质分析,结合 Haken 关于难例证明的方法,有助于难例的构造和证明.

1 基本性质

一个子句 C 是若干个文字的析取 $C=(L_1\vee L_2\vee\ldots\vee L_n)$,一个合取范式(conjunctive normal form,简称 CNF)公式(以下简称公式)F 是若干子句的合取 $F=(C_1\wedge C_2\wedge\ldots\wedge C_m)$.有时用文字的集合表示子句,用子句集合表示公式.一个变元 x 在一个公式 F 中的正(负)出现,是指文字 x(文字$\neg x$)在 F 中出现.对于公式 F_1 和 F_2,记 F_1+F_2 表示 $F_1\wedge F_2$.

设 $F=\{C_1,C_2,\ldots,C_m\}$是一个公式.称 F 是极小不可满足公式(minimal unsatisfiable formula,简称 MU 公式),如果 F 不可满足,并且从中删去任意一个子句 $C_i(1\le i\le m)$后得到的公式可满足.

用$[n]$,$[n]\backslash i$ 分别表示集合$\{1,2,\ldots,n\}$,$\{1,2,\ldots,i-1,i+1,\ldots,n\}$.

鸽巢原理:n+1 只鸽子进入 n 个巢,必有一个巢至少有 2 只鸽子.引入变元 $x_{i,j}$ 表示 i 号鸽子进入 j 号巢,则鸽

巢原理可用如下公式表示:$\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\rightarrow\vee_{1\leqslant i<i'\leqslant n+1}(\vee_{1\leqslant j\leqslant n}(x_{i,j}\wedge x_{i',j}))$.

由鸽巢原理,考虑一对矛盾:n+1 只鸽子进入 n 个巢,要求每只鸽子都进巢,且每个巢中不允许有两只鸽子.改写鸽巢原理表示公式得到鸽巢公式:

$$PH_n^{n+1}:=\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n}(\neg x_{i,j}\vee\neg x_{i',j})).$$

引理 1. PH_n^{n+1} 是一个极小不可满足公式.

证明:

(1) 证明 PH_n^{n+1} 不可满足.假定公式 $PH_n^{n+1}:=\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n}(\neg x_{i,j}\vee\neg x_{i',j}))$ 可满足,则存在变元集合$\{x_{i,j}|1\leqslant i\leqslant n+1,1\leqslant j\leqslant n\}$上的一个真值指派$\varphi$,使得:

(1.1) 对每个 $1\leqslant i\leqslant n+1,\varphi(x_{i,1}\vee\ldots\vee x_{i,n})=1$.

(1.2) 对每对 $1\leqslant i<i'\leqslant n+1$ 以及每个 $1\leqslant j\leqslant n,\varphi(\neg x_{i,j}\vee\neg x_{i',j})=1$.

由 (1.1),对每个 $1\leqslant i\leqslant n+1$,存在某个 $1\leqslant j\leqslant n$,使得$\varphi(x_{i,j})=1$.由鸽巢原理:存在某对 $i,i'(1\leqslant i<i'\leqslant n+1)$以及某个 $j'(1\leqslant j'\leqslant n)$,使得$\varphi(x_{i,j'})=\varphi(x_{i',j'})=1$.这与情形(1.2)矛盾.

(2) 证明 PH_n^{n+1} 极小不可满足.即证明:从 PH_n^{n+1} 中删去任意一个子句 C 后,得到的公式可满足.分两种情形讨论:

情形 1:对某个$(1\leqslant i\leqslant n+1),C=(x_{i,1}\vee\ldots\vee x_{i,n})$.

不失一般性,假定 $C=(x_{n+1,1}\vee\ldots\vee x_{n+1,n})$.从 PH_n^{n+1} 中删去子句 C 后,得到公式:

$$F_1=\wedge_{1\leqslant i\leqslant n}(x_{i,1}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n}(x_{i,j}\vee x_{i',j})).$$

取一个真值指派φ_1如下:

$$\varphi_1(x)=\begin{cases}0, & x\in\{x_{n+1,1},x_{n+1,2},\ldots,x_{n+1,n}\}\\ 1, & x\in\{x_{1,1},x_{2,2},\ldots,x_{n,n}\}\\ 0, & x\in\{x_{i,j}\,|\,1\leqslant i\neq j\leqslant n\}\end{cases}.$$

我们有$\varphi_1(F_1)=1$.直观上,删去子句 $C=(x_{n+1,1}\vee\ldots\vee x_{n+1,n})$后,$n$+1 号鸽子可以不进巢.于是,可以让 i 号鸽子进 i 号巢,$1\leqslant i\leqslant n$.

情形 2:对某对$(1\leqslant i<i'\leqslant n+1)$及某个$(1\leqslant j\leqslant n),C=(\neg x_{i,j}\vee\neg x_{i',j})$.

不失一般性,假定 $C=(\neg x_{n,n}\vee\neg x_{n+1,n})$.从 PH_n^{n+1} 中删去子句 C 后,得到公式:

$$F_2=\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n-1}(\neg x_{i,j}\vee\neg x_{i',j}))\wedge\wedge_{1\leqslant i\leqslant n-1}(\neg x_{i,n}\vee\neg x_{n+1,n})\wedge\wedge_{1\leqslant i<i'\leqslant n}(\neg x_{i,n}\vee\neg x_{i',n}).$$

取一个真值指派φ_2如下:

$$\varphi_2(x)=\begin{cases}1, & x\in\{x_{n,n},x_{n+1,n}\}\\ 1, & x\in\{x_{1,1},\ldots,x_{n-1,n-1}\}\\ 0, & x\in\{x_{i,j}\,|\,1\leqslant i\neq j\leqslant n\}\cup\{x_{n+1,1},x_{n+1,2},\ldots,x_{n+1,n-1}\}\end{cases}.$$

我们有$\varphi_2(F_2)=1$.直观上,删去子句 $C=(\neg x_{n,n}\vee\neg x_{n+1,n})$后,允许 n,n+1 号鸽子同时进 n 号巢.于是,可以让 i 号鸽子进 i 号巢,$1\leqslant i\leqslant n-1$.

综上所述,PH_n^{n+1} 是极小不可满足公式. □

设 $C_1=(x\vee c_1),C_2=(\neg x\vee c_2)$为一对子句,$\{x,\neg x\}$称为出现在子句 C_1,C_2 中的互补文字对.如果子句 c_1,c_2 中不含互补文字对,则称子句 $C_{12}=(c_1\vee c_2)$为 C_1,C_2 关于变元 x 的消解子句(简称消解);特别地,如果 $c_1=\varnothing$或 $c_2=\varnothing$,则称为单位消解.设 $F=\{(x\vee c_1),(\neg x\vee c_2)\}+F_{rest}$,称公式 $F'=\{(c_1\vee c_2)\}+F_{rest}$ 为 F 关于变元 x 的消解.

设 $F=\{C_1,\ldots,C_m\}$为一个不可满足公式,称子句序列 $c_1,\ldots,c_n$ 为 F 的一个消解(反驳)证明,如果以下条件成立:(1) $c_1,c_2\in F$;(2) $c_n=\varnothing$(空子句);(3) 对每个 $3\leqslant k\leqslant n$,或 $c_k\in F$,或存在 $1\leqslant i\neq j<k,c_k$ 是 c_i,c_j 关于某个变元的消解.F 的一个消解证明 $c_1,\ldots,c_n$ 可以用一棵标记二叉树 $T=(V,E,\lambda)$表示.其中,标记函数$\lambda:V\rightarrow\{c_1,\ldots,c_n\}$满足条件:如果 v_k 是 v_i,v_j 的父节点,则$\lambda(v_k)$是$\lambda(v_i),\lambda(v_j)$关于某个变元的消解.于是,$T$的叶节点都被原始子句或某些消解子句标记,$T$的内节点被消解子句标记,$T$ 的根节点被空子句标记.称 T 为 F 的反驳证明树.

可以证明:树证明方法是可靠的和完备的[2,14−16].即,(可靠性)如果 T 为 F 的一个反驳树证明,则 F 是不可满足的;(完备性)如果 F 是不可满足的,则存在 F 的一个反驳树证明.

设公式 $F=\{(x\vee c),(\neg x\vee c_1),(\neg x\vee c_2),\dots,(\neg x\vee c_k)\}+F_{rest}$,其中,$F_{rest}$ 中不含变元 x,称公式 $F'=\{(c\vee c_1),(c\vee c_2),\dots,(c\vee c_k)\}+F_{rest}$ 为 F 关于 x 的(1,*)-消解(类似可定义 F 关于 $\neg x$ 的(1,*)-消解).

引理 2[12]. 极小不可满足公式类在(1,*)-消解下封闭.即,极小不可满足公式通过(1,*)-消解得到的公式仍然是极小不可满足公式.

2 最大可满足指派的标准形式

一个公式的最大可满足指派是满足子句数最多的指派.本节得到公式 PH_n^{n+1} 最大可满足指派的两类标准形式,在 Haken 关于 PH_n^{n+1} 消解困难的证明中用到了其中一种标准形式[4].

公式 PH_n^{n+1} 含有 $n(n+1)$个变元,现将公式的变元集排成如下$(n+1)\times n$ 阵列:

$$var(PH_n^{n+1}):=\begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n-1} & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n-1} & x_{2,n} \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n-1} & x_{n,n} \\ x_{n+1,1} & x_{n+1,2} & \cdots & x_{n+1,n-11} & x_{n+1,n} \end{bmatrix}.$$

同时,PH_n^{n+1} 中一个子句可以用一个$(n+1)\times n$ 矩阵表示.当变元在子句中正出现时,在对应位置上用"+"标记;当变元在子句中负出现时,在对应位置上用"–"标记;其余位置为空白,为方便阅读,用"*"标记空白.例如,PH_2^3 含有如下子句:

$$\begin{bmatrix} + & + \\ * & * \\ * & * \end{bmatrix},\begin{bmatrix} * & * \\ + & + \\ * & * \end{bmatrix},\begin{bmatrix} * & * \\ * & * \\ + & + \end{bmatrix},\begin{bmatrix} - & * \\ - & * \\ * & * \end{bmatrix},\begin{bmatrix} - & * \\ * & * \\ - & * \end{bmatrix},\begin{bmatrix} * & * \\ - & * \\ - & * \end{bmatrix},\begin{bmatrix} * & - \\ * & - \\ * & * \end{bmatrix},\begin{bmatrix} * & - \\ * & * \\ * & - \end{bmatrix},\begin{bmatrix} * & * \\ * & - \\ * & - \end{bmatrix}.$$

注: PH_n^{n+1} 含有 $(n+1)+n\binom{n+1}{2}=\frac{n^2(n+1)}{2}+n+1$ 个子句.

同样,公式 PH_n^{n+1} 的一个(变元)真值指派可以用一个$(n+1)\times n$ 的 0/1 矩阵表示.如,引理 1 证明中的两个真值指派φ_1,φ_2 可以分别表示为

$$M_1=\left[\begin{array}{ccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ \hdashline 0 & 0 & \cdots & 0 & 0 \end{array}\right],\ M_2=\left[\begin{array}{ccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ \hdashline 0 & 0 & \cdots & 0 & 1 \end{array}\right].$$

M_1 具有如下特征:矩阵中第 n+1 行全为 0,前 n 行和前 n 列构成一个 n 阶单位矩阵.

M_2 具有如下特征:矩阵中第 n+1 行上恰有一个 1(在最后一列),前 n 行和前 n 列构成一个 n 阶单位矩阵.

事实上,如下赋值都满足公式引理 1 中的 $F_1=\wedge_{1\leqslant i\leqslant n}(x_{i,1}\vee\dots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n}(x_{i,j}\vee x_{i',j}))$:

$$\varphi_\pi(x)=\begin{cases} 0, & x\in\{x_{n+1,1},x_{n+1,2},\dots,x_{n+1,n}\} \\ 1, & x\in\{x_{1,\pi(1)},x_{2,\pi(2)},\dots,x_{n,\pi(n)}\} \\ 0, & x\in\{x_{i,j}\,|\,1\leqslant i\leqslant n, j\neq\pi(i)\} \end{cases},$$

其中,π为$[n]$上的任一置换.

同样,如下赋值都满足公式引理 1 中的 $F_2=\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee\dots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n-1}(\neg x_{i,j}\vee\neg x_{i',j}))\wedge$

$\wedge_{1\leqslant i\leqslant n-1}(\neg x_{i,n}\vee\neg x_{n+1,n})\wedge\wedge_{1\leqslant i<i'\leqslant n}(\neg x_{i,n}\vee\neg x_{i',n})$:

$$\varphi_\tau(x)=\begin{cases}1, & x\in\{x_{n,n},x_{n+1,n}\}\\ 1, & x\in\{x_{1,\tau(1)},\ldots,x_{n-1,\tau(n-1)}\}\\ 0, & x\in\{x_{i,j}\mid 1\leqslant i\leqslant n-1, j\neq\tau(i)\}\cup\{x_{n,1},x_{n+1,1},x_{n,2},x_{n+1,2},\ldots,x_{n,n-1},x_{n+1,n-1}\}\end{cases},$$

其中,τ为$[n-1]$上的任一置换.

我们现在给出两种赋值形式:I-型赋值,II-型赋值.

- I-型赋值:$(n+1)\times n$ 的 0/1 矩阵 M 中恰有一行全为 0(此行称为 M 的纯 0-行),删去纯 0-行,其余 $n\times n$ 行列中,每行每列恰有一个 1.
- II-型赋值:$(n+1)\times n$ 的 0/1 矩阵 M 中恰有一列有两个 1(此列称为 M 的双 1-列),删去双 1-列及其两个 1 所在的行,其余$(n-1)\times(n-1)$行列中,每行每列恰有一个 1.

显然,通过适当的行列调整,I-型赋值可以变换为 M_1(称为 I-型标准赋值),II-型赋值可以变换为 M_2(称为 II-型标准赋值).

事实上,如果 M 为一个$(n+1)\times n$ 的 I-型赋值矩阵,首先将纯 0-行与第 $n+1$ 行对换,然后取一个$[n]$上的置换π作用在列上,则可将 M 变换为 M_1.如果 M 为一个$(n+1)\times n$ 的 II-型赋值矩阵,首先将双 1-列与第 n 列对换,然后,双 1-列上两个 1 所在行分别与第 n 行和第 $n+1$ 行对换,最后取一个$[n-1]$上的置换τ作用在列上,则可将 M 变换为 M_2.

赋值矩阵的行列变换对应于变元矩阵的行列变换,只涉及变元改名,不影响公式的可满足性.

如下定理表明,PH_n^{n+1}的任一最大可满足真值赋值矩阵通过适当的行列变换都可以转换为标准型.

定理 1. PH_n^{n+1}的任一最大可满足真值指派 M 必具有 I-型赋值或 II-型赋值形式之一.即:

(1) 存在一个 $1\leqslant i\leqslant n+1$,将 M 中第 i 行与第 $n+1$ 行对调,再取$[n]$上的一个置换作用于列号,可得到 I-型标准赋值 M_1.

(2) 存在一对 $1\leqslant i<i'\leqslant n+1,1\leqslant j\leqslant n$,将 M 中第 j 列与第 n 列对调,i,i'与 $n,n+1$ 分别对调后,再取$[n-1]$上的一个置换作用于列号,可得到 II-型标准赋值 M_2.

证明:由引理 1,PH_n^{n+1}为极小不可满足公式,从而,每一个最大可满足指派除一个子句外,其余子句均被满足.设 M 为 PH_n^{n+1}的一个最大可满足真值指派,则存在唯一子句 C_M 不被 M 满足,其余子句均被 M 满足.由 PH_n^{n+1}的子句结构类型,C_M 只可能为如下两种形式之一:

(1) 对某个 $1\leqslant i\leqslant n+1,C_M=(x_{i,1}\vee\ldots\vee x_{i,n})$.

(2) 对某对 $1\leqslant i<i'\leqslant n+1$ 及某个 $1\leqslant j\leqslant n,C_M=(\neg x_{i,j}\vee\neg x_{i',j})$.

M 为一个$(n+1)\times n$ 的 0/1 矩阵,其中,$M(s,t)=M(x_{s,t})$(在变元 $x_{s,t}$ 上的赋值).

情形 1:对某个 $1\leqslant i\leqslant n+1,C_M=(x_{i,1}\vee\ldots\vee x_{i,n})$唯一不被 M 满足.

M 中第 i 行全为 0,在 M 中删去第 i 行后得到一个 $n\times n$ 矩阵 $M^{[i]}$,则 $M^{[i]}$具有性质:每一行、每一列中恰有一个 1.

为叙述方便,保持 $M^{[i]}$与 M 的行(列)号标记一致,$M^{[i]}$中的行号仍用$\{1,2,\ldots,i-1,i+1,\ldots,n,n+1\}$标记,列号用$\{1,2,\ldots,n\}$标记.

断言 1. $M^{[i]}$中每一行至少含有 1 个 1.

如若不然,则 $M^{[i]}$中有一行全为 0.设第 $s(s\neq i)$行全为 0,则子句$(x_{s,1}\vee\ldots\vee x_{s,n})$不被 M 满足.这与 M 唯一不满足 C_M 矛盾.

(1.1) $M^{[i]}$中每一行恰有一个 1.

由断言 1,只需证明:不存在某行含有两个以上的 1.如若不然,则存在某行至少含有 2 个 1.设 $M^{[i]}(s,t)=M^{[i]}(s,t')=1(1\leqslant t<t'\leqslant n)$,其中,$s\neq i$.

如果$(\exists s'\neq s)[(M^{[i]}(s',t)=1)\vee(M^{[i]}(s',t')=1)]$,则 M 不满足子句$(\neg x_{s,t}\vee\neg x_{s',t}),(\neg x_{s,t'}\vee\neg x_{s',t'})$之一.

如果$(\forall s'\neq s)[(M^{[i]}(s',t)=0)\wedge(M^{[i]}(s',t')=0)]$,则由鸽巢原理及断言 1,存在 $k\neq t,t'$列上至少含有 2 个 1.设为

$(M^{[i]}(m,k)=1)\wedge(M^{[i]}(m',k)=1)$,则 M 不满足子句$(\neg x_{m,k}\vee\neg x_{m',k})$.

可见,均与 M 唯一不满足 C_M 矛盾.

(1.2) $M^{[i]}$中每一列恰有一个 1.

如果 $M^{[i]}$有一列全为 0,此时,由断言 1 及鸽巢原理,必有一列至少含有 2 个 1.设$(M^{[i]}(m,k)=1)\wedge(M^{[i]}(m',k)=1)$,则 M 不满足子句$(\neg x_{m,k}\vee\neg x_{m',k})$.

如果 $M^{[i]}$有一列至少含有 2 个 1,类似地可以证明:M 不满足形如$(\neg x_{m,k}\vee\neg x_{m',k})$的子句.

可见,均与 M 唯一不满足 C_M 矛盾.

上述结果表明:M 是一个 I-型赋值.在 M 中,将第 i 行与第 n+1 行对调,再取$[n]$上的一个置换π作用于列号,即可得到 I-型标准赋值 M_1.

情形 2:对某对 $1\leqslant i<i'\leqslant n+1$ 及某个 $1\leqslant j\leqslant n$,$C_M=(\neg x_{i,j}\vee\neg x_{i',j})$唯一不被 M 满足.

在 M 中删去第 i,i'两行及第 j 列,得到一个$(n-1)\times(n-1)$矩阵 $M^{[(i,i'),j]}$,则 $M^{[(i,i'),j]}$具有性质:每一行、每一列中恰有一个 1.

同样,为使 $M^{[(i,i'),j]}$与 M 的行(列)号标记一致,$M^{[(i,i'),j]}$中的行号仍用$\{1,2,\dots,i-1,i+1,\dots,i'-1,i'+1,\dots,n,n+1\}$标记,列号仍用$\{1,2,\dots,j-1,j+1,\dots,n\}$标记.

断言 2. $M^{[(i,i'),j]}$中每一行至少含有 1 个 1.

若不然,则 $M^{[(i,i'),j]}$中有一行全为 0.设第 $s(s\neq i,i')$行全为 0.如果 $M(s,j)=0$,则 M 中第 s 行全为 0.此时,子句$(x_{s,1}\vee\dots\vee x_{s,n})$不被 M 满足;如果 $M(s,j)=1$,则子句$(\neg x_{s,j}\vee\neg x_{i,j})$,$(\neg x_{s,j}\vee\neg x_{i',j})$不被 M 满足.两种情形均与“C_M 唯一不被 M 满足”矛盾.

(2.1) $M^{[(i,i'),j]}$中每一行恰有一个 1.

由断言 2,只需证明:$M^{[(i,i'),j]}$中每一行不能含有两个以上的 1.

如果 $M^{[(i,i'),j]}$有一行至少含有 2 个 1,设 $M^{[(i,i'),j]}(s,t)=M^{[(i,i'),j]}(s,t')=1$.注意:$s\neq i,i';j\neq t,t';t\neq t'$.由断言 2 及鸽巢原理,必有如下情形之一出现:

(a) 存在 $j'\neq t,j'\neq t'$,$M^{[(i,i'),j]}$中第 j'列上至少出现 2 个 1;

(b) $M^{[(i,i'),j]}$中第 t 列或第 t'列上至少出现 2 个 1.

类似地可以证明,有形如$(\neg x_{m,n}\vee\neg x_{m',n})$这样的子句不被 $M^{[(i,i'),j]}$满足.由于是在 $M^{[(i,i'),j]}$中取行列号,故$(\neg x_{m,n}\vee\neg x_{m,n'})$与 C_M 不相同,从而与 $M^{[(i,i'),j]}$唯一不满足 C_M 矛盾.

(2.2) $M^{[(i,i'),j]}$中每一列恰有 1 个 1.

如果 $M^{[(i,i'),j]}$有一列全为 0.此时,由断言 2 及鸽巢原理,$M^{[(i,i'),j]}$必有一列至少含有 2 个 1.如果 $M^{[(i,i'),j]}$有一列至少含有 2 个 1,类似地,有与 C_M 不同的子句$(\neg x_{m,n}\vee\neg x_{m',n})$不被 $M^{[(i,i'),j]}$满足.与 $M^{[(i,i'),j]}$唯一不满足 C_M 矛盾.

到此,我们得到结论:$M^{[(i,i'),j]}$每行每列恰有一个 1.

此外,我们还需讨论如下结论:

(A) $(\forall s\neq i,i')[M(s,j)=0]$.

如果$(\exists s\neq i,i')[M(s,j)=1]$,则$^{[(i,i'),j]}$不满足子句$(\neg x_{s,j}\vee\neg x_{i,j})$,$(\neg x_{s,j}\vee\neg x_{i',j})$,$C_M=(\neg x_{i,j}\vee\neg x_{i',j})$.

(B) $(\forall t\neq j)[(M(i,t)=0)\wedge(M(i',t)=0)]$.

如果$(\exists t\neq j)[(M(i,t)=1)\vee(M(i',t)=1)]$,由于 $M^{[(i,i'),j]}$每行每列恰有一个 1.我们有

$$(\exists s\neq i,i')\{[(M(s,t)=1)\wedge(M(i,t)=1)]\vee[(M(s,t)=1)\wedge(M(i',t)=1)]\},$$

则$(\neg x_{s,t}\vee\neg x_{i,t})$,$(\neg x_{s,t}\vee\neg x_{i',t})$中至少有 1 个(与 C_M 不同)子句不被 M 满足子.与 M 唯一不满足 C_M 矛盾.

上述结果表明:M 是一个 I-型赋值.在 M 中,将第 j 列与第 n 列对调,i,i'与 n,n+1 分别对调后,再取$[n-1]$上的一个置换τ作用于列号,可得到 II-型标准赋值 M_2. □

推论 1. PH_n^{n+1} 的最大可满足真值指派数为 $\#\max\text{-}sat(PH_n^{n+1})=\left(\dfrac{n}{2}+1\right)(n+1)!$.

证明:I-型赋值共有$(n+1)!$个,因为纯 0-行有$(n+1)$种选择,$[n]$上的置换有 $n!$个;II-型赋值有$n\binom{n+1}{2}(n-1)!$,因为双-1 列有 n 种选择,同一列上两个 1 有$\binom{n+1}{2}$种选择,$[n-1]$上的置换有$(n-1)!$个.

所以,$\#\max\text{-}sat(PH_n^{n+1})=(n+1)!+n\binom{n+1}{2}(n-1)!=\left(\frac{n}{2}+1\right)(n+1)!$. □

3 子结构同构性质

本文中,公式的子结构是指:在一个部分指派下,代入化简得到公式的(部分)子句构成的子公式的结构.

设 $N=\{1,2,\ldots\}$,对于自然数子集 $L\subseteq N,R\subseteq N,S\subseteq N$,其中,$|L|=l,|R|=r,1\leqslant r<l$.

引入记号:$X_{i,S}=\vee_{j\in S}x_{i,j}$,$H_{L,R}=\{(\neg x_{i,k}\vee\neg x_{j,k}):i<j,i,j\in L,k\in R\}$,$G_{L,R}=\{(X_{i,R}\vee X_{j,R}):i,j\in L,i<j\}$.

定义 $Q_{L,R}:=G_{L,R}+H_{L,R}$.特别地,当 $L=[n+1],R=[n-1]$时,

$$Q_{[n+1],[n-1]}=\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n+1\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n+1,1\leqslant k\leqslant n-1\}.$$

公式 $PH_n^{n+1}:=\wedge_{1\leqslant i\leqslant n+1}(x_{i,1}\vee x_{i,2}\vee\ldots\vee x_{i,n})\wedge\wedge_{1\leqslant i<i'\leqslant n+1}(\wedge_{1\leqslant j\leqslant n}(\neg x_{i,j}\vee\neg x_{i',j}))$ 依次关于 $x_{1,n},x_{2,n},\ldots,x_{n+1,n}$ 做 $n+1$ 次(1,*)-消解,得到公式 $Q_{[n+1],[n-1]}$.如

$$\begin{aligned}PH_3^4=\Bigg\{&\begin{bmatrix}+&+&+\\ *&*&*\\ *&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ +&+&+\\ *&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&*\\ +&+&+\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&*\\ *&*&*\\ +&+&+\end{bmatrix},\\
&\begin{bmatrix}-&*&*\\ -&*&*\\ *&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}-&*&*\\ *&*&*\\ -&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}-&*&*\\ *&*&*\\ *&*&*\\ -&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ -&*&*\\ -&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ -&*&*\\ *&*&*\\ -&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&*\\ -&*&*\\ -&*&*\end{bmatrix},\\
&\begin{bmatrix}*&-&*\\ *&-&*\\ *&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&-&*\\ *&*&*\\ *&-&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&-&*\\ *&*&*\\ *&*&*\\ *&-&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&-&*\\ *&-&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&-&*\\ *&*&*\\ *&-&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&*\\ *&-&*\\ *&-&*\end{bmatrix},\\
&\begin{bmatrix}*&*&-\\ *&*&-\\ *&*&*\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&-\\ *&*&*\\ *&*&-\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&-\\ *&*&*\\ *&*&*\\ *&*&-\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&-\\ *&*&-\\ *&*&*\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&-\\ *&*&*\\ *&*&-\end{bmatrix},\begin{bmatrix}*&*&*\\ *&*&*\\ *&*&-\\ *&*&-\end{bmatrix}\Bigg\}.\end{aligned}$$

关于 $x_{1,3},x_{2,3},x_{3,3},x_{4,3}$ 做(1,*)-消解后得到公式 $Q_{[4],[2]}$:

$$\begin{aligned}Q_{[4],[2]}=G_{[4],[2]}+H_{[4],[2]}=\Bigg\{&\begin{bmatrix}+&+\\ +&+\\ *&*\\ *&*\end{bmatrix},\begin{bmatrix}+&+\\ *&*\\ +&+\\ *&*\end{bmatrix},\begin{bmatrix}+&+\\ *&*\\ *&*\\ +&+\end{bmatrix},\begin{bmatrix}*&*\\ +&+\\ +&+\\ *&*\end{bmatrix},\begin{bmatrix}*&*\\ +&+\\ *&*\\ +&+\end{bmatrix},\begin{bmatrix}*&*\\ *&*\\ +&+\\ +&+\end{bmatrix},\begin{bmatrix}-&*\\ -&*\\ *&*\\ *&*\end{bmatrix},\begin{bmatrix}-&*\\ *&*\\ -&*\\ *&*\end{bmatrix},\begin{bmatrix}-&*\\ *&*\\ *&*\\ -&*\end{bmatrix},\\
&\begin{bmatrix}*&*\\ -&*\\ -&*\\ *&*\end{bmatrix},\begin{bmatrix}*&*\\ -&*\\ *&*\\ -&*\end{bmatrix},\begin{bmatrix}*&*\\ *&*\\ -&*\\ -&*\end{bmatrix},\begin{bmatrix}*&-\\ *&-\\ *&*\\ *&*\end{bmatrix},\begin{bmatrix}*&-\\ *&*\\ *&-\\ *&*\end{bmatrix},\begin{bmatrix}*&-\\ *&*\\ *&*\\ *&-\end{bmatrix},\begin{bmatrix}*&*\\ *&-\\ *&-\\ *&*\end{bmatrix},\begin{bmatrix}*&*\\ *&-\\ *&*\\ *&-\end{bmatrix},\begin{bmatrix}*&*\\ *&*\\ *&-\\ *&-\end{bmatrix}\Bigg\}.\end{aligned}$$

由引理 2,我们有:

引理 3. 公式 $Q_{[n+1],[n-1]}$是一个极小不可满足公式.

引理 4. 对于公式 $Q_{[n+1],[n-1]}$,通过令 $x_{n+1,n-1}=1$ 代入公式 $Q_{[n+1],[n-1]}$化简后,可以从化简公式中取出一个子公式,对其进行(1,*)-消解后,得到公式 $Q_{[n],[n-2]}$.

证明:(1) 由定义,$Q_{[n+1],[n-1]}=G_{[n+1],[n-1]}+H_{[n+1],[n-1]}$.令 $x_{n+1,n-1}=1$,得到:

$$G_{[n+1],[n-1]}(x_{n+1,n-1}=1)=G_{[n],[n-1]}=\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n\}$$

及

$$\begin{aligned}H_{[n+1],[n-1]}(x_{n+1,n-1}=1)=&\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-2\}+\\&\{(\neg x_{i,k}\vee\neg x_{n+1,k}):1\leqslant i\leqslant n,1\leqslant k\leqslant n-2\}+\\&\{(\neg x_{i,n-1}\vee\neg x_{j,n-1}):1\leqslant i<j\leqslant n\}+\{\neg x_{i,n-1}:1\leqslant i\leqslant n\}.\end{aligned}$$

公式 $H_{[n+1],[n-1]}(x_{n+1,n-1}=1)$中含有如下子公式:

$$\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-2\}+\{\neg x_{i,n-1}:1\leqslant i\leqslant n\}.$$

于是,取 $Q_{[n+1],[n-1]}(x_{n+1,n-1}=1)$的子公式:

$$\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n\}+\{\neg x_{i,n-1}:1\leqslant i\leqslant n\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-2\}.$$

(2) 利用得到的 n 个单位子句$\neg x_{1,n-1},\neg x_{2,n-1},\ldots,\neg x_{n,n-1}$,依次做(1,*)-消解(共 n 次),得到

$$\{(X_{i,[n-2]}\vee X_{j,[n-2]}):1\leqslant i<j\leqslant n\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-2\}=G_{[n],[n-2]}+H_{[n],[n-2]}=Q_{[n],[n-2]}.\qquad\square$$

以 $Q_{[4],[2]}$为例,令 $x_{4,2}=1$,公式化简为

$$\left\{\begin{bmatrix}+&+\\+&+\\*&*\\*&*\end{bmatrix},\begin{bmatrix}+&+\\*&*\\+&+\\*&*\end{bmatrix},\begin{bmatrix}*&*\\+&+\\+&+\\*&*\end{bmatrix},\begin{bmatrix}-&*\\-&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\*&*\\-&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\-&*\\-&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\*&*\\*&*\\-&*\end{bmatrix},\begin{bmatrix}*&*\\-&*\\*&*\\-&*\end{bmatrix},\begin{bmatrix}*&*\\*&*\\-&*\\-&*\end{bmatrix},\right.$$
$$\left.\begin{bmatrix}*&-\\*&-\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&-\\*&*\\*&-\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&-\\*&-\\*&*\end{bmatrix},\begin{bmatrix}*&-\\*&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&-\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&*\\*&-\\*&*\end{bmatrix}\right\}.$$

取出如下子公式:

$$\left\{\begin{bmatrix}+&+\\+&+\\*&*\\*&*\end{bmatrix},\begin{bmatrix}+&+\\*&*\\+&+\\*&*\end{bmatrix},\begin{bmatrix}*&*\\+&+\\+&+\\*&*\end{bmatrix},\begin{bmatrix}*&-\\*&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&-\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&*\\*&-\\*&*\end{bmatrix},\begin{bmatrix}-&*\\-&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\*&*\\-&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\-&*\\-&*\\*&*\end{bmatrix}\right\}.$$

该子公式含有 3 个单位子句:

$$\left\{\begin{bmatrix}*&-\\*&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&-\\*&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\*&*\\*&-\\*&*\end{bmatrix}\right\}.$$

依次按$\neg x_{1,2},\neg x_{2,2},\neg x_{3,2}$做(1,*)-消解(共 3 次),得到公式:

$$\left\{\begin{bmatrix}+&*\\+&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}+&*\\*&*\\+&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\+&*\\+&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\-&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\*&*\\-&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\-&*\\-&*\\*&*\end{bmatrix}\right\}.$$

此公式为极小不可满足公式 $Q_{[3],[1]}$:

$$Q_{[3],[1]}=\left\{\begin{bmatrix}+&*\\+&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}+&*\\*&*\\+&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\+&*\\+&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\-&*\\*&*\\*&*\end{bmatrix},\begin{bmatrix}-&*\\*&*\\-&*\\*&*\end{bmatrix},\begin{bmatrix}*&*\\-&*\\-&*\\*&*\end{bmatrix}\right\}.$$

设 $F(x_1,\ldots,x_n),F'(y_1,\ldots,y_n)$为一个公式,变元集 $var(F)=\{x_1,\ldots,x_n\},var(F')=\{y_1,\ldots,y_n\}$.如果存在$[n]$上的一个置换$\pi$,使得 $F'(y_1,\ldots,y_n)=F(y_{\pi(1)},\ldots,y_{\pi(n)})$,则称 $F(x_1,\ldots,x_n)$与 $F'(y_1,\ldots,y_n)$同构.映射$\psi:\{x_1,\ldots,x_n\}\to\{y_1,\ldots,y_n\},\psi(x_i)=y_{\pi(i)}$ $(i=1,\ldots,n)$称为一个变元改名(或变元置换).可见,在变元改名下,对给定的 $i,d(1\leqslant i\leqslant n+1,0\leqslant d\leqslant n-1),Q_{[n],[n-2]}$, $Q_{[n],[n-1]\backslash d},Q_{[n+1]\backslash i,[n-1]\backslash d}$三者同构.

由于子公式的不可满足性可以导致整个公式的不可满足性,从而子公式的反驳证明可以构成整个公式的不可满足性证明.所以,在引理 4 中取一个不可满足的子公式进行(1,*)-消解证明是有效的.

将引理 4 一般化,我们有如下子结构同构性质:

定理 2(子结构同构性质). 公式 $Q_{[n+1],[n-1]}$具有如下性质:

(1) 令 $x_{n+1,n-1}=1$ 代入公式 $Q_{[n+1],[n-1]}$化简后,可从得到的公式中取出一个子公式,对此子公式进行(1,*)-消解后,得到公式 $Q_{[n],[n-2]}$;

(2) 令 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0$ 代入公式 $Q_{[n+1],[n-1]}$化简后,可从得到的公式中取出子公式 PH_{n-1}^{n},对公式 PH_{n-1}^{n} 进行(1,*)-消解后,得到公式 $Q_{[n],[n-2]}$;

(3) 对于固定的 $d(n-2\geqslant d\geqslant 1)$,令 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,d+1}=0,x_{n+1,d}=1$ 代入公式 $Q_{[n+1],[n-1]}$化简后,可从得到的公式中取出一个子公式,对此子公式进行(1,*)-消解后,得到公式 $Q_{[n],[n-1]\backslash d}$.

证明:公式 $Q_{[n+1],[n-1]}$的表达式为

$$\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n+1\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n+1,1\leqslant k\leqslant n-1\},$$

其中,$X_{i,[n-1]}=(x_{i,1}\vee\ldots\vee x_{i,n-1})$.

性质(1):即为引理 4.将此纳入本定理主要是为了完整性.故只对性质(2)、性质(3)进行证明.

性质(2):以 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0$ 代入公式 $Q_{[n+1],[n-1]}$化简后得到:

$$G_{[n+1],[n-1]}(x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0)=G_{[n],[n-1]}=\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n\}+\{X_{i,[n-1]}:1\leqslant i\leqslant n\}$$

及

$$H_{[n+1],[n-1]}(x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0)=\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-2\}+\{(\neg x_{i,n-1}\vee\neg x_{j,n-1}):1\leqslant i<j\leqslant n\}.$$

公式 $Q_{[n+1],[n-1]}(x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0)$含有

$$\{X_{i,[n-1]}:1\leqslant i\leqslant n\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-1\}=PH_{n-1}^{n}.$$

在 PH_{n-1}^{n} 中,依次关于 $x_{1,n-1},x_{2,n-1},\ldots,x_{n,n-1}$ 做 n 次(1,*)-消解,得到公式 $Q_{[n],[n-2]}$.

性质(3):固定的 $d(n-2\geqslant d\geqslant 1)$,以 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,d+1}=0,x_{n+1,d}=1$ 代入公式 $Q_{[n+1],[n-1]}$化简后得到:

$$G_{[n+1],[n-1]}(x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,d+1}=0,x_{n+1,d}=1)=G_{[n],[n-1]}=\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n\}$$

及

$$\begin{aligned}H_{[n+1],[n-1]}(x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,d+1}=0,x_{n+1,d}=1)=&\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-1,k\neq d\}+\\&\{(\neg x_{i,k}\vee\neg x_{n+1,k}):1\leqslant i\leqslant n,1\leqslant k\leqslant d-1\}+\\&\{\neg x_{i,d}:1\leqslant i\leqslant n\}+\{(\neg x_{i,d}\vee\neg x_{j,d}):1\leqslant i<j\leqslant n\}.\end{aligned}$$

取出子公式:

$$\{(X_{i,[n-1]}\vee X_{j,[n-1]}):1\leqslant i<j\leqslant n\}+\{\neg x_{i,d}:1\leqslant i\leqslant n\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-1,k\neq d\}.$$

依次按得到的 n 个单位子句$\neg x_{1,d},\neg x_{2,d},\ldots,\neg x_{n,d}$,做消解(1,*)-消解(共 n 次),得到

$$\begin{aligned}&\{(X_{i,[n-1]\backslash d}\vee X_{j,[n-1]\backslash d}):1\leqslant i<j\leqslant n\}+\{(\neg x_{i,k}\vee\neg x_{j,k}):1\leqslant i<j\leqslant n,1\leqslant k\leqslant n-1,k\neq d\}=\\&\qquad G_{[n],[n-1]\backslash d}+H_{[n],[n-1]\backslash d}=Q_{[n],[n-1]\backslash d}.\end{aligned}$$

□

在定理 2 中,将 i 替换 n+1 可以得到如下结论:

对于固定的 $i,d(1\leqslant i\leqslant n+1,1\leqslant d\leqslant n-1)$,令 $x_{i,n-1}=x_{i,n-2}=\ldots=x_{i,d+1}=0,x_{i,d}=1$ 代入公式化简后,可从得到的公式中取出一个子公式.对此子公式进行(1,*)-消解后,得到公式 $Q_{[n+1]\backslash i,[n-1]\backslash d}$.

注意到 $Q_{[n],[n-2]}\cong Q_{[n],[n-1]\backslash d}\cong Q_{[n+1]\backslash i,[n-1]\backslash d},i\in[n+1],d\in[n-1]$,并且其同构验证可以在 $O(n^2)$时间内完成.基于这样的观察,我们在 DPLL 算法中引入同构规则,即同构公式只处理其中之一,以空子句取代同构公式进行剪枝.在 DPLL 算法引入同构规则的算法称 ISODP 算法.

定理 3. 对于公式 PH_n^{n+1},存在 ISODP 算法下的反驳证明,其证明树上的节点数为 $O(n^3)$.

证明:对于公式 PH_n^{n+1},经过如下步骤得到 PH_n^{n+1} 的一棵反驳证明树:

(1) 对于公式 PH_n^{n+1},依次关于 $x_{1,n},x_{2,n},\ldots,x_{n+1,n}$ 做 n+1 次(1,*)-消解,得到公式 $Q_{[n+1],[n-1]}$;

(2) 对于公式 $Q_{[n+1],[n-1]}$,依次对 $d=n-1,n-2,\ldots,1,0$ 取值 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,d+1}=0,x_{n+1,d}=1$,化简后取出一个子公式,对其依次做 n 次(1,*)-消解,得到 $Q_{[n],[n-1]\backslash d}$;
注:当 $d=n-1$ 时,对应取 $x_{n+1,n-1}=1$;当 $d=0$ 时,对应取 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0$.

(3) 使用同构规则,依次将 $Q_{[n],[n-1]\backslash d}(d=n-1,\ldots,1,0)$用空子句“□”替换;

(4) 对于分枝 $x_{n+1,n-1}=x_{n+1,n-2}=\ldots=x_{n+1,1}=0$,化简公式后取出子公式 PH_{n-1}^{n}.

递归地进行,直至得到 $PH_1^2=x_{11}\wedge x_{21}\wedge(\neg x_{11}\vee\neg x_{21})$,最后做两次单位消解.

可见,证明树的节点数 $T(n)$满足递归关系:$T(n)=(n+1)+2n^2+T(n-1)$,其中包括(1,*)-消解对应的节点计数.因此,$T(n)=O(n^3)$. □

为方便阅读,用图 1 表示从 PH_n^{n+1} 到 PH_{n-1}^{n} 的证明过程.

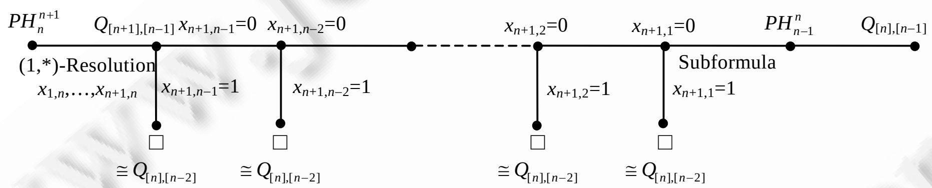

Fig.1 Proof tree from PH_n^{n+1} to PH_{n-1}^{n}

图 1 证明树(从 PH_n^{n+1} 到 PH_{n-1}^{n})

4 结束语

本文研究了鸽巢公式 PH_n^{n+1} 的极小不可满足性以及子结构同构性质,找到了公式 PH_n^{n+1} 最大可满足真值指派的标准形式.基于子结构的同构性质,如果在 DPLL 算法引入同构规则,则证明树的节点数可以降至 $O(n^3)$.得到的 PH_n^{n+1} 最大可满足真值指派的标准形式,以及有关同构性质的分析,结合 Haken 关于难例证明的方法,有助于难例的构造和证明.

References:

[1] Krishnamurthy B. Short proofs for tricky formulas. Acta Informatica, 1985,22(3):253−275.

[2] Urquhart A. The symmetry rule in propositional logic. Discrete Applied Mathematics, 1999,96−97:177−193. [doi: 10.1016/S0166-218X(99)00039-6]

[3] Chvátal V, Szemerédi T. Many hard examples for resolution. Journal of the Association for Computing Machinery, 1988,35(4):759−768. [doi: 10.1145/48014.48016]

[4] Haken A. The intractability of resolution. Theoretical Computer Science, 1985,39:297−308. [doi: 10.1016/0304-3975(85)90144-6]

[5] Urquhart A. Hard examples for resolution. Journal of the ACM, 1987,34(1):209−219. [doi: 10.1145/7531.8928]

[6] Roberts FS, Tesman B, Wrote; Feng S, Trans. Applied combinatorics (2nd ed.). Beijing: China Machine Press, 2005 (in Chinese).

[7] Atserias A, Galesi N, GavaldàR. Monotone proofs of the pigeon hole principle. In: Montanari U, Rolin J, Welzl E, eds. Proc. of the ICALP 2000. LNCS 1853, Berlin, Heideberg: Springer-Verlag, 2000. 151−162.

[8] Xu DY, Liu CY. DPLL algorithm with literal renaming strategy. Journal of Frontiers of Computer Science and Technology, 2007, 1(1):116−125 (in Chinese with English abstract).

[9] Büning HK, Lettman T. Propositional Logic: Deduction and Algorithms. Cambridge: Cambridge University Press, 1999.

[10] Büning HK, Xu DY. The complexity of homomorphisms and renamings for minimal unsatisfiable formulas. Annals of Mathematics and Artificial Intelligence, 2005,43(1-4):113−127. [doi: 10.1007/s10472-005-0422-8]

[11] Büning HK, Zhao XS. Minimal unsatisfiability: Results and open questions. In: Proc. of the Conf. on SAT 2002. Cincinati, 2002. 1−66.

[12] Xu DY. Applications of minimal unsatisfiable formulas to polynomially reduction for formulas. Journal of Software, 2006,17(5): 1204−1212 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1204.htm [doi: 10.1360/jos171204]

[13] Xu DY, Deng TY, Zhang QS. *k*-LSAT(k≥3) is NP-complete. Journal of Software, 2008,19(3):511−521 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/511.htm [doi: 10.3724/SP.J.1001.2008.00511]

[14] Davis M, Logemann G, Loveland D. A machine program for theorem proving. Communications of the ACM, 1962,5(7):394−397. [doi: 10.1145/368273.368557]

[15] Davis M, Putnam H. A computing procedure for quantification theory. Journal of the ACM, 1960,7(3):201−215. [doi: 10.1145/321033.321034]

[16] Nerode A, Shore RA. Logic for Applications. 2nd ed., New York: Springer-Verlag, 1993.

附中文参考文献:

[6] Roberts FS,Tesman B,著;冯速,译.应用组合学(第 2 版).北京:机械工业出版社,2007.

[8] 许道云,刘长云.带文字改名策略的 DPLL 算法.计算机科学与探索,2007,1(1):116−125.

[12] 许道云.极小不可满足公式在多项式归约中的应用.软件学报,2006,17(5):1204−1212. http://www.jos.org.cn/1000-9825/17/1204.htm [doi: 10.1360/jos171204]

[13] 许道云,邓天炎,张庆顺.*k*-LSAT(k≥3)是 NP 完全的.软件学报,2008,19(3):511−521. http://www.jos.org.cn/1000-9825/19/511.htm [doi: 10.3724/SP.J.1001.2008.00511]

许道云(1959－),男,贵州安顺人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为可计算分析,计算复杂性.

王晓峰(1980－),男,博士生,CCF 学生会员,主要研究领域为可计算性与计算复杂性,算法分析与设计.

韦立(1981－),男,博士生,主要研究领域为可计算性与计算复杂性.