

文章编号:1001-9081(2012)09-2624-04

doi:10.3724/SP.J.1087.2012.02624

权限扩展 RBAC 模型的本体表示和实现

周加根*, 叶春晓

(重庆大学 计算机学院, 重庆 400044)

(* 通信作者电子邮箱 zhoujiagen@gmail.com)

摘要: 针对基于角色的访问控制(RBAC)模型对权限实体的刻画能力不足, 提出了带权限层次扩展的 RBAC 模型。为结合本体在知识表示和推理方面的优势, 提出了该模型的本体表示和实现方法。该方法使用 Web 本体语言(OWL)表示该扩展模型, 借助语义 Web 规则语言(SWRL)定义模型中应用逻辑规则, 隐式授权知识经规则推理获得。在此基础上, 通过 SPARQL 协议和 RDF 查询语言(SPARQL)查询命令生成显式和隐式授权视图, 实现系统安全状态分析。最后, 给出了具体应用示例, 表明该方法的可行性。

关键词: 基于角色的访问控制; 本体; Web 本体语言; 授权视图

中图分类号: TP309.2 **文献标志码:** A

Ontology representation and realization of extended permission in RBAC

ZHOU Jia-gen*, YE Chun-xiao

(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: Role Based Access Control (RBAC) has deficiency in characterizing permissions, so an extended RBAC model with permission hierarchy was presented. To utilize advantages of ontology in knowledge representing and reasoning, an ontology based representation and realization method of the extended model was proposed. Web Ontology Language (OWL) was used to formalize the ontology of this model, and some specific reasoning rules in the model were defined by Semantic Web Rule Language (SWRL). Implicit knowledge about authorization was derived through rule based reasoning. Based on this, explicit and implicit authorization views were generated for security analysis through the SPARQL Protocol and RDF Query Language (SPARQL). Finally, a case study was introduced to show the feasibility of the method.

Key words: Role Based Access Control (RBAC); ontology; Web Ontology Language (OWL); authorization view

0 引言

基于角色的访问控制(Role Based Access Control, RBAC)^[1-2], 引入角色概念将用户与权限逻辑分离, 极大地简化了授权管理操作, 一经提出即受到广泛关注。RBAC 中, 权限由操作和操作实施的客体对象构成。在实际应用中, 客体对象之间可以构成一定的层次关系, 对上层对象的操作包含了对下层对象的操作。以文件系统为例, 若用户对某一目录具有读写权限, 相应地可以认为他也具有该目录下所有文件和目录的读写操作权限。同时, 实际应用中也存在操作之间的包含层次关系, 例如修改操作包含读、写等操作。当系统中权限存在大量相同的操作和客体对象时, 权限指派和管理的工作量较大。因此在 RBAC96 模型基础上, 定义操作层次和客体对象层次关系意义上的权限层次关系, 提出权限扩展的 RBAC 模型——RBAC-PH。

在研究和开发满足不同应用环境的访问控制模型的工作之外, 访问控制策略语言及表示方法的研究也正在同步进行。作为 OASIS 发布的工业标准, 可扩展访问控制标记语言(eXtensible Access Control Markup Language, XACML)通过策略引用的方式支持 RBAC 策略的表达^[3], 但基于 XML 的表示形式限制其获得策略分析推理的能力。Barker^[4]采用逻辑程序形式化表示 RBAC 模型, 通过定理证明确定用户的权限, 在此基础上, Barker 等^[5]将访问控制策略表示为受限逻辑程序,

在评估访问请求的同时, 支持特定策略选项、约束检查和管理查询操作。Ferraiolo 等^[6]提出了访问控制策略描述和实施的框架和体系——策略机器, 定义了一系列基本元素和关系、管理命令和引用中介, 支持多种策略在单一机制下的表达和实施, 但未涉及策略的具体表示形式。此外, 语义 Web 和本体技术的出现为知识的表示提供了有效的工具, 将这些技术应用到安全策略的表示和推理中已成为研究的热点^[7-9]。在 RBAC 的形式化表示和推理方面, 王志纲等^[10]提出了基于本体的 RBAC 策略定义机制, 支持 RBAC96 模型, 并通过规则推理实现访问控制决策。Finin 等^[11]提出了在描述逻辑知识库中, 以 Web 本体语言(Web Ontology Language, OWL)本体形式实现对象层次扩展 RBAC 模型的方法, 通过描述逻辑的推理服务获得最终用户授权。

在诸多策略语言定义和标准中, 基于语义 Web 和本体技术的访问控制策略表示已体现出策略理解、共享和集成等方面的优势^[12]。为结合本体知识表示方法和 RBAC-PH 模型知识的理解和共享, 本文使用语义 Web 中知识表示的标准语言 OWL^[13], 形式化定义出 RBAC-PH 模型本体。因 OWL 语言和作为其理论基础的描述逻辑, 在表达规则方面存在一定的不足, 引入语义 Web 规则语言(Semantic Web Rule Language, SWRL)^[14], 对模型中相关应用逻辑规则进行定义。为便于安全管理员通过授权视图分析系统的授权状态, 引入本体查询机制, SPARQL 协议和 RDF 查询语言 SPARQL^[15]成为理想的

收稿日期:2012-02-28; 修回日期:2012-05-29。 基金项目: 重庆大学研究生科技创新基金资助项目(CDJXS11180022)。

作者简介: 周加根(1987-), 男, 江苏南通人, 硕士研究生, 主要研究方向: 访问控制、本体建模; 叶春晓(1973-), 男, 重庆人, 教授, 博士, 主要研究方向: 本体、访问控制。

选择。

1 权限扩展的 RBAC 模型

RBAC 96 及其后继模型包含三类基本实体:用户、角色和权限,两类基本关系:用户角色指派(UA)和权限角色指派(PA),将权限细分为操作和客体对象,以及角色之间的继承结构(RH)。权限扩展的 RBAC 模型中增加了由操作层次和客体对象层次产生的权限层次关系,如图 1 所示。

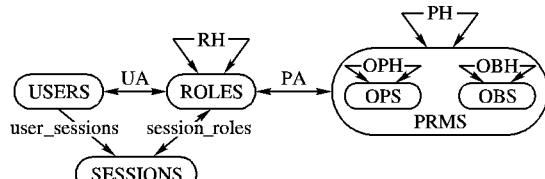


图 1 权限扩展的 RBAC 模型

在文献[16]工作基础上给出权限扩展的 RBAC 模型(RBAC-PH)的形式化定义:

定义 1 RBAC-PH

- 1) 实体集 USERS(用户集), ROLES(角色集), PERMS(权限集), OPS(操作集), OBS(客体对象集)。
- 2) $UA \subseteq USERS \times ROLES$, 多对多的用户角色指派关系。
- 3) $PRMS \subseteq OPS \times OBS$, 权限的集合。
- 4) $PA \subseteq PRMS \times ROLES$, 多对多的权限角色指派关系。

5) $OPH \subseteq OPS \times OPS$ 是 OPS 上的偏序关系, 称为操作层次关系, 记为 \geq 。对于 $op_1, op_2 \in OPS$ 和 $ob \in OBS$, 若对 ob 允许做 op_1 操作, 则 ob 上允许做 op_2 操作, 记为 $op_1 \geq op_2$, 称 op_1 是 op_2 的上层操作。

6) $OBH \subseteq OBS \times OBS$ 是 OBS 上的偏序关系, 表示客体对象之间的包含和归属关系, 称为对象层次关系, 记为 \geq 。对 $ob_1, ob_2 \in OBS, op \in OPS$, 若对 ob_1 允许做 op 操作, 则 ob_2 上允许做 op 操作, 记为 $ob_1 \geq ob_2$, 称 ob_1 是 ob_2 的上层客体对象。

7) $PH \subseteq PRMS \times PRMS$ 是 PRMS 上的偏序关系, 称为权限层次关系, 同样记为 \geq 。

对于 $p_1(op_1, ob_1), p_2(op_2, ob_2) \in PRMS$, 存在 3 种情况:

- a) 若 $op_1 = op_2, ob_1 \geq ob_2$, 则 $p_1 \geq p_2$;
- b) 若 $op_1 \geq op_2, ob_1 = ob_2$, 则 $p_1 \geq p_2$;
- c) 若 $op_1 \geq op_2, ob_1 \geq ob_2$, 则 $p_1 \geq p_2$, 称 p_1 是 p_2 的上层权限。

8) $RH \subseteq ROLES \times ROLES$ 是 ROLES 上的偏序关系, 称为角色继承关系, 记为 \geq 。若指派给角色 r_1 的权限可以指派给角色 r_2 , 指派了角色 r_2 的用户能够被指派角色 r_1 , 则 $r_1 \geq r_2$, 称 r_1 是 r_2 的上层角色。

2 基于本体的 RBAC-PH 表示

本体作为共享概念模型的明确的形式化规范说明, 在概念、关系、实例和公理等基本语义构造的基础上, 提供了特定领域知识的形式化表示和推理方法。本文使用基于描述逻辑的 Web 本体语言 OWL 建立 RBAC-PH 模型本体(见图 2), 在准确表达模型中基本概念和关系的语义信息的同时, 为模型中访问决策推理奠定基础。

图 2 中方框分别表示模型中基本概念对象(Concept), 包括用户(User)、角色(Role)、权限(Permission)、操作

(Operation) 和客体对象(Object)。实线箭头表示属性(Property), 刻画模型中概念之间的特定关系。其中, 属性 assignRole 表示用户角色指派关系 UA, assignPerm 表示权限角色指派关系 PA, op, ob 分别用于刻画权限包含操作和客体对象关系; subRole, subOp, subOb 分别刻画角色继承、操作和对象层次关系。上述的属性用于表达模型中显式的授权关系, 而经角色继承、权限层次关系引起的隐含授权关系用属性 derived* 刻画, 如 derivedRole 表示用户通过角色继承关系获得的新角色。

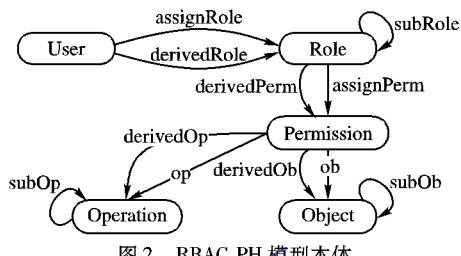


图 2 RBAC-PH 模型本体

3 本体上基于规则的推理

描述逻辑作为一类基于类别的推理系统, 是一阶逻辑的可判定子集, 可用于抽象刻画现实世界中的概念和概念之间的简单或复杂关系, 并实现在此基础上的可满足性、概念蕴含等推理。然而它的表达能力也存在一定的不足, 这类在专家系统等应用中很常见的产生式规则(IF-THEN), 在描述逻辑中, 只能借助概念和属性间的蕴含关系或者添加属性约束得到部分的表达。在实际应用中, 仅依赖于描述逻辑很难甚至不能表达复杂的应用逻辑规则。鉴于本体描述语言 OWL 的使用, 本文引入语义 Web 规则语言 SWRL, 这一结合了 Horn 子句和描述逻辑的规则描述语言可表达用户自定义规则, 作为本体的表达和推理能力的补充。根据 RBAC-PH 模型的应用逻辑, 建立的推理规则如下:

- R1: $subRole(?r1, ?r2) \wedge subRole(?r2, ?r3) \rightarrow subRole(?r1, ?r3)$
- R2: $subOb(?o1, ?o2) \wedge subOb(?o2, ?o3) \rightarrow subOb(?o1, ?o3)$
- R3: $subOp(?op1, ?op2) \wedge subOp(?op2, ?op3) \rightarrow subOp(?op1, ?op3)$

subRole 定义了模型中基本的角色继承关系, 规则 R1 说明角色继承关系具有传递性, 可用于构建出应用环境中完整的角色层次树。类似地, 规则 R2 和 R3 分别表示客体对象层次关系、操作层次关系具有传递性。这三条规则是后续规则逻辑推理的基础。

- R4: $assignRole(?user, ?r1) \wedge subRole(?r1, ?r2) \rightarrow derivedRole(?user, ?r2)$
- R5: $assignPerm(?r1, ?p) \wedge subRole(?r2, ?r1) \rightarrow derivedPerm(?r2, ?p)$

规则 R4 说明了用户角色指派关系在角色层次树中向下传递, 即经显式的用户角色指派, 用户可以隐式地获得这个角色的下层角色。规则 R5 说明了权限角色指派在角色层次树中向下传递。

- R6: $Permission(?p) \wedge op(?p, ?op1) \wedge subOp(?op2, ?op1) \rightarrow derivedOp(?p, ?op2)$
- R7: $Permission(?p) \wedge ob(?p, ?ob1) \wedge subOb(?ob2, ?ob1) \rightarrow derivedOb(?p, ?ob2)$

规则 R6 和 R7 说明因操作层次关系和客体对象层次关系的存在, 特定的权限被隐式赋予下层的操作和客体对象。

4 授权视图生成

在实施 RBAC-PH 模型的系统中,授权视图由用户角色指派和权限角色指派构成,系统安全管理员通过授权视图分析系统的安全状态。OWL 基于 RDF 表示的特征,使得模型

本体中的授权知识以三元组的形式存在,本身无法表现出用户与权限关联的语义信息,需要引入类似于数据库中查询的机制。本章使用 RDF 查询语言 SPARQL 生成系统原始授权视图(显式授权视图)和经规则推理后的授权视图(隐式授权视图),查询命令见表 1。

表 1 SPARQL 查询命令

基本关系	原始授权视图	规则推理后授权视图
UA	SELECT DISTINCT ?u ?r WHERE { ?u : assignRole ?r. }	SELECT DISTINCT ?u ?r WHERE { {?u : assignRole ?r} UNION {?u : derivedRole ?r}. }
PA	SELECT DISTINCT ?r ?op ?ob WHERE { ?r : assignPerm ?perm. ?perm : op ?op. ?perm : ob ?ob. }	SELECT DISTINCT ?r ?op ?ob WHERE { {?r : assignPerm ?perm} UNION {?r : derivedPerm ?perm }. {?perm : op ?op} UNION{?perm : derivedOp ?op}. {?perm : ob ?ob} UNION{?perm : derivedOb ?ob}. }

查询命令中选用了 SPARQL 中基本的 SELECT 查询形式,其查询结果以表的形式返回。DISTINCT 和 UNION 是查询修饰符,分别用于消除查询结果中的重复项和合并查询结果形成新的结果集。

在基本的 UA 和 PA 授权视图查询命令基础上,最终的用户授权关系通过如下命令获得:

```
SELECT DISTINCT ?u ?r ?op ?ob
WHERE [
{?u : assignRole ?r} UNION {?u : derivedRole ?r}.
{?r : assignPerm ?perm} UNION {?r : derivedPerm ?perm }.
{?perm : op ?op} UNION{?perm : derivedOp ?op}.
{?perm : ob ?ob} UNION{?perm : derivedOb ?ob}. ]
```

5 应用实例

以典型的软件开发系统为例,见图 3,箭头表示实体的层次关系,由下层实体对象指向高层实体对象。在进行权限分配时,系统安全管理员可以充分利用权限层次关系中隐含的操作层次和客体对象层次关系简化授权工作。系统运行后,系统安全管理员的显式授权如表 2 所示。

表 2 显式授权

用户	角色	权限
Alice	项目成员	(读,项目概况文件)
Bob	测试工程师	(执行,可执行文件) (确认完成,程序文件)
John	程序员	(修改,程序文件)
Tom	项目经理	(修改,系统文件)

表 3 最终用户授权

用户	角 色	权 限
Alice	项目成员	(读,项目概况文件)
Bob	项目成员,测试工程师	(读,项目概况文件)(执行,可执行文件)(确认完成,程序文件)
John	项目成员,程序员	(读,项目概况文件)(修改,程序文件) (读,程序文件)(写,程序文件)
Tom	项目成员,测试工程师,程序员,项目经理	(读,项目概况文件)(执行,可执行文件)(确认完成,程序文件) (修改,程序文件)(读,程序文件)(写,程序文件)(修改,系统文件) (读,系统文件)(写,系统文件)(修改,配置文件)(读,配置文件) (写,配置文件)(修改,日志文件)(读,日志文件)(写,日志文件)

6 结语

RBAC 是策略中立的访问控制模型,可以配置模拟实现其他的访问控制模型(DAC、MAC),是目前受到广泛应用的

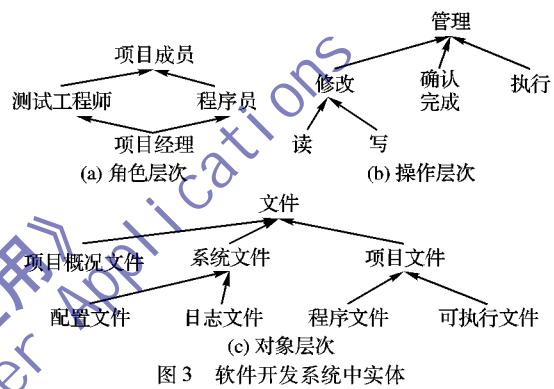


图 3 软件开发系统中实体

经规则 R1 ~ R3 推理后,模型本体中存在系统中实体的层次结构。由图 3(a),项目成员是测试工程师的上层角色,Bob 当前拥有的角色为测试工程师,经规则 R4 推理后,Bob 可以获得项目成员角色。同样地,根据规则 R5,测试工程师通过角色继承获得项目成员的权限(读,项目概况文件)。由图 3(b),修改操作是读、写操作的上层操作,指派给程序员的权限(修改,程序文件),经规则 R6 推理后,生成权限(读,程序文件)和(写,程序文件)。由图 3(c),系统文件是配置文件、日志文件的上层客体对象,指派给项目经理的权限(修改,系统文件),经规则 R6 和 R7 推理后,生成权限(读,系统文件)、(写,系统文件)、(修改,配置文件)、(读,配置文件)、(写,配置文件)、(修改,日志文件)、(读,日志文件)、(写,日志文件)。经 SPARQL 查询获得的最终用户授权视图如表 3 所示。

安全模型。RBAC 模型中对权限实体的刻画粒度较粗,无法形成有效的权限分配和管理结构,引入权限层次概念,扩展 RBAC 模型。鉴于本体技术在知识表示方面的优势,选择 Web 本体语言 OWL 构建模型知识本体,区分显式授权和隐

式授权关系，并给出了模型本体知识库上特定的应用逻辑推理规则。引入本体查询语言生成授权视图，进行系统授权状态分析。

进一步的工作包括完善 RBAC 模型本体和推理规则，以支持 RBAC 重要特征之一的约束的表达和实施；利用 RBAC 策略中立的特点，研究本文方法在表达其他的访问控制模型时的适用性。

参考文献：

- [1] SANDHU R. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38–47.
- [2] SANDHU R, FERRAIOLI D, KUHN R. The NIST model for role-based access control: towards a unified standard[C]// RBAC '00: Proceedings of the 5th ACM Workshop on Role-Based Access Control. New York: ACM Press, 2000: 47–63.
- [3] RISSANEN E, AXIOMATICS A B. XACML v3.0 core and hierarchical Role Based Access Control (RBAC) profile v1.0[EB/OL]. [2011-12-10]. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-cs-01-en.pdf>.
- [4] BARKER S. Data protection by logic programming[C]// Proceedings of the First International Conference on Computational Logic, LNAI 1861. Berlin: Springer-Verlag, 2000: 1300–1314.
- [5] BARKER S, STUCKEY P J. Flexible access control policy specification with constraint logic programming[J]. ACM Transactions on Information and System Security (TISSEC), 2003, 6(4): 501–546.
- [6] FERRAIOLI D, ATLURI V, GAVRILA S. The policy machine: a novel architecture and framework for access control policy specification and enforcement[J]. Journal of System Architecture, 2011, 57(4): 412–424.
- [7] YAGUE M I, MANA A, LOPEZ J, et al. Applying the semantic Web layers to access control[C]// DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications. Washington, DC: IEEE Computer Society, 2003: 622–626.
- [8] KAGAL L, FININ T, JOSHI A. A policy language for a pervasive computing environment[C]// Proceedings of IEEE the 4th International Workshop on Policies. Washington, DC: IEEE Computer Society, 2003: 63–76.
- [9] USZOK, A, BRADSHAW J M, JEFFERS R, et al. KAoS policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement [C]// POLICY 2003: Proceedings of IEEE the 4th International Workshop on Policies for Distributed Systems and Networks. Washington, DC: IEEE Computer Society, 2003: 93–96.
- [10] 王治纲,王晓刚,卢正鼎,等. OntoRBAC: 基于本体的 RBAC 策略描述与集成[J]. 计算机科学, 2007, 34(2): 82–85.
- [11] FININ T, JOSHI A, KAGAL L, et al. ROWLBAC: Representing role based access control in OWL[C]// SACMAT '08: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2008: 73–82.
- [12] TONTI G, BRADSHAW J M, JEFFERS R, et al. Semantic Web languages for policy representation and reasoning: a comparison of KAoS, Rei, and Ponder[C]// ISWC 2003: Proceedings of the 2003 International Semantic Web Conference, LNCS 2870. Berlin: Springer-Verlag, 2003: 419–437.
- [13] MCCGUINNESS D L, HARMELEN F. OWL Web ontology language overview[EB/OL]. [2012-01-10]. <http://www.w3.org/TR/owl-features>.
- [14] HORROCKS I, PATEL-SCHNEIDER, BOLEY H, et al. SWRL: A semantic Web rule language combining OWL and RuleML[EB/OL]. [2012-01-20]. <http://www.w3.org/Submission/SWRL/>.
- [15] HEBELER J, FISHER M, BALACE R, et al. Web 3.0 与 Semantic Web 编程[M]. 唐富年, 唐荣年, 译. 北京: 清华大学出版社, 2010.
- [16] 叶春晓, 符云清, 吴中福. RBAC 中权限扩展的实现[J]. 计算机工程, 2005, 39(2): 141–142, 172.

(上接第 2555 页)

表 1 伪分支剔除算法用时比较 ms

算法	汉字图	数字图	字母图
算法 1	17.41	16.04	16.50
算法 2	7.32	6.28	6.83

4 结语

本文凭借 ICM 脉冲并行发放的优良性能，结合骨架伪分支和噪声的特征，提出一种基于 ICM 的图像骨架伪分支剔除算法。该方法根据实际情况引入并修正了端点和连接点的定义，以判断图像骨架上的伪分支和目标周围的噪声带，避免破坏骨架的几何尺寸。同时，ICM 动态脉冲并行发放特性大大提高算法的处理效率。实验结果表明，本文算法不但计算速度快、抗噪声能力强，而且图像骨架结构能完好保存下来，进一步提高了骨架曲线描述目标形状及拓扑特征的能力，较之传统数学形态学方法有着更为广阔的应用前景。

参考文献：

- [1] 马锐. 基于广义势场的三维形体多层次线骨架构建[J]. 计算机应用, 2011, 31(1): 16–19.
- [2] 蒋莉. 骨架驱动的 MLS 卡通角色变形[J]. 计算机辅助设计与图

形学学报, 2011, 23(5): 863–869.

- [3] 江贺. 启发式算法设计中的骨架分析与应用[J]. 自动化学报, 2011, 37(3): 257–269.
- [4] 雷涛. 复杂环境下的运动人体骨架提取算法[J]. 计算机应用研究, 2010, 27(8): 3194–3197.
- [5] 刘宏申. 击中与击不中变换在笔画细化中的应用[J]. 安徽工业大学学报, 2002, 19(3): 251–253.
- [6] 徐莹. 基于数学形态学的图像骨架提取和复原的改进算法[J]. 成都信息工程学院学报, 2009, 24(3): 259–263.
- [7] 刘怡静. 基于向量内积的骨架提取算法[J]. 东华大学学报: 自然科学版, 2010, 36(2): 158–163.
- [8] 高山, 毕笃彦, 魏娜. 基于交叉视觉皮质模型的彩色图像自动分割方法[J]. 中国图象图形学报, 2009, 14(8): 1638–1642.
- [9] GAO SHAN. Image enhancement algorithm based on NF-ICM [J]. Chinese Optics Letters, 2010, 8(5): 474–478.
- [10] 徐建军, 高山. 一种新的图像分割算法[J]. 西安电子科技大学学报, 2011, 38(2): 8–16.
- [11] 牛建伟. 基于修正交叉视觉皮质模型的图像分割新方法[J]. 北京邮电大学学报, 2010, 33(1): 56–60.
- [12] LAM L, LEE S W. Thinning methodologies — a comprehensive survey [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1992, 14(9): 869–895.