ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.5, May 2006, pp.1204−1212
DOI: 10.1360/jos171204

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

极小不可满足公式在多项式归约中的应用*

许道云+

(贵州大学 计算机科学系,贵州 贵阳 550025)

Applications of Minimal Unsatisfiable Formulas to Polynomially Reduction for Formulas

XU Dao-Yun+

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

+ Corresponding author: Phn: +86-851-3627649, E-mail: dyxu@gzu.edu.cn

Xu DY. Applications of minimal unsatisfiable formulas to polynomially reduction for formulas. *Journal of Software*, 2006,17(5):1204−1212. http://www.jos.org.cn/1000-9825/17/1204.htm

Abstract: A conjunctive normal form (CNF) formula F is minimal unsatisfiable if F is unsatisfiable and the resulting formula removing any clause from F is satisfiable. (r,s)-CNF is a subclass of CNF in which each clause of formula has exactly r distinct literals and every variable occurs at most s times. The corresponding satisfiable problem (r,s)-SAT means that the instances are restricted in (r,s)-CNF. For positive integer r≥3, there exists a critical function $f(r)$ such that all formulas in (r,$f(r)$)-CNF are satisfiable, but (r,$f(r)$+1)-SAT is already NP-Complete. It is open whether or not the function f is computable. One can only estimate some bounds of $f(r)$ except for $f(3)=3$ and $f(4)=4$. In this paper, the applications of minimal unsatisfiable formulas are described for transformations between CNF formulas. A new algorithm is presented to introduce less new variables in transformation from CNF to 3-CNF, which for clauses with length l(>3) only $\left\lceil \frac{l}{2} \right\rceil$ new variables are introduced. The principle and method for transforming CNF to (r,s)-CNF and constructing unsatisfiable formulas in (r,s)-CNF are presented.

Key words: minimal unsatisfiable formula; SAT-problem; polynomially reduction; NP-completeness; construction of formula

摘 要: 合取范式(CNF)公式 F 是极小不可满足的,如果 F 不可满足,并且从 F 中删去任意一个子句后得到的公式可满足,(r,s)-CNF 是限制 CNF 公式中每个子句恰有 r 个不同的文字,且每个变元出现的次数不超过 s 次的公式类,对应的满足性问题(r,s)-SAT 指实例公式限制于(r,s)-CNF.对于正整数 r≥3,有一个临界函数 $f(r)$,使得(r,$f(r)$)-CNF 中的公式都是可满足的,而(r,$f(r)$+1)-SAT 却是 NP-完全的.函数 f 是否可计算是一个开问题,除了知道 $f(3)=3$,$f(4)=4$ 外,只能估计 $f(r)$的界.描述了极小不可满足公式在 CNF 公式类之间转换中的作用.为使转换过程中引入较少的新变元,给出了 CNF 公式到 3-CNF 公式的一种新的转换方法,对于长度为 l(>3)的子句,仅需引入 $\left\lceil \frac{l}{2} \right\rceil$

* 本文为 2005 年中国计算机大会推荐优秀论文.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 (贵州省高层次人才科研条件特助基金); the Special Foundation of Government of Guizhou Province (贵州省省长基金)

Received 2005-06-15; Accepted 2005-12-16

个新变元.并且,给出了 CNF 到(*r*,*s*)-CNF 公式转换以及(*r*,*s*)-CNF 中不可满足公式构造的原理和方法.

关键词: 极小不可满足公式;问题;多项式归约;NP-完全;公式构造
中图法分类号: TP18 文献标识码: A

一个合取范式(CNF)公式 $F=C_1\wedge\ldots\wedge C_m$ 称为极小不可满足公式(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 后得到的公式可满足.用 $CNF(n,m)$表示含有的 n 个变元、m 个子句的 CNF 公式类.通常,我们是用 $m-n$(称为公式差)对 MU 进行分类的.已经知道,如果 F 为一个 MU 公式,则公式差(记为 $d(F)$)为一个正整数[1].因此,只对公式差 $d(\cdot)>0$ 进行分类,并记 $MU(k)=\{F\in MU|d(F)=k\}$.Kleine Büning H.等人给出了 $MU(1)$和 $MU(2)$中公式的标准型[1,2].特别对 $MU(1)$中的公式给出了一种归纳构造方法,并用所谓的基础矩阵予以表示[1].$MU(1)$公式具有许多良好的性质,如至少有一个变元恰好一正一负出现在一对子句中,取这两个子句进行消解后的公式仍然在 $MU(1)$中.这表明存在一种确定性算法,对 $MU(1)$公式进行消解证明.在文献[3]中,我们给出了一个同态证明方法:对于每一个不可满足公式 F,存在一个 $MU(1)$公式 H,使得 H 可以同态映射到 F.从而,我们可以从 H 的消解证明诱导出 F 的一个消解证明.进一步地,对 $MU(k)$中的公式,我们可以借助于有关极小不可满足公式的分裂技术[1],将一个 $MU(k)$公式分解为若干个 $MU(1)$公式.这对于利用 $MU(1)$公式的消解证明去研究 $MU(k)$公式的消解证明提供了一些有用的手段.

一个子句的长度是指该子句所含文字的个数,一个变元在一个公式中出现的次数是指相应的正、负文字出现的次数之和.我们用(*r*,*s*)-CNF 表示这样的 CNF 公式类:公式中每个子句的长度恰为 r,每个变元出现的次数不超过 s.(*r*,*s*)-SAT 表示实例取自于(*r*,*s*)-CNF 的满足性判定问题.在文献[4]中,C.Tovey 对 3-SAT 问题的实例进行了限制,证明了(3,4)-SAT 是 NP-完全的.在文献[4–7]中,作者对形如(*r*,*s*)-SAT 的简化的 NP-完全类作了一些研究.研究表明,(*r*,*s*)-SAT 的 NP-完全性与(*r*,*s*)-CNF 中是否含有不可满足公式密切相关:对于任意的 $r,s\geq 3$,如果(*r*,*s*)-CNF 中存在一个不可满足公式,则(*r*,*s*)-SAT 是 NP-完全的.而(*r*,*r*)-CNF 中的每个公式都是可满足的[4].从而,问题(*r*,*s*)-SAT 对于 $r\geq 3$ 有一种临界现象.

考虑一个临界函数 $f(r)$,使得$(r,f(r))$-CNF 中的公式都是可满足的,而$(r,f(r)+1)$-SAT 却是 NP-完全的.由 $f(r)$的性质,$f(r)$可以表示为 $f(r)=\max\{s:(r,s)\text{-CNF}\cap UNSAT=\varnothing\}=\max\{s:(r,s)\text{-CNF}\cap MU=\varnothing\}$.

可见,对于正整数 $r\geq 3$,$f(r)\geq r$.直到现在,函数 f 是否可计算仍然是一个开问题.仅仅知道 $f(3)=3$ 和 $f(4)=4$.对于 $r\geq 5$ 的情形,相关的研究只能估计 $f(r)$的界.

由前所述,如果(*r*,*s*)-CNF 中含有一个不可满足公式,则(*r*,*s*)-SAT 是 NP-完全的.从而,构造(*r*,*s*)-CNF 中的不可满足公式,是改进 $f(r)$的上界的一种方法.在文献[5–7]中,S. Hoory 和 S. Szeider,P.Savicky 和 J. Sgall 等人分别利用不同方法对 $f(k)$的上界作了不同估计,其原理是在(*r*,*s*)-CNF 中构造不可满足公式,尽可能使 s 不断降低.在文献[7]中,S. Hoory 和 S. Szeider 将 $f(r)$修正为 $f_1(r)=\max\{s:(r,s)\text{-CNF}\cap MU(1)=\varnothing\}$.可见,$f(r)\leq f_1(r)$.S. Hoory 和 S. Szeider 利用 $MU(1)$公式可以归纳构造的原理,采用有限(下降的)整数序列的构造方法,对 $f_1(3)\sim f_1(9)$的上界作了估计,并证明 $f_1(r)$是一个可计算函数.换言之,虽然我们不能精确地计算出 $f(r)$,但可以计算出 $f(r)$的一个上界 $f_1(r)$.然而,S. Hoory 和 S. Szeider 的算法并不实用,其主要原因是:(1) 算法是非确定的;(2) 每进行一步构造,引入新变元的个数几乎翻 1 倍.因此,文献[7]中也只能在 $r\leq 9$ 内对 $f_1(r)$的上界作估计.

在本文中,我们阐述了极小不可满足公式在构造(*r*,*s*)-CNF 中不可满足公式的作用.文献[8]中给出了一个将 CNF 公式化归到 3-CNF 公式的经典方法.我们发现:在不改变公式的可满足性的前提下,转换 CNF 公式类或 3-CNF 到具有某些限制(如限制子句长度、变元出现次数等)的公式类时,在其构造中借助于某些 MU 公式的作用即可实现.其实,在将一个 CNF 公式 F 化归到一个 3-CNF 公式的过程中,对于长度大于 3 的子句 $C=(L_1\vee\ldots\vee L_p)$,通常是引入 $p-3$ 个新变元 $y_1,\ldots,y_{p-3}$,化为子句组:$(L_1\vee L_2\vee y_1),(L_3\vee\neg y_1\vee y_2),\ldots,(L_{p-2}\vee\neg y_{p-4}\vee y_{p-3}),(L_{p-1}\vee L_p\vee\neg y_{p-3})$[8].在此,公式$[y_1,(\neg y_1\vee y_2),\ldots,(\neg y_{p-4}\vee y_{p-3}),\neg y_{p-3}]$本身是一个 $MU(1)$公式.为使引入新变元个数尽可能地少,我们在本文中给出了一种新的转换方法,只需引入 $\left\lceil\frac{l}{2}\right\rceil$ 个新变元.同时,给出了一般转换原理(见后文中的引理 3 和定理 2).

本文给出了 CNF 到(r,s)-CNF 公式转换以及(r,s)-CNF 中不可满足公式构造的原理和方法.以此说明极小不可满足公式在简化的 NP-完全类研究中的作用.

1 基本知识

一个子句 C 是若干个文字的析取($C=L_1\vee L_2\ldots\vee L_n$),子句 C 可以视为一个文字的集合($C=\{L_1\vee L_2\ldots\vee L_n\}$).一个合取范式(CNF)公式(以下简称公式)$F$ 是若干子句的合取($F=C_1\wedge C_2\wedge\ldots\wedge C_m$),合取范式公式 F 可以视为一个子句的集合($F=\{C_1,C_2,\ldots,C_m\}$)或一个子句表($F=[C_1,C_2,\ldots,C_m]$).一个公式 F 的子公式是指由 F 的部分子句所构成的公式.如果一个子句含有一对互补文字,称该子句为重言子句.在一个公式中删去重言子句后,不影响公式的可满足性.只含一个文字的子句称为单位子句.一个变元 x 在一个公式 F 中的正(或负)出现,指文字 x(或文字$\neg x$)在 F 中出现.我们分别用 $pos(x,F)$和 $neg(x,F)$表示 x 在 F 中的正、负出现次数,并记 $occs(x,F)=pos(x,F)+neg(x,F)$;分别用$\#var(F)$和$\#cl(F)$表示出现在公式 F 中的变元数以及 F 所包含的子句数.$\#cl(F)-\#var(F)$称为公式 F 的子句-变元差(简称公式差),记为 $d(F)$.对于 CNF 公式 F_1 和 F_2,记 F_1+F_2 表示 $F_1\wedge F_2$.

定义 **1**. 设 $F=[C_1,C_2,\ldots,C_n]$是一个公式.称 F 是极小不可满足公式(minimal unsatisfiable formula,简记为 MU 公式),如果 F 不可满足,并且从中删去任意一个子句 $C_i(1\le i\le n)$后得到的公式可满足.

可以证明:极小不可满足公式的子句数与变元数之差(即公式差)是一个正整数[1,2].通常,我们是按公式的公式差对 MU 公式进行分类的.对于正整数 $k\ge1$,记 $MU(k)=\{F\in MU|F$ 的公式差为 $k\}$.$MU(k)$中的公式称为 $MU(k)$公式.

设公式 F 是一个带有 n 个变元 $x_1,x_2,\ldots,x_n$、m 个子句 $C_1,C_2,\ldots,C_m$ 的 CNF 公式,我们可以用一个 $n\times m$ 矩阵 $\boldsymbol{M}_F=(a_{i,j})$表示公式 F,其中:如果正文字 x_i 出现在子句 C_i 中时,$m_{i,j}=+$;如果负文字$\neg x_i$ 出现在子句 C_i 中时,$m_{i,j}=-$;否则,$m_{i,j}$为 0(一般用空白表示).设 L 为一个文字,F 是一个 CNF 公式,定义 $L\vee_{cl}F=\{L\vee f|f\in F\}$.容易证明如下引理.

引理 **1**. 设 F_1,F_2 为一对 $MU(1)$公式,$var(F_1)\cap var(F_2)=\varnothing$.假定 x 是一个新引入的变元,则公式 $F=x\vee_{cl}F'_{11}+F'_{12}+\neg x\vee_{cl}F'_{21}+F'_{22}$ 是一个 $MU(1)$.其中: $F'_{i1}+F'_{i2}=F_i$; $F'_{i1}\cap F'_{i2}=\varnothing$;且 $F'_{i1}\neq\varnothing$ (i=1,2).

证明:假定 $F_1=[f_1,\ldots,f_{t_1},f_{t_1+1},\ldots,f_{n_1}]$及 $F_2=[g_1,\ldots,g_{t_2},g_{t_2+1},\ldots,g_{n_2}]$,其中:$var(F_1)\cap var(F_2)=\varnothing$, $F'_{11}=[f_1,\ldots,f_{t_1}]$且 $F'_{21}=[g_1,\ldots,g_{t_2}](t_1,t_2\ge1)$.因此对于新变元 x,F 可以表示为如下简化矩阵:

f_1	$\ldots$	f_{t_1}	f_{t_1+1}	$\ldots$	f_{n_1}						
x	$\ldots$	x				$\neg x$	$\ldots$	$\neg x$			
						g_1	$\ldots$	g_{t_2}	g_{t_2+1}	$\ldots$	g_{n_2}

由于 $F_1,F_2\in MU(1)$,$\#var(F_1)=n_1-1$ 及$\#var(F_2)=n_2-1$,所以,$\#var(F)=n_1+n_2-1$,且 $cl(F)=n_1+n_2$.即 F 的公式差为 1.

现在验证 F 是一个 MU 公式.

首先,F 是不可满足的.如若不然,存在一个真值指派τ满足 F.如果$\tau(x)=0$,则τ满足 F_1;如果$\tau(x)=1$,则τ满足 F_2.这与 $F_1,F_2\in MU(1)$矛盾.其次,F 是极小不可满足的,即对于任意子句 $h\in F$,$F-\{h\}$可满足.我们考虑如下两种情形:

情形 1. $h=x\vee f_i(1\le i\le t_1)$或 $h=f_i(t_1+1\le i\le n_1)$.

由于 F_1 是一个 $MU(1)$公式,所以 $F_1-\{f_i\}$可满足.从而存在 $var(F_1)$上的一个真值指派τ_1 满足 $F_1-\{f_i\}$.由 F_2 为 $MU(1)$公式,$F_2-\{g_1,\ldots,g_{t_2}\}$可满足.存在 $var(F_2)$上的一个真值指派τ_2 满足 $F_2-\{g_1,\ldots,g_{t_2}\}$.我们定义一个 $var(F_1)\cup var(F_2)\cup\{x\}$上满足 $F-\{h\}$的真值指派τ为 $\tau(x)=0$,对于 $y\in var(F_1)$, $\tau(y)=\tau_1(y)$;对于 $z\in var(F_2)$, $\tau(z)=\tau_2(z)$.

情形 2. $h=x\vee g_i(1\le i\le t_2)$或 $h=g_i(t_2+1\le i\le n_2)$.

其证明与情形 1 类似. □

显然,如果 $occs(y,F_1)\le s$(对于 $y\in var(F_1)$),$occs(z,F_2)\le s$(对于 $z\in var(F_2)$),且 $t_1+t_2\le s$,则对于$\omega\in var(F)$,有 $occs(\omega,F)\le s$.进一步地,如果 F 能表示为 $\{(x\vee f_1),\ldots,(x\vee f_{t_1}),f_{t_1+1},\ldots,f_{n_1},(\neg x\vee g_1),\ldots,(\neg x\vee g_{t_2}),g_{t_2+1},g_{n_2}\}$ (其中 $t_1,t_2\ge1$),使得 $F_1=[f_1,\ldots,f_{t_1},f_{t_1+1},\ldots,f_{n_1}]$和 $F_2=[g_1,\ldots,g_{t_2},g_{t_2+1},\ldots,g_{n_2}]$ 皆为 $MU(1)$公式,$var(F_1)\cap var(F_2)=\varnothing$,且对于固定的 $k>1$,如果 F 中每个子句 C 的长度均为 k,则 $F\in(k,s)$-CNF$\cap MU(1)$.请注意,此时 $f_1,\ldots,f_{t_1},g_1,\ldots,g_{t_2}$ 均为长度为

k–1 的子句.

引理 1 启示 $MU(1)$公式可以逐步构造.$MU(1)$公式的结构与如下归纳定义的矩阵有密切关系:

定义 **2**(基础矩阵)[2]. 如下归纳定义的带有 n 行、(n+1)列的矩阵称为基础矩阵:

(1) (+ –)是基础矩阵;

(2) 如果 $\boldsymbol{B}_1$ 是基础矩阵,则矩阵

$$\begin{pmatrix} \boldsymbol{B}_1 & 0 \\ \boldsymbol{b}_1 & - \end{pmatrix}$$

是基础矩阵,其中,$\boldsymbol{b}_1$ 是一个向量(取值于{0,+}),且至少有一个“+”出现;

(3) 如果 $\boldsymbol{B}_2$ 是基础矩阵,则矩阵

$$\begin{pmatrix} + & \boldsymbol{b}_2 \\ 0 & \boldsymbol{B}_2 \end{pmatrix}$$

是基础矩阵,其中,$\boldsymbol{b}_2$ 是一个向量(取值于{0,–}),且至少有一个“–”出现;

(4) 如果 $\boldsymbol{B}_1$ 和 $\boldsymbol{B}_2$ 是基础矩阵,则矩阵

$$\begin{pmatrix} \boldsymbol{B}_1 & 0 \\ \boldsymbol{b}_1 & \boldsymbol{b}_2 \\ 0 & \boldsymbol{B}_2 \end{pmatrix}$$

是基础矩阵,其中,$\boldsymbol{b}_1$ 是一个向量(取值于{0,+}),且至少有一个“+”出现;$\boldsymbol{b}_2$ 是一个向量(取值于{0,–}),且至少有一个“–”出现.

定理 **1**[2]. 公式 F 为 $MU(1)$公式,当且仅当 F 的表示矩阵作适当行列调整后是一个基础矩阵.

如下定义的(1,∗)-消解是单位消解的一般化.

定义 **3**. 设 $F=[(L\vee f),(\neg L\vee g_1),\ldots,(\neg L\vee g_m),F_{rest}]$是一个公式,其中:$L$ 是一个文字;$f,g_1,\ldots,g_m$ 是子句;F_{rest} 是一个不含文字 $L,\neg L$ 出现的公式,我们称公式 $F'=[(f\vee g_1),\ldots,(f\vee g_m),F_{rest}]$为 F 关于文字 L 的一个(1,∗)-消解.

如下引理表明,$MU(k)$关于(1,∗)-消解是封闭的,即一个极小不可满足公式通过一次(1,∗)-消解后仍然是极小不可满足公式,而且公式差不改变.

引理 **2**. 设 $F=[(L\vee f),(\neg L\vee g_1),\ldots,(\neg L\vee g_m),F_{rest}]$是一个公式,其中:$L$ 是一个文字;$f,g_1,\ldots,g_m$ 是子句;F_{rest} 是一个不含文字 $L,\neg L$ 出现的公式,$F'=[(f\vee g_1),\ldots,(f\vee g_m),F_{rest}]$为 F 关于文字 L 的(1,∗)-消解,则 F 为 $MU(k)$公式⇔F'为 $MU(k)$公式.

证明:不失一般性,假定 $F=[(x\vee f),(\neg x\vee g_1),\ldots,(\neg x\vee g_p),F_{rest}]$,其中 F_{rest} 不含 $x,\neg x$ 的出现,从而 $F'=[(f\vee g_1),\ldots,(f\vee g_p),F_{rest}]$.

(⇒) 假定 $F\in MU(k)$且 $\#var(F)=n$,则 $\#cl(F)=n+k$,$\#var(F')=n-1$,且 $\#cl(F')=n+k-1$.于是,$d(F')=k$.我们将证明 $F'\in MU(k)$.

(1) F'不可满足.否则,存在一个真值指派 v,使得 $v(F')=1$.此蕴含 $v(f\vee g_1)=\ldots=v(f\vee g_p)=v(F_{rest})=1$.如下是将 v 扩展成为另一个真值指派 v' ,使得 $v'(F)=1$:

$$v'(y)=\begin{cases} v(y), & y\in var(F)\setminus\{x\} \\ 0, & y=x \text{ 且 } v(f)=1 \\ 1, & y=x \text{ 且 } v(f)=0 \end{cases}.$$

显然, $v'(F)=1$.这与 F 的不可满足性矛盾.

(2) F'是极小不可满足的.否则,存在一个子句 $h\in F'$,使得 $F'\setminus\{h\}$不可满足.我们分如下两种情形加以讨论:

情形 1.1. 对某个 $i(1\le i\le p)$,$h=(f\vee g_i)$.

不失一般性,假定 $h=(f\vee g_1)$.因为 F 为极小不可满足公式,有 $F_1=[(x\vee f),(\neg x\vee g_2),\ldots,(\neg x\vee g_p),F_{rest}]$可满足,从而存在一个真值指派 v 使得 $v(F_1)=1$.这蕴含 $v(x\vee f)=v(\neg x\vee g_2)=\ldots=v(\neg x\vee g_p)=v(F_{rest})=1$.如果 $v(x)=1$,则 $v(g_2)=\ldots=v(g_p)=v(F_{rest})=1$;如果 $v(x)=0$,则 $v(f)=v(F_{rest})=1$.因此,恒有 $v(F'\setminus\{h\})=1$.矛盾.

情形 1.2. $h\in F_{rest}$.

由于 F 极小不可满足,所以 $F_1=[(x\vee f),(\neg x\vee g_1),\ldots,(\neg x\vee g_p), F'_{rest}]$可满足,其中 $F'_{rest}=F_{rest}\backslash\{h\}$.从而存在一个真值指派 v,使得 $v(F_1)=1$.这蕴含 $v(x\vee f)=v(\neg x\vee g_1)=\ldots=v(\neg x\vee g_p)=v(F'_{rest})=1$.如果 $v(x)=1$,则 $v(g_1)=\ldots=v(g_p)=v(F'_{rest})=1$.如果 $v(x)=0$,则 $v(f)=v(F'_{rest})=1$.因此,恒有 $v(F'\backslash\{h\})=1$.矛盾.

($\Leftarrow$) 假定 $F'=[(f\vee g_1),\ldots,(f\vee g_p),F_{rest}]\in MU(k)$,我们将证明 $F\in MU(k)$.

首先,F 是不可满足的.否则,存在一个真值指派 v,使得 $v(F)=1$.如果 $v(x)=1$,则 $v(g_1)=\ldots=v(g_p)=v(F_{rest})=1$;如果 $v(x)=0$,则 $v(f)=v(F_{rest})=1$.因此,恒有 $v(F')=1$.矛盾.

其次,F 是极小不可满足的.否则,存在一个子句 $h\in F$,使得 $F\backslash\{h\}$不可满足.我们分如下 3 种情形讨论:

情形 2.1. $h=(x\vee f)$.

请注意:F_{rest}是可满足的.从而存在一个真值指派 v,使得 $v(F_{rest})=1$.我们可以扩展 v 成为另一个真值指派 v',使得 $v'(F\backslash\{h\})=1$.

$$v'(y)=\begin{cases}v(y), & y\in var(F)\backslash\{x\}\\ 0, & y=x\end{cases}.$$

情形 2.2. 对某个 $i(1\le i\le p)$,$h=(\neg x\vee g_i)$.

不失一般性,假定 $h=(\neg x\vee g_1)$.因为 F'为极小不可满足公式,有:$F_2=[(f\vee g_2),\ldots,(f\vee g_p),F_{rest}]$是一个可满足公式.从而存在一个真值指派 v,使得 $v(F_2)=1$.同样地,我们可以扩展 v 成为另一个真值指派 v',使得 $v'(F\backslash\{h\})=1$.

$$v'(y)=\begin{cases}v(y), & y\in var(F)\backslash\{x\}\\ 0, & y=x\text{且}v(f)=1\\ 1, & y=x\text{且}v(f)=0\end{cases}.$$

情形 2.3. $h\in F_{rest}$.

由于 F'极小不可满足,所以 $F_3=[(f\vee g_1),\ldots,(f\vee g_p), F'_{rest}]$可满足,其中 $F'_{rest}=F_{rest}\backslash\{h\}$.因此,存在一个真值指派 v,使得 $v(F_3)=1$.我们可以取情形 2.2 中 v 的扩展方式,得到真值指派 v',并有 $v'(F\backslash\{h\})=1$.矛盾. □

2 公式归约

将一个 CNF 公式 F 化归到一个 3-CNF 公式中,一个经典的做法是,通过适当引入新变元,将每一个子句 $C=(L_1\vee\ldots\vee L_p)$化为一组长度为 3 的子句.

(1) 当 $p=1$ 时,$C=L_1$.

引入新变元 y_1,y_2,化为子句组:$(L_1\vee y_1\vee y_2),(L_1\vee y_1\vee\neg y_2),(L_1\vee\neg y_1\vee y_2),(L_1\vee\neg y_1\vee\neg y_2)$.请注意,公式$[(y_1\vee y_2),(y_1\vee\neg y_2),(\neg y_1\vee y_2),(\neg y_1\vee\neg y_2)]$是一个 $MU(2)$公式.

(2) 当 $p=2$ 时,$C=L_1\vee L_2$.

引入新变元 y_1,化为子句组:$[(L_1\vee L_2\vee y_1),(L_1\vee L_2\vee\neg y_1)]$.请注意,公式$[y_1,\neg y_1]$是一个 $MU(1)$公式.

(3) 当 $p>3$ 时,$C=(L_1\vee\ldots\vee L_p)$.

引入 $p-3$ 个新变元 $y_1,\ldots,y_{p-3}$,化为子句组:$[(L_1\vee L_2\vee y_1),(L_3\vee\neg y_1\vee y_2),\ldots,(L_{p-2}\vee\neg y_{p-4}\vee y_{p-3}),(L_{p-1}\vee L_p\vee\neg y_{p-3})]$.请注意,公式 $H=[y_1,(\neg y_1\vee y_2),\ldots,(\neg y_{p-4}\vee y_{p-3}),\neg y_{p-3}]$是一个 $MU(1)$公式.

我们将$(L_1\vee\ldots\vee L_p)$剖分为 $p-2$ 个子句:$(L_1\vee L_2),L_3,\ldots,L_{p-2},(L_{p-1}\vee L_p)$.由此生成一个 CNF 公式 $F_C=[(L_1\vee L_2),L_3,\ldots,L_{p-2},(L_{p-1}\vee L_p)]$.于是,上述(3)中的构造可以视为 F_C 和 H 中对应子句“拼接”(简称子句对接)后得到的公式.直观上,我们用下面的矩阵表示:

$$\begin{array}{c} \\ y_1 \\ y_2 \\ \vdots \\ \vdots \\ y_{p-4} \\ y_{p-3} \end{array}\begin{pmatrix} L_1 & & & & & L_{p-1} \\ L_2 & L_3 & L_4 & \ldots & L_{p-2} & L_p \\ + & - & & & & \\ & + & - & & & \\ & & + & & & \\ & & & \ldots & & \\ & & & & - & \\ & & & & + & - \end{pmatrix}.$$

这里,我们引入一个新的变换,使得引入的新变元个数仅为$\left\lceil \frac{l}{2} \right\rceil$.

设 $p=2q$,作公式 $F_C'=[L_1,\ldots,L_p]$,引入 q 个新变元 $y_1,\ldots,y_q$,取一个 $MU(q)$ 公式 $H=[(y_1\vee y_q),(\neg y_1\vee y_2),\ldots,(\neg y_{q-1}\vee y_q),(\neg y_q\vee y_{q-1}),\ldots,(\neg y_2\vee y_1),(\neg y_1\vee\neg y_q)]$. 构造子句组:$(L_1\vee y_1\vee y_q),(L_2\vee\neg y_1\vee y_2),\ldots,(L_q\vee\neg y_{q-1}\vee y_q),(L_{q+1}\vee\neg y_q\vee y_{q-1}),\ldots,(L_{p-1}\vee\neg y_2\vee y_1),(L_p\vee\neg y_1\vee\neg y_q)$.直观上,我们用下面的矩阵表示:

$$\begin{array}{c} \\ y_1 \\ y_2 \\ \vdots \\ \vdots \\ y_{q-1} \\ y_q \end{array}\begin{pmatrix} L_1 & L_2 & L_3 & \ldots & L_{\frac{p}{2}} & L_{\frac{p}{2}+1} & \ldots & L_{p-2} & L_{p-1} & L_p \\ + & - & & & & & & & + & - \\ & + & - & & & & & + & - & \\ & & + & & & & & - & & \\ & & & \ldots & & & \ldots & & & \\ & & & & - & + & & & & \\ + & & & & + & - & & & & - \end{pmatrix}.$$

若 $p=2q+1$,引入 $q+1$ 个新变元 $y_1,\ldots,y_q,y_{q+1}$,取一个 $MU(q)$ 公式 $H''=[(y_1\vee y_q),(\neg y_1\vee y_2),\ldots,(\neg y_{q-1}\vee y_q),(\neg y_q\vee y_{q-1}),\ldots,(\neg y_2\vee y_1),(\neg y_1\vee y_{q+1}),(\neg y_q\vee\neg y_{q+1})]$.构造子句组:$(L_1\vee y_1\vee y_q),(L_2\vee\neg y_1\vee y_2),\ldots,(L_q\vee\neg y_{q-1}\vee y_q),(L_{q+1}\vee\neg y_q\vee y_{q-1}),\ldots,(L_{p-2}\vee\neg y_2\vee y_1)(L_{p-1}\vee\neg y_1\vee y_{q+1}),(L_p\vee\neg y_q\vee\neg y_{q+1})$.

上述做法的正确性由下面的引理保证.

引理 **3**. 设 $C=(L_1\vee\ldots\vee L_p)(p>3)$是一个子句,公式 $F_C=[C_1,\ldots,C_m](m\geq 2)$是子句 C(作为文字集合)的一个划分生成的 CNF 公式.$H=[f_1,\ldots,f_m]$是一个 MU 公式,且 $var(C)\cap var(H)=\varnothing$,$F_C$ 和 H 的子句对接公式为 $F_C\vee_{cl}H=[(C_1\vee f_1),\ldots,(C_m\vee f_m)]$,则对任意一个满足 $F_C\vee_{cl}H$ 的真值指派 τ,必有 $\tau(C)=1$.反之,对任意一个满足 C 的真值指派 τ_0,必可扩充为一个满足 $F_C\vee_{cl}H$ 的真值指派 τ.

证明:不失一般性,假定 $C_1=(L_1\vee\ldots\vee L_{i_1})$, $C_2=(L_{i_1+1}\vee\ldots\vee L_{i_2})$,…, $C_m=(L_{i_{m-1}+1}\vee\ldots\vee L_n)$.

设 τ 是一个满足 $F_C\vee_{cl}H$ 的真值指派,由于 H 是一个 MU 公式,存在某个 $k_0(1\leq k_0\leq m)$使得 $\tau(f_{k_0})=0$.如果 τ 不满足 C,则 $\tau(L_1)=\tau(L_2)=\ldots=\tau(L_n)=0$.此蕴含 $\tau(C_1)=\ldots=\tau(C_m)=0$.因此, $\tau(C_{k_0}\vee f_{k_0})=0$.从而 $\tau(F_C\vee_{cl}H)=0$.矛盾.

反之,设 τ_0 是一个满足 C 的真值指派,则必有某个 $k_0(1\leq k_0\leq n)$使得 $\tau_0(L_{k_0})=1$.不妨假定 $\tau_0(L_1)=1$,则 $\tau_0(C_1)=1$.因为 H 是一个 MU 公式,所以 $H-\{f_1\}$是一个可满足公式.从而存在一个真值指派 τ_1 满足 $\tau_1(H-\{f_1\})$.请注意,$var(C)\cap var(H)=\varnothing$.于是,我们可以构造一个真值指派 τ,满足 $F_C\vee_{cl}H$:对于 $x\in var(C)$,定义 $\tau(x)=\tau_0(x)$;对于 $x\in var(H)$,定义 $\tau(x)=\tau_1(x)$. □

由引理 3,容易证明如下结论:

定理 **2**. 设 $F=C_1\vee\ldots\vee C_n$ 是一个 CNF 公式,并且,对于每一个 $1\leq i\leq n$,F_i 是由 C_i 的文字划分生成的一个 CNF 公式,并且 $\#cl(F_i)=m_i\geq 2$.设 $H_1,\ldots,H_n$ 是满足如下条件的 MU 公式:

(1) 对每一个 $1\leq i\leq n$,$\#cl(F_i)=m_i$;

(2) $(\cup_{1\leq i\leq n}var(H_i))\cap var(F)=\varnothing$;

(3) 对任意的 $1\leq i\neq j\leq n$,$var(H_i)\cap var(H_j)=\varnothing$.

定义 $F^*=(F_1\vee_{cl}H_1)\wedge(F_2\vee_{cl}H_2)\wedge\ldots\wedge(F_n\vee_{cl}H_n)$,则 F 可满足⇔F^*可满足.

3 简化的 NP-完全类

我们用(r,s)-CNF 表示这样的 CNF 公式类:(r,s)-CNF 中的任意公式 F 对任意的子句 $C\in F$,子句长度$|C|=r$;并且,对任意的变元 $x\in var(F)$,出现次数 $occs(x,F)=pos(x,F)+neg(x,F)\le s$.$(r,s)$-SAT 是限制实例在$(r,s)$-CNF 中的满足性判定问题.

我们考虑 $MU(2)$公式 $H_p=[(x_1\vee x_2\vee\ldots\vee x_p),(\neg x_1\vee x_2),(\neg x_2\vee x_3),\ldots,(\neg x_{p-1}\vee x_p),(\neg x_p\vee x_1),(\neg x_1\vee\ldots\vee\neg x_p)]$,其中 $p\ge 2$. H_p 的表示矩阵为

$$\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ \vdots \\ x_{p-1} \\ x_p \end{array}\begin{pmatrix} + & - & & & & + & - \\ + & + & - & & & & - \\ \vdots & & \ldots & & & & \vdots \\ \vdots & & & \ldots & & & \vdots \\ + & & & & + & - & - \\ + & & & & & + & - & - \end{pmatrix}.$$

取 H_p 中长度为 2 的子句构成公式 $H_p^c=[(\neg x_1\vee x_2),(\neg x_2\vee x_3),\ldots,(\neg x_{p-1}\vee x_p),(\neg x_p\vee x_1)]$.由 H_p 的极小不可满足性,公式 $H_p^c+\{(x_1\vee x_2\vee\ldots\vee x_p)\}$和 $H_p^c+\{(\neg x_1\vee\ldots\vee\neg x_p)\}$均可满足,并且 $H_p^c+\{(x_1\vee x_2\vee\ldots\vee x_p)\}\models(x_1\wedge x_2\wedge\ldots\wedge x_p)$, $H_p^c+\{(\neg x_1\vee\ldots\vee\neg x_p)\}\models(\neg x_1\wedge\neg x_2\wedge\ldots\wedge\neg x_p)$.因此,对于任何满足 H_p^c 的真值指派 τ,有 $\tau(x_1)=\ldots=\tau(x_p)$.

设 $F=[(x_1\vee f_1),\ldots,(x\vee f_q),(\neg x\vee f_{q+1}),\ldots,(\neg x\vee f_p),F_{rest}]$为一个公式,其中,$occs(x,F)=p\ge 4$ 且变元 x 不出现在 F_{rest} 中.我们引入 p 个新变元 $x_1,x_2,\ldots,x_p$,并定义公式 $F^{\{x\}}$如下:

$$F^{\{x\}}=[(x_1\vee f_1),\ldots,(x_q\vee f_q),(\neg x_{q+1}\vee f_{q+1}),\ldots,(\neg x_p\vee f_p),F_{rest}]+H_p^c.$$

显然,对每个 $1\le i\le p$,$occs(x_i,F^{\{x\}})=3$,且 H_p^c 中的每个子句均具有形式$(x\vee\neg y)$(恰好含有一正一负两个文字).

上述做法的目的是降低变元出现的次数.在原始公式中,变元 x 出现 p 次,用一组新变元 $x_1,\ldots,x_p$ 取代 x,每个新变元 x_i 在新的公式中恰好出现 3 次,自然要求上述转换不改变公式的可满足性.

引理 **4**. 对于上述的公式 F 和 $F^{\{x\}}$,F 可满足$\Leftrightarrow F^{\{x\}}$可满足.

证明:假定 τ是满足 F 的一个真值指派.定义一个真值指派 τ'满足 $F^{\{x\}}$如下:

$$\tau'(y)=\begin{cases}\tau(y), & \text{if } y\in var(F)-\{x\}\\ 1, & \text{if } \tau(x)=1\text{且 } y\in\{x_1,\ldots,x_p\}\\ 0, & \text{if } \tau(x)=0\text{且 } y\in\{x_1,\ldots,x_p\}\end{cases}.$$

反之,假定 v 是满足 $F^{\{x\}}$的一个真值指派.定义一个真值指派 v'满足 F 如下:

$$v'(y)=\begin{cases}v(y), & \text{if } y\in var(F)-\{x\}\\ 1, & \text{if } v(x_1)=1\text{且 } y=x\\ 0, & \text{if } v(x_1)=0\text{且 } y=x\end{cases}.$$ □

因为每一个 CNF 公式均可转换为一个 3-CNF 公式而不改变可满足性,重复应用引理 4,如下定理是一个自然结果.

定理 **3**[4]. 限制实例取自于(2,3)-CNF∪(3,3)-CNF 的满足性判定问题(2,3)-SAT∪(3,3)-SAT 是 NP-完全的.

定理 4. 对于任意的 $s\ge 3$,如果$(3,s)$-CNF 中含有一个不可满足公式 H,则$(3,s)$-CNF 是 NP-完全的.

证明:假定$(3,s)$-CNF 中含有一个不可满足公式 $H=[C_1,\ldots,C_m]$,则 H 含有一个极小不可满足子公式 $H'=[C_{i_1},\ldots,C_{i_{m'}}]$,其中$1\le i_1\le i_2<\ldots<i_{m'}\le m$.显然,$H'$是$(3,s)$-CNF 中的一个公式.因此,我们可以假设 H 本身就是一个极小不可满足公式.

设 $var(H)=\{x_1,\ldots,x_n\}$, $H=[(x_1\vee C_1'),C_2,\ldots,C_m]$,$G=[C_2,\ldots,C_m]$,则 G 可满足,且 x_1 在 G 中至多出现 $s-1$ 次,并且对于满足 G 的任意一个真值指派 τ,有 $\tau(x_1)=0$.对于 3-SAT 的任何实例 F,重复引理 4 中的方法,依次分别对其出现次数超过 3 次的每个变元进行处理,我们可以在多项式时间内将 F 转换为(2,3)-SAT∪(3,3)-SAT 的一个实例 F^*.由 F^*的构造,F^*具有形式:$[(y_1\vee\neg z_1),\ldots,(y_k\vee\neg z_k),g_1,\ldots,g_l]$,其中每个子句 $g_j(1\le j\le l)$恰好含有 3 个文字(注意:由引

理 4 中 $F^{\{x\}}$的结构,这里的 $y_1,z_1,\ldots,y_k,z_k$ 可能有重复出现,但每个子句$(y_i\vee\neg z_i)$中的两个文字必不相同).

我们现在处理 F^*中长度为 2 的子句.对每个 $1\le i\le k$,引入 n 个新变元 $x_1^i,\ldots,x_n^i$, 分别用 $x_1^i,\ldots,x_n^i$, 代替 $x_1,\ldots,x_n$, 构造 G 的一个拷贝 G^i.我们现在从 F^*构造一个公式 F^{**}:

$$F^{**}=[(y_1\vee\neg z_1\vee x_1^1),\ldots,(y_k\vee\neg z_k\vee x_1^k),g_1,\ldots,g_l]+G^1+\ldots+G^k.$$

请注意,G^i 的可满足力迫使 x_1^i 取"假",从而 F 可满足$\Leftrightarrow F^*$可满足$\Leftrightarrow F^{**}$可满足.

显然,F^{**}是(3,s)-SAT 的一个实例.因此,只要(3,s)-SAT 有一个不可满足实例,则(3,s)-SAT 是 NP-完全的. □

推论 **1**. (3,4)-SAT 是 NP-完全的.

证明:由定理 4,我们只需在(3,4)-CNF 中构造一个不可满足公式.如下公式是一个 MU 公式:

$$\boldsymbol{G}=\begin{array}{c}\\ y\\ x_1\\ y_1\\ z_1\\ x_2\\ y_2\\ z_2\\ x_3\\ y_3\\ z_3\end{array}\begin{pmatrix} - & + & & & & + & & & & + & & & \\ & + & + & - & - & & & & & & & & \\ & + & - & + & - & & & & & & & & \\ & & + & + & + & & & & & & & & - \\ & & & & & + & + & - & - & & & & \\ & & & & & + & - & + & - & & & & \\ & & & & & & + & + & + & & & & - \\ & & & & & & & & & + & + & - & - \\ & & & & & & & & & + & - & + & - \\ & & & & & & & & & & + & + & + & - \end{pmatrix}.$$

即 $G=\wedge_{1\le j\le 3}((y\vee x_j\vee y_j)\wedge(x_j\vee\neg y_j\vee z_j)\wedge(\neg x_j\vee y_j\vee z_j)\wedge(\neg x_j\vee\neg y_j\vee z_j))\wedge(\neg z_1\vee\neg z_2\vee\neg z_3)\wedge(\neg y)$.

请注意,在 G 中,每个变元恰好出现 4 次,除单位子句$\neg y$ 外,其余子句的长度恰好为 3.

容易证明,如果 $F_1=[C_1,\ldots,C_{m_1}]$ 和 $F_2=[C_1',\ldots,C_{m_2}']$ 是 MU 公式,且 $var(F_1)\cap var(F_2)=\varnothing$,则从两个公式中分别任意选出一个子句作析取,其余子句保留,得到的公式仍然为一个 MU 公式.比如,$[C_1\vee C_1',C_2,\ldots,C_{m_1},C_2',\ldots,C_{m_2}']$ 是一个 MU 公式.

我们现在将 G 作 3 个拷贝(保证不同备份变元集互不相同),以构造(3,4)-CNF 中的一个(极小)不可满足公式如下:

$$F=\wedge_{1\le i\le 3}\wedge_{1\le j\le 3}((y^i\vee x_j^i\vee y_j^i)\wedge(x_j^i\vee\neg y_j^i\vee z_j^i)\wedge(\neg x_j^i\vee y_j^i\vee z_j^i)\wedge(\neg x_j^i\vee\neg y_j^i\vee z_j^i))$$
$$\wedge_{1\le i\le 3}(\neg z_1^i\vee\neg z_2^i\vee\neg z_3^i)\wedge(\neg y^1\vee\neg y^2\vee\neg y^3).$$

因此,由定理 4,(3,4)-SAT 是 NP-完全的. □

对于(r,s)-SAT($s\ge r\ge 3$)的任意实例 F,利用第 2 节中的方法,我们可以在多项式时间内将 F 转换为(3,s)-SAT 的一个实例 F',并使其逻辑等价.于是,我们有一个一般性结论:

定理 **5**. 对于任意的 $r\ge 3$ 及 $s\ge r$,如果存在(r,s)-CNF 中的一个不可满足公式 H,则(r,s)-SAT 是 NP-完全的.

4 结论和进一步工作

利用极小不可满足公式的构造,给出了从CNF公式到3-CNF公式的一个新的转换方法.在此方法中,对于长度大于 3 的子句 $C=(L_1\vee\ldots\vee L_p)$,只需引入$\left\lceil\frac{l}{2}\right\rceil$个新变元.同时,给出了极小不可满足公式在研究简化的 NP-完全问题(r,s)-SAT 中的原理和方法.进一步的工作是,利用 $MU(1)$公式的消解性质,研究不可满足公式消解方法及其消解的复杂性,并研究 S.Hoory 和 S.Szeider 引入的可计算函数 $f_1(r)=\max\{s:(r,s)\text{-CNF}\cap MU(1)=\varnothing\}$的确定性算法.

References:

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

[2] 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.

[3] Xu DY. Homomorphism proof system for unsatisfiable formulas. Journal of Software, 2005,16(3):336−345 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/336.htm

[4] Tovey CR. A simplified NP-Complete satisfiability problem. Discrete Applied Mathematics, 1984,8(1):85−89.

[5] Hoory S, Szeider S. Computing unsatisfiable *k*-SAT instances with few occurrences per variable. Theoretical Computer Science, 2005,337(1-3):347−359.

[6] Hoory S, Szeider S. Families of unsatisfiable *k*-CNF formulas with few occurences per variables. arXiv.org e-Print Archive, Math. CO/041167. 2004.

[7] Savicky P, Sgall J. Note DNF tautologies with a limited number of occurences of every variable. Theoretical Computer Science, 2000,238(1-2):495−498.

[8] Garey MR, Johnson DS. Computer and Intractability—A Guide to the Theory of NP-Completeness. San Francisco: W. H. Freeman and Company, 1979.

附中文参考文献:

[3] 许道云.不可满足公式的同态证明系统.软件学报,2005,16(3):336−345. http://www.jos.org.cn/1000-9825/16/336.htm

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

第 23 届中国数据库学术会议 NDBC 2006

征 文 通 知

主办单位： 中国计算机学会数据库专业委员会（www.ccf-dbs.org.cn）

承办单位： 中山大学（www.zsu.edu.cn）

协办单位： 暨南大学，华南理工大学，广东工业大学，华南师范大学，广东计算机学会

会议网址： http://ndbc2006.zsu.edu.cn

重要日期： 论文提交截止时间：2006 年 5 月 10 日

论文录用通知时间：2006 年 7 月中旬

排版稿件截止时间：2006 年 7 月下旬

会议论文将以《计算机研究与发展》增刊、《计算机科学》正刊和增刊的形式发表，有关会议信息可以访问网站 http://ndbc2006.zsu.edu.cn,也可以与会务组联系。

E-mail:ndbc2006@zsu.edu.cn

电话：020-84112137, 020-84110087

传真：020-84112290

通讯地址：中山大学信息学院计算机科学系 NDBC2006 会务组（广州 510275）