概率规划的研究

刘 莹[1,2] 谷文祥[2]

(东北师范大学人文学院 长春 130117)[1] (东北师范大学计算机科学与信息技术学院 长春 130117)[2]

摘 要 概率规划是智能规划的一个研究热点,由于其自身的现实意义而被越来越多的学者关注。目前,已有许多学者对概率规划做出了新的扩展,使其应用的范围更广。着重介绍近年来概率规划的发展现状以及用重规划方法解决概率规划问题的规划器(FF-Replan),并介绍了近几届国际概率规划竞赛(IPPC),使广大学者可以对概率规划有一个更新、更全面的了解。

关键词 智能规划,概率规划,PPDDL,FF-Replan

中图法分类号 TP18 **文献标识码** A

Research of Probabilistic Planning

LIU Ying[1,2] GU Wen-xiang[2]

(College of Humanities & Science, Northeast Normal University, Changchun 130117, China)[1]

(School of Computer Science and Information Technology, Northeast Normal University, Changchun 130117, China)[2]

Abstract The probabilistic planning is a hot spot of intelligent planning research and is paid attention to its own practical significance by more and more scholars. At present, many scholars have made the new expansion to the probabilistic planning. This paper emphatically introduced the development of probabilistic planning in recent years, as well as the probabilistic planner(FF-Replan). Then the International Probabilistic Planning Competition was presented. It enables the general scholars to have a more comprehensive understanding to the probabilistic planning.

Keywords Intelligent planning, Probabilistic planning, PPDDL, FF-repaln

1 引言

智能规划是近年来人工智能研究中发展十分迅速的一个领域,由于具有很好的应用前景,受到广大学者的普遍重视,现在已经成为人工智能领域中一个极为活跃的研究热点。以往的经典规划问题需要符合某些限定条件[1]:1)动作执行后的结果都是确定的,即在任何状态下,动作的执行只能得到唯一的一个结果状态;2)Agent 对于规划世界的全部信息都是已知的;3)Agent 要实现的目标是已知的、确定的。这些限定是一种对客观世界简化了的描述,但并不符合实际。我们知道不是所有的事情都是可以预测的,即我们所得到的信息往往是不完整的、不确定的,这就使得规划理念在现实应用中受到了极大的限制。为了解决实际存在的不确定的规划问题,产生了一些不确定规划器,如 SNLP[2],Buridan[3],MAXPLAN[4]等,但这些规划器都是针对特定应用领域的,不具有一般性。为了扩大智能规划的应用范围,国内外诸多学者开始寻找更一般的算法来处理这些不确定性问题、非决定性和不完全信息问题[5]。

本文首先介绍了近年来概率规划的发展及国际概率规划竞赛的情况,其次简述了概率规划的表示及其扩展,最后介绍如何使用重规划方法来解决概率规划问题,即在 2004 年的国际规划竞赛中脱颖而出的 FF-Replan[6]。

2 概率规划的发展与近况

1995 年,由 Kushmerick, Hanks 和 Weld 提出的 Buridan 就是第一批专门针对概率 STRIPS 域的第一个规划器,其主要思想是先将一个不确定的规划问题转换为一个空规划,然后通过规划改进和规划估价来求得满足给定条件的规划,而 C-Buridan[7]扩展了 Buridan 并产生了随机规划。这些规划器可以处理的动作结果是部分可观察的情况,但其求解速度较慢。

1998 年,S. M. Majercik 和 M. L. Littman 提出了一款名为 MAXPLAN[4]的规划器,它的主要思想是将一个不确定的规划问题转换为一个随机的可满足性问题,然后利用标准的求解器进行求解。这是一种基于编译的不确定规划方法。

1999 年,A. Blum 和 J. Langford 在规划图的基础上提出了概率规划算法 PGraphplan[8](简称 PGP),该算法包括规划图扩张和有效规划提取两个阶段,处理的对象是动作结果不确定的规划问题。它采用一个概率分布来描述动作结果的不确定性,动作执行后产生的每个可能的结果都附有相关的概率值。PGP 相比当时存在的规划器,速度较快,但也有不足之处,如每个时间步只允许执行一个非空动作,不能处理初始

到稿日期:2010-08-02 返修日期:2010-11-08 本文受国家自然科学基金(61070084,60473042,60573067 和 60803102)资助。

刘 莹(1980—),女,博士生,主要研究方向为智能规划与规划识别,E-mail:liuy125@nenu.edu.cn;谷文祥(1947—),男,教授,博士生导师,主要研究方向为智能规划与规划识别、形式语言与自动机、模糊数学及其应用。

条件不确定的情况等。

2003 年，谷文祥、欧华杰等人开发出了一款在图规划框架下改进的概率规划器[9]，它可以解决大部分规划问题，生成的规划图结点少，速度快。

2005 年，Mausam 和 Daniel S. Weld 在并行马尔可夫决策过程[10]的基础上，提出了并行概率时序规划 CPTP[11]。其主要思想是在增量的状态空间中，通过将问题编码为并行马尔可夫决策过程，在并行马尔可夫模型中加入明确的动作持续时间，并通过加入两个新颖可纳的启发式和一个不可纳的启发式来加速这个算法。实验表明，该算法的速度比其它方法的更快。

2006 年，Mausam 和 Daniel S. Weld 又提出了动作持续时间不确定的实时概率规划[12]，共描述了 5 种求解方法，如 ΔDUR_{samp}，ΔDUR_{arch}，ΔDUR_{exp}，ΔDUR_{hyb}，ΔDUR_{prun}。该规划算法可以处理随机持续时间下的概率效果，并在持续时间分布是复合式的情况下也是有效的。

同年，Iain Little 和 Sylvie Thiébaux 提出了一款并行概率规划器 Paragraph[13]，其主要思想就是将整个图规划框架扩展到概率规划问题域中，利用状态信息将使用 Graphplan 目标回溯搜索所找出的所有路径合并在一起，生成最优并行随机规划。

2007 年，Daniel Bryce 和 William Cushing 等提出了一款 MOLAO* 的多目标概率规划器[14]，它可以得到所有目标尽量满足的可行解。

2008 年举办的国际规划竞赛中的概率规划器 RFF[15]，FSP*[16]等也都是非常优秀的。

3 国际概率规划竞赛(IPPC)

国际规划竞赛(IPC)是每两年举行一次的调度和规划国际会议，其目标包括分析和推进先进的规划系统与先进自动化的配合，为评价自动规划的不同方法提供新的数据集基准，强调规划中新问题的研究，推进规划技术的发展和应用。概率规划在实际应用中越来越广，进而受到越来越多的研究者关注。在 2004 年的第四届国际规划竞赛中，首次将概率规划单独分组进行比赛。

3.1 IPPC-04

2004 年，第四届国际规划比赛(IPC-4)[17]在加拿大举行，概率部分由 Michael Littman 和 Hakan Younes 共同组织，称其为 IPPC-04，共有 NMRDPP，mGPT[18]，FCPlanner，Probapop 等 7 个规划器参加了概率组的比赛。

经过所有测试域的验证，规划器 J3 取得冠军，它采用的是重规划(FF-rePlan)方法，是一个带有启发式的算法。规划器 P(mGPT)经实验，取得了第二名的成绩，它所使用的方法是实时动态规划算法(LRTDP)。在 Overall，Non-Blocks/Box 域上，规划器 C 取得冠军，它采用的是一种符号启发式搜索方法，使用的算法是 LAO*[19]。而在 Domain-specific 域上，规划器 J1 取得了第一名的好成绩[25]。

3.2 IPPC-06

2006 年在英国的 Cumbria 召开了第五届国际规划比赛 IPC-5[20]，由 Blai Bonet 和 Bib Giran 组织。共有 FOALP，sfDP，FPG，Paragraph 这 4 个规划系统参加了概率部分的比赛(IPPC-06)。大赛使用了 9 个域，每一个域上设计了 15 个问题实例。规划器通过每个实例 30 轮、共 4050 轮的比赛来评价其性能。本文只列出了在 blocksworld 域和 random 域的比较结果，如表 1 所列。综合比较，最后由澳大利亚的 Olivier Buffet 和 Douglas Aberdeen 设计的 FPG 获得了冠军。其他规划器的名次依次为 FOALP，Paragraph，sfDP。

表 1 4 种规划器在 blocksworld 域和 random 域的比较结果

域	规划器	成功率	平均动作数	平均求解时间
Blocks-world	FOALP	100.00	37.27	2.14
	sfDP	29.11	6.00	9.37
	FPG	62.89	39.27	1.73
	Paragraph	0.00	—	—
random	FOALP	0.00	—	—
	sfDP	0.00	—	—
	FPG	64.67	103.40	10.04
	Paragraph	5.11	0.07	0.00

3.3 IPPC-08

2008 年，Daniel Bryce 和 Olivier Buffet 组织了第六届国际规划竞赛，由 3 个部分组成：1)确定性部分，即具有完全确定性和可观察的规划(以前也被称为“经典”规划)；2)不确定部分(IPPC-08[21])，即规划考虑的是在完全可观察、部分可观察或不可观察领域内的不确定性和概率性的动作；3)新增的学习规划部分，规划器探测域的相关知识，这些知识是在离线训练期间自动提取的。

在不确定部分又分为 3 个小组：完全可观察概率小组(Fully Observable Probabilistic track)、不可观察不确定小组(Non Observable Non-Deterministic track)和完全可观察不确定小组(Fully Observable Non-Deterministic track)。每组的获奖情况如表 2 所列。

表 2 不确定部分每小组获奖情况

组名	规划器	作者
FOP	RFF-(BG/PG)	Guillaume Infantès, Florent Teichteil-Königsbuch and Ugur Kuter
NOND	CPA(H)	Vien Tran, Khoi Nguyen, Enrico Pontelli and Son Tran
FOND	Gamer	Stefan Edelkamp and Peter Kissmann

RFF[15]对 MDP 规划问题进行放宽，即将其转换成确定性的规划问题，其中每个动作对应一个在初始 MDP 规划问题中的可能动作的效果，而每一个这样的效果都是确定的，没有概率值、代价和回报值。在这个放宽的规划问题中，RFF 通过生成连续的执行路径来计算一个策略(Policy)，并从初始状态到目标状态均使用 FF 算法，可以返回一个失败概率很低的策略。

CPA(H)[22]可以处理初始状态不确定且有任意状态约束的规划问题，它可以归类为基于逼近的规划，其解的搜索是在部分状态集合空间而不是在信念状态空间。该方法依赖于这样的观察，即它的信念状态有时可以替换为成员的交集，从而可以非常显著地减小搜索空间，提高规划器的工作效率。

Gamer[23]使用二元判定图来求解非确定动作的规划问题，该方法是基于将不确定规划问题转换成两个玩家轮流玩的游戏，并通过求解器来选择动作集合。

4 概率规划的语言表示

在 2004 年的国际规划竞赛中，概率规划使用的规划语言就是 PPDDL1.0[24]。该语言是在 PDDL2.1 上的扩展，增加

了新的表达能力，如对概率效果和回报值的支持、对马尔可夫决策过程的支持等。

为了定义概率和决策理论的规划问题，需要添加对概率效果的支持，其概率效果的语法表示为(probabilistic p_1 e_1，…，p_k e_k)，其中 e_i 表示动作效果，p_i 表示 e_i 可能出现的概率，并且 p_i 需要满足如下约束：

$$p_i \geqslant 0, \sum_{i=1}^{k} p_i = 1$$

但有时也允许某个空的概率效果出现，即(probabilistic p_1 e_1，…，p_l e_l)，$\sum_{i=1}^{l} \leqslant 1$，这种表示也可用下面的表示代替：

(probabilistic p_1 e_1，…，p_l e_l q(and))

$$q = 1 - \sum_{i=1}^{l} p_i$$

(and)表示效果为空。

PPDDL 允许任意的条件和概率效果的嵌套，而一些主流的命题编码，如概率 STRIPS 算子(PSOs)和因子 PSOs 就不允许将条件效果嵌套在概率效果中。并且，任何 PPDDL 动作都可以转换为一个 PSOs 集合，该集合的表示最多是多项式的。因此，Littman 的研究结果指出 PPDDL 的表示等价于动态贝叶斯网络，其已成为另一种流行的 MDP 规划问题的表示方法。

5 概率规划的扩展

随着概率规划的日趋完善，越来越多的研究者将其进行扩展，使其能解决越来越复杂的不确定问题。

5.1 图规划框架下的并行概率规划

PGP 在每个时间步只允许执行一个非空动作，不能在概率规划中实现并行，而由 Iain Little 和 Sylvie Thiébaux 提出的 Paragraph[13] 规划器就要解决这个问题。该规划器的主要思想就是将整个图规划框架扩展到概率规划问题域中，利用状态信息回溯搜索 Graphplan 目标，并找出所有的路径将其合并在一起，进而生成一个最优的并行随机规划。

Paragraph 规划器可以生成循环和非循环两种规划。为了能包含非循环解和循环解，将规划定义为一个确定的有穷自动机，并在规划图定义中增加描述动作的多种可能结果结点(Outcomes)和结果结点间的互斥关系。根据对并行程度的限制情况，将并行性分为 3 种模型：不限制并行模型、限制并行模型和非-并行模型。Paragraph 规划器可以实现对非-并行模型和限制模型的处理，并生成最优随机规划[25]。

Paragraph 的优点是充分利用规划图的互斥关系和搜索方法来提高求解效率，但它没有采用启发式的方法，并且在规划图的互斥中，只考虑了相同层的互斥，没有考虑互斥的延迟问题。运用启发式的知识以及将 Paragraph 扩展到概率时序域上，是非常有研究前景的。

5.2 并行概率时序规划

Mausam 和 Daniel S. Weld 在并行马尔可夫决策过程(CoMDP)[26] 的基础上，提出了并概率时序规划 CPTP[11]。其主要思想是在增量的状态空间中，通过将问题编码为并行马尔可夫决策过程，在并行马尔可夫模型中加入明确的动作持续时间，并通过加入两个新颖可纳的启发式和一个不可纳的启发式来加速这个算法。

CPTP 将解决持续动作加入到并行概率规划中的问题，除了动作代价用持续的动作($\Delta(a)$)代替外，其输入模型类似于 CoMDP。为了扩展持续动作，作者提出了 3 条假设：1)所有的动作都有确定的持续时间；2)所有动作的持续时间都是整数值；3)所有的动作都遵循下列模式：

- 由于在动作执行过程中效果实现的时间点不确定，因此该效果在动作完成后只能使用一次。
- 动作在开始执行前必须获得前提条件。
- 动作在执行过程中，其前提和转换函数必须保持不变，除非是动作自身去修改它们。

文中提出的并行性和互斥定义就是以这些假设为前提的。

CPTP 将并行性和持续动作融入到概率规划模型当中，并正式地定义了并行概率时序规划问题。同时，扩展了两种状态空间，即交错时间空间和对齐时间空间，使用标识的 RTDP[27] 来搜索最优策略。该算法的缺点是搜索空间巨大，不能处理带有回报值、混合代价值和随机动作持续时间的规划问题。

5.3 多目标概率规划

现实生活中的规划问题往往都是非常复杂的，智能体不仅面临执行任务的不确定性，而且生成的可执行规划需要满足多个目标，即满足多个约束条件。概率规划问题本质上就是多目标问题，它需要同时满足规划的成功概率最大且消耗的代价最小。实际上，大部分规划问题都包含多个目标约束。如有些规划问题，它需满足以下所有目标约束：规划消耗的代价最小、成功的概率最大、规划的分支最少，并且规划完成的时间和消耗的资源也最少等等，这就需要智能体同时考虑这些目标来生成规划[28]。

到目前为止，概率规划的合成算法都还集中于单目标，并绑定了一些不太实际的假设。Daniel Bryce 针对这一情况，提出了一个多目标的概率规划，它不仅与实际问题相符，还可以生成一个规划的柏拉图集合，并利用了概率规划可达性启发式的最新发展成果，可以非常优雅地解决受限的随机规划问题。

多目标概率规划的主要工作是：1)在信念状态空间中，应用自底向上的动态编程算法来推迟每个分支中未成熟的承诺；2)应用 LAO * 算法归纳出的多目标 LAO * 算法(MO-LAO *)从初始的信念状态空间进行前向搜索，并计算出规划的柏拉图集合；3)通过采取一些加速的方法来进行搜索的复杂性改良，其中最显著的方法就是使用规划图的可达性启发式来引导搜索；4)在受限的随机规划中，将其分支数量作为另一个目标。

多目标概率规划的规划解是可以满足所有限定目标约束的最优规划，该规划解称为理想解。但在实际的求解过程中，这种最优解是很难得到的。通常情况下，规划器求得的解权衡了多个目标，使得所有目标尽量满足可行解。

6 概率规划与重规划

通常人们认为概率规划和经典规划在不同的环境下都有其适用范围。例如，当重规划失败，周围的世界又不确定，且该世界也不值得去建模推理时，经典规划就是一个不错的选择。另一方面，当经典规划不能够避免不可修复的或高代价的失败，并且可以建立一个精确的概率不确定模型时，就应使用概率规划作为解决问题的方法。重规划技术不仅适用于经

典规划，也适用于概率规划。2004 年，在国际概率规划竞赛中脱颖而出的 FF-Replan 就是一个很好的例子。下面简单地介绍一下概率规划、重规划以及 FF-Replan。

6.1 概率规划与重规划

概率规划通常定义为用概率方法表示的不确定规划，其动作效果带有概率值，可以处理许多或者是所有的可预见性的随机事件。由于随机规划一边分析环境一边产生新的结果，这就使得其非常适用于闭合回路的控制情况。为了很好地说明如何使用 Replanner 来解决概率规划问题[29]，Iain Little 等人将概率规划问题定义如下：

1)一个有限的状态集合 S；

2)初始状态为 s_0，且 $s_0 \in S$；

3)一个目标集合 G，且 $G \subseteq S$；

4)一个结果集合 O，且 $o \in O$，$\Pr(o)$表示 o 的概率值；

5)一个确定性的转换函数 $T(o,s) \in S$，适用于所有的结果 o 和状态 s；

6)集合 $A(s)$表示在每个状态 $s \in S$ 下所应用的动作，函数 $out(a) \subseteq O$ 将每个动作映射到一个结果集合：①每个结果 $o \in O$ 都精确地属于一个动作 $act(o)$，②对于所有的动作 a 都有 $\sum_{o \in out(a)} \Pr(o) = 1$。

Replanner 的目标是使用专门的确定性规划器来解决概率规划问题，这就需要将概率规划问题编译成确定性问题。所以，Iain Little 等人又提出了 6 条假设来完成编译过程。假设确定性问题有如下特点：

1)有限的状态集合 S^d；

2)初始状态为 S_0^d，且 $S_0^d \in S^d$；

3)目标状态集合 G^d，且 $G^d \subset S^d$；

4)集合 $A^d(s)$为在每个状态 s 下所应用的动作，且 $s \in S^d$；

5)确定性的转换函数 $T^d(a,s) \in S^d$，适用于所有的动作 $a \in A^d(s)$和状态 $s \in S^d$；

6)$c^d(a)$定义为每个动作的代价。

这里，将从初始状态可以应用的动作序列定义为一个路径，其代价为路径中所有动作的代价之和。

将概率规划问题编译为确定性规划问题需要使用满足如下条件的函数 Δ，即对于每个概率规划问题 $P=\langle S, s_0, G, O, T, A\rangle$和它的编译 $\Delta(P)=\langle S^d, s_0^d, G^d, A^d, T^d, c^d\rangle$都有两个函数 $\sigma: S^d \mapsto S$ 和 $\alpha: A^d \mapsto O$ 使其满足：

1)$\sigma(s_0^d)=s_0$；

2)$s \in G^d$，当且仅当 $\sigma(s) \in G$；

3)$\Delta(P)$中的每个路径 $a_1, a_2, \cdots$ 在 P 中都有路径 $o_1, o_2, \cdots$ 与其对应，使得所有的 i 需满足：

①$\alpha(a_i)=o_i$；

②$\sigma(T^d(a_i, \cdots, T^d(a_1, s_0^d)))=T(o_i, \cdots, T(o_1, s_0))$。

这些条件确保了 Replanner 生成规划的正确性。

上面所考虑的 Replanner 是一种在线规划器，它使用确定性规划器对编译后的问题生成一个规划解，并试图执行这个解。只要当前状态背离了预期状态，它就重新规划，即生成一个从当前状态到目标状态的新路径。

6.2 FF-Replan

FF-Replan 是 2004 年国际概率规划竞赛的冠军。在 IPPC-06 中，虽然它没有正式参加比赛，但在各个实验域中，它的执行能力都是最强的。令人吃惊的是它使用的方法十分简单，即在构造的确定性规划问题变体上调用 FF[30]，依照规划来选择动作。如果观察到了不希望出现的效果，则重新进行规划。尽管 FF-Replan 也存在明显的缺点，但它在概率规划中是最先进的，近年来被用作概率规划竞赛的标准。

FF-Replan 是一种在概率域中为在线规划进行动作选择的算法。它在规划开始时确定输入域，并将概率域转换为确定域进行求解。这个简单的思想在许多的竞赛域中都是十分有效的。FF-Replan 有两种简单的确定方法：一种是单一结果确定(single-outcome determinization)，另一种是所有结果确定(all-outcomes determinization)。

单一结果确定过程在效果 $e_1, \cdots, e_n$ 中选择一个效果 e_i，而忽略其概率值 p_i 和其他的效果。概率效果可以嵌套，而结果确定过程在嵌套的概率结构中可以递归地选择一个效果。单一结果确定过程为每个概率动作产生一个确定的动作，其中为选择结果设计几个启发式算法，例如选择最有可能的效果或者选择带有最多添加效果的效果作为首要的候选结果。单一结果方法的关键问题是规划器的执行效率与选择效果所使用的方法紧密相关，但无论哪种选择都会忽略掉一些重要的可能效果。

所有结果确定过程将每个概率结果看作是不同的确定性动作。对于每个可能的结果 e_i，FF-Replan 为每个效果生成一个单独的动作。如果 e_i 是确定的，那么它所对应的动作也是确定的。不同地，若 e_i 是概率的效果(即嵌套的概率效果)，则递归地应用所有结果确定过程。因此在概率嵌套层数过深的情况下，确定动作的数量是指数级的。但事实上，嵌套的层数都不多，并且在竞赛中使用也没有引起什么问题。该方法考虑所有可能的概率结果，因此其执行效率不依赖于每个动作结果的选择。

FF-Replan 使用哈希表来保存一个局部的状态动作(state-action)映射，哈希表的初始状态为空。FF-Replan 遇到一个不在表中的状态时，便将这个问题确定化，并使用 FF 方法合成一个规划。然后按照确定动作的定义来模拟这个规划，从而生成一个状态动作序列，并将其中的序对放入哈希表中。环境中规划执行的第一个动作可返回一个新的当前状态，因此，在在线的方式下，FF-Replan 会产生一个局部的策略。一般情况下，这个局部的策略没有质量保证，还需做进一步的修改。

结束语 本文比较全面地介绍了概率规划，如近年来概率规划的发展及国际概率规划竞赛的情况、概率规划的表示及其扩展以及如何用重规划技术解决概率规划问题，希望可以为广大研究者提供参考。概率规划的优点在于可以在不确定的环境下，求得有效的规划解，这正好满足了人们对未知世界的探索要求。目前所使用的方法一般都是在 MDP 的基础上完成的，使用重规划(FF-Replan)来求解概率规划是一种非常新颖而有效的方法，也是对传统方法的一种突破。

参 考 文 献

[1] Ghallab M, et al. 自动规划：理论和实践[M]. 姜云飞，等译. 北京：清华大学出版社，2008：341-342

[2] Soderland S, Weld D. Evaluating nonlinear planning[R]. TR 91-02-03. University of Wasington CSE, 1991

[3] Kushmerick N, Hanks S, Weld D. An algorithm for probabilistic planning[J]. Artificial Intelligence, 1995, 76(1/2): 239-286

(下转第 60 页)

为了能作为衡量设计的性能标准，本文引入单位时空吞吐率的概念。

定义 1 单位时空吞吐率(TPPAT)是吞吐率与时空积的比值：

TPPAT=(max throughput)/(AT product)。

表 3 将本文结果与 Helion 提供的 Altera 的商用 SHA-1 算法 IP 核进行了比较。

表 3 两种实现方式性能指标的比较

	Cyclone II C6	Cyclone III C6	Stratix II C3	Stratix III C2
本文	415	491	2103	3370
IP 核	120	138	497	710
比率(%)	345.83	355.79	423.13	474.64

从表 3 可以看出，利用本文提出的流水线结构实现 SHA-1 算法的单位时空吞吐率是商用 SHA-1 算法 IP 核的 3 倍以上。

结束语 本文提出的流水线结构方法在 FPGA 上实现 SHA-1 算法，缩短了关键路径，使用片内 RAM 代替 LE 寄存器实现流水线中间变量的数据传递，改善了布线资源，有效地提高了资源使用率，提高了单位 SHA-1 算法的计算速度。

本文结果对并行处理多个 SHA-1 算法的使用环境有着显著的加速效果。与 Helion 提供的 Altera 的商用 SHA-1 算法 IP 核相比较，单位时空吞吐率(TPPAT)提高了 3 倍以上。

参 考 文 献

[1] FIPS PUB 180-1, Secure Hash Standard(SHA-1)[S]. National Institute of Standards and Technology(NIST), 1995

[2] Bosselaers A, Dovaerts R, Vandewalle J. SHA: A design for parallel architectures [C]// Fumy W. Adances in Cryptology-EUROCYPT'97. Heidelberg: Springer-Verlag, 1997: 348-362

[3] 黄谆，白国强，陈弘毅. 快速实现 SHA-1 算法的硬件结构[J]. 清华大学学报：自然科学版，2005，45(1)

[4] Sklavos N, Kitsos P, Alexopoulos E, et al. Open Mobile Alliance (OMA) Security Layer: Architecyure, Implementation and Performance Evaluation of the Integrity Unit[C]// New Generatation Computing: Computing Paradigms and Computatioal Intelligence. Springer-Verlag, 2004

[5] Sklavos N, Alexopoulos E, Koufopavlou O. Networking Data Integrity: High Speed Architectures and Hardware Implementations[J]. IAJIT Journal, 2003, 1: 54-59

[6] Helion Inc[OL]. http://www.heliontech.com/downloads/sha1_altera_datasheet.pdf, 2010

(上接第 34 页)

[4] Majercik S M, Littman M L. MAXPLAN: A new approach to *probabilistic planning*[J]. Artificial Intelligence Planning Systems, 1998: 86-93

[5] 徐丽，赵成丽，等. 图规划框架下的概率规划[C]// 第三届不确定系统年会. 2005: 105-111

[6] Yoon S, Fern A, Givan B. FF-replan: a baseline for probabilistic planning[C] // 17th International Conferenceon Automated Planning and Scheduling(ICAPS-07). 2007

[7] Draper D, Hanks S, Weld D. Probabilistic Planning with Information Gathering and Ontingent Execution[C] // Proceedings AIPS-94. 1994: 31-36

[8] Blum A, Langford J. Probabilistic planning in the Graphplan framework[C]// Proceedings of the Fifth European Conference on Planning. Durham, United Kingdom, 1999

[9] Gu Wen-xiang, Ou Hua-jie, Liu Ri-xian, et al. An Improved Probabilistic Planning Algorithm Based on Pgraphplan[C]// Proceedings of the Third International Conference on Machine Learning and Cybernetics. 2004: 2374-2377

[10] Mausam, Weld D. Solving concurrent Markov decision processes [C]// AAAI'04. 2004

[11] Mausam, Weld D. Cuncurrent probabilistic temporal planning [C]// ICAPS'05. 2005: 120-129

[12] Mausam, Weld D. Probabilistic Temporal Planing with Uncertain Durations[C]// AAAI'06. 2006

[13] Little I, Thiébaux S. Concurrent probabilistic planning in the Graphplan framework[C]// The 16th International Conference on Automated Planning and Scheduling(ICAPS). The English Lake District, Cumbria, U. K, 2006

[14] Bryce D. Probabilistic Planning is Multi-objective! [C]// ASU CSE-07-006. 2007

[15] Florent T K, Infantes G, Kuter U. RFF: A Robust, FF-based MDP Planning Algorithm for Generating Policies with Low Probability of Failure[C]// AAAI' 08. 2008

[16] Florent T K, Infantes G, Kuter U. FSP*: Optimal Forward Stochastic Planning Using Relaxed PPDDL Operators[C]// AAAI' 08. 2008

[17] http://andorfer.cs.uni-dortmund.de/~edelkamp/ipc-4/

[18] Bonet B, Geffner H. mGPT: Aprobagilistic planner based on heuristic search[J]. Journal of Artificial Intelligence Research, 2005, 24: 933-944

[19] Hansen E, Zilberstein S. LAO*: A heuristic search algorithm that finds solutions with loops[J]. Artifical Intelligence, 2001, 129: 35-62

[20] http://zeus.ing.unibs.it/ipc-5/

[21] http://ippc-2008.loria.fr/wiki/index.php/Main_Page

[22] Tran D-V, Nguyen H-K, Pontelli E, et al. CPA(C)/(H): Two Approximation-based Conformant Planners[C]// AAAI' 08. 2008

[23] Kissmann P, Edelkamp S. Gamer: Fully-observable Non-deterministic Planning via PKKL-Translation into a Game[C]// AAAI' 08. 2008

[24] Younes H L S, Littman M L. PPDDL1.0: An extension to PDDL for expressing planning domains with probabilistic effects [R]. CMU-CS-04-167. Carnegie Mellon University, 2004

[25] 闫书亚，殷明浩，谷文祥，等. 概率规划的研究与发展[J]. 智能系统学报，2008

[26] Mausam, Weld D. Solving concurrent Markov decision processes [C]// AAAI'04. 2004: 716

[27] Bonet B, Geffner H. Labeled RTDP: Improving the convergence of realtime dynamic programming[A]// Proceedings of 13th International Conference on Automated Planning and Scheduling (ICAPS)[C]. Trento, Italy, 2003

[28] 刘小飞. 多目标概率规划算法的研究与实现[D]. 长春：东北师范大学，2009

[29] Little I, Thiebaux S. Probabilistic palnning vs replanning[C]// ICAPS Workshop on Planning Competitions: Past, Present, and Future. 2007

[30] Hoffmann J, Nebel B. The FF planning system: Fast plan generation through heuristic search[J]. Journal of Artificial Intelligence Research, 2001, 14: 263-302