不可满足公式的同态证明系统*

许道云+

(贵州大学 计算机科学系,贵州 贵阳 550025)

Homomorphism Proof Systems for Unsatisfiable Formulas

XU Dao-Yun+

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

+ Corresponding author: Phn: +86-851-3627649, E-mail: daoyun.gzu@263.net

Received 2003-08-29; Accepted 2004-10-09

Xu DY. Homomorphism proof systems for unsatisfiable formulas. *Journal of Software*, 2005,16(3):336–345.
DOI: 10.1360/jos160336

Abstract: A homomorphism φ of CNF formulas from H to F is a function mapping the set of literals in H to the set of literals in F and it preserves complements and clauses. If the formula H is homomorphic to the formula F, then the unsatisfiability of H implies the unsatisfiability of F. A *CNF* formula F is minimally unsatisfiable if F is unsatisfiable and the resulting formula deleting any one clause from F is satisfiable. $MU(1)$ is a class of minimally unsatisfiable formulas with the deficiency of the number of clauses and variables to be one. A triple (H,φ,F) is called a homomorphism proof from H of F if φ is a homomorphism from H to F. In this paper, a method from the basic matrix of $MU(1)$ formula is used to prove that a tree resolution proof for an unsatisfiable formula F can be transformed into a homomorphism proof from a $MU(1)$ formula for F. Whence, the homomorphism proof system from formulas in $MU(1)$ is complete, and this proof system and the tree resolution proof system can be transformed mutually in polynomial time on the size of proof.

Key words: unsatisfiable formulas; homomorphism; proof system; basic matrix; completeness

摘 要: 合取范式(CNF)公式 H 到 F 的同态φ是一个从 H 的文字集合到 F 的文字集合的映射,并保持补运算和子句映到子句.同态映射保持一个公式的不可满足性.一个公式是极小不可满足的是指该公式本身不可满足,而且从中删去任意一个子句后得到的公式可满足.$MU(1)$是子句数与变元数的差等于 1 的极小不可满足公式类.一个三元组(H,φ,F)称为 F 的一个来自 H 的同态证明,如果φ是一个从 H 到 F 的同态.利用基础矩阵的方法证明了:一个不可满足公式 F 的树消解证明,可以在多项式时间内转换成一个来自 $MU(1)$中公式的同态证明.从而,由 $MU(1)$中的公式构成的同态证明系统是完备的,并且由 $MU(1)$中的公式构成的同态证明系统与树消解证明系统之间是多项式等价的.

关键词: 不可满足公式;同态;证明系统;基础矩阵;完备性

中图法分类号: TP301 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.60463001 (国家自然科学基金); the Special Foundation for Improving Scientific Research Condition of Guizhou Province of China (贵州省高层次人才科研条件特助基金); the Government Foundation of Guizhou Province of China (贵州省省长基金)

作者简介: 许道云(1959－),男,贵州安顺人,博士,教授,主要研究领域为计算复杂性,可计算分析.

命题变元或其否定统称为文字,文字的析取称为子句,子句的合取称为合取范式(CNF).假定 $F=(c_1\wedge\ldots\wedge c_n)$为一个合取范式,有时我们将 F 表为一个子句集合$\{c_1,\ldots,c_n\}$或一个字句表$[c_1,\ldots,c_n]$,将一个子句表示为一个文字集合.出现在 F 中的变元集合和文字集合分别记为 $var(F)$,$lit(F)$.$\#var(F)$表示出现在 F 中变元的个数.$\#cl(F)$表示 F 所含的子句个数.$\#cl(F)-\#var(F)$称为公式 F 的差,记为 $d(F)$.Szeider[1]引入公式间的同态概念,以研究公式的不可满足性.合取范式公式 H 到 F 的同态φ是一个从 H 的文字集合到 F 的文字集合的映射,并保持补运算和子句映到子句.如果$\varphi(H)=F$,称 F 可以被 H 同态表示.同态保持一个公式的不可满足性,同时可以压缩公式的变元个数.因此,在利用同态方法研究公式的不可满足性时,可以降低证明的计算复杂性.从而研究不可满足公式间的同态关系具有一定的意义.

一个从 H 到 F 的同态φ称为一个限制,如果存在一个从 F 到 H 的同态ψ使得 $\psi\circ\varphi=Id_F$,其中 Id_F 为恒等映射.如果存在一个从 H 到 F 的限制,我们称 F 是 H 的一个限制.公式 F 称为公式 H 的核,如果 H 的每个限制都同构于 F.Szeider[1]证明了:(1) 一个公式的核是相互同构的;(2) 识别一个公式的核的判定问题是 co-NP-完全的.

一个公式 F 称为极小不可满足,如果 F 本身不可满足,而且从中删去任意一个子句后所得到的公式是可满足的.Papadimitriou 和 Wolfe[2]证明了:对每一个公式 F,都可以在多项式时间内转换为一个公式 $f(F)$,使得

- F 可满足当且仅当 $f(F)$可满足;
- F 不可满足当且仅当 $f(F)$极小不可满足.

可见,一个不可满足公式可以在多项式时间内转换为一个极小不可满足公式.因此,借助于极小不可满足公式研究不可满足公式具有十分重要的意义.

所有极小可满足公式类记为 MU(minimal unsatisfiable formulas).我们可以用公式的差 $d(.)$对 MU 进行分类.在文献[3,4]中,已经证明了一个结果:如果 $d(F)\le 0$,则 F 不可能是极小不可满足公式.于是,我们只对 $d(.)\ge 1$进行分类.对于 $k>0$,定义 $MU(k)=\{F\in MU|d(F)=k\}$.$MU(k)$中公式的成员判定问题是多项式时间内可解的[5],而 MU 中公式的成员判定问题却是 D^P-完全的[2].

对于 $MU(1)$中的公式,Kleine Büning 在文献[4]中给出了一个很精致的完备构造方法:基础矩阵方法.$MU(1)$中的公式可以用矩阵形式表示,这样的表示矩阵通过适当调整行(列)顺序后是一个基础矩阵,而基础矩阵可以递归构造.这表明:$MU(1)$中的公式具有良好的递归特征,这给研究 $MU(1)$中公式的结构和构造 $MU(1)$中的公式带来了方便.同时,也为利用 $MU(1)$中的公式去研究其他公式类的一些性质提供了帮助.Kleine Büning 和赵希顺在文献[6]中证明:对于给定的 $k,t\ge 1$ 和任意公式 $F\in MU(t)$,存在一个公式 $H\in MU(k)$和一个从 H 到 F 的同态ϕ使得 $\phi(H)=F$.有关公式间是否存在同态的判定问题,在文献[7]中,Kleine Büning 和许道云证明:判定问题"固定 $k,t\ge 1$,对于给定的公式 $F\in MU(t)$和 $H\in MU(k)$,是否存在一个从 H 到 F 的同态ϕ使得$\phi(H)=F$?"是 NP-完全的,即使这两个公式都是 Horn 公式.

对于一个不可满足公式 F,一个三元组(H,φ,F)称为 F 的一个来自 H 的同态证明,如果φ是一个从 H 到 F 的同态.我们知道:每一个不可满足公式 F,都可以通过树消解验证其不可满足性.形式上给出了一个树消解证明.我们记 $\prod_{tree}$表示树消解证明系统,$\prod_{MU(1)}$表示来自 $MU(1)$中公式的同态证明系统.给定一个不可满足 F,总有一个 F 的树消解证明.换言之,树消解证明系统是完备的.

假定 P 是 F 的一个树消解证明,文献[8]中,Szeider 给出了不可满足公式的一种同态证明系统,将 P 转换为 F 的一个同态证明.本文利用基础矩阵的方法,在多项式时间内,从 P 构造了一个 $MU(1)$中的公式 H 和一个同态φ,使得(H,φ,F)是 F 的一个来自于 H 的同态证明.结论表明:同态证明系统 $\prod_{MU(1)}$是完备的.

给定两个证明系统 $\prod_1$,$\prod_2$ 以及一个不可满足公式 F.如果 $P_1\in\prod_1$是 F 的一个证明,而且在多项式时间内可以将 P_1 转换为 $P_2\in\prod_2$,使 P_2 是 F 的一个证明,我们称系统 $\prod_1$ 可以被 $\prod_2$ 多项式模拟,记为 $\prod_1\le_{sim}\prod_2$.如果 $\prod_1\le_{sim}\prod_2$ 而且 $\prod_2\le_{sim}\prod_1$,则称系统 $\prod_1$ 和 $\prod_2$ 多项式等价,记为 $\prod_1\equiv_{sim}\prod_2$.本文的一个自然结论是:$\prod_{MU(1)}\equiv_{sim}\prod_{tree}$.即,树消解证明系统与来自 $MU(1)$中的公式所构成的同态证明系统之间是可以在多项式时间内相互模拟的.

1 基本知识

本节介绍一些必要的基本定义、记号和结果.

一个子句 C 可以视为一个文字的集合,一个合取范式公式 F 视为一个子句的集合或一个子句表.本文中提及的公式均指合取范式公式.变元 x 在公式 F 中正、负出现的次数分别记为 $pox(x,F)$,$neg(x,F)$,并记 $occ(x,F)=(pox(x,F),neg(x,F))$.

定义 1. 设 $F=[C_1,...,C_m]$ 是带有 n 个变元 $x_1,...,x_n$,m 个子句的公式.如下定义的 $n\times m$ 矩阵 $M_F=(a_{i,j})$ 称为 F 的表示矩阵,其中

$$a_{i,j}=\begin{cases}+, & x_i\in C_j\\ -, & \neg x_i\in C_j\\ 0, & x_i,\neg x_i\notin C_j\end{cases}\quad\text{(有时用空白表示 0).}$$

定义 2. 设 H 和 F 是公式,映射 $\varphi: lit(H)\to lit(F)$ 称为从 H 到 F 的一个同态,若对每个变元 x,$\varphi(\neg x)=\neg\varphi(x)$,而且对每个子句 $h\in H$,$\varphi(h)$ 是 F 中的一个子句.

一个公式 H 同态于另一个公式 F,如果存在一个从 H 到 F 同态.一个序对 (H,φ) 称为 F 的一个同态表示,如果 φ 是一个从 H 到 F 的同态,而且 $\varphi(H)=F$.

我们注意到:

(1) 如果公式 H 不可满足,而且 φ 是一个从 H 到 F 的同态,则 $\varphi(H)$ 不可满足,从而 F 不可满足.

(2) 如果公式 H 可满足,而且 φ 是一个从 H 到 F 的同态,此时 $\varphi(H)$ 可能不可满足.例如:取 $H=[(x\vee y),\neg x]$ 和 $F=[x,\neg x]$,考虑映射 $\varphi(x)=\varphi(y)=x$.

定义 3. 一个公式 F 称为极小不可满足,如果 F 不可满足,而且对于 F 中任一个子句 f,$F\backslash\{f\}$ 可满足.

用 CNF 公式的子句数与变元数的差或比对 CNF 公式进行分类,是对 CNF 公式进行分类的两种重要手段.这两个重要参数对于某些判定问题的复杂性有着本质的影响.对于极小不可满足公式类(MU),通常采用子句数与变元数的差(即公式差)对 MU 进行分类,记 $MU(k)=\{F\in MU\mid d(F)=k\}$,其中 $k\geq 1$.k 是极小不可满足公式类的一个重要参数.对于 MU 的成员判定问题是 D^P-完全的[2].然而,对于固定的 k,$MU(k)$ 的成员判定问题却是多项式时间内可判定的.

$MU(1)$ 是一类基本而且重要的极小不可满足公式类.我们将会看到,$MU(1)$ 中的公式具有良好的递归结构.极小不可满足的 Horn 公式必为 $MU(1)$ 中公式[4].如下的分裂定理可以将 $MU(k)(k>1)$ 中任意一个公式化归到一个 $MU(1)$ 中的公式集.

定理 1(分裂定理)[9]. 假定 $F\in MU(k)(k>1)$,而且对每个变元 x,满足条件 $pox(x,F)\geq 2$ 且 $neg(x,F)\geq 2$,则 F 可以表示为 $F=[(x\vee f_1),...,(x\vee f_s),B_x,C,B_{\neg x},(\neg x\vee g_1),...,(\neg x\vee g_t)]$,其中,$B_x$,$C$,$B_{\neg x}$ 不含 x 和 $\neg x$,并且使得 $F_x=[f_1,...,f_s,B_x,C]\in MU(k_x)$,$F_{\neg x}=[g_1,...,g_t,B_{\neg x},C]\in MU(k_{\neg x})$,其中 $1\leq k_x,k_{\neg x}<k$.

在分裂定理中,公式对 $(F_x,F_{\neg x})$ 称为 F 关于变元 x 的分裂对.分裂定理表明:$MU(k)$ 中的公式可以进行适当的分裂,降至 $MU(1)$ 中的公式.这对于利用 $MU(1)$ 中公式的一些良好性质去研究 $MU(k)$ 中的公式提供了帮助.

在文献[4]中,Davydov 和 Kleine Büning 引入了 $MU(1)$ 公式的一种完备化表示方法:基础矩阵.下面有关基础矩阵的定义表明,基础矩阵可以递归构造.

定义 4. 如下归纳定义的具有 n 行、$(n+1)$ 列的矩阵称为基础矩阵:

(1) (+–)是基础矩阵(对应最简单的极小不可满足公式 $[x,\neg x]$);

(2) 如果 B_1 是基础矩阵,则如下定义的矩阵是基础矩阵:

$$\begin{pmatrix}B_1 & 0\\ b_1 & -\end{pmatrix},$$

其中,向量 b_1 中的分量 $(b_1)_j\in\{0,+\}$,而且至少有一个正号出现;

(3) 如果 B_2 是基础矩阵,则如下定义的矩阵是基础矩阵:

$$\begin{pmatrix}+ & b_2\\ 0 & B_2\end{pmatrix},$$

其中,向量 b_2 中的分量 $(b_2)_j\in\{0,-\}$,而且至少有一个负号出现;

(4) 如果 B_1 和 B_2 是基础矩阵,则如下定义的矩阵是基础矩阵:

$$\begin{pmatrix} B_1 & 0 \\ b_1 & b_2 \\ 0 & B_2 \end{pmatrix},$$

其中,向量 b_1 中的分量 $(b_1)_j \in \{0,+\}$,而且至少有一个正号出现;向量 b_2 中的分量 $(b_2)_j \in \{0,-\}$,而且至少有一个负号出现.

我们知道:调整一个公式的表示矩阵的行(列)顺序,相当于调整公式中的变元(子句)顺序,本质上并不改变公式的可满足性.

如下定理表明:$MU(1)$中任意一个公式均可用基础矩阵的方法递归构造出来.

定理 2[4]. 公式 $F \in MU(1)$当且仅当忽略矩阵的行(列)顺序的情况下,其表示矩阵是一个基础矩阵.

关于极小不可满足公式类之间的相互同态表示,在文献[6]中,Kleine Büning 和赵希顺利用分裂定理证明了如下结论:

定理 3[6]. 对于任意固定的 $k \geq 1$,给定 $MU(t)$中的任意一个公式 F,可以在多项式时间内构造一个 $MU(k)$中的公式 H 和一个同态 φ,使得(H,φ)是 F 的一个同态表示.

特别地,对于任意固定的 $k \geq 1$,给定 $MU(1)$中的任意一个公式 F,可以在多项式时间内构造一个 $MU(k)$中的公式 H 和一个同态 φ,使得(H,φ)是 F 的一个同态表示.反之,给定 $MU(k)$中的任意一个公式 F,可以在多项式时间内构造一个 $MU(1)$中的公式 H 和一个同态 φ,使得(H,φ)是 F 的一个同态表示.

定义 5. 假定 $C_1 = (x \vee C_1')$, $C_2 = (\neg x \vee C_2')$ 为两个子句,子句 $C_1' \vee C_2'$ 称为 C_1 和 C_2 关于变元 x 的消解子句.

我们知道:每个不可满足公式 F,均可以通过有限次消解产生一个空子句.请注意:消解产生空子句的过程中,可能只用到 F 中的部分子句.

有关图论的术语和记号请参见文献[10].一棵规则二叉树 $T = (V, E)$ 是指树中每个枝结点恰好有两个孩子结点.由于每次消解只取两个子句,所以消解产生空子句的过程可以联系到一棵规则二叉树.在此二叉树上,叶结点用 F 中的子句标记,每个枝结点用其两个孩子结点所标记的子句的消解子句进行标记.对应的两条边上用相应的消解变元所对应的一对互补文字分别标记.最后,根结点用空子句标记.由此产生的标记树称为公式 F 的一棵消解树.请注意:一个不可满足公式的消解树不一定唯一.由消解树形成公式的一个形式化证明称为树消解证明.

设 $F = [(x \vee f),(\neg x \vee g_1),...,(\neg x \vee g_m),F_{rest}]$,其中($F$ 的其余部分) F_{rest} 中不含变元 x 的出现,称公式

$$F' = [(f \vee g_1),...,(f \vee g_m),F_{rest}]$$

为 F 关于 x 的(1,*)-消解.特别地,当 m=1 时,称公式 $F' = [(f \vee g_1),F_{rest}]$ 为 F 关于 x 的(1,1)-消解.

容易证明:$MU(k)$关于(1,*)-消解是封闭的.在文献[4]中,已经证明:如果 F 是 $MU(1)$中的一个公式,则存在一个变元 x 使得 $occ(x,F)$=(1,1).即,至少有一个变元恰好一正一负地出现在公式的两个子句中.由(1,1)-消解的封闭性,$MU(1)$中的公式可以用(1,1)-消解得到空子句.这表明:对于 $MU(1)$中的公式 F,如果将每次(1,1)消解的所用到的变元对应到消解树 T 上相应的枝结点,则 T 上的不同枝结点对应于不同的变元.

定义 6. 假定 F 是一个不可满足公式,T 是一棵规则二叉树,结点标记函数 λ_{cl} 将每个结点 $v \in V(T)$ 映射到一个子句,边标记函数 λ_{lit} 将每条边 $e \in E(T)$ 映射到一个文字.我们称四元组 $\Gamma = (T, \lambda_{cl}, \lambda_{lit}, F)$ 为公式 F 的树消解证明,其中:

(1) $\lambda_{cl}(v_0) = \square$(空子句)($v_0$ 是 T 的根结点);

(2) $\lambda_{cl}(v) \in F$ (v 是 T 的叶结点);

(3) 对于 T 的枝结点 v 及其左孩子 v_l 和右孩子 v_r, $\lambda_{cl}(v)$ 是 $\lambda_{cl}(v_l)$ 和 $\lambda_{cl}(v_r)$ 关于某个变元 x 的消解子句.而且,如果 $x \in \lambda_{cl}(v_l)$,则 $\lambda_{lit}(v,v_l) = x$ 且 $\lambda_{lit}(v,v_r) = \neg x$;如果 $\neg x \in \lambda_{cl}(v_l)$,则 $\lambda_{lit}(v,v_l) = \neg x$ 且 $\lambda_{lit}(v,v_r) = x$.

对于一个不可满足公式 F 的树消解证明 $(T, \lambda_{cl}, \lambda_{lit}, F)$,我们可以进一步要求:在消解树的从根结点到每个叶结点的路径上,消解所用到的变元互不相同[11].因此,在以下的讨论中,我们总是假设:在消解树的从根结点到每个叶结点的路径上,消解所用到的变元互不相同.引用此假定的目的是后面叙述方便.

2 *MU*(1)公式的树表示

为了研究 *MU*(1)中公式的结构与树消解证明之间的关系,本节给出 *MU*(1)中公式的一种树型结构表示.

由基础矩阵的定义可知:我们可以将一个基础矩阵与一棵带有标记函数的规则二叉树相关联.为此,对应于定义 4 中的 3 种归纳情形,我们用如下方法构造一棵带标记函数的规则二叉树,使之与一个基础矩阵相对应.我们需要如下成分:

(1) 一棵规则二叉树: $T=(V,E)$;

(2) 结点标记函数 ψ_{cl} :将 T 上的一个结点映射到一个子句;

(3) 边标记函数 ψ_{lit} :将 T 上的一条边映射到一个文字.

定义 4′. 如下归纳定义的具有 n 枝结点、(n+1)叶结点的标记二叉树 (T,ψ_{cl},ψ_{lit}) 称为基础标记二叉树:

(1) (T,ψ_{cl},ψ_{lit}) 是基础标记二叉树,其中,

(1.1) $T=(V,E), V=\{v,u_1,u_2\}, E=\{(v,u_1),(v,u_2)\}$,$v$ 是 T 的根结点;

(1.2) 引入一个新变元 x 标记结点 v,定义 $\psi_{cl}(u_1)=\{x\}$, $\psi_{cl}(u_2)=\{\neg x\}$, $\psi_{cl}(v)=\square$(空子句);

(1.3) 定义 $\psi_{lit}(v,u_1)=x$, $\psi_{lit}(v,u_2)=\neg x$.

如图 1 所示.

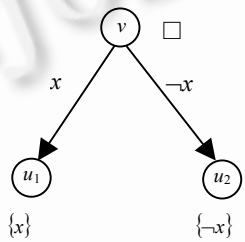

Fig.1

图 1

(2) 如果 $(T_1,\psi'_{cl},\psi'_{lit})$ 是基础标记二叉树,则如下定义的标记二叉树 (T,ψ_{cl},ψ_{lit}) 是基础标记二叉树.

(2.1) $T=(V,E), V=V(T_1)\cup\{v_0,u_0\}, E=E(T_1)\cup\{(v_0,v),(v_0,u_0)\}$,$v$ 是 T_1 的根结点, v_0, u_0 为新结点,并且 v_0 是 T 的根结点;

(2.2) 引入一个新变元 x 标记结点 v_0,定义 $\psi_{lit}(v_0,v)=x$, $\psi_{lit}(v_0,u_0)=\neg x$;

(2.3) 定义 $\psi_{cl}(v)=\{x\}, \psi_{cl}(u_0)=\{\neg x\}, \psi_{cl}(v_0)=\square$;

(2.4) 在 T_1 中至少取一个叶结点 u:定义 $\psi_{cl}(u)=\psi'_{cl}(u)\cup\{x\}$,而且对于从 v 到 u 的路径上每一个枝结点 w,定义 $\psi_{cl}(w)=\psi'_{cl}(w)\cup\{x\}$;

(2.5) 上述定义之外的每个结点 w:定义 $\psi_{cl}(w)=\psi'_{cl}(w)$.

(3) 如果 $(T_2,\psi'_{cl},\psi'_{lit})$ 是基础标记二叉树,则如下定义的标记二叉树 (T,ψ_{cl},ψ_{lit}) 是基础标记二叉树.

(3.1) $T=(V,E), V=V(T_2)\cup\{v_0,u_0\}, E=E(T_2)\cup\{(v_0,v),(v_0,u_0)\}$,$v$ 是 T_2 的根结点, v_0, u_0 为新结点,并且 v_0 是 T 的根结点;

(3.2) 引入一个新变元 x 标记结点 v_0,定义 $\psi_{lit}(v_0,u_0)=x$, $\psi_{lit}(v_0,v)=\neg x$;

(3.3) 定义 $\psi_{cl}(u_0)=\{x\}, \psi_{cl}(v)=\{\neg x\}, \psi_{cl}(v_0)=\square$;

(3.4) 在 T_2 中至少取一个叶结点 u:定义 $\psi_{cl}(u)=\psi'_{cl}(u)\cup\{\neg x\}$,而且对于从 v 到 u 的路径上每一个枝结点 w,定义 $\psi_{cl}(w)=\psi'_{cl}(w)\cup\{\neg x\}$;

(3.5) 上述定义之外的每个结点 w:定义 $\psi_{cl}(w)=\psi'_{cl}(w)$.

(4) 如果 $(T_1,\psi'_{cl},\psi'_{lit}), (T_2,\psi'_{cl},\psi'_{lit})$ 是基础标记二叉树,而且 $V(T_1)\cap V(T_2)=\varnothing$.即,两棵标记树上引入的变元集合不相交,则如下定义的标记二叉树 (T,ψ_{cl},ψ_{lit}) 是基础标记二叉树.

(4.1) $T=(V,E), V=V(T_1)\cup V(T_2)\cup\{v_0\}, E=E(T_1)\cup E(T_2)\cup\{(v_0,v'),(v_0,v'')\}$,$v'$ 是 T_1 的根结点,v'' 是 T_2 的根结点, v_0 为新结点,并且 v_0 是 T 的根结点;

(4.2) 引入一个新变元 x 标记结点 v_0,定义 $\psi_{lit}(v_0,v')=x$, $\psi_{lit}(v_0,v'')=\neg x$;

(4.3) 定义 $\psi_{cl}(v')=\{x\}$, $\psi_{cl}(v'')=\{\neg x\}$, $\psi_{cl}(v_0)=\square$;

(4.4) 在 T_1 中至少取一个叶结点 u':定义 $\psi_{cl}(u')=\psi'_{cl}(u')\cup\{x\}$,而且对于从 v'到 u'的路径上每一个枝结点 w',定义 $\psi_{cl}(w')=\psi'_{cl}(w')\cup\{x\}$;

(4.5) 在 T_2 中至少取一个叶结点 u'':定义 $\psi_{cl}(u'')=\psi'_{cl}(u'')\cup\{\neg x\}$,而且对于从 v''到 u''的路径上每一个枝结点 w'',定义 $\psi_{cl}(w'')=\psi'_{cl}(w'')\cup\{\neg x\}$;

(4.6) 上述定义之外的每个结点 w:如果 w 是 T_1 中的结点,定义 $\psi_{cl}(w)=\psi'_{cl}(w)$;如果 w 是 T_2 中的结点,定义 $\psi_{cl}(w)=\psi''_{cl}(w)$.

比较定义 4 和定义 4′,可以看出:基础标记二叉树是基础矩阵的一个树型版本.由定义 4′可知,在基础标记二叉树上,每一个枝结点对应不同的变元.我们可以通过标记函数 ψ_{lit} 记录下相应的变元.由定理 2,给定一个 $MU(1)$中的公式 $H=[C_1,C_2,...,C_{n+1}]$,对应有一棵带有 n 个枝结点、n+1 个叶结点的基础标记二叉树 (T,ψ_{cl},ψ_{lit}).通过标记函数 ψ_{cl} 在叶结点集合上的限制,叶结点集合与子句集合 $\{C_1,C_2,...,C_{n+1}\}$ 一一对应.定义 4′中标记函数 ψ_{cl} 在枝结点集合上的限制,刻画了枝结点的两个孩子结点上所标记的子句的消解子句,并通过标记函数 ψ_{lit} 记录了相应的消解变元.

我们可以通过如下例子观察公式、基础矩阵、基础标记二叉树之间的关系.

例 1:考虑 $MU(1)$中的公式 $H=[(x_1\vee x_2),\neg x_1,(\neg x_2\vee x_3),(x_4\vee x_5),(\neg x_3\vee\neg x_4\vee x_5),\neg x_5]$.

(1) H 的基础矩阵为

$$M=\begin{pmatrix} + & - & & & & & \\ + & 0 & - & & & & \\ 0 & 0 & + & 0 & - & 0 & \\ & & & + & - & & \\ & & & + & + & - & \end{pmatrix}\begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{matrix}.$$

(2) H 的基础标记二叉树如图 2 所示(图中数字 i 代表变元 x_i, $-i$ 代表文字 $\neg x_i$).

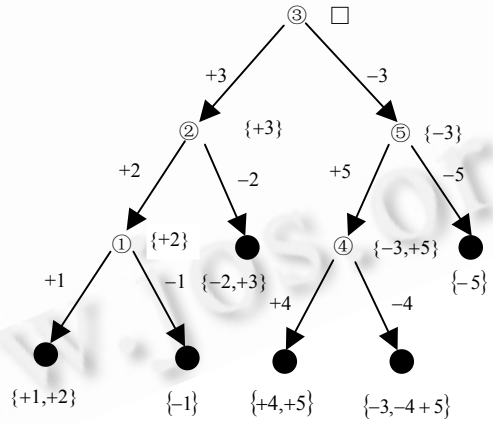

Fig.2

图 2

为方便阅读,图 2 中枝结点标号用每次引入的新变元的下标数字进行标识,它恰好对应于对子句进行消解时的消解变元.一个 $MU(1)$中的公式 H 对应的基础标记二叉树具有如下重要特征:

(1) 枝结点上所标识的变元互不相同.

(2) 基础标记二叉树就是公式 H 的一棵消解树,并且消解变元互不相同.

反之,由于基础标记二叉树与基础矩阵相对应,由定理 2,一棵基础标记二叉树对应 $MU(1)$中的一个公式.对于一个不可满足公式 $F=\{C_1,C_2,...,C_m\}$,我们总可以用树消解证明方法得到一个空子句.即,从 F 的一个子句子集可以消解出空子句.不妨设该子句子集为 $F'=\{C_1,C_2,...,C_{n+1}\}$,并且可以保证其消解树中从根结点到每一个叶

结点的路径上消解变元互不相同.但是,不同子树上可能出现相同的消解变元.

我们的想法是:在 $F'=\{C_1,C_2,...,C_{n+1}\}$ 的消解树上,恰好有 n 个枝结点(分别用消解变元(可能相同)标识),有 n+1 个叶结点(分别用 $C_1,C_2,...,C_{n+1}$ 标记).我们重新引入 n 个新变元,分别替代 n 个枝结点上的消解变元,目的是使不同枝结点对应不同消解变元.替代后,消解树变成一棵基础标记二叉树,自然产生一个 $MU(1)$中的公式 H,由变元的替代关系自然生成一个从 H 到 F'的同态映射φ.显然,φ是一个从 H 到 F 的同态映射.

我们用如下例子来理解上述思想.

例 2:考虑公式 $F=[(x\vee y),(\neg x\vee y),(x\vee\neg y),(\neg x\vee\neg y)]$.

(1) F 的表示矩阵为

$$M=\begin{pmatrix}+ & - & + & - \\ + & + & - & -\end{pmatrix}\begin{matrix}x\\ y\end{matrix}.$$

(2) F 的消解树如图 3 所示.

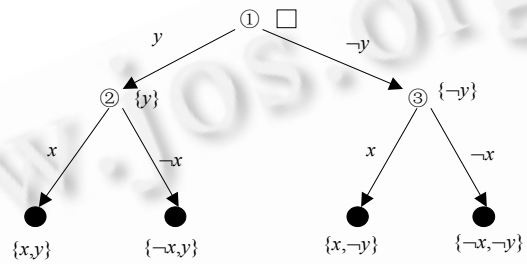

Fig.3
图 3

请注意:枝结点 2 和枝结点 3 对应的消解变元都是 x.

(3) 为了使不同枝结点对应的消解变元不相同,我们引入一个新变元 z 取代枝结点 3 对应的消解变元 x.得到如图 4 所示的基础标记二叉树.

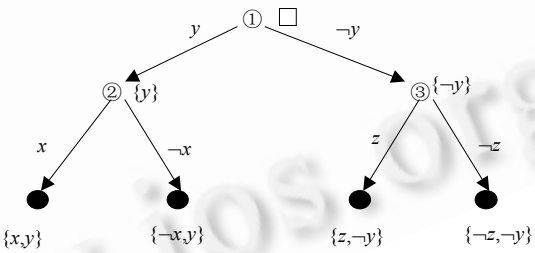

Fig.4
图 4

(4) 该基础标记二叉树对应的基础矩阵为

$$M'=\begin{pmatrix}+ & - & & \\ + & + & - & - \\ & & + & -\end{pmatrix}\begin{matrix}x\\ y\\ z\end{matrix}.$$

对应 $MU(1)$中的公式 $H=[(x\vee y),(\neg x\vee y),(\neg y\vee z),(\neg y\vee\neg z)]$.

(5) 我们定义从 H 到 F 的同态φ如下:

$$\varphi(x)=\varphi(z)=x,\varphi(y)=y,\varphi(\neg x)=\varphi(\neg z)=\neg x,\varphi(\neg y)=\neg y.$$

3 同态证明系统

对于 F 的一个树消解证明 $\Gamma=(T,\lambda_{cl},\lambda_{lit},F)$,我们定义该证明的大小为 $size(\Gamma)=|V(T)|+E(T)$.由前一节中

对 $MU(1)$中公式的基础标记二叉树的表示方法,我们有:

定理 4. 对于给定的不可满足公式 F 和 F 的一个树消解证明 $\Gamma=(T,\lambda_{cl},\lambda_{lit},F)$,在多项式时间内可以将 $\Gamma=(T,\lambda_{cl},\lambda_{lit},F)$ 转换成 F 的一个同态证明(H,φ,F),其中,H 是 $MU(1)$中的公式.

证明:假定 $F=[C_1,...,C_m]$ 是一个不可满足公式,$\Gamma=(T,\lambda_{cl},\lambda_{lit},F)$ 是 F 的一个树消解证明,对应的消解树为 $(T,\lambda_{cl},\lambda_{lit})$,则 T=(V,E)是一棵规则二叉树.不妨设 T 有 n 个枝结点,从而 T 有 n+1 个叶结点,2n 条边.可以进一步假定:消解树的从根结点到每一个叶结点的路径上所标记的文字对应的变元互不相同.

由树消解证明的结构,存在 F 中的 n+1 子句(不妨设为 $F'=[C_1,...,C_{n+1}]$, $n+1\le m$)作为 $(T,\lambda_{cl},\lambda_{lit})$ 中的叶结点标记子句.对于 T=(V,E)中每一个枝结点 v,恰好有两个孩子结点 v_l (左孩子)和 v_r (右孩子),并且对应有一个变元 x_v (消解变元),使得如下关系成立:

(1) $\lambda_{cl}(v_l)=(x_v\vee c_1),\lambda_{cl}(v_r)=(\neg x_v\vee c_2),\lambda_{cl}(v)=(c_1\vee c_2)$;

(2) $\lambda_{lit}(v,v_l)=x_v,\lambda_{lit}(v,v_r)=\neg x_v$.

或

(1′) $\lambda_{cl}(v_l)=(\neg x_v\vee c_1),\lambda_{cl}(v_r)=(x_v\vee c_2),\lambda_{cl}(v)=(c_1\vee c_2)$;

(2′) $\lambda_{lit}(v,v_l)=\neg x_v,\lambda_{lit}(v,v_r)=x_v$.

我们现在引进一个识别函数 f: 将 T=(V,E)中的枝结点映射到一个消解变元.即, $f(v)=x_v$.请注意:在 $(T,\lambda_{cl},\lambda_{lit})$ 中,一个叶结点 u、从根结点 v_0 到 u 的路径 P_u 以及 $F'=[C_1,...,C_{n+1}]$ 中的一个子句 $\lambda_{cl}(u)$,这三者之间是一一对应的.设 $P_u=v_0v_1v_2...v_pu$, $\lambda_{cl}(u)=\{L_1,...,L_q\}$,则 $\{L_1,...,L_q\}\subseteq\{\lambda_{lit}(v_0,v_1)$, $\lambda_{lit}(v_1,v_2)$,…, $\lambda_{lit}(v_{p-1},v_p)$, $\lambda_{lit}(v_p,u)\}$,而且 $\lambda_{lit}(v_p,u)\in\{L_1,...,L_q\}$.

相应地,我们得到一个变元序列: $f(v_0)f(v_1)...f(v_p)$,并且对于任意的 $0\le i\ne j\le p$, $f(v_i)\ne f(v_j)$.

我们现在引入 n 个新变元 $y_1,...,y_n$,构造一个 $MU(1)$中的公式 $H=[C_1^*...C_{n+1}^*]$ 和一个从 H 到 T 的 F'同态如下:

(1) 定义子句 $C_i^*(1\le i\le n+1)$.

对 $F'=[C_1,...,C_{n+1}]$ 中的每一个子句 C_j ,设 $C_j=\{L_1,...,L_q\}$ 对应 T 中一个叶结点 u,u 对应于 T 中一条根结点 v_0 到 u 的路径 $P_u=v_0v_1v_2...v_pu$,以及一个变元序列 $f(v_0)f(v_1)...f(v_p)$.

让引入的 n 个新变元 $y_1,...,y_n$ 与 T 中的 n 个枝结点 $v_1',...,v_n'$ 相对应.即,定义一个一对一函数 g,使 $g(v_i')=y_i(i=1,2,...,n)$.

不妨假设:文字序列 $\lambda_{lit}(v_0,v_1)$, $\lambda_{lit}(v_1,v_1)$,…, $\lambda_{lit}(v_{p-1},v_p)$, $\lambda_{lit}(v_p,u)$ 与文字序列 $L_1,...,L_q$ 的顺序相一致,则存在一个子序列: $\lambda_{lit}(v_{t_1},v_{t_1+1})$, $\lambda_{lit}(v_{t_2},v_{t_2+1})$,…, $\lambda_{lit}(v_{t_{q-1}},v_{t_{q-1}+1})$, $\lambda_{lit}(v_p,u)$ 与 $L_1,...,L_q$ 相同. $v_{t_1},...,v_{t_{q-1}},v_p$ 均为枝结点,我们记 $v_{t_1}=v'_{s_1},...,v_{t_{q-1}}=v'_{s_{q-1}},v_p=v'_{s_q}$,则有 $g(v_{t_1})=y_{s_1}$, $g(v_{t_2})=y_{s_2}$,…, $g(v_{t_{q-1}})=y_{s_{q-1}}$, $g(v_p)=y_{s_q}$.对于 $1\le j\le q$, 如果 L_j 是正文字,则定义文字 $L_j^*=y_{s_j}$,否则定义 $L_j^*=\neg y_{s_j}$.

最后,定义子句 $C_i^*=\{L_1^*,...,L_q^*\}$.

(2) 用上面(1)中的方法,逐一定义每一个子句,最终构成公式 $H=[C_1^*...C_{n+1}^*]$.由于消解树上每一个枝点对应不同的变元,由基础标记二叉树的定义,H 是 $MU(1)$中的公式.

(3) 由函数 f 和 g,我们可以定义一个从 H 到 F'的同态映射 $\varphi:\varphi(y_i)=f(g^{-1}(y_i))$,其中 g^{-1} 为 g 的逆函数.

扩充φ到负文字的定义: $\varphi(\neg y_j)=\neg\varphi(y_j)(1\le j\le n)$.我们有:$\varphi$是从 H 到 F'的一个同态.显然,φ是一个从 H 到 F 的同态映射(因为 F'是由 F 的部分子句构成的).

由于树 T 只有 n 个枝结点、n+1 个叶结点、2n 条边,从而 F'中每个子句的长度(所含文字的个数)至多为 n 个.因此,上述 H 和φ可以在 $O(n^2)$时间内构造出来. □

推论 1. 由 $MU(1)$中的公式构成的同态证明系统是完备的.即,对于任意一个不可满足公式,均存在一个来自 $MU(1)$中公式的同态证明.

推论 2. 由 $MU(1)$中的公式构成的同态证明系统与树消解证明系统之间是多项式等价的.即,对于给定的不可满足公式,两种不同的形式化证明均可以在多项式时间内相互转换.

为了将定理 4 中的证明方法加以应用,我们给出如下例子:

例 3:考虑不可满足公式 $F=\{x_1\vee x_2,x_2\vee x_3,x_3\vee x_4,\neg x_1\vee\neg x_3,\neg x_2\vee\neg x_4,\neg x_2\vee\neg x_3\}$.$F$ 的一个树消解证明如图 5 所示(为方便阅读,消解树中枝结点用消解变元直接标记):

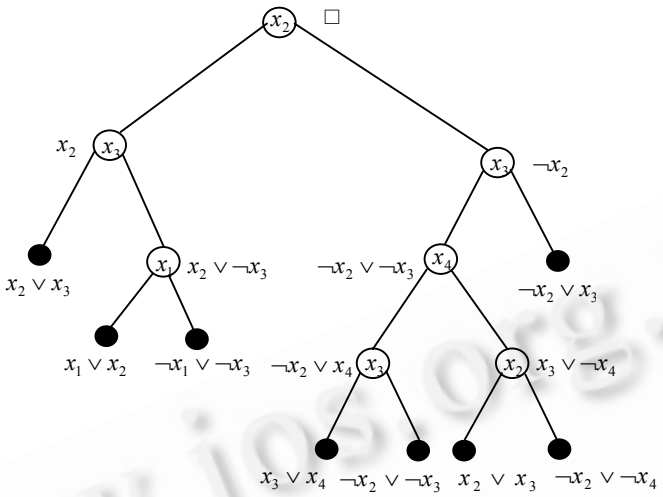

Fig.5

图 5

图 5 中,由枝结点到左、右孩子结点的边分别用消解变元的正、负文字标记(由于具有左正右负的规律性,故在图中未标出).可见,消解树 T 中有 7 个枝结点(每一次消解对应 T 的一个枝结点,枝结点与消解变元相对应),T 中有 8 个叶结点(分别用原始子句标记叶结点,有子句被重复使用,用每次消解得到的中间子句标记枝结点).

定理 4 中的证明方法是:不同的枝结点必须对应不同的消解变元.为此,重复出现的消解变元需要引入新的变元以示区别.为方便起见,重新引入一组新变元,新变元个数与消解树的枝结点个数相等,在消解树上依次用新变元替换该消解变元及其与之关联的标记子句中的出现.由此形成一个 $MU(1)$公式,并由新变元与所替换的消解变元之间的关系构造同态映射.

为了观察变元替换过程,我们引入 7 个新变元 $y_1,...,y_7$,分别替换上述消解树中的枝结点中的消解变元和相关联的子句,替换后的结果如图 6 所示.

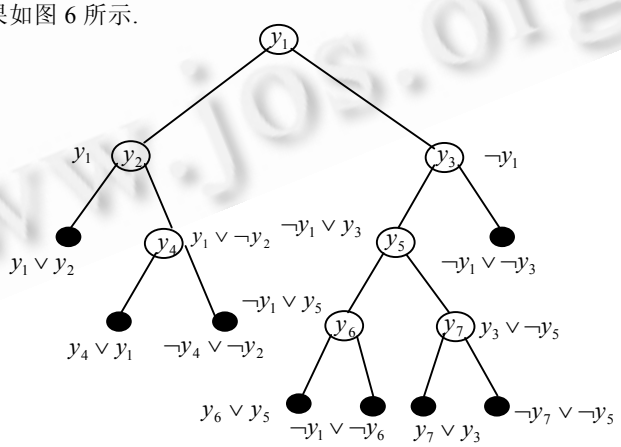

Fig.6

图 6

由图 6,我们可以得到一个 $MU(1)$公式:

$$H=\{y_1\vee y_2,y_1\vee y_4,y_3\vee y_7,y_5\vee y_6,\neg y_1\vee\neg y_3,\neg y_1\vee\neg y_6,\neg y_2\vee\neg y_4,\neg y_5\vee\neg y_7\}.$$

比较图 5 和图 6 中相同位置上消解变元的对应关系,我们可以得到从 H 到 F 的同态映射 φ:

$\{y_1,y_7\}\mapsto x_2,\{y_2,y_3,y_6\}\mapsto x_3,y_4\mapsto x_1,y_5\mapsto x_4,\ \{\neg y_1,\neg y_7\}\mapsto \neg x_2,\{\neg y_2,\neg y_3,\neg y_6\}\mapsto \neg x_3,\neg y_4\mapsto \neg x_1,\neg y_5\mapsto \neg x_4$.

4 结论与进一步工作

本文将基础矩阵转换为基础标记二叉树,将 $MU(1)$中的公式及其消解证明与基础标记二叉树相联系.利用基础标记二叉树的方法,证明了:一个不可满足公式 F 的树消解证明,可以在平方次时间内转换成一个来自 $MU(1)$中公式的同态证明.从而,由 $MU(1)$中的公式构成的同态证明系统是完备的,并且由 $MU(1)$中的公式构成的同态证明系统与树消解证明系统之间是多项式等价的.进一步的工作是:对于给定的不可满足公式,如何利用 $MU(1)$中公式的特殊结构以及同态转换,寻找较优的树消解证明.其主要思想是:限制每个变元出现的次数研究树消解证明.对于给定的一个 CNF 公式,我们总可以在多项式时间内将其转换为一个 3-CNF 公式.进一步地,对于一个 3-CNF 公式,通过适当引进新变元,可以将其转换为另一个 3-CNF 公式,使其每个变元出现的次数不超过 4 次.因此,我们可以在变元次数受限的情况下使用本文中的方法研究树消解证明的优化问题.

References:

[1] Szeider S. Homomorphisms of conjunctive normal forms. Discrete Applied Mathematics, 2003,130(2):351−365.

[2] Papadimitriou CH, Wolfe D. The complexity of facets resolved. Journal of Computer and System Sciences, 1988,37(1):2−13.

[3] Aharoni R. Minimal non-two-colorable hypergraphs and minimal unsatisfiable formulas. Journal of Combinatorial Theory, 1996,43(A):196−204.

[4] Davydov G, Davydova I, Büning HK. An efficient algorithm for the minimal unsatisfiability problem for a subclass of CNF. Annals of Mathematics and Artificial Intelligence, 1998,23(3-4):229−245.

[5] Fleischner H, Kullmann O, Szeider S. Polynomial-Time recognition of minimal unsatisfiable formulas with fixed clause-variable difference. Theoretical Computer Science, 2002,289(1):503−516.

[6] Büning HK, Zhao XS. Polynomial time algorithms for computing a representation for minimal unsatisfiable formulas with fixed deficiency. Information Processing Letters, 2002,84(3):147−151.

[7] 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.

[8] Szeider S. How to Prove Unsatisfiability by Homomorphisms. Discrete Applied Mathematics, 2003,130(2):351−365.

[9] Büning HK. On subclasses of minimal unsatisfiable formulas. Discrete Applied Mathematics, 2000,107(1-3):83−98.

[10] Bondy J A, Murty USR. Graph Theroy with Applications. London: Macmillan, 1996.

[11] Urquhart A. The complexity of propositional proofs. The Bulletin of Symbolic Logic, 1995,1(4):425−467.