基于Euclid算法的广义猫映射构造方法及在图像置乱中的应用

李用江[1,2] 李昌利[2] 葛建华[1] 孙志林[3]

(西安电子科技大学综合业务网国家重点实验室 西安 710071)[1]

(广东海洋大学信息学院 湛江 524088)[2] (河南宇通信息技术有限公司 郑州 450003)[3]

摘 要 基于欧几里得算法求乘法逆元的思想,提出了两种构造广义猫映射的简单方法。一种基于Fibonacci序列,一种基于Dirichlet序列;还给出了结合这两个序列的构造方法。仿真实验表明广义猫映射的变换周期是可变的并且相对于猫映射更大,从而有较好的置乱效果,这也使得它的安全性优于猫映射和Fibonacci等置乱变换。在图像信息隐蔽存储与传输中,这类图像变换具有重大的应用价值,为图像置乱提供了更坚实的理论基础。

关键词 欧几里得算法,图像置乱,广义猫映射,Dirichlet序列,Fibonacci序列

中图法分类号 TP301.6 **文献标识码** A

Study on Construction Methods Based on the Euclid Algorithm for Generalized Cat Map and its Application in Image Scrambling

LI Yong-jiang[1,2] LI Chang-li[2] GE Jian-hua[1] SUN Zhi-lin[3]

(State Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071, China)[1]

(School of Information, Guangdong Ocean University, Zhanjiang 524088, China)[2]

(Henan Yu-tong Information Technology Co. Ltd., Zhengzhou 450003, China)[3]

Abstract Based on the idea of multiplication inverse of Euclid algorithm, two easy construction methods for generalized cat map were presented. One is based on the Fibonacci series and the other is based on the Dirichlet series. Moreover, one construction method was presented combined with these two series. Simulation experiments show that the period of generalized cat map is alterable and greater compared with that of cat map, thus they have better scrambling effect and also make them much securer than cat map and Fibonacci transform. In practice they can find great value in practice in image information hiding for storage and transmission and provide a much solider theoretical foundation for image scrambling.

Keywords Euclid algorithm, Image scrambling, Generalized cat map, Dirichlet series, Fibonacci series

信息安全已成为当前学术界和产业界关注的热点,图像版权保护就是其中一个重要的课题。而传统的保密方法对于图像信息保护的研究远远不能满足用户的需求。随着计算机技术与数字图像处理技术的发展,对图像信息的处理已有一些成果[1],如数字水印技术、图像信息隐藏[2-5],而图像置乱是信息隐藏的基础[2]。Arnold变换,或者说猫映射具有很好的混沌特性[2,6],将它引入到图像的置乱处理获得了良好的效果。但由于猫映射有周期性[2,7],且参数仅有4个,用于数据加密时容易受到攻击。文献[8]将猫映射进行了推广,但在图像加密系统中密钥所要求输入的参数较少,广义猫映射的形式也只有4种,尽管系统也具有置换、替代、扩散等加密系统的基本要素,但抗明文攻击的能力较弱,这就带来了不安全。文献[9]提出了基于拟仿射变换的数字图像置乱加密算法,研究了QATLIC的性质及构造方法。受此启发本文提出了两种使用欧几里得算法[10]构造广义猫映射的简单方法。

1 猫映射及广义猫映射

猫映射最早由Arnold引入,因经常用一张猫脸进行演示而得名[6]。设有单位正方形上的点(x_n, y_n),将点(x_n, y_n)通过下式变换为另一点(x_{n+1}, y_{n+1}):

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ 1) \tag{1}$$

对任意x有$x \bmod 1 = x - [x]$,其中$[x]$表示x的整数部分。猫映射具有保面积性、实数上的一一映射性和混沌性。文献[8]将猫映射推广为广义猫映射。首先将相空间推广为$Z_N \times Z_N$($Z_N = \{0, 1, 2, \cdots, N-1\}$),即只取0到$N-1$的正整数。其次将方程推广为最一般的二维可逆保面积方程:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ N) \tag{2}$$

到稿日期:2009-12-10 返修日期:2010-02-11 本文受"863"计划课题(B50306290182),国家自然科学基金(J60104010107),国家卫星应用高技术产业化重大专项:北斗/GPS宽温兼容型卫星定位导航应用系统资助。

李用江(1967-),男,博士生,副教授,主要研究方向为网络安全与信息隐藏、电子商务等,E-mail:LyjRiver@21cn.com;**李昌利**(1976-),男,博士生,讲师,主要研究方向为盲信号处理;**葛建华**(1961-),男,教授,博士生导师,主要研究方向为信息安全、通信系统、数字电视等;**孙志林**(1963-),男,博士,教授级高工,博士生导师,主要研究方向为网络安全和GPS卫星定位技术。

式中，$a,b,c,d,x_n,y_n,x_{n+1},y_{n+1}$均为整数，且$\Delta=\begin{vmatrix}a & b\\ c & d\end{vmatrix}=\pm1$和$0\leqslant x_n,y_n,x_{n+1},y_{n+1}<N$。

广义猫映射具有保面积性、整数上的一一映射性，但不再具有严格意义上的混沌性。此外它具有周期性。一幅图像经若干次迭代之后又恢复到原来图像，所以广义猫映射在选择迭代次数时要注意其周期性。

2 两种广义猫映射的构造方法

2.1 使用 Fibonacci 序列构造广义猫映射

对于整数序列a_k，如果$a_1=0,a_2=1$，当$k>2$有$a_k=ma_{k-1}+a_{k-2}$，其中m为非零的整数，则称a_k为广义 Fibonacci 序列。当$m=1$时a_k即为经典的 Fibonacci 序列。

定理 1 任意给出广义 Fibonacci 序列中连续的两个整数a_k,a_{k+1}，其中$k>1$，都可以构造出一个整数矩阵$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$，使得$ad-bc=\pm1$。

证明：当a_k和a_{k+1}不同时为 1 时，使用欧几里得算法[10]求乘法逆元的计算方法，对a_k和a_{k+1}组成的列向量进行以下初等行变换：

$$\begin{pmatrix}0 & 1\\ 1 & -m\end{pmatrix}\begin{pmatrix}a_{k+1}\\ a_k\end{pmatrix}=\begin{pmatrix}a_k\\ a_{k+1}-ma_k\end{pmatrix}=\begin{pmatrix}a_k\\ a_{k-1}\end{pmatrix}\tag{3}$$

不断重复式(3)的过程，最后这两个数将成为 1 和 0，即有

$$\begin{pmatrix}0 & 1\\ 1 & -m\end{pmatrix}^{k-1}\begin{pmatrix}a_{k+1}\\ a_k\end{pmatrix}=\begin{pmatrix}a_2\\ a_1\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}\tag{4}$$

显然矩阵$\begin{pmatrix}0 & 1\\ 1 & -m\end{pmatrix}$的逆矩阵为$Q_m\triangleq\begin{pmatrix}m & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}a_3 & a_2\\ a_2 & a_1\end{pmatrix}$，$Q_m$的行列式为$|Q_m|=-1$。由于

$$\begin{pmatrix}m & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}m & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}m & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a_3 & a_2\\ a_2 & a_1\end{pmatrix}=\begin{pmatrix}a_4 & a_3\\ a_3 & a_2\end{pmatrix}$$

用递推法，很容易得出Q_m有以下重要性质：

$$Q_m^k=\begin{pmatrix}a_{k+2} & a_{k+1}\\ a_{k+1} & a_k\end{pmatrix}$$

上式两边取行列式得$|Q_m^k|=|Q_m|^k=(-1)^k=a_{k+2}a_k-a_{k+1}^2$，从而$a_{k+2}a_k-a_{k+1}^2=\pm1$，令$\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a_{k+2} & a_{k+1}\\ a_{k+1} & a_k\end{pmatrix}$，即完成了广义猫映射的构造。

2.2 使用 Dirichlet 序列构造广义猫映射

若a,b互素，序列$\{a_k\}$满足$a_k=(k-1)a+b$，其中k为非零的整数，称这个序列为 Dirichlet 序列[10]。实际上它是一个特殊的等差序列。

引理 1 任意给出两个互素的整数a,c都可以构造出一个整数矩阵$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$，使得$ad-bc=\pm1$。

证明：分 3 种情况证明。

当$a=c=1$时，b,d取两个连续的整数即可。当a,c仅有一个为 1 时，不妨设$a=1$。任取一个整数作为b，取d为$bc\pm1$。当a,c均不为 1 时，为简化讨论，不妨设$a>c>1$。下面使用欧几里得算法[10]求乘法逆元的计算方法，对a,c组成的列向量进行初等行变换：

$$\begin{pmatrix}0 & 1\\ 1 & -\left[\frac{a}{c}\right]\end{pmatrix}\begin{pmatrix}a\\ c\end{pmatrix}=\begin{pmatrix}c\\ a\ (\mathrm{mod}\ c)\end{pmatrix}=\begin{pmatrix}c\\ a'\end{pmatrix}\tag{5}$$

显然$c>a'>1$成为类似$a>c>1$的情形，继续重复式(5)的过程，最后这两个数将成为 1 和 0。根据欧几里得算法可以知道，所需的矩阵个数不多于$2\log_2 C$[10]，记这一序列的矩阵为A_i，很显然$|A_i|=-1$。定义$A=\prod_i A_i$，显然$|A|=-1$，上述变换过程可表示为：

$$A\begin{pmatrix}a\\ c\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}\tag{6}$$

现在任取一个整数z和z'，其中$z'=\pm1$，构造向量$\begin{pmatrix}z\\ z'\end{pmatrix}$。现在对矩阵$\begin{pmatrix}1 & z\\ 0 & z'\end{pmatrix}$按式(6)所示的变换进行逆变换，最终得到的矩阵为：

$$A^{-1}\begin{pmatrix}1 & z\\ 0 & z'\end{pmatrix}=\begin{pmatrix}a & A^{-1}\begin{pmatrix}z\\ z'\end{pmatrix}\end{pmatrix}\triangleq\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

显然$\begin{vmatrix}a & b\\ c & d\end{vmatrix}=\left|A^{-1}\begin{pmatrix}1 & z\\ 0 & z'\end{pmatrix}\right|=|A^{-1}|\left|\begin{pmatrix}1 & z\\ 0 & z'\end{pmatrix}\right|=\pm1$。至此完成了式中$a,b,c,d$的构造。

定理 2 任意给出 Dirichlet 序列中连续的两个整数a_k，a_{k+1}，其中$k>1$，都可以构造出一个整数矩阵$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$使得$ad-bc=\pm1$。

证明：当a,b同时为 1 时，Dirichlet 序列退化为自然数序列，很容易构造出一个满足条件的矩阵$\begin{pmatrix}k+2 & k+1\\ k+1 & k\end{pmatrix}$，其中$k$为任意正整数。

当a,b不同时为 1 时，使用欧几里得乘法[10]求乘法逆元的计算方法，对 Dirichlet 序列中的两个整数a_k,a_{k+1}组成的列向量进行以下变换：

$$\begin{pmatrix}0 & 1\\ 1 & -(k-1)\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}a_{k+1}\\ a_k\end{pmatrix}$$
$$=\begin{pmatrix}0 & -1\\ -(k-1) & k\end{pmatrix}\begin{pmatrix}ka+b\\ (k-1)a+b\end{pmatrix}=\begin{pmatrix}a\\ b\end{pmatrix}$$

由引理知对$\begin{pmatrix}a\\ b\end{pmatrix}$可完成广义猫映射的构造。

事实上，从上式证明过程中得$\begin{pmatrix}a_{k+1}\\ a_k\end{pmatrix}=Q_1D_{k-1}\begin{pmatrix}a\\ b\end{pmatrix}$，其中$Q_1=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$(即$m=1$时的$Q_m$)，$D_{k-1}=\begin{pmatrix}(k-1) & 1\\ 1 & 0\end{pmatrix}$。

在实际构造时，a,b可以取经典 Fibonacci 序列中的两个整数a_n,a_{n+1}，由此可以构造出一个矩阵$Q_1^n=\begin{pmatrix}a_{n+2} & a_{n+1}\\ a_{n+1} & a_n\end{pmatrix}=\begin{pmatrix}a+b & a\\ a & b\end{pmatrix}$。那么由 Dirichlet 序列中连续的两个整数a_k，a_{k+1}构造的满足条件的矩阵可以表示为：

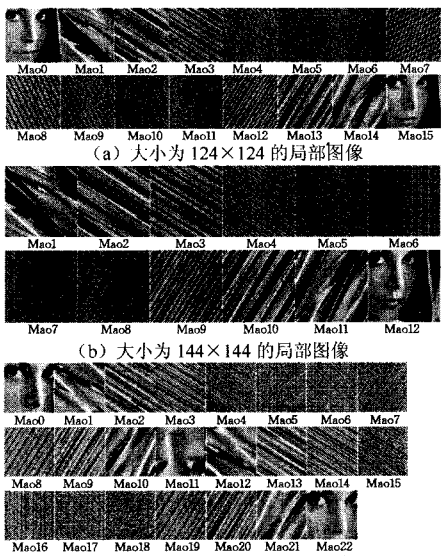
$$Q_1D_{k-1}Q_1^n=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}k-1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a+b & a\\ a & b\end{pmatrix}$$
$$=\begin{pmatrix}k(a+b)+a & a_{k+1}\\ (k-1)(a+b)+a & a_k\end{pmatrix}\tag{7}$$

例如当$a=5,b=3$时，$k=3,5,10$所对应的矩阵分别为：$\begin{pmatrix}29 & 18\\ 21 & 13\end{pmatrix}$，$\begin{pmatrix}45 & 38\\ 37 & 23\end{pmatrix}$和$\begin{pmatrix}85 & 53\\ 77 & 48\end{pmatrix}$。或者$k,n$分别取大于 2 的正整数，计算$Q_1D_{k-1}Q_1^n$得到对应的矩阵。例如$k=3,n=6$

对应的矩阵为 $\begin{pmatrix}47 & 29\\ 34 & 21\end{pmatrix}$，$k=4$，$n=5$ 对应的矩阵为 $\begin{pmatrix}37 & 23\\ 29 & 18\end{pmatrix}$。

3 仿真实验与分析

本文对 512×512 的 Lena 图像进行了仿真实验。不失一般性，只对其局部进行了实验。首先给出 3 个基于猫映射的图像变换实例。当图像大小分别为 124×124，144×144，89×89 时，猫映射的变换周期分别为 15，12，22，对应的猫映射图像状态如图 1 所示。接着给出 3 个基于广义猫映射的图像变换实例。当图像尺寸分别为 95×95，144×144，121×121 时，它们的广义猫映射变换的图像状态如图 2 所示。

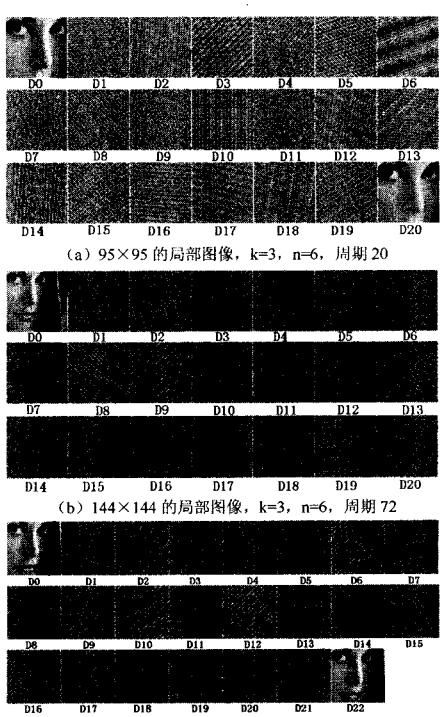


（a）大小为 124×124 的局部图像

（b）大小为 144×144 的局部图像

（c）大小为 89×89 的局部图像

图 1　猫映射的图像变换状态



（a）95×95 的局部图像，k=3，n=6，周期 20

（b）144×144 的局部图像，k=3，n=6，周期 72

（c）121×121 的局部图像，k=3，n=6，周期 22

图 2　广义猫映射的图像状态变换

图像置乱的功能是扰乱图像的像素位置，将原始图像变换成一个杂乱无章的新图像，如果不知道所使用的置乱变换，就很难恢复出原始图像。通常图像置乱是图像信息隐藏、图像信息分存和数字水印等任务的基础性工作，置乱方法的优劣将直接影响其它任务的效果。而基于猫映射的图像置乱效果较差。从图 1 中可以直观地看出，当变换次数为 1～3 时置乱的效果都差。因为图像变换在有限域中是有周期性的[7]，所以对不同的图像大小来说，猫映射的周期是不同的，有时它的周期很小，在工程中是无法使用的。相对于以上不足，基于广义猫映射的图像置乱变换的置乱效果很好。从图 2 中可以直观地看出，即使只有一次变换，图像的置乱效果在统计上和视觉上都具有服从均匀分布的白噪声的特性。

其次，广义猫映射的周期可以选择较大的。例如当图像大小为 144×144 时，猫映射的变换周期为 12，而使用 $k,n=3,6$ 的广义猫映射时，它的变换周期为 72，它的周期是猫映射的变换周期的 6 倍。当局部图像的大小为其它值时，结论是一致的，猫映射和广义猫映射对应的周期如表 1 所列。广义猫映射可以通过计算 $Q_1 D_{k-1} Q_1^n$ 得到，由于 k,n 的取值范围大，因此算法具有很好的适应性，也就是说对任意大小的图像总可以选出一个周期比较大的广义猫映射，从而解决了猫映射图像置乱效果差的问题，而两者的计算复杂性是一样的。

表 1　猫映射和广义猫映射的周期比较

图像大小	猫映射	广义猫映射	倍数
55×55	10	110	11
144×144	12	72	6
165×165	20	330	16.5
231×231	40	462	11.55
252×252	24	252	10.5
275×275	50	550	11
329×329	16	322	20.125
385×385	40	770	19.25
396×396	60	396	6.6
422×422	21	210	10
440×440	30	220	7.3333
451×452	20	154	7.7
461×462	23	231	10.043
495×495	60	990	16.5
504×504	24	252	10.5

再次，在图像加密时，可以让用户输入 k,n 及叠代次数作为密钥，由于输入的参数可多选，密钥空间大，真正可以做到一次一密，彻底解决文献[8]中广义猫映射的形式只有 4 种选择的困境，增了加图像加密系统的安全。

结束语　本文分析了猫映射和广义猫映射在图像置乱处理中的效果，结果表明后者的周期可变，置乱效果更好。本文提出两种有效的方法用于构造广义猫映射，一种基于 Fibonacci 序列，一种基于 Dirichlet 序列。此外文章还给出结合这两个序列构造广义猫映射的方法。这些方法为图像置乱提供了更坚实的理论基础。广义 Fibonacci 序列和 Dirichlet 序列的一个突出性质是它们的任意两个相邻的元素互素，故广义猫映射中的参数 a,c 可任取序列中的两个相邻元素。在程序实现时，可以将用户的自行输入作为加密的密钥，可以做到一次一密，从而大大增加了图像加密系统的安全性。

参 考 文 献

[1] 王朔中，张新鹏，张开文. 数字密写和密写分析[M]. 北京：清华大学出版社，2005：5-7

[2] Qi D X，Zou J C H，Han X Y. A new class of scrambling trans-

formation and its application in the image information covering [J]. Science in China (Series E), 2000, 43(3): 304-412

[3] 王泽辉. 二维随机矩阵置乱变换的周期及在图像信息隐藏中的应用[J]. 计算机学报, 2006, 29(12): 2218-2224

[4] 杨军, 覃伯平, 雷开彬, 等. 基于广义猫映射的组播密钥管理方案研究[J]. 计算机科学, 2008, 35(1): 80-82

[5] 邵利平, 覃征, 刘波, 等. 二维双尺度矩形映射及其在图像置乱上的应用[J]. 计算机辅助设计与图形学学报, 2009, 21(7): 1025-1033

[6] Arnold V I, Avez A. Ergodic Problems of Classical Mechanics [M]// Mathematical Physics Monograph Series. NewYork: W A Benjamin, INC, 1968

[7] 李用江, 李昌利, 李司东, 等. Fibonacci 数列模 p^r 的周期性研究[J]. 数学的实践与认识, 2009, 39(17): 138-143

[8] 马在光, 丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报, 2003, 24(2): 51-57

[9] 朱桂斌, 曹长修, 胡中豫, 等. 基于仿射变换的数字图像置乱加密算法[J]. 计算机辅助设计与图形学学报, 2003, 15(6): 711-715

[10] Garrett P. 密码学导论[M]. 吴世忠, 等译. 北京: 机械工业出版社, 2003: 94-100, 154

(上接第 256 页)

但针对不同的 QBF 公式所得结果并不稳定，对于某些问题仍然会花费较长时间，但这种非 CNF 的思想是值得深入研究的。

基于 QBF 的规划方法的求解性能依赖于 QBF 编码的构造和求解两个方面，不同 QBF 编码的选用很大程度上依赖于对应的 QBF 求解器的性能。可以考虑两种解决策略：设计与具体求解器完美匹配的有效编码或者设计求解具体编码的最佳性能的 QBF 求解器。显然，区别于 QBF 求解技术的研究，有效的 QBF 编码设计是基于转换的规划方法的核心问题。随着各种复杂规划问题的提出，并进一步参与规划系统性能的衡量，迫切要求为其设计新的对应编码方式，使得日趋成熟的 QBF 技术得以在智能规划领域中得到利用。

参 考 文 献

[1] Peot M A, Smith D E. Conditional nonlinear planning[C]// Hendler J, ed. Proceedings of the First International Conference on Artificial Intelligence Planning Systems. 1992: 189-197

[2] Pryor L, Collins G. Planning for contingencies: A decision-based approach[J]. Journal of Artificial Intelligence Research, 1996 (4): 287-339

[3] Cimatti A, Roveri M, Traverso P. Automatic OBDD - based generation of universal plans in non-deterministic domains[C]// Proceedings of the Fifteenth National Conference on Artificial Intelligence(AAAI-98) and the Tenth Conference on Innovative Applications of Artificial Intelligence (IAAI-98). 1998: 875-881

[4] Bonet B, Geffner H. Planning with incomplete information as heuristic search in belief space[C]// Chien S, Kambhampati S, Knoblock C A, eds. Proceedings of the Fifth International Conference on Artificial Intelligence Planning Systems. 2000: 52-61

[5] Kautz H, Selman B. Planning as satisfiability[C]// Neumann B, ed. Proceedings of the 10th European Conference on Artificial Intelligence. 1992: 359-363

[6] Kautz H, Selman B. Pushing the envelope: planning, propositional logic, and stochastic search[C]// Proceedings of the 13th National Conference on Artificial Intelligence and the 8th Innovative Applications of Artificial Intelligence Conference. 1996: 1194-1201

[7] Kautz H, McAllester D, Selman B. Encoding plans in propositional logic[C]// Proc. 5th International Conference of Principles of Knowledge Representation and Reasoning. 1996

[8] Rintanen J. Constructing conditional plans by a theorem-prover [J]. Journal of Artificial Intelligence Research, 1999 (10): 323-352

[9] Giunchiglia E, Lifschitz V. An action language based on causal explanation: Preliminary report[C]// Proceedings of The Fifteenth National Conference on Artificial Intelligence. 1998: 623-630

[10] Giunchiglia E. Planning as satisfiability with expressiveaction languages: concurrency, constraints and nondeterminism[C]// Cohn A G, Giunchiglia F, Selman B, eds. Proceedings of the Seventh International Conference of Principles of Knowledge Representation and Reasoning. 2000: 657-666

[11] Brafman R I, Hoffmann J. Conformant planning via heuristic forward search: A new approach[C]// Proceedings of the 14th International Conference on Automated Planning and Scheduling. 2004: 355-364

[12] Palacios H, Geffner H. Reducción de la planificación conformante a SAT mediante compilación a d-DNNF[C]// 11th Conferencia de la Asociación Espanola para la Inteligencia Artificial; an ICAPS' 05 Workshop as Mapping Conformant Planning into SAT Through Compilation and Projection. 2005

[13] Palacios H, Bonet B, Darwiche A, et al. Pruning conformant plans by counting models on compiled d-DNNF representations [C]// Biundo S, Myers K, Rajan K, eds. Proceedings of the Fifteenth International Conference on Automated Planning and Scheduling(ICAPS 2005). 2005: 141-150

[14] Rintanen J, Heljanko K, Niemelä I. Planning as satisfiability: parallel plans and algorithms for plan search[J]. Artificial Intelligence, 2006, 170(12/13): 1031-1080

[15] Rintanen J. Asymptotically optimal encodings of conformant planning in QBF[C]// Proceedings of the 22nd AAAI Conference on Artificial Intelligence (AAAI-07). 2007: 1045-1050

[16] Balcázar J L, Díaz I, Gabarró J. Structural Complexity I[M]. Berlin: Springer-Verlag, 1995

[17] Giunchiglia E, Narizzano M, Tacchella A. Backjumping for Quantified Boolean Logic Satisfiability [J]. Artificial Intelligence, 2003, 145(1/2): 99-120

[18] Giunchiglia E, Narizzano M, Tacchella A. Learning for quantified Boolean logic satisfiability[C]// Proceedings of the 18th National Conference on Artificial Intelligence (AAAI-2002) and the 14th Conference on Innovative Applications of Artificial Intelligence (IAAI-2002). 2002: 649-654

[19] Biere A. Resolve and expand: Theory and Applications of Satisfiability Testing[C]// 7th International Conference SAT. Vancouver, BC, Canada, May 2004

[20] Zhang L, Malik S. Conflict driven learning in a quantified Boolean satisfiability solver[C]// Proceedings of the 2002 IEEE/ACM International Conference on Computer Aided Design (ICCAD2002). 2002: 442-448

[21] Stockmeyer L J, Meyer A R. Word problems requiring exponential time[J]. Journal of the ACM, 1973: 1-9

[22] Florian L, Armin B. Expanding NNF for QBF Solving[C]// SAT 2008. Vol. 4996. Springer, 2008: 196-210