计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190400018

一种布尔公式的代数逻辑约化新方法

刘 江 周鸿昊
中国科学院重庆绿色智能技术研究院高性能计算应用研究中心 重庆 400714
中国科学院大学 北京 100049

摘 要 布尔可满足问题是最早被证明的NP完全问题之一,1-in-3-SAT问题是一个NP完全的布尔可满足子类问题。1-in-3-SAT的计算复杂度取决于对应公式的变量以及子句的个数。将1-in-3公式归约为一个变量数或者子句数更少的1-in-3公式,是提高1-in-3-SAT问题求解效率的一个关键。基于一个新的范式形式——XCNF,针对1-in-3-SAT问题提出一种新的代数逻辑约化方法,用于在多项式时间内约减一个1-in-3公式的变量数和子句数。所提算法的主要思想为:首先将1-in-3公式转化为XCNF公式,然后尝试找出XCNF公式中的X-纯文字,并利用X-纯文字法则对1-in-3公式中相应的布尔变量赋值,最后得到一个约减公式,该约减公式与原公式的1-in-3可满足性等价。

关键词:NP完全问题;布尔可满足性问题;1-in-3-SAT;XCNF;X-纯文字
中图法分类号 TP311

New Algebraic Logic Reduction Method for Boolean Formula

LIU Jiang and ZHOU Hong-hao
High Performance Computing Application Research Center,Chongqing Institute of Green and Intelligent Technology,Chinese Academy of Sciences,Chongqing 400714,China
University of Chinese Academy of Sciences,Beijing 100049,China

Abstract Boolean satisfiability problem is one of the earliest proven NP complete problem. 1-in-3-SAT problem is an NP complete subclass of Boolean satisfiability problem. The computational complexity of 1-in-3-SAT depends on the number of the variables and clauses in the formula. How to reduce the 1-in-3 formula to one with less variables or clauses is the key to improve the efficiency of solving 1-in-3-SAT. Based on a new type of normal form—XCNF,this paper proposes a new algebraic logic reduction method to reduce the number of variables and clauses in polynomial time. The main idea is as follows. First,the method transforms the 1-in-3 formula into a XCNF formula,then tries to find out the X pure literal in the XCNF formula and assign the corresponding Boolean variable in the 1-in-3 formula with X pure literal rule. At last,a reduced formula which has the same 1-in-3 satisfiability with the original one can be obtained.

Keywords NP complete problem,Boolean satisfiability problem,1-in-3-SAT,XCNF,X pure literal

1 引言

1-in-3-SAT问题是指,给定一个3-CNF公式,判断是否存在一组赋值,使得公式中的每一个子句中恰有一个文字为真[1]。1-in-3-SAT问题是NP完全问题,在计算复杂性方面有着重要的研究意义。为了与一般的3-SAT问题区分,本文将1-in-3-SAT问题中的3-CNF公式称为1-in-3公式。

目前,求解1-in-3-SAT问题的途径主要有两种。

(1)首先将1-in-3-SAT问题转化为一般的3-SAT问题,然后用SAT求解算法进行求解。当前的SAT求解算法分为完备算法和不完备算法。完备算法总是能够找到一个满足公式的赋值,或者证明公式的不可满足性,主流的完备算法由DPLL算法[2-3]发展而来。DPLL算法是基于推理和搜索的方法,每次给一个布尔变量赋值,如果推出矛盾,则进行回溯。为了提高效率,CDCL(Conflict-Drive Clause Learning)算法[4-6]在发生矛盾时,分析引起矛盾的赋值,并通过子句学习以及非时序回溯来减少回溯的次数。尽管完备算法已历经多次改进,但其最坏时间复杂度仍是指数级别。鉴于此,一部分学者开始将研究热点转向不完备算法。不完备算法大大提高了对实际布尔可满足性问题的求解效率。但是,当不完备算

到稿日期:2019-03-02 返修日期:2019-05-01 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61672488)
This work was supported by the National Natural Science Foundation of China (61672488).
通信作者:刘江(liujiang@cigit.ac.cn)

法找不到一个满足公式的赋值时，便无法确定公式的可满足性。局部搜索(Local Search)算法[7-9]为了提高搜索效率，只对赋值空间中的一部分进行搜索。当问题难解时，局部搜索算法可能会放弃搜索解所在的空间，最终找不到解。还有一种不完备算法将 SAT 问题转化为优化的问题，然后用拉格朗日法[10]、牛顿法[11]等进行求解，但这些方法往往会陷入局部最优。此外，有研究者从统计物理学中得到启发，提出基于消息传递的纵览传播(Survey Propagation)算法[12-13]。纵览传播算法可以处理数百万变量的 SAT 问题，但是这种方法存在可能不收敛的问题[14]。

(2)直接求解 1-in-3-SAT 问题。近年，一种称为 LAF (Linear Algebra Formulation)的算法[15-16]将 1-in-3-SAT 问题通过两次线性化转化为线性方程组是否有 0-1 解的问题。这种算法可以有效处理大部分不可满足的 1-in-3 实例。但是，对于可满足的实例，LAF 算法还有待进一步的改进。

无论用何种方法求解，减少 1-in-3-SAT 问题中的变量和子句个数，都是提高求解效率的一个关键问题。从 1-in-3-SAT 问题的复杂度方面来看，1-in-3-SAT 问题是 NP 完全问题，其时间复杂度取决于变量个数 n 和子句个数 m[17]，当 n 和 m 减小时，解决问题的时间可大幅度缩短。从 1-in-3 公式的结构来看，1-in-3 公式中含 3 个变量的子句越少，判定其 1-in-3 可满足性的效率就越高。在极端情况下，当 1-in-3 公式中的每个子句都包含不多于 2 个变量时，可以在多项式时间内判定其 1-in-3 可满足性。此外，1-in-3 公式中变量个数的减少，可能导致变量个数更加接近子句个数。此时，可以尝试用其他高效的方法(如 LAF 方法[15-16])来判定这个公式的 1-in-3 可满足性。

本文提出了 1-in-3 公式的约减方法，用于减少 1-in-3 公式中变量和子句的数目。本文第 2 节提出一种新的范式——XCNF，并详述了其构造原理及方法，为第 3 节叙述 X-纯文字法则做铺垫；第 3 节提出 X-纯文字法则，根据 X-纯文字法则消去原 1-in-3 公式的变量，并证明了其正确性；第 4 节介绍如何在 1-in-3 公式中找出具有特殊结构的变量，并以此化简公式；最后总结全文，并提出下一步研究的方向。

如果 1-in-3 公式中没有文字是布尔变量的非，则称这个公式具有正极性。所有的 1-in-3 公式都可以在多项式时间内转化为具有正极性的 1-in-3 公式，并且两个公式具有等价的 1-in-3 可满足性[15]，因此本文仅研究具有正极性的 1-in-3 公式。此外，按照约定，本文中布尔值的真和假分别对应自然数 1 和 0。

2　XCNF 公式

2.1　1-in-3 公式可满足的充要条件

给定一组布尔变量 $X=\{X_1,\cdots,X_n\}$，由 X 构成一个具有正极性的 1-in-3 公式 $\mathscr{F}=\bigwedge\limits_{1\leqslant i\leqslant m}\left(\bigvee\limits_{1\leqslant j\leqslant j_i}X_{i,j}\right)$，其中 $j_i\leqslant 3$ 为每个子句中布尔变量的个数。$\mathscr{F}$ 具有 1-in-3 可满足性，当且仅当方程组：

$$\sum_{j\leqslant j_i}X_{i,j}=1,1\leqslant i\leqslant m \tag{1}$$

在整数环上有 0-1 解。方程组的解 $X_{i,j}=1$ 和 $X_{i,j}=0$ 分别对应 1-in-3 满足 $\mathscr{F}$ 的布尔赋值 $X_{i,j}=1$ 和 $X_{i,j}=0$。为了简洁，本文不再用新的符号来表示方程组中的变量。将 $\mathscr{F}$ 转化为方程组的过程称为线性化(Linear Transformation)。将 $\mathscr{F}$ 线性化所得的方程组称为 LT(Linear Transformation)方程组。判定方程组在整数环上有无 0-1 解是 NP 完全问题[18]，目前没有发现多项式时间的判定方法。$\mathscr{F}$ 的 LT 方程组在二元有限域$\mathbb{GF}(2)$上的 0-1 解集是其在整数环上 0-1 解集的超集，本文用 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上的 0-1 解逼近其在整数环上的 0-1 解。可以使用高斯消去法[19]在$\mathbb{GF}(2)$上求解 $\mathscr{F}$ 的 LT 方程组。当存在 1-in-3 满足 $\mathscr{F}$ 的赋值时，这组赋值在$GF(2)$上对应的 0-1 值一定是 $\mathscr{F}$ 的 LT 方程组的解。这说明当 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上无解时，$\mathscr{F}$ 是 1-in-3 不可满足的。当 $\mathscr{F}$ 的 LT 方程组在 GF(2)上有解时，$\mathscr{F}$ 的 1-in-3 可满足性需要分情况讨论。1)$j_i\leqslant 2,1\leqslant i\leqslant m$(即 $\mathscr{F}$ 的每个子句中变量个数都不多于 2)，$\mathscr{F}$ 一定是 1-in-3 可满足的。2)存在 i，使得 $j_i=3$(即 $\mathscr{F}$ 中存在变量个数等于 3 的子句)，需要验证 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上的解能否 1-in-3 满足 $\mathscr{F}$。一种直接的方法是依次代入所有的解进行验证，但由于 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上的解有 $2^{n-rank(LT)}$ 个($rank(LT)$是方程组在$\mathbb{GF}(2)$上的秩)，因此代入验证的效率很低。本文根据定理 1，给出了不同的验证思路。

定理 1　1-in-3 公式 $\mathscr{F}$ 是 1-in-3 可满足的充分必要条件为：1)$\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上有解；2)存在 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上的解，使得方程组中 $j_i=3$ 的每一个方程 $\sum\limits_{j\leqslant j_i}X_{i,j}=1$ 满足 $X_{i,1}X_{i,2}=0,X_{i,1}X_{i,3}=0,X_{i,2}X_{i,3}=0$。

证明：(必要性)$\mathscr{F}$ 是 1-in-3 可满足的，因此满足 $\mathscr{F}$ 的赋值是 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上的一个解。对于 $j_i=3$ 的每一个子句，1-in-3 满足 $\mathscr{F}$ 的赋值一定是下面 3 种情况之一：$(X_{i,1},X_{i,2},X_{i,3})=(1,0,0)$；$(X_{i,1},X_{i,2},X_{i,3})=(0,1,0)$；$(X_{i,1},X_{i,2},X_{i,3})=(0,0,1)$。这 3 种情况必然满足：$X_{i,1}X_{i,2}=0,X_{i,1}X_{i,3}=0,X_{i,2}X_{i,3}=0$。

(充分性)当 $\mathscr{F}$ 的 LT 方程组在$\mathbb{GF}(2)$上有解时，$\mathscr{F}$ 的 $j_i=1$ 的子句必有 $X_{i,1}=1$，此时子句是 1-in-3 满足的。在 $\mathscr{F}$ 的每一个 $j_i=2$ 的子句中，变量在 $\mathscr{F}$ 的 LT 方程组中$\mathbb{GF}(2)$上的解最多有两种情况，即$(X_{i,1},X_{i,2})=(0,1)$和$(X_{i,1},X_{i,2})=(1,0)$，子句是 1-in-3 满足的。$\mathscr{F}$ 的每一个 $j_i=3$ 的子句中的变量在 $\mathscr{F}$ 的 LT 方程组中$\mathbb{GF}(2)$上的解最多有 4 种情况：$(X_{i,1},X_{i,2},X_{i,3})=(1,0,0)$，$(X_{i,1},X_{i,2},X_{i,3})=(0,1,0)$，$(X_{i,1},X_{i,2},X_{i,3})=(0,0,1)$，$(X_{i,1},X_{i,2},X_{i,3})=(1,1,1)$。若要满足约束 $X_{i,1}X_{i,2}=0,X_{i,1}X_{i,3}=0,X_{i,2}X_{i,3}=0$，则 4 种解中须排除$(X_{i,1},X_{i,2},X_{i,3})=(1,1,1)$。在其余 3 种解对应的

布尔赋值下，子句是 1-in-3 满足的。（证毕）

事实上，可以证明，要使定理 1 的结论成立，条件 2）只需满足 3 个约束中的一个即可，如推论 1 所述。

推论 1 1-in-3 公式 $\mathcal{F}$ 是 1-in-3 可满足的充分必要条件为：1）$\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解；2）存在 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上的解，使得方程组中 $j_i=3$ 的每一个方程 $\sum_{j\leqslant j_i} X_{i,j}=1$ 满足约束 $X_{i,1}X_{i,2}=0, X_{i,1}X_{i,3}=0, X_{i,2}X_{i,3}=0$ 中的一个。

证明：（必要性）与定理 1 类似，不再赘述。

（充分性）$\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解，$j_i=1$ 和 $j_i=2$ 的子句是 1-in-3 满足的，原因同定理 1。下面证明 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解时，对于 $\mathcal{F}$ 的每一个 $j_i=3$ 的方程，3 个约束 $X_{i,1}X_{i,2}=0, X_{i,1}X_{i,3}=0, X_{i,2}X_{i,3}=0$ 是等价的。$\mathcal{F}$ 的 LT 方程组有解时：

$$\begin{aligned}X_{i,1}X_{i,3}&=X_{i,1}(1+X_{i,1}+X_{i,2})\\&=X_{i,1}+X_{i,1}^2+X_{i,1}X_{i,2}\\&=X_{i,1}X_{i,2}=0\end{aligned}$$

因此 $X_{i,1}X_{i,2}=0$ 和 $X_{i,1}X_{i,3}=0$ 是等价的。同理，$X_{i,1}X_{i,2}=0$ 和 $X_{i,2}X_{i,3}=0$ 是等价的。因此，$\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解时，要使子句 $X_{i,1}\vee X_{i,2}\vee X_{i,3}$ 是 1-in-3 满足的，3 个约束 $X_{i,1}X_{i,2}=0, X_{i,1}X_{i,3}=0, X_{i,2}X_{i,3}=0$ 只需满足一个。（证毕）

2.2 XCNF 公式的构建

设 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上的通解为 $X_u=\sum_{k_t\in K_u}k_t+c_u, 1\leqslant u\leqslant n$。其中，$K_u\subseteq K(1\leqslant u\leqslant n)$，$K=\{k_t\mid k_t\in \mathrm{GF}(2), 1\leqslant t\leqslant n-rank(LT)\}$ 是 $\mathcal{F}$ 的 LT 方程组的一组自由变量，$rank(LT)$ 是方程组在 GF(2) 上的秩，$c_u\in \mathrm{GF}(2)$ 是常数。如果将 $X_u=\sum_{k_t\in K_u}k_t+c_u$ 中的 k_t 和 c_u 看作布尔变量（这里同样不再用新的符号表示），则将其中的加法运算符号“+”替换为布尔异或运算符号“⊕”后，得到关于布尔变量 K 的布尔公式 $X_u=\bigoplus_{k_t\in K_u}k_t\oplus c_u$，则布尔公式 $X_u=\bigoplus_{k_t\in K_u}k_t\oplus c_u$ 的 0-1 值与 GF(2) 上 $X_u=\sum_{k_t\in K_u}k_t+c_u$ 的 0-1 值是一致的。如果 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上存在常数解 $X_u=c_u$，则可以代入对应的布尔赋值化简 $\mathcal{F}$。此外，如果 $\mathcal{F}$ 的 LT 方程组中存在 X_{u_1} 和 X_{u_2} 有相同的通解，则可以通过以 X_{u_1} 代换 X_{u_2} 并且删除重复子句的方式化简 $\mathcal{F}$。下文假设 $\mathcal{F}$ 是已完成化简的公式，即 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上没有常数解，也没有两个变量有相同的通解。为了叙述的简洁性，下面定义布尔变量 X_u 的 K 表示。

定义 1（K 表示） 若 1-in-3 公式 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上有通解 $X_u=\sum_{k_t\in K_u}k_t+c_u$，则布尔公式 $\bigoplus_{k_t\in K_u}k_t\oplus c_u$ 称为 X_u 的 K 表示（K Expression），记为 $KE(X_u)$。$|K_u|$ 称为 $KE(X_u)$ 的长度。

根据定义，每个变量 X_u 都有一个长度为 $|K_u|$ 的 K 表示 $KE(X_u)=\bigoplus_{k_t\in K_u}k_t\oplus c_u(K_u\subseteq K)$，$X_u$ 的值为 1 当且仅当 $KE(X_u)$ 的值为 1。

定理 2 $\neg X_u$ 值为 1，当且仅当 $KE(\neg X_u)=KE(X_u)\oplus 1$ 值为 1，即 $KE(\neg X_u)=KE(X_u)\oplus 1$。

由推论 1 可知，在 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解的情况下，该解对应的布尔赋值使 $\mathcal{F}$ 中 $j_i=3$ 的子句 $X_{i,1}\vee X_{i,2}\vee X_{i,3}$ 是 1-in-3 可满足的充分必要条件是：存在这个子句中的一对变量使得它们解值的乘积为 0。为了更有效地使用后文所述的 X-纯文字法则，这里选长度最短的两个变量。不失一般性，假设这两个变量是 $X_{i,1}$ 和 $X_{i,2}$。根据定理 2，$X_{i,1}X_{i,2}=0$ 等价于：

$$\neg X_{i,1}\vee\neg X_{i,2}=(KE(X_{i,1})\oplus 1)\vee(KE(X_{i,2})\oplus 1)=1 \tag{2}$$

为了陈述的简洁性，引入以下定义。

定义 2（XCNF 公式） 由布尔变量 $k_t(1\leqslant t\leqslant T)$ 构成的异或布尔公式 $\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$ 称为 X-文字。相应地，X-文字 $\mathcal{XL}_j(1\leqslant j\leqslant J)$ 的析取 $\mathcal{XC}=\bigvee_{1\leqslant j\leqslant J}\mathcal{XL}_j$ 称为 X-子句；X-子句 $\mathcal{XC}_i(1\leqslant i\leqslant I)$ 的合取 $\mathcal{XF}=\bigwedge_{1\leqslant i\leqslant I}\mathcal{XC}_i$ 称为 XCNF（X-Conjunctive Normal Form）公式。

当 1-in-3 公式 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解时，可以根据等式对 $\mathcal{F}$ 中所有满足 $j_i=3$ 的子句构建相应的 X-子句 $\mathcal{XC}_i=(KE(X_{i,1})\oplus 1)\vee(KE(X_{i,2})\oplus 1)$，然后合取这些 X-子句得到一个 XCNF 公式 $\mathcal{XC}=\bigwedge_{i:j_i=3,1\leqslant i\leqslant m}XC_i$。$\mathcal{F}$ 的子句 $X_{i,1}\vee X_{i,2}\vee X_{i,3}$ 是 1-in-3 可满足的，当且仅当 X-子句 $XC_i=(KE(X_{i,1})\oplus 1)\vee(KE(X_{i,2})\oplus 1)$ 是布尔可满足的。又根据推论 1，$\mathcal{F}$ 中 $j_i<3$ 的子句不需要构建 X-子句。

定理 3 如果 1-in-3 公式 $\mathcal{F}$ 的 LT 方程组在 GF(2) 上有解，则 $\mathcal{F}$ 是 1-in-3 可满足的，当且仅当其对应的 XCNF 公式 $\mathcal{XF}$ 是布尔可满足的。

例 1 给定 1-in-3 公式：

$$\begin{aligned}\mathcal{F}=&(X_1\vee X_2\vee X_4)\wedge(X_1\vee X_3\vee X_8)\wedge\\&(X_2\vee X_3\vee X_5)\wedge(X_2\vee X_6\vee X_7)\wedge\\&(X_3\vee X_7\vee X_9)\wedge(X_4\vee X_6\vee X_{10})\end{aligned}$$

其 LT 方程组为：

$$\begin{cases}X_1+X_2+X_4=1\\X_1+X_3+X_8=1\\X_2+X_3+X_5=1\\X_2+X_6+X_7=1\\X_3+X_7+X_9=1\\X_4+X_6+X_{10}=1\end{cases}$$

在 GF(2) 上有多解。各变量的 K 表示为 $KE(X_1)=k_1$，$KE(X_2)=k_2$，$KE(X_3)=k_3$，$KE(X_4)=1\oplus k_1\oplus k_2$，$KE(X_5)=1\oplus k_2\oplus k_3$，$KE(X_6)=k_4$，$KE(X_7)=1\oplus k_2\oplus k_4$，$KE(X_8)=1\oplus k_1\oplus k_3$，$KE(X_9)=1\oplus k_2\oplus k_3\oplus k_4$，$KE(X_{10})=1\oplus k_1\oplus k_2\oplus k_4$。$\mathcal{F}$ 的子句 $X_1\vee X_2\vee X_4$ 中，由于 X_4 的 K 表示的长度比 X_1 和 X_2 的 K 表示的长度大，因此原 1-in-3 子句 $X_1\vee X_2\vee X_4$ 转化为 X-子句 $KE(\neg X_1)\vee$

$KE(\neg X_2)=(1\oplus k_1)\vee(1\oplus k_2)$。

根据定理3，将$\mathcal{F}$的每个子句都转化为X-子句，得到XCNF公式：

$$\mathcal{XF}=((1\oplus k_1)\vee(1\oplus k_2))\wedge((1\oplus k_1)\vee(1\oplus k_3))\wedge((1\oplus k_2)\vee(1\oplus k_3))\wedge((1\oplus k_2)\vee(1\oplus k_4))\wedge((1\oplus k_3)\vee(k_2\oplus k_4))\wedge((k_1\oplus k_2)\vee(1\oplus k_4))$$

$\mathcal{F}$是1-in-3可满足的，当且仅当$\mathcal{XF}$是布尔可满足的。

3　XCNF公式上的X-纯文字法则

3.1　XCNF到CNF的转化

关于XCNF公式，本节将证明其中的X-文字$\mathcal{XL}$可以转化为等可满足的CNF公式$\mathcal{G}$；基于此结论，可进一步证明每个XCNF公式$\mathcal{XF}$可以转化为某个等可满足的CNF公式$\mathcal{H}$。设X-文字$\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$。对于$\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$，考虑一个CNF公式，如式(3)所示：

$$\mathcal{G}=\bigwedge_{0\leqslant 2\alpha\leqslant T}\bigwedge_{R_\alpha\in S_\alpha}\Big(\bigvee_{k_t\in R_\alpha}\neg k_t\bigvee_{k_j\in K'-R_\alpha}k_j\Big)\tag{3}$$

其中$S_\alpha=\{R_\alpha\mid R_\alpha$为从$K'$中任取$2\alpha$个变量构成的集合$\}$，因此有下文所述结果。

定理4　X-文字$\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$与CNF公式$\mathcal{G}$是等可满足的，即$\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$是布尔可满足的充分必要条件是$\mathcal{G}$是布尔可满足的。

证明：固定对$K'=\{k_1,k_2,\cdots,k_T\}$的一组赋值$b=(b_1,b_2,\cdots,b_T)\in\{0,1\}^{\mathrm{T}}$。令$B_1=\{k_i\mid k_i=b_i=1$且$k_i\in K'\}$，$I_\alpha=\{k_i\mid k_i=b_i=1$且$k_i\in R_\alpha\}$。一般地，$I_\alpha\subseteq B_1$且$I_\alpha\subseteq R_\alpha\subseteq K'$。此外，如果一个布尔公式$\mathcal{F}$由变量$X$构成，给定对$X$的赋值$a$，则将赋值$a$代入布尔公式$\mathcal{F}$化简所得公式记为$\mathcal{F}/a$。

(必要性)假设b是一组满足$\mathcal{XL}=\bigoplus_{1\leqslant t\leqslant T}k_t$的赋值，即$(\mathcal{XL}/b)=1$。此时，$|B_1|$一定是奇数。固定$\alpha$，考虑$c_\alpha=\bigvee_{k_t\in R_\alpha}\neg k_t\bigvee_{k_j\in K'-R_\alpha}k_j$。如果$|I_\alpha|<|R_\alpha|$，一定存在$k_i=0(k_i\in R_\alpha)$，此时$(c_\alpha/b)=1$。如果$|I_\alpha|=|R_\alpha|$，则分两种情况讨论。1)当$|I_\alpha|$为奇数时，因为$|R_\alpha|=2\alpha$为偶数，所以存在$k_i=0(k_i\in R_\alpha)$，此时$(c_\alpha/b)=1$；2)当$|I_\alpha|$为偶数时，则由$|B_1|$为奇数可知存在$k_j\in K_u-R_\alpha$满足$k_j=b_j=1$，此时$(c_\alpha/b)=1$。总之，对任意满足$(\mathcal{XL}/b)=1$的赋值$b$和任意满足$0\leqslant 2\alpha\leqslant T$的$\alpha$，总有$(c_\alpha/b)=1$。因此，对于任意满足$(\mathcal{XL}/b)=1$的赋值$b$，总有$(\mathcal{G}/b)=1$。

(充分性)使用逆否命题证明，即证明对于任意赋值b，$(\mathcal{XL}/b)=0$一定蕴含$(\mathcal{G}/b)=0$。当$(\mathcal{XL}/b)=0$时，$|B_1|$一定是偶数。令$R'=\{k_i\mid k_i\in K'$且$k_i=b_i=1\}$，则$R'\in S_{|B_1|/2}$，且对任意$k_j\in K'-R'$都有$k_j=b_j=0$。现在考虑$\mathcal{G}$的一个子句$c'=\bigvee_{k_i\in R'}\neg k_i\bigvee_{k_j\in K'-R'}k_j$。由$R'$与$c'$的构造可知$(c'/b)=0$，故$(\mathcal{G}/b)=0$。(证毕)

推论2　给定一个1-in-3公式$\mathcal{F}$，其对应的XCNF公式为$\mathcal{XF}$。$\mathcal{XF}$可以转化为等可满足的CNF公式$\mathcal{H}$。即，$\mathcal{XF}$是布尔可满足的，当且仅当$\mathcal{H}$是布尔可满足的。

证明：根据定理4，$\mathcal{XF}$的每个X-子句$\mathcal{XC}_i=\bigvee_{1\leqslant j\leqslant J_i}\mathcal{XL}_{i,j}$中的X-文字$\mathcal{XL}_{i,j}(1\leqslant j\leqslant J_i)$都可以转化为等可满足的形如式(3)的CNF公式。不妨设转化所得的CNF公式为$\mathcal{G}_{i,j}=\bigwedge_{1\leqslant t\leqslant T_{i,j}}\mathcal{D}_{i,j,t}$，其中$\mathcal{D}_{i,j,t}$表示$\mathcal{G}_{i,j}$中的子句，$T_{i,j}$表示$G_{i,j}$中的子句个数。由分配律[20]$(x\wedge y)\vee z=z\vee(x\wedge y)=(x\vee z)\wedge(y\vee z)$得$\bigvee_{1\leqslant j\leqslant J}\mathcal{G}_{i,j}=\bigvee_{1\leqslant j\leqslant J}\bigwedge_{1\leqslant t\leqslant T_{i,j}}\mathcal{D}_{i,j,t}=\bigwedge_{S\in W_i}\big(\bigvee_{\mathcal{D}\in S}\mathcal{D}\big)$，其中$W_i=\{S\mid S$为从$\mathcal{G}_{i,1},\mathcal{G}_{i,2},\cdots,\mathcal{G}_{i,J_i}$中各取一个子句构成的集合$\}$。又因$\mathcal{XF}$是$\mathcal{XC}_i$的合取，故$\mathcal{XF}=\bigwedge_{1\leqslant i\leqslant I}\mathcal{XC}_i$可转化为一个等可满足的CNF公式$\mathcal{H}=\bigwedge_{1\leqslant i\leqslant I}\bigwedge_{S\in W_i}\big(\bigvee_{\mathcal{D}\in S}\mathcal{D}\big)$。(证毕)

3.2　X-纯文字法则

观察例1中的XCNF公式$\mathcal{XF}=((1\oplus k_1)\vee(1\oplus k_2))\wedge((1\oplus k_1)\vee(1\oplus k_3))\wedge((1\oplus k_2)\vee(1\oplus k_3))\wedge((1\oplus k_2)\vee(1\oplus k_4))\wedge((1\oplus k_3)\vee(k_2\oplus k_4))\wedge((k_1\oplus k_2)\vee(1\oplus k_4))$的结构，可以看到所有关于变量$k_3$的X-文字都以$1\oplus k_3$的形式出现。我们称X-文字$1\oplus k_3$为XCNF公式$\mathcal{G}$的一个X-纯文字。一般地，给定1-in-3公式$\mathcal{F}$，假设$\mathcal{F}$的XCNF公式为$\mathcal{XF}$，定义$\mathcal{XF}$的X-纯文字如下。

定义3(X-纯文字)　如果在XCNF公式$\mathcal{XF}$中存在变量k_t只满足下面两者之一，则称k_t或$k_t\oplus 1$为XCNF公式的X-纯文字。

1)所有关于k_t的X-文字在$\mathcal{XF}$中只以k_t的形式出现；

2)所有关于k_t的X-文字在$\mathcal{XF}$中只以$1\oplus k_t$的形式出现。

可使用如下X-纯文字法则对$\mathcal{XF}$进行化简：当XCNF公式$\mathcal{XF}$中出现X-纯文字k_t(或$k_t\oplus 1$)时，删除含有k_t的X-子句得到XCNF公式$\mathcal{XF}'$。

定理5　$\mathcal{XF}$和$\mathcal{XF}'$是等可满足的，即$\mathcal{XF}$是布尔可满足的，当且仅当$\mathcal{XF}'$是布尔可满足的。

证明：不失一般性，设XCNF公式$\mathcal{XF}=\bigwedge_{1\leqslant i\leqslant I}\mathcal{XC}_i$中存在X-纯文字$k_t$。根据推论2，$\mathcal{XF}$可转化为等可满足的CNF公式$\mathcal{H}$。设$\mathcal{XF}$中每一个出现$k_t$的X-子句为$\mathcal{XC}_i=\bigvee_{1\leqslant j\leqslant J_i-1}\mathcal{XL}_{i,j}\vee k_t$。根据定理4，$\mathcal{XC}_i$中的X-文字$\mathcal{XL}_{i,j}(1\leqslant j\leqslant J_i-1)$都可以转化为等可满足的形如式(3)的CNF公式$\mathcal{G}_{i,j}$。根据X-纯文字的定义，$k_t$一定不在$\mathcal{G}_{i,j}(1\leqslant j\leqslant J_i-1)$中。根据推论2，$\bigvee_{1\leqslant j\leqslant J_i-1}\mathcal{XL}_{i,j}=\bigvee_{1\leqslant j\leqslant J_i-1}\mathcal{G}_{i,j}$可以转化为等可满足的CNF公式$\bigwedge_{S\in W_i'}\big(\bigvee_{D\in S}\mathcal{D}\big)$，其中$W_i'=\{S\mid S$为从$\mathcal{G}_{i,1},\mathcal{G}_{i,2},\cdots,\mathcal{G}_{i,J_i-1}$中各取一个子句构成的集合$\}$。因此，$\mathcal{XC}_i$可以通过$\mathcal{XC}_i=\bigvee_{1\leqslant j\leqslant J_i-1}\mathcal{XL}_{i,j}\vee k_t=\bigvee_{1\leqslant j\leqslant J_i-1}\mathcal{G}_{i,j}\vee k_t=\big(\bigwedge_{S\in W_i'}\big(\bigvee_{\mathcal{D}\in S}\mathcal{D}\big)\big)\vee k_t=\bigwedge_{S\in W_i'}\big(\bigvee_{\mathcal{D}\in S}\mathcal{D}\vee k_t\big)$转化为等可满足的CNF公式$\bigwedge_{S\in W_i'}\big(\bigvee_{\mathcal{D}\in S}\mathcal{D}\vee k_t\big)$，其中每一个子句$\mathcal{D}\vee k_t$都是$\mathcal{H}$的子句，并且变量$k_t$不在$\mathcal{D}$中出现。因此，在CNF公式$\mathcal{H}$中，$k_t$为有正极性的纯文字[2]，即在$\mathcal{H}$中只有$k_t$出现，而没有$\neg k_t$出现。根据一般SAT问题的纯文

字法则[2]，将 $k_t=1$ 代入 $\mathscr{H}$ 化简所得的 CNF 公式 $\mathscr{H}'$ 与 $\mathscr{H}$ 具有等可满足性。又因为基于 $k_t=1$ 对 $\mathscr{XF}$ 使用 X-纯文字法则化简所得公式 $\mathscr{XF}'$ 对应的 CNF 公式与对 $\mathscr{H}$ 使用 X-纯文字法则得到的 CNF 公式是同一个 CNF 公式 $\mathscr{H}'$，所以根据推论 2，$\mathscr{XF}'$ 与 $\mathscr{H}'$ 具有等可满足性。因此，$\mathscr{XF}$ 与 $\mathscr{XF}'$ 具有等可满足性。(证毕)

当 1-in-3 公式 $\mathscr{F}$ 对应的 XCNF 公式 $\mathscr{XF}$ 有 X-纯文字 k_t (或 $k_t \oplus 1$)时，对 $\mathscr{XF}$ 和 k_t 运用 X-纯文字法则，得 $k_t=1$(或 $k_t=0$)。相应地，对满足 $KE(\neg X_u)=k_t$(或 $KE(\neg X_u)=k_t \oplus 1$)的 X_u 有 $X_u=0$。将 $X_u=0$ 代入 $\mathscr{F}$ 化简得到 $\mathscr{F}'$，则有如下结论。

定理 6 $\mathscr{F}$ 是 1-in-3 可满足的，当且仅当 $\mathscr{F}'$ 是 1-in-3 可满足的。

证明：当 $\mathscr{F}$ 的 LT 方程组的通解以 K 为自由变量时，$\mathscr{F}'$ 的 LT 方程组与 $\mathscr{F}$ 代入 k_t 的赋值后化简所得公式的 LT 方程组存在相同的通解。此时，可由 $K-\{k_t\}$ 构成 $\mathscr{F}'$ 对应的 XCNF 公式 $\mathscr{XF}''$。根据定理 5，基于 X-纯文字 k_t(或 $k_t \oplus 1$)对 $\mathscr{XF}$ 使用 X-纯文字法则化简后所得的公式 $\mathscr{XF}'$ 与 $\mathscr{XF}$ 有等可满足性。下面通过证明 $\mathscr{XF}''=\mathscr{XF}'$ 来证明定理 6。

(1)根据 XCNF 公式的构造方法，$\mathscr{F}$ 中 $j_i \leqslant 2$ 的子句 C_i 在 $\mathscr{XF}$ 和 $\mathscr{XF}'$ 中没有相应的 X-子句。无论 X_u 是否出现在 C_i 中，C_i 在 $\mathscr{F}'$ 中对应的子句一定满足 $j_i \leqslant 2$，因此 C_i 在 $\mathscr{XF}''$ 中也没有相应的 X-子句。

(2)如果 $\mathscr{F}$ 中 $j_i=3$ 的子句 C_i 没有出现 X_u，则子句 C_i 仍然在 $\mathscr{F}'$ 中。由于 $\mathscr{F}$ 的 LT 方程组的通解代入 k_t 的赋值后是 $\mathscr{F}'$ 的 LT 方程组的通解，因此在 $\mathscr{F}$ 和 $\mathscr{F}'$ 中，$j_i=3$，且没有出现 X_u 的子句中的变量通解是相同的，这些子句在 $\mathscr{XF}'$ 和 $\mathscr{XF}''$ 中相应的 X-子句也是相同的。

(3)如果 $\mathscr{F}$ 中 $j_i=3$ 的子句 C_i 出现了 X_u，设 $C_i=X_u \vee X_{i,2} \vee X_{i,3}$，则 C_i 代入 $X_u=0$ 后在 $\mathscr{F}'$ 中为 $C_i'=X_{i,2} \vee X_{i,3}$，$C_i'$ 在 $\mathscr{F}'$ 中满足 $j_i=2$。根据 XCNF 公式的构造方法，C_i' 在 $\mathscr{XF}''$ 中没有对应的 X-子句。而对 $\mathscr{XF}$ 使用 X-纯文字法则后，k_t 所在的 X-子句也不会存在于 $\mathscr{XF}'$ 中。

综上，$\mathscr{XF}''=\mathscr{XF}'$。(证毕)

下面举例说明如何使用 X-纯文字法则来化简 1-in-3 公式。

例 2 在例 1 中，$1 \oplus k_3$ 为 $\mathscr{XF}$ 的一个 X-纯文字。根据 X-纯文字法则和定理 6，将 $X_3=0$ 代入 $\mathscr{F}$ 得到化简公式：

$$\mathscr{F}'=(X_1 \vee X_2 \vee X_4) \wedge (X_1 \vee X_8) \wedge (X_2 \vee X_5) \wedge (X_2 \vee X_6 \vee X_7) \wedge (X_7 \vee X_9) \wedge (X_4 \vee X_6 \vee X_{10})$$

$\mathscr{F}'$ 与 $\mathscr{F}$ 具有等价的 1-in-3 可满足性。

上文证明了 X-纯文字化简法则的正确性，下文将证明这个化简法则的高效性。实际上，可以证明：用 X-纯文字法则化简 1-in-3 公式 $\mathscr{F}$ 的最坏时间复杂度是多项式的。假设 $\mathscr{F}$ 有 n 个变量和 m 个子句，其 LT 方程组在 $\mathbb{GF}(2)$ 上的秩为 $rank(LT)$。首先，用高斯消去法求解 $\mathscr{F}$ 的 LT 方程组的时间复杂度为 $O(n^3)$[19]。然后，在构建 XCNF 公式 $\mathscr{XF}$ 时需要比较 K 表示的长度，其中计算每个 K 表示的长度需要的时间复杂度为 $O(n-rank(LT))$，因此构建 XCNF 公式 $\mathscr{XF}$ 的时间复杂度为 $O(m(n-rank(LT)))$。找出 $\mathscr{XF}$ 中的 X-纯文字 k_t 需要遍历 $\mathscr{XF}$ 中所有的 X-文字，时间复杂度同样为 $O(m(n-rank(LT)))$。最后，将 k_t 对应的 X_u 的赋值代入 $\mathscr{F}$ 化简需要的时间复杂度为 $O(m)$。

定理 7 用 X-纯文字法则化简 1-in-3 公式 $\mathscr{F}$ 的最坏时间复杂度为 $O(n^3)$。

4 其他约减规则

假设用 X-纯文字法则化简 1-in-3 公式 $\mathscr{F}$ 得到 $\mathscr{F}'$。若 $\mathscr{F}'$ 的每个子句变量个数不多于 2，则可以通过在 $\mathbb{GF}(2)$ 上求解 $\mathscr{F}'$ 的 LT 方程组来判定 $\mathscr{F}'$ 的 1-in-3 可满足性。若 $\mathscr{F}'$ 中存在子句变量个数等于 3，则可以根据下面的定理继续约减公式。

定理 8 设 1-in-3 公式 $\mathscr{F}$ 的某个子句 $\mathscr{C}$ 有 $k(k \in \{2,3\})$ 个变量。如果在这 k 个变量中至少有 $k-1$ 个变量在 $\mathscr{F}$ 中只出现一次，那么 $\mathscr{F}$ 删除 $\mathscr{C}$ 后所得的公式 $\mathscr{F}'$ 与 $\mathscr{F}$ 的 1-in-3 可满足性是等价的。

例 3 在例 2 中，化简 $\mathscr{F}$ 得到 $\mathscr{F}'$。$\mathscr{F}'$ 的子句 $C_2=X_1 \vee X_8$ 含有 2 个变量，其中 X_8 在 $\mathscr{F}'$ 中只出现了一次。根据定理 7，$\mathscr{F}'$ 删去子句 C_2 所得的 $\mathscr{F}''$ 与 $\mathscr{F}'$ 具有等价的 1-in-3 可满足性。同理，$\mathscr{F}''$ 删除子句 $X_2 \vee X_5$ 和 $X_7 \vee X_9$ 后所得的公式 $(X_1 \vee X_2 \vee X_4) \wedge (X_2 \vee X_6 \vee X_7) \wedge (X_4 \vee X_6 \vee X_{10})$ 与 $\mathscr{F}'$ 具有等价的1-in-3 可满足性。

定理 9 设 1-in-3 公式 $\mathscr{F}$ 有子句 $\mathscr{C}_0=X_i \vee X_j$，且有子句 $\mathscr{C}_1$ 包含 X_i 和 X_k，以及子句 $\mathscr{C}_2$ 包含 X_j 和 X_k，则将 $X_k=0$ 代入 $\mathscr{F}$ 化简得到公式 $\mathscr{F}'$。$\mathscr{F}$ 是 1-in-3 可满足的充分必要条件是 $\mathscr{F}'$ 是 1-in-3 可满足的。

证明：(必要性)不失一般性，设 $\mathscr{C}_1=X_i \vee X_k \vee X_s$，$\mathscr{C}_2=X_j \vee X_k \vee X_t$。若 $X_k=1$，则要使 $\mathscr{F}$ 是 1-in-3 可满足的，必有 $X_i=X_j=0$。此时，$\mathscr{C}_0$ 一定是不可满足的时。因此，$X_k=0$ 为 $\mathscr{F}$ 是 1-in-3 可满足的必要条件，即，当 $\mathscr{F}$ 是 1-in-3 可满足的，必有 $X_k=0$。综上，将 $X_k=0$ 代入 $\mathscr{F}$ 所得的 $\mathscr{F}'$ 是 1-in-3 可满足的。

(充分性)当 $\mathscr{F}'$ 是 1-in-3 可满足的，只须赋值 $X_k=0$，满足 $\mathscr{F}'$ 的赋值一定也可以满足 $\mathscr{F}$。(证毕)

例 4 给定 1-in-3 公式：

$$\mathscr{F}=(X_1 \vee X_2 \vee X_3) \wedge (X_1 \vee X_4) \wedge (X_2 \vee X_3 \vee X_4)$$

$\mathscr{F}$ 中有子句 $X_1 \vee X_4$，且有子句 $X_1 \vee X_2 \vee X_3$ 包含 X_1 和 X_2，以及子句 $X_2 \vee X_3 \vee X_4$ 包含 X_2 和 X_4。根据定理 8，将 $X_2=0$ 代入 $\mathscr{F}$ 化简得到公式 $\mathscr{F}'=(X_1 \vee X_3) \wedge (X_1 \vee X_4) \wedge (X_3 \vee X_4)$，$\mathscr{F}$ 与 $\mathscr{F}'$ 具有等价的 1-in-3 可满足性。

下面简要证明使用定理 7 和定理 8 化简 1-in-3 公式 $\mathscr{F}$ 的最坏时间复杂度也是多项式的。假设 $\mathscr{F}$ 有 n 个变量和 m 个子句，使用定理 7 化简 $\mathscr{F}$ 时，需要遍历每个子句，时间复杂度

为 $O(m)$。使用定理 8 化简 $\mathcal{F}$ 时，首先需要遍历所有子句，找到形如 $C_0=X_i \vee X_j$ 的子句；然后再次遍历公式，找到符合条件的变量 X_k；最后重复上述过程，重复次数不超过 m。因此，使用定理 8 化简 1-in-3 公式的复杂度为 $O(m^3)$。

结束语　本文从两个角度提出了 1-in-3-SAT 的文字约减法则。1)根据 1-in-3 公式 $\mathcal{F}$ 构建了一个 XCNF 公式($\mathcal{F}$ 是 1-in-3 可满足的，当且仅当其 XCNF 公式是布尔可满足的)，利用 X-纯文字法则，得出 $\mathcal{F}$ 中对应变量的赋值。将这个赋值代入 $\mathcal{F}$ 后，可以得到一个具有等价 1-in-3 可满足性的化简公式。2)直接观察 1-in-3 公式的结构。如果公式中存在变量有某些特性，则可以消去一些变量或者子句，从而化简公式。上述约减方法都可以在多项式时间内完成。本文所提出的 1-in-3-SAT 文字约减规则可减小问题规模，提高问题的求解效率。未来可从以下方面进行进一步的研究。首先，在构建 XCNF 公式的过程中，研究自由变量 K 的选择是否会影响 XCNF 公式中 X-纯文字的个数。其次，能否找到一种方法，在不转化为 CNF 的情况下，直接判定 XCNF 公式的布尔可满足性。另外，还计划将本文所述的约减方法与 1-in-3-SAT 问题的求解方法相结合，并将这些方法进行对比。

参 考 文 献

[1] SCHAEFER T J. The complexity of satisfiability problems [C]// Proceedings of the Tenth Annual ACM Symposium on Theory of Computing. New York: ACM, 1978: 216-226.

[2] DAVIS M, PUTNAM H. A computing procedure for quantification theory [J]. Journal of the ACM, 1960, 7(3): 201-215.

[3] DAVIS M, LOGEMANN G, LOVELAND D. A machine program for theorem proving [J]. Communications of the ACM, 1962, 5(7): 394-397.

[4] MARQUES-SILVA J P, SAKALLAH K A. GRASP: A search algorithm for propositional satisfiability[J]. IEEE Transactions on Computers, 1999, 48(5): 506-521.

[5] LIANG J H, GANESH V, ZULKOSKI E, et al. Understanding VSIDS branching heuristics in conflict driven clause learning SAT solvers[C]// Haifa Verification Conference. Cham: Springer, 2015: 225-241.

[6] CHENG R, ZHOU C L, XU N, et al. Comprehensive analysis of restart strategies of cdcl sat solver[J]. Journal of Computer-Aided Design and Computer Graphics, 2018, 30(6): 1136-1144.

[7] HOOS H H, STUTZLE T. Local search algorithms for SAT: an empirical evaluation [J]. Journal of Automated Reasoning, 2000, 24(4): 421-481.

[8] BALINT A, FROHLICH A. Improving stochastic local search for SAT with a new probability distribution[C]// International Conference on Theory and Applications of Satisfiability Testing. Heidelberg: Springer, 2010: 10-15.

[9] HONG J K, ZHANG Z H, XU G P. SAT local search algorithm based on enhanced probability controlling strategies[J]. Computer Engineering and Applications, 2017, 53(14): 56-60, 110.

[10] SHANG Y, WAH B W. A discrete Lagrangian-based global-search method for solving satisfiability problems[J]. Journal of global optimization, 1998, 12(1): 61-99.

[11] GU J. Optimization algorithms for the satisfiability (SAT) problem[C]// Advances in Optimization and Approximation. Boston: Springer, 1994: 72-154.

[12] BRAUNSTEIN A, ZECCHINA R. Survey and belief propagation on random k-SAT[C]// International Conference on Theory and Applications of Satisfiability Testing. Berlin: Springer, 2003: 519-528.

[13] WANG F, ZHOU Y R, YE L. Ant colony algorithm combined with survey propagation for satisfiability problem[J]. Computer Science, 2012, 39(4): 227-231.

[14] WANG X F, XU D Y, JIANG J L, et al. Sufficient conditions for convergence of the survey propagation algorithm [J]. Science China Information Sciences, 2017, 47(12): 1646-1661.

[15] FANG C, LIU J. A linear algebra formulation for boolean satisfiability testing[J/OL]. http://arxiv.org/abs/1701.02401.

[16] LIU J, ZHOU H H. A development of laf for satisfying assignments search [C]// 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019: 719-726.

[17] PATRASCU M, WILLIAMS R. On the possibility of faster SAT algorithms[C]// Proceedings of the Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms. Austin: Society for Industrial and Applied Mathematics, 2010: 1065-1075.

[18] KARP R M. Reducibility among combinatorial problems[M]// Complexity of computer computations. Boston: Springer, 1972: 85-103.

[19] LAMACCHIA B, ODLYZKO A. Solving large sparse linear systems over finite fields[C]// Conference on the Theory and Application of Cryptography. Berlin: Springer, 1990: 109-133.

LIU Jiang, born in 1979, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include computability theory, formal methods and computer algorithms.