doi:10.13582/j.cnki.1672-7835.2021.03.005

关于“秘密”的逻辑语义研究

熊作军[1],张玉志[2]

(1.西南大学 逻辑与智能研究中心,重庆 400715; 2.曲阜师范大学 政治与公共管理学院,山东 日照 276825)

摘　要:“秘密”是知识与信念中的一个重要概念,也是信息网络隐私与安全所讨论的重要对象。文章从知识逻辑与信念逻辑两个方面分析了“秘密”的逻辑语义,并给出了其归约公理以及基于知识逻辑与信念逻辑的完全的公理化系统。然后从知识逻辑与信念逻辑两个方面剖析“纯秘密逻辑系统”的公理与规则,发现它们都是一个非正规模态逻辑系统 ECKT4 的扩张,这两个“纯秘密逻辑系统”只在讨论不同主体间的互动推理时存在差异,只是这两个系统的完全性问题还有待进一步研究。

关键词:秘密;知识逻辑;信念逻辑;非正规模态逻辑

中图分类号:B815　　**文献标志码:**A　　**文章编号:**1672-7835(2021)03-0027-12

一　研究背景

在网络信息中,网络信息的安全与否不只受信息主体对信息保护程度的影响,还受到网络结构本身的影响。一个简单的例子是在“子集式网络”结构中,子集网络中的主体是无法保证其在该网络中信息的私密性(父集网络主体将有能力获取子集网络主体的信息)。语义研究是弄清概念的重要方法与手段,对“秘密”进行系统的逻辑语义研究,有助于我们弄清“信息保密”的逻辑特性,以及“网络结构”与“信息保密”间的内在规律,为网络信息中的相关研究提供理论参考。就像关于真势模态逻辑(必然模态、可能模态)的语义研究推动了认知科学尤其是知识逻辑、信念逻辑以及道义逻辑等认知逻辑的发展,对“秘密模态”的语义研究也将促进信息科学尤其是保密学、社会网络分析学等学科的研究与发展。

国内外逻辑学与信息科学领域已有将“秘密”这一概念作为知识逻辑中的具体原子命题信息或情境等方面的研究尝试,但暂无将“秘密”当作具体的模态命题,系统化分析秘密的逻辑结构与语义特性方面的研究。范·蒂特马斯等研究了“流言”(gossip)在主体间传播的问题,这些文献谈论的“流言”只是主体自己所知道的事件,该事件并不一定需要是秘密,他们研究了不同协议下“流言”在不同网络结构上的扩散特点①。莫尔与瑙莫夫则将“秘密”作为原子命题,研究了“秘密”间的独立性(independence)关系②。范杰等人讨论了主体认知的模糊性问题,如从“主体知道是否 A 或 B”“其他主体不知道某一主体是否知道 A 或 B”等一些模糊命题中能够推演出什么命题的问题,并未将“秘密”这一特殊命题作为逻辑的分析对象③。

张玉志将“秘密”作为“模态算子”在知识逻辑上做了讨论,但“秘密模态词”被限定为一个不能嵌套的初始算子(相当于原子命题),因而不能谈论形如“‘主体 a 知道 p 是自己的秘密’是自己的秘密”这样秘密被嵌套了的句子,并且该文中

收稿日期:2020-09-11

基金项目:教育部人文社会科学研究青年基金项目(20YJC72040002);国家社会科基金重大项目(14ZDB016)

作者简介:熊作军(1985—),男,湖北潜江人,博士,讲师,主要从事现代逻辑及其应用研究。

①严格而言,“秘密”经常通过“流言”或“传言”来传播,但“流言”并非一定是“秘密”,它不要求所知事情属实或所知事情不为他人所知等等,见:van Ditmarsch, H., et al. “The logic of gossiping”, *Artificial Intelligence*, https://dio.org/10.1016/j.artint.2020.103306.; A., Krzysztof R., et al. “Epistemic Protocols for Distributed Gossiping”, *Proceedings TARK*, 2015(215):51-66.

②More, S. M. and Naumov, P. “An Independence Relation for Sets of Secrets”, *Studia Logica*, 2010,94(1):73-85;More, S. M. and Naumov, P. “Logic of secrets in collaboration networks”, *Annals of Pure and Applied Logic*, 2011,162(11):959-969.

③Fan, J., et al. “Contingency and knowing whether”, *The Review of Symbolic Logic*, 2015,8(1):75-107.

并未对秘密所具有的公理与规则展开讨论①。本文则是对非嵌套的“秘密算子”的扩张,将从知识嵌套、信念嵌套、知识与信念相互嵌套的角度来分析“秘密算子”的语义。更准确地说,我们将使用知识逻辑②(Epistemic Logic)与信念逻辑③(Doxastic logic)等模态逻辑④(Modal logic)语言来定义与刻画“(人)知道(事/物)是(人)的秘密”这样的模态关系。在此基础上进一步给出基于知识逻辑与信念逻辑的“秘密模态词”更一般的定义,给出“秘密模态词”在这两个逻辑上的归约公理,分别构建、比较其公理系统间的区别与联系,分析探讨“秘密”这一概念本身的逻辑语义。

二　作为知识逻辑语义下的“秘密”

从知识逻辑的角度看秘密,我们说“φ 是主体 a 的秘密”意味着:(1)主体 a 知道 φ,且(2)其他人都不知道 φ。当然,实际上(2)应该进一步强化为(3)主体 a 知道其他人都不知道 φ。这一性质已经暗含在我们关于“秘密”的理解上。倘若小安不知道别人是否知道他自己的心愿,那么他则不会认为他的心愿一定是一个秘密。根据这样的约定,在基本知识逻辑的语言中,“φ 是主体 a 的秘密”则可用“知道模态词 K”定义如下:

$$K_a\varphi \wedge K_a(\bigwedge_{b\neq a} \neg K_b\varphi)$$

上述公式等值于:

$$K_a\varphi \wedge K_a(\bigwedge_{b\neq a} (\neg K_b\varphi \wedge \neg K_b\neg \varphi))$$

即“b 不知道 φ 为真”被替换成了“b 不知道 φ 为真也不知道 φ 为假(不知道 φ 是否为真)”⑤。我们引入一个新的模态算子 S_a 来表达这样的秘密(知识),如 $S_a\varphi$ 就可以理解为“φ 是主体 a 的秘密(知识)”,其语义定义则可表示为上述的认知公式。

虽然我们可以用“知道算子” K_a 和 K_b 来定义 S_a,但我们并不只是对“秘密”与“知道”间的关系感兴趣,我们还希望弄清楚“秘密”本身(即不包含知道算子 K_a)的一些逻辑性质(逻辑有效式、无效式等),故我们将给出两种关于秘密的模态语言的定义。一种是在知识逻辑的基础上引入 S_a,即 L_{KS} 语言;另一种是将 S_a 当作初始模态词给出一个只包含“秘密”模态算子的语言 L_S。

定义(语言)　令 $Prop$ 表示非空的原子命题集,Agt 表示(非空)有穷主体集。$p \in Prop$、$a \in Agt$ 分别表示原子公式与主体,则关于 $\varphi \in L_{KS}$ 与 $\psi \in L_S$ 的归纳定义如下:

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$$

$$\psi ::= p \mid \neg\psi \mid (\psi \wedge \psi) \mid S_a\psi$$

定义(认知模型)　一个认知模型 $M = (W, \sim, V)$ ⑥是定义如下的三元组:

○ W 是一个非空的世界集(*worlds*, *states*);

○ $\sim$ 是从 Agt 到 W 幂集的映射,表示每一个主体关于世界集 W 上的等价关系。如 $\sim_a \subseteq (W \times W)$ 则是关于主体 a 的等价关系集,$\sim$ 又被称为认知不可区分关系(*epistemic indistinguishable relation*);

○ V 是从 $Prop$ 到 W 的幂集的赋值函数,即对每一个原子命题,指派一集世界。表示这个原子命题在这些世界上为真。如 $V(p) \subseteq W$ 即表达了所有使得原子命题 p 为真的世界集。

定义(满足关系)　公式 $\varphi \in \mathcal{L}_{KS}$ 在认知模型 $M = (W, \sim, V)$ 的世界 w 上的可满足关系,$M, w \models \varphi$ 的定义如下:

$M,w\models p$	当且仅当	$w \in V(p)$。
$M,w\models \neg\psi$	当且仅当	并非 $M,w\models\psi$(简记为 $M,w\models\psi$)。
$M,w\models(\psi\wedge\chi)$	当且仅当	$M,w\models\psi$ 且 $M,w\models\chi$。
$M,w\models K_a\psi$	当且仅当	对任意 $u \in W$,如果 $w \sim_a u$,那么 $M,u\models\psi$。
$M,w\models S_a\psi$	当且仅当	对任意 $w' \in W$,如果 $w \sim_a w'$,那么 $M,w'\models\psi$,且对任意 $b \neq a \in Agt$,存在 $u \in W$ 使得 $w' \sim_b u$ 且 $M,u\models\neg\psi$。

①张玉志:《社会网络中信息流动与主体完美回忆研究》,西南大学 2020 年博士学位论文。

②van Ditmarsch, H., et al. *Dynamic Epistemic Logic*. Springer, 2008, p.178.

③Leitgeb, H. and Segerberg, K.“Dynamic doxastic logic: why, how, and where to?” *Synthese*, 2007,155(2):167-190.

④Blackburn, P., et al. *Modal Logic*. Cambridge University Press, 2001, p.33.

⑤在上述公式中,我们默认主体集是非空有穷集,形如 $\bigwedge_{b\neq a} \neg K_b\chi$ 是关于 $\neg K_{b_1}\chi \wedge \neg K_{b_2}\chi \wedge \cdots \wedge \neg K_{b_m}\chi$ 的简写,其中主体集为集合 $\{a, b_1, b_2, \cdots, b_m\}$。

⑥又称为 S5 模型,即模型中的二元关系 $\sim$ 是等价关系,它满足自反性、传递性与对称性。自反性:对任意的 x,有 $x \sim x$;传递性:对任意 x,y,z,如果 $x \sim y$ 且 $y \sim z$,则 $x \sim z$;对称性:对任意 x,y,如果 $x \sim y$ 则 $y \sim x$。

由于 $\mathcal{L}_S \subset \mathcal{L}_{KS}$,上述语义定义也是关于 $\varphi \in \mathcal{L}_S$ 的语义定义。从上面的语义定义中,不难发现(见命题 1 中对(S)的证明):

$M,w\models S_a\varphi$	当且仅当	$M,w\models K_a\varphi \wedge K_a(\wedge_{b\in Agt\setminus\{a\}}\neg K_b\varphi)$。
$M,w\models\neg S_a\neg\varphi$	当且仅当	存在 $w'\in W$ 对任意的 $u\in W$,如果 $w\sim_a w'$ 蕴涵 $M,w'\models\neg\varphi$,则存在 $b\neq a\in Agt$,$w'\sim_b u$ 蕴涵 $M,u\models\neg\varphi$。

令 p 表示“火星上有水”这一命题,则 S_ap 表示“火星上有水是主体 a 的秘密”,该句话等价于“主体 a 知道火星上有水,且知道其他主体 b 不知道火星上有水”。根据这一语义,$\neg S_ap$ 表示“火星上有水不是主体 a 的秘密”。这一句话等价于说“或者主体 a 不知道火星上有水,或者主体 a 可能知道另一个主体 b 知道火星上有水”①。还有,$\neg S_a\neg p$ 则表示“火星上无水不是主体 a 的秘密”,这一句话还可以等价于“或者主体 a 可能知道火星上有水,或者主体 a 可能知道另一个主体 b 知道火星上无水”。

在生活中,我们说“某事 φ 不是一个秘密”通常指的是“说话者知道这件事 φ 是真的,且其知道有其他人也知道这件事 φ”。而用我们的逻辑语言 $\mathcal{L}_{KS}$ 来表示时,则可用形如 $\neg S_a\varphi \wedge K_a\varphi$ 的公式来表达。由此可见,我们给定的“秘密”的语义能够刻画出关于“秘密”这一概念的重要特点。

根据上述语义,在 $\mathcal{L}_{KS}$ 语言中,认知算子 K_a 与秘密算子 S_a 之间的相互关系见表 1。在知识逻辑的证明系统(表 2)中引入表 1 中的(S)公理,则可以得到 $\mathcal{L}_{KS}$ 语言的完全的证明系统。所有表 1 中其他的定理都在表 2 和(S)公理下可证。

命题 1:表 1 中的所有公式都是有效式。

表 1　知识与秘密互动

(**S**)	$S_a\varphi\leftrightarrow(K_a\varphi\wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$	秘密的定义
(4SK)	$S_a\varphi\rightarrow K_aS_a\varphi$	秘密的认知正自省性
(5SK)	$\neg S_a\varphi\rightarrow K_a\neg S_a\varphi$	秘密的认知负自省性
(P)	$S_a\varphi\rightarrow(K_a\varphi\wedge\neg K_b\varphi)$	秘密的隐私性
(NKS)	$\neg K_bS_a\varphi$	己秘非他知
(NSK1)	$\neg S_aK_b\varphi$	他知非己秘
(NSK2)	$\neg S_a\neg K_b\varphi$	他未知非己秘
(NC)	$K_aS_a\varphi\vee K_a\neg S_a\varphi$	己秘完全性

注:$\mathcal{L}_{KS}$ 语言中 K_a 与 S_a 间的交互关系,其中令 $b\neq a$。加粗的公理称为核心公理,其他未加粗的公理可从加粗的公理中推导出来。

证明:对于(S)的证明可直接从语义定义中得到。(M,w) 为认知模型的任意点模型。$M,w\models S_a\varphi$,根据语义定义,当且仅当对任意 $w'\in W$,如果 $w\sim_a w'$,那么 $M,w'\models\varphi$,且对任意 $b\neq a\in Agt$,存在 $u\in W$ 使得 $w'\sim_b u$ 且 $M,u\models\neg\varphi$,当且仅当 $M,w\models K_a\varphi$ 且对任意 $b\neq a\in$ Agt,存在 $u\in W$ 使得 $w'\sim_b u$ 且 $M,u\models\neg\varphi$,当且仅当 $M,w\models K_a\varphi$ 且 $M,w'\models\wedge_{b\in \mathrm{Agt}\setminus\{a\}}\neg K_b\varphi$,当且仅当 $M,w\models K_a\varphi$ 且 $M,w\models K_a\wedge_{b\neq a}\neg K_b\varphi$(根据 w' 的任意性以及 $w\sim_a w'$),当且仅当 $M,w\models K_a\varphi\wedge K_a(\wedge_{b\neq a}\neg K_b\varphi)$。然后其他公式的证明则可根据表 2 的可靠性来证明。对(S)使用关于 K_a 的必然化规则(Nec),以及 K_a 对 $\leftrightarrow$ 的分配,有 $\models K_aS_a\varphi\leftrightarrow K_a(K_a\varphi\wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$,根据(T)以及命题演算,$\models S_a\varphi\rightarrow K_a(K_a\varphi\wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$,再根据(S)与等值替换,$\models S_a\varphi\rightarrow K_aS_a\varphi$,(4SK)得证。从(S)的等值例示有 $\models\neg S_a\varphi\leftrightarrow\neg(K_a\varphi\wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$,故

①在知识逻辑中,“可能知道”($\widehat{K}$)是“知道”(K)的对偶模态,我们有 $\widehat{K}_a\varphi:=\neg K_a\neg\varphi$(主体 a 可能知道 φ,即主体 a 不知道 φ 为假;或存在主体 a 认知不可区分的世界满足 φ。)

$\models K_a\neg S_a\varphi\leftrightarrow K_a\neg(K_a\varphi \wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$，从 $\models K_a\neg(K_a\varphi \wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))\leftrightarrow K_a\neg K_a(\varphi \wedge (\wedge_{b\neq a}\neg K_b\varphi))$ 与 $\models\neg K_a(\varphi\wedge(\wedge_{b\neq a}\neg K_b\varphi))\rightarrow K_a\neg K_a(\varphi\wedge(\wedge_{b\neq a}\neg K_b\varphi))$((5)公理的例示)，有 $\models\neg K_a(\varphi \wedge (\wedge_{b\neq a}\neg K_b\varphi))\rightarrow K_a\neg(K_a\varphi \wedge K_a(\wedge_{b\neq a}\neg K_b\varphi))$，则根据(S)有 $\models\neg S_a\varphi\rightarrow K_a\neg S_a\varphi$。其余有效式的证明略。

定理 2：基本知识逻辑的公理系统(表 2)是可靠且强完全的。

证明：见《动态认知逻辑》[①]。

定理 3：在表 2 中的公理系统中引入(S)作为公理后得到的系统是可靠且强完全的。

表 2　知识公理系统

(PROP)	所有的命题重言式例示	
(K)	$K_a(\varphi\rightarrow\psi)\rightarrow(K_a\varphi\rightarrow K_a\psi)$	知识的分配性
(T)	$K_a\varphi\rightarrow\varphi$	知识的真值性
(4)	$K_a\varphi\rightarrow K_aK_a\varphi$	知识的正自省性
(5)	$\neg K_a\varphi\rightarrow K_a\neg K_a\varphi$	知识的负自省性
(MP)	从 φ 和 $(\varphi\rightarrow\psi)$，可得 ψ	肯定前件规则
(**Nec**)	从 φ，可得 $K_a\varphi$	知识必然化规则

注：知识逻辑的公理系统 S5，可靠且强完全的证明系统。

证明：根据命题 1，可知(S)公理是可靠的。则逻辑语言 $\mathcal{L}_{KS}$ 中的公式都可以化归为基本的知识逻辑语言，因而根据定理 2，也是可靠且完全的。

表 3　秘密认识系统

关于 S_a 算子的公理：		
(**K**)	$\models S_a(\varphi\rightarrow\psi)\rightarrow(S_a\varphi\rightarrow S_a\psi)$	秘密的分配性
(**T**)	$\models S_a\varphi\rightarrow\varphi$	秘密的真值性
(**4**)	$\models S_a\varphi\rightarrow S_aS_a\varphi$	秘密的正自省性
(**C**)	$\models(S_a\varphi\wedge S_a\psi)\rightarrow S_a(\varphi\wedge\psi)$	秘密的组合性
(**D**)	$\models S_a\varphi\rightarrow\neg S_a\neg\varphi$	秘密的持续性
($\top$)	$\models\neg S_a\top$	永真不是秘密
($\bot$)	$\models\neg S_a\bot$	矛盾不是秘密
关于 S_a 算子的规则：		
(**RE**)	从 $\models(\varphi\leftrightarrow\psi)$，得 $\models(S_a\varphi\leftrightarrow S_a\psi)$	等值替换规则
(Nnec)	从 $\models\varphi$，得 $\models\neg S_a\varphi$	否定的必然化规则
(Dnec)	从 $\models\varphi$，得 $\models\neg S_a\neg\varphi$	可能必然化规则
关于 S_a 与 S_b 算子间的交互公理：		
(**Ex**1)	$S_a\varphi\rightarrow\neg S_b\varphi$	秘密的独占性
(Ex2)	$S_a\neg S_a\varphi\rightarrow\neg S_b\neg S_b\varphi$	秘密嵌套的独占性
(**N**1)	$\neg S_a\neg S_b\varphi$	无秘密之非秘密
(N2)	$\neg S_aS_b\varphi$	无秘密之秘密

注：$\mathcal{L}_S$ 语言中秘密模态词的公理、规则及重要定理(ECKT4 系统的扩张)，其中主体 $a\neq b$。加粗的公理或规则称为核心公理或规则，其他未加粗的公理和规则可从加粗的公理或规则中推导出来。

①van Ditmarsch, H., et al. *Completeness. Dynamic Epistemic Logic*. Springer, 2008, p. 178.

命题 4:表 3 中的公理是有效的,规则是保持有效的。

证明:我们在 $\mathcal{L}_S$ 语言中给出证明。

· 对(K)公理的证明。令 (M,w) 为认知模型中的任意点模型。$M,w\models S_a(\varphi\rightarrow\psi)$ 且 $M,w\models S_a\varphi$,只需要证 $M,w\models S_a\psi$。(反证法)假设 $M,w\models S_a\psi$,则 $M,w\models\neg\ S_a\psi$。根据语义定义有 a)若对任意 $w'\in W$ 如果 $w\sim_a w'$ 那么 $M,w'\models\psi$,则存在 $b\neq a\in$ Agt,对任意 $u\in W$ 有 $w'\sim_b u$ 蕴涵 $M,u\models\psi$。再根据 $M,w\models S_a(\varphi\rightarrow\psi)$ 与 $M,w\models S_a\varphi$ 的语义,对任意 $w'\in W$ 如果 $w\sim_a w'$ 那么有 $M,w'\models\varphi\rightarrow\psi$ 与 $M,w'\models\varphi$,从而有 $M,w'\models\psi$。再根据 a),存在 $b\neq a\in$ Agt,对任意 $u\in W$ 有 $w'\sim_b u$ 蕴涵 $M,u\models\psi$。再根据 $M,w\models S_a(\varphi\rightarrow\psi)$ 的语义以及 $w\sim_a w'$,有对任意 $b\neq a\in$ Agt,存在 $u_1\in W$ 使得 $w'\sim_b u_1$,$M,u_1\models\neg\ (\varphi\rightarrow\psi)$,$M,u_1\models\neg\ \psi$。又根据 a)有存在 $b\neq a\in$ Agt,对任意 $u\in W$ 有 $w\sim_b u$ 蕴涵 $M,u\models\psi$,即 $M,u_1\models\psi$,矛盾。

· 对(T)公理的证明可以结合语义定义与 $\sim_a$ 关系的自反性得证。同理,对(4)可根据语义定义结合 $\sim_a$ 关系的传递性得证。对(C)公理,令 (M,w) 为认知模型中的任意点模型。$M,w\models S_a\varphi$ 且 $M,w\models S_a\psi$,则必有对任意 $w'\in W$,如果 $w\sim_a w'$,那么 $M,w'\models\varphi\wedge\psi$,且对任意 $b\neq a\in$ Agt,存在 $u,u'\in W$ 使得 $w'\sim_b u$,$w'\sim_b u'$,$M,u'\models\neg\ \varphi$ 且 $M,u\models\neg\ \psi$。根据命题演算,则有 $M,u'\models\neg\ (\varphi\wedge\psi)$ 且 $M,u\models\neg\ (\varphi\wedge\psi)$,从而根据语义定义有 $M,w\models S_a(\varphi\wedge\psi)$。

· 对($\top$)公理的证明(反证法),假设 $M,w\models S_a\top$,则根据语义定义有对任意 $w'\in W$,如果 $w\sim_a w'$,那么 $M,w'\models\top$,且对任意 $b\neq a\in$ Agt,存在 $u\in W$ 使得 $w'\sim_b u$ 且 $M,u\models\neg\ \top$。根据 $\sim_a$ 的自反性,则必有 $w\sim_a w$ 且 $M,w\models\top$。从而对任意 $b\neq a\in$ Agt,存在 $u\in W$ 使得 $w\sim_b u$ 且 $M,u\models\neg\ \top$,矛盾。

· (D)公理可由(T)公理的逆否命题例示通过命题演算得证,即从 $\models\varphi\rightarrow\neg\ S_a\neg\ \varphi$ 与 $\models S_a\varphi\rightarrow\varphi$ 可证 $\models S_a\varphi\rightarrow\neg\ S_a\neg\ \varphi$。

· 规则是保持有效性的(反证法)。令 $\models(\varphi\leftrightarrow\psi)$ 但存在认知模型 M 与世界 w 使得 $M,w\models S_a\varphi\wedge\neg\ S_a\psi$。从 $M,w\models\neg\ S_a\psi$,根据语义定义,有存在 $w'\in W$:如果有 $w\sim_a w'$ 蕴涵 $M,w'\models\psi$,那么存在 $b\neq a\in$ Agt 对任意的 $u\in W$,$w'\sim_b u$ 蕴涵 $M,u\models\psi$。又因为 $\models(\varphi\leftrightarrow\psi)$,故有 $w\sim_a w'$ 蕴涵 $M,w'\models\varphi$,那么存在 $b\neq a\in$ Agt 对任意的 $u\in W$,$w'\sim_b u$ 蕴涵 $M,u\models\psi$。从而,根据语义定义有 $M,w\models\neg\ S_a\varphi$,与 $M,w\models S_a\varphi$ 矛盾($M,w\models\neg\ S_a\varphi\wedge S_a\psi$ 的证明与之类似,省略)。

· (Nnec)规则可以从(RE)规则中推导出来。令 $\models\varphi$,则有 $\models\varphi\leftrightarrow\top$。根据(RE)规则,有 $\models S_a\varphi\leftrightarrow S_a\top$,即 $\models\neg\ S_a\varphi\leftrightarrow\neg\ S_a\top$,根据($\top$)公理,则有 $\models\neg\ S_a\varphi$。同理(Dnec)也可以从(RE)规则中推导出来。令 $\models\varphi$,则有 $\models\neg\ \varphi\leftrightarrow\bot$。根据(RE)规则,有 $\models S_a\neg\ \varphi\leftrightarrow S_a\ \bot$,$\models\neg\ S_a\neg\ \varphi\leftrightarrow\neg\ S_a\ \bot$,根据($\bot$)公理,则有 $\models\neg\ S_a\neg\ \varphi$。

· (Ex1)公理是有效的(反证法)。令 $a\neq b$。假设存在 (M,w) 为认知模型中的点模型使得 $M,w\models S_a\varphi\wedge S_b\varphi$,根据语义定义则有:

1.对任意 $w'\in W$,如果 $w\sim_a w'$,那么 $M,w'\models\varphi$,且对任意 $b\neq a\in$ Agt,存在 $u\in W$ 使得 $w'\sim_b u$ 且 $M,u\models\neg\ \varphi$,且

2.对任意 $w'\in W$,如果 $w\sim_b w'$,那么 $M,w'\models\varphi$,且对任意 $a\neq b\in$ Agt,存在 $u\in W$ 使得 $w'\sim_a u$ 且 $M,u\models\neg\ \varphi$

根据认知模型的自反性,必有 $w\sim_a w,w\sim_b w$。从 $w\sim_a w$,根据 1 有故 $M,w\models\varphi$ 且对任意 $b\neq a\in$ Agt,存在 $u\in W$ 使得 $w\sim_b u$ 且 $M,u\models\neg\ \varphi$,又根据 2 对任意 $w'\in W$,如果 $w\sim_b w'$,那么 $M,w'\models\varphi$,则有 $M,u\models\varphi$,矛盾。故 $M,w\models S_a\varphi\wedge S_b\varphi$,$M,w\models S_a\varphi\rightarrow\neg\ S_b\varphi$。因为 (M,w) 为任意点模型,故 $\models S_a\varphi\rightarrow\neg\ S_b\varphi$。

·(Ex2)公理可运用(Ex1)公理推导出来。首先根据(Ex1)公理的逆否命题例示,有 $\models S_b\psi\rightarrow\neg\ S_a\psi$。令 $\psi=\neg\ S_b\varphi$,则有 $\models S_b\neg\ S_b\varphi\rightarrow\neg\ S_a\neg\ S_b\varphi$,则由其逆否命题得 $\models S_a\neg\ S_b\varphi\rightarrow\neg\ S_b\neg\ S_b\varphi$。

· (N2)公理可推导。根据(Ex1)公理的例示有① $\models S_aS_b\varphi\rightarrow\neg\ S_bS_b\varphi$,再根据(4)公理的逆否命题例示,有② $\models\neg\ S_bS_b\varphi\rightarrow\neg\ S_b\varphi$。①和②根据命题演算有③ $\models S_aS_b\varphi\rightarrow\neg\ S_b\varphi$。再根据(T)公理的逆否命题例示,有④ $\models\neg\ S_b\varphi\rightarrow\neg\ S_aS_b\varphi$。③和④根据命题演算有 $\models S_aS_b\varphi\rightarrow\neg\ S_aS_b\varphi$,即 $\models\neg\ S_aS_b\varphi$。

· (N1)公理是有效的。假设存在一个点模型使得 $M,w\models S_a\neg\ S_b\varphi$,则根据归约公理(S)有 $M,w\models K_a\neg\ S_b\varphi\wedge K_a(\wedge_{b\neq a}\neg\ K_b\neg\ S_b\varphi)$,则有 $M,$

$w\models\neg S_b\varphi\wedge\wedge_{b\neq a}\neg K_b\neg S_b\varphi$，则存在 $w\sim_b u$ 使得 $M,u\models S_b\varphi$ 根据表 1 中的(NC)公理，则有 $M,u\models K_bS_b\varphi$，从而根据认知模型的对称性有 $u\sim_b w$，故有 $M,w\models S_b\varphi$，与已知矛盾。故不存在一个点模型 (M,w) 使得 $M,w\models S_a\neg S_b\varphi$，从而必有 $\models\neg S_a\neg S_b\varphi$。

命题 5：表 4 中的公式和规则都是无效的。

表 4　无效推理

$\not\models\neg S_a(\varphi\rightarrow\psi)\rightarrow(\neg S_a\varphi\rightarrow\neg S_a\psi)$
$\not\models\neg S_a\neg(\varphi\rightarrow\psi)\rightarrow(\neg S_a\neg\varphi\rightarrow\neg S_a\neg\psi)$
$\not\models\neg S_a\neg\varphi\rightarrow S_a\varphi$
$\not\models S_a(\varphi\wedge\psi)\rightarrow S_a\varphi$
$\not\models\neg S_a\neg S_a\varphi$
从 $\models\varphi$，得不出 $\models S_a\varphi$。
从 $\models\varphi\rightarrow\psi$，得不出 $\models S_a\varphi\rightarrow S_a\psi$。
从 $\models\varphi\rightarrow\psi$，得不出 $\models\neg S_a\varphi\rightarrow\neg S_a\psi$。
从 $\models\varphi\rightarrow\psi$，得不出 $\models S_a\neg\varphi\rightarrow S_a\neg\psi$。
从 $\models\varphi\rightarrow\psi$，得不出 $\models\neg S_a\neg\varphi\rightarrow\neg S_a\neg\psi$。

注：当主体集 $|\mathrm{Agt}|\geqslant 2$ 时，上述公式和推理都是无效的。

证明：对命题 5 中无效公式最简单的证明是构造反模型。

○ 令 $\varphi=p,\psi=q$，图 1 中的模型 M_0 有 $M_0,w\models\neg S_ap$ 且 $M_0,w\models\neg S_a(p\rightarrow q)$，但 $M_0,w\models S_aq$。故 $\not\models\neg S_a(\varphi\rightarrow\psi)\rightarrow(\neg S_a\varphi\rightarrow\neg S_a\psi)$ 得证。

○ 令 $\varphi=p,\psi=q$，图 1 中的模型 M_1 有 $M_1,w\models\neg S_a\neg p$ 且 $M_1,w\models\neg S_a\neg(p\rightarrow q)$，但 $M_1,w\models S_a\neg q$，即 $M_1,w\models\neg S_a\neg q$。故 $\not\models\neg S_a\neg(\varphi\rightarrow\psi)\rightarrow(\neg S_a\neg\varphi\rightarrow\neg S_a\neg\psi)$ 得证。

○ 令 $\varphi=p$，图 1 中的模型 M_2 有 $M_2,w\models\neg S_a\neg p$ 且 $M_2,w\models\neg S_ap$。故 $\not\models\neg S_a\neg\varphi\rightarrow S_a\varphi$ 得证。

○ 令 $\varphi=p,\psi=q$，图 1 中的模型 M_3 有 $M_3,w\models S_a(p\wedge q)$，但 $M_3,w\models\neg S_ap$，即 $M_3,w\models S_ap$。故 $\not\models S_a(\varphi\wedge\psi)\rightarrow S_a\varphi$ 得证。

○ 令 $\varphi=p$，图 1 中的模型 M_4 有 $M_4,w\models S_a\neg S_ap$，即 $M_4,w\models\neg S_a\neg S_ap$。故 $\not\models\neg S_a\neg S_a\varphi$ 得证。

对命题 5 中的不保持有效性的规则证明可通过反例得证。

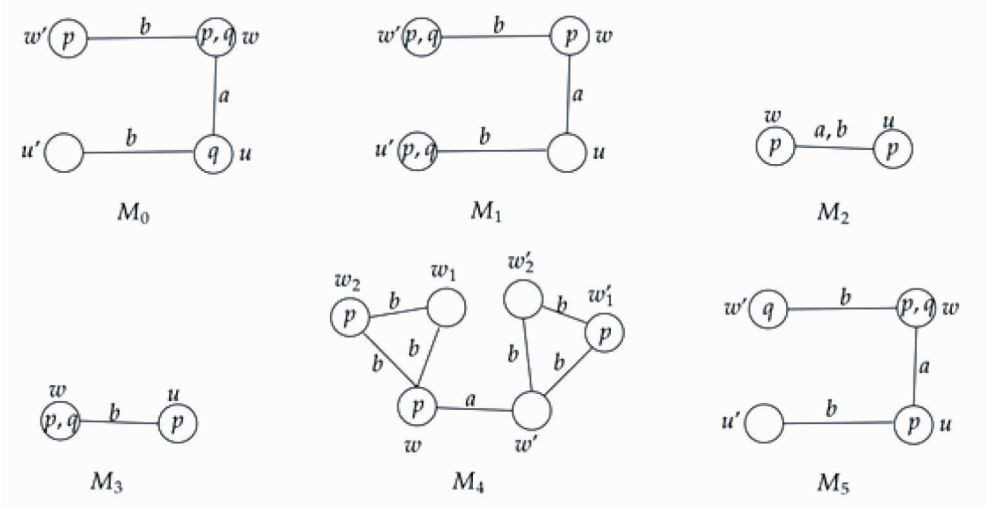

图 1　认知模型 $\mathrm{M}_0\sim\mathrm{M}_5$

注：认知模型 $M_0,\cdots,M_5$，圆圈表示世界，圈外的标签即代表该世界的名字，圈内的命题字母即该在该世界上为真的命题(为假的命题字母则不写在圈里)，带有标签的线段表示对应主体的认知不可区分关系，每一个世界上的自反关系省略。

○ 令 $\varphi=\top$，显然有 $\models\top$，但 $\not\models S_a\top$(因为 $\models\neg S_a\top$)，故从 $\models\varphi$，得不出 $\models S_a\varphi$。

○ 令 $\varphi=p,\psi=(q\vee\neg q)$，则有 $\models p\rightarrow(q\vee\neg q)$，但 $\not\models S_ap\rightarrow S_a(q\vee\neg q)$(因为 $\models S_a(q\vee\neg q)$ 且 S_ap 是可满足的)，故从 $\models\varphi\rightarrow\psi$，得不出 $\models S_a\varphi\rightarrow S_a\psi$。

○ 令 $\varphi=(p\wedge q),\psi=p$，则有 $\models(p\wedge q)\rightarrow p$，但 $\not\models S_ap\rightarrow S_a(p\wedge q)$，因为根据图 1 中的模型 M_5 有 $M_5,w\models S_ap\rightarrow S_a(p\wedge q)$。即 $\not\models\neg S_a(p\wedge q)\rightarrow\neg S_ap$，故从 $\models\varphi\rightarrow\psi$，得不出 $\models\neg S_a\varphi\rightarrow\neg S_a\psi$。

○ 令 $\varphi=q,\psi=(p\vee\neg p)$，则有 $\models q\rightarrow(p\vee$

$\neg p)$,但 $\models S_a\neg q \rightarrow S_a\neg(p \vee \neg p)$,以图 1 中的模型 M_1 为例,有 $M_1, w \models S_a\neg q \rightarrow S_a\neg(p \vee \neg p)$。则从 $\models \varphi \rightarrow \psi$,得不出 $\models S_a\neg\varphi \rightarrow S_a\neg\psi$。

○ 令 $\varphi = (p \wedge \neg p)$,$\psi = q$,则有 $\models (p \wedge \neg p) \rightarrow q$,但 $\models \neg S_a\neg(p \wedge \neg p) \rightarrow \neg S_a\neg q$,以图 1 中的模型 M_1 为例,有 $M_1, w \models \neg S_a\neg(p \wedge \neg p) \rightarrow \neg S_a\neg q$。则从 $\models \varphi \rightarrow \psi$,得不出 $\models \neg S_a\neg\varphi \rightarrow \neg S_a\neg\psi$。

根据命题 5 可知,不含有认知算子 K 的逻辑语言 $\mathcal{L}_S$ 的系统不是一个正规模态逻辑(Normal modal logic)系统,因为 S_a 算子不满足必然化规则,其对偶算子 $\neg S_a\neg$ 又不满足分配公理(K 公理),因而在关系语义学(Relational semantics)上的典范模型方法(Canonical model method)难以直接证明其完全性①。根据命题 4 可知,逻辑语言 $\mathcal{L}_S$ 的系统是 ECKT4 系统,其中 E 指的是(RE)规则。在邻域语义学②中,EK 与 ECK 系统的完全性已经得到了证明,而其扩张 ECKT4 系统的完全性还依旧是一个开问题③,ECKT4 系统的完全性并不能简单的从 ECK 的完全性中得证。换言之,关于秘密的模态逻辑系统是 ECKT4 系统的一个真扩张(引入了(⊤)公理、($Ex1$)公理与($N1$)公理),其完全性问题也依旧是一个开问题,但我们猜想表 3 表达了所有带有秘密算子的公理和规则。

定理 6:知道算子 K 在 $\mathcal{L}_S$ 语言中是不可定义的。

证明:假设 $\mathcal{L}_S$ 语言中存在着一个公式 $\alpha(\varphi)$(即不包含 K 模态算子)使得在在 $\mathcal{L}_{KS}$ 语言中有 $\models \alpha(\varphi) \leftrightarrow K_a\varphi$(即 $\alpha(\varphi)$ 定义了 $K_a\varphi$),则有 $\mathcal{L}_K \subseteq \mathcal{L}_S$($\mathcal{L}_K$ 表示只含有 K 算子的知识逻辑语言)。从命题 5 已知 $\mathcal{L}_S$ 不是一个正规的模态逻辑语言,故 $\mathcal{L}_K$ 也不是一个正规的模态逻辑语言,与 $\mathcal{L}_K$ 的正规性矛盾。

三　作为信念逻辑语义的“秘密”

在知识逻辑语言中,我们定义的秘密模态算子 S_a 具有独占性,即当 $a \neq b$ 时 $S_a\varphi \rightarrow \neg S_b\varphi$ 是有效式,这一公式的直观意思是“如果命题 φ 是主体 a 的秘密,则它就不是另一个主体 b 的秘密”。再者,在知识逻辑的语言中,根据(S)公理,我们要求“命题 φ 是主体 a 的秘密”当且仅当“主体 a 知道 φ,且主体 a 知道其他人都不知道 φ”。这一点在现实情况下过于理想,主体受限于自己的认知能力或环境,无法确定地知道其他人都不知道 φ。我们可以考虑这样的一个情景:

小马一个人在江边闲逛时,无意中发现了一个古人掩藏的宝箱,但手中并无处理箱子的工具,他四处张望确认自己没有被其他人发现,所以他做了个标记后就离开去准备工具了。恰巧在小马走后,小王也无意中发现了这个宝箱,宝箱掩藏完好,但他也没有合适的工具。四处张望发现无人看见自己后,他也做了个标记后就离开去准备工具了。

在这样的一个情景中,令 p 表示“江边有一个无主宝箱”,a 表示“小马”,b 表示“小王”。则有 S_ap 与 S_bp 同时成立,因为小王和小马都坚信没有其他人知道这个宝箱,都认为只有自己知道这个秘密 p。显然,(Ex1)公理在这里是不成立的。因而为了表达这样的情形,我们需要基于信念的语义重新给出“秘密”的定义:

$$K_a\varphi \wedge B_a(\bigwedge_{b\neq a} \neg K_b\varphi)$$

上式表达了“主体 a 知道 φ,且相信其他主体不知道 φ”,φ 则称作主体 a 的秘密。显然,在这样的定义下,我们接受“p 是小马秘密”的原因是:(1)小马知道了 p,且(2)小马相信其他人都不知道 p。因而他认为这个宝箱是安全的,故可以离开去准备工具。倘若,我们要求小马必须知道其他人都不知道 p 的话,那么在小马发现宝箱时,可以认为小马知道其他人都不知道,但是在小王发现了宝箱后,则小马就不能说自己还知道其他人都不知道④。但在这个例子中,在小马准备工具时他的“认知状态”并没有被更新(他无从得知小王也发现了江边的那个宝箱),故此时只能得出“小马相信其他人都不知道 p”,因而还会认为宝箱是安全的,并准备带着工具去开启。下面

①Blackburn, P., et al. *Modal Logic. Cambridge University Press*, 2001, p.217.

②Pacuit, E. *Neighborhood Semantics for Modal Logic*. Springer, 2017, p.61.

③https://www.researchgate.net/publication/336642538_Canonical_Completeness_for_EK_and_ECK_an_Exercise_in_Modal_Logic.

④在知识逻辑中,我们有“如果主体知道 φ,那么 φ 为真”这样的公理。而这里“小王知道了 p”,故“其他人都不知道 p”为假,从而有“小马知道其他人都不知道 p”为假,即“小马不知道其他人都不知道 p”为真。

我们给出信念逻辑下“秘密”模态词的严格定义。

定义(语言)　令 $Prop$ 表示非空的原子命题集,Agt 表示(非空)有穷主体集。$p \in Prop$ 、$a \in Agt$ 分别表示原子公式与主体,则关于 $\varphi \in \mathcal{L}_{BS}$ 与 $\Psi \in \mathcal{L}_S$ 的归纳定义如下:

$\varphi ::= p \mid \neg \varphi \mid (\varphi \wedge \varphi) \mid B_a\varphi \mid S_a\varphi$

$\psi ::= p \mid \neg \psi \mid (\psi \wedge \psi) \mid S_a\psi$

定义(信念模型)　一个信念模型 $M = (W, R, V)$ 是定义如下的三元组:

○ W 是一个非空的世界集;

○ R 是从 Agt 到 W 幂集的映射,表示每一个主体关于世界集 W 上的信念关系。如 $R_a \subseteq W \times W$ 则是关于主体 a 的信念关系集,每一个主体的信念关系是满足持续性、传递性与欧性的二元关系;

○ V 是从 $Prop$ 到 W 的幂集的赋值函数,即对每一个原子命题,指派一集世界。表示这个原子命题在这些世界上为真。如 $V(p) \subseteq W$ 即表达了所有使得原子命题 p 为真的世界集。

信念模型又称“KD45”模型,即除了满足 K 公理外,还有 D 公理、4 公理以及 5 公理[①]。即在信念逻辑中,我们没有形如 $B_a\varphi \rightarrow \varphi$ 这样的有效式,我们允许主体相信假命题,但我们要求主体相信的东西应该是一致的,即不能相信一个矛盾命题($\neg B_a \bot$)。除此之外,“相信”与“知道”是一样的,它们都满足正负自省性(即 4 公理和 5 公理)。$B_a\varphi$ 表示“主体 a 相信 φ”,$S_a\varphi$ 则表示“主体 a 知道 φ 是自己的秘密”,其具体语义定义如下:

定义(满足关系)　公式 $\varphi \in \mathcal{L}_{BS}$ 在认知模型 $M = (W, R, V)$ 的世界 w 上的可满足关系,$M, w \models \varphi$ 的定义如下:

原子公式与命题逻辑联结词的定义与知识逻辑的定义一样。

$M, w \models B_a\psi$　当且仅当　对任意 $u \in W$,如果 $w \sim_a u$,那么 $M, u \models \psi$。

$M, w \models S_a\psi$　当且仅当　$M, w \models \psi$,且对任意 $w' \in W$,如果 $w \sim_a w'$,那么 $M, w' \models \psi$,且对任意 $b \neq a \in Agt$,存在 $u \in W$ 使得 $w' \sim_b u$ 且 $M, u \models \neg \psi$。

由于 $\mathcal{L}_S \subset \mathcal{L}_{BS}$,上述语义定义也是关于 $\varphi \in \mathcal{L}_S$ 的语义定义。为了便利,我们在信念逻辑中将 $K_a\varphi$(主体 a 知道 φ)定义如下:

$K_a\varphi := (\varphi \wedge B_a\varphi)$

显然,我们有 $K_a\varphi \rightarrow \varphi$ 和 $K_a\varphi \rightarrow K_aK_a\varphi$ 都为有效式,但值得注意的是 $\neg K_a\varphi \rightarrow K_a \neg K_a\varphi$(认知模态的负自省性,5 公理)不是有效式。$\neg K_a\varphi \rightarrow K_a \neg K_a\varphi$ 实际上是 $\neg (\varphi \wedge B_a\varphi) \rightarrow (\neg (\varphi \wedge B_a\varphi) \wedge B_a \neg (\varphi \wedge B_a\varphi))$ 的简写,令 $\varphi = p$,我们可以给出一个信念模型 M 与世界 w 使得 $M, w \models \neg (p \wedge B_ap)$ 但 $M, w \models \neg B_a \neg (p \wedge B_ap)$[②],故该定义关于认知模态 K_a 的定义是不满足 5 公理的,信念模型上定义的知识(确证为真的信念)是不具有负自省性的。根据对知识算子的定义,“主体 a 知道 φ 是自己的秘密($S_a\varphi$),并非主体 a 知道 $\neg \varphi$ 是自己的秘密($\neg S_a \neg \varphi$)”也可表示如下:

$M, w \models S_a\varphi$　当且仅当　$M, w \models \varphi \wedge B_a\varphi \wedge \bigwedge_{b \in Agt \setminus \{a\}} B_a \neg B_b\varphi$。

$M, w \models \neg S_a\varphi$　当且仅当　$M, w \models \varphi$,或者存在 $w' \in W$ 有 wR_aw' 且 $M, w' \models \varphi$,或者存在 $b \neq a \in Agt$ 以及 $w' \in W$ 有 wR_aw' 且对任意的 $u \in W$,$w'R_bu$ 蕴涵 $M, u \models \neg \varphi$。

关于上述语义关系,可以直接从语义定义中推导出来。并且,在信念逻辑系统下,我们有:

(1) $\models S_a\varphi \leftrightarrow (K_a\varphi \wedge B_a(\bigwedge_{b \in Agt \setminus \{a\}} \neg K_b\varphi)$ 以及

(2) $\models (K_a\varphi \wedge B_a(\bigwedge_{b \in Agt \setminus \{a\}} \neg K_b\varphi) \leftrightarrow (\varphi \wedge B_a\varphi \wedge \bigwedge_{b \in Agt \setminus \{a\}} B_a \neg B_b\varphi)$

成立。对于(1)的证明可直接由语义定义得出(结合信念模型的 KD45 性质,与命题 1 中对(S)

①即每一个 R_a 关系都具有持续性:对任意的 x 都存在 y 使得 xR_ay(由 $B_a\varphi \rightarrow \neg B_a \neg \varphi$ 或 $\neg B_a \bot$ 定义)。传递性与欧性的定义与知识逻辑中 $\sim_a$ 是满足传递性(4 公理)与欧性(5 公理)的定义是一样的。

②令 $M = (\{w, u\}, R_a = \{(w, u), (u, u)\}, V(p) = \{u\})$,则有 $M, w \models \neg (p \wedge B_ap) \wedge \neg B_a \neg (p \wedge B_ap)$。

公理的证明类似)。对于(2)的证明见命题 7。

命题 7:公式$(K_a\varphi \wedge B_a(\wedge_{b\in Agt\setminus\{a\}}\neg K_b\varphi))$与$(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a\neg B_b\varphi)$是逻辑等值的。

证明:令 M 为任意的信念模型,w 为模型上的任意世界。则根据 $K_a\varphi$ 的定义有 $M,w\models(K_a\varphi \wedge B_a(\wedge_{b\in Agt\setminus\{a\}}\neg K_b\varphi))$,当且仅当 $M,w\models(\varphi \wedge B_a\varphi \wedge B_a(\wedge_{b\in Agt\setminus\{a\}}\neg(\varphi \wedge B_b\varphi)))$,当且仅当 $M,w\models(\varphi \wedge B_a\varphi \wedge B_a(\wedge_{b\in Agt\setminus\{a\}}(\varphi \rightarrow \neg B_b\varphi)))$。根据$\models B_a(\varphi\wedge\psi)\leftrightarrow(B_a\varphi\wedge B_a\psi)$有 $M,w\models(\varphi \wedge B_a\varphi \wedge B_a(\wedge_{b\in Agt\setminus\{a\}}(\varphi\rightarrow\neg B_b\varphi)))$,当且仅当 $M,w\models(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a(\varphi \rightarrow \neg B_b\varphi))$。又根据$\models(B_a\varphi \wedge B_a(\varphi\rightarrow\psi))\leftrightarrow(B_a\varphi \wedge (B_a\varphi \rightarrow B_a\psi))$,有 $M,w\models(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a(\varphi\rightarrow\neg B_b\varphi))$,当且仅当 $M,w\models(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}(B_a\varphi\rightarrow B_a\neg B_b\varphi))$,当且仅当 $M,w\models(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a\neg B_b\varphi)$(根据命题演算$\models(\varphi \wedge (\varphi\rightarrow\psi))\leftrightarrow(\varphi \wedge \psi))$。故命题 5 得证。

根据命题 7 可知在信念模型下,命题“主体 a 知道 φ,并且相信其他人都不知道 φ”与“φ 为真且主体 a 相信 φ,并且相信其他人都不相信 φ”是逻辑等值的。因而对于秘密模态算子 S_a 有等值关系成立:

$$\models S_a\varphi\leftrightarrow(\varphi \wedge B_a\varphi \wedge \bigwedge_{b\in Agt\setminus\{a\}}B_a\neg B_b\varphi)(S)$$

因而对于 $\mathcal{L}_{BS}$ 语言而言,其公理系统则是在基本的信念逻辑公理系统(KD45 系统)的基础上引入关于秘密的归约公理 (S) 即可,因而是可靠且强完全的(从命题 7,易证 (S) 的可靠性,$\mathcal{L}_{BS}$ 语言的公理系统的完全性则是正规的 KD45 系统的完全性)。

表 5　信念公理系统

(PROP)	所有的命题重言式例示	
(K)	$B_a(\varphi\rightarrow\psi)\rightarrow(B_a\varphi\rightarrow B_a\psi)$	信念的分配性
(D)	$B_a\varphi\rightarrow\neg B_a\neg\varphi$	信念的一致性
(4)	$B_a\varphi\rightarrow B_aB_a\varphi$	信念的正自省性
(5)	$\neg B_a\varphi\rightarrow B_a\neg B_a\varphi$	信念的负自省性
(MP)	从 φ 和 $(\varphi\rightarrow\psi)$,可得 ψ。	肯定前件规则
(Nec)	从 φ,可得 $B_a\varphi$。	知识必然化规则

注:基本信念逻辑的公理系统 KD45,可靠且强完全的证明系统。

若在形式语言中,舍弃 B_a 算子,只使用秘密算子 S_a,我们可以得到信念模型下的纯秘密模态语言 $\mathcal{L}_S$。与认知模型下的秘密模态语言一样,我们关注在这样的语言中,有哪些关于秘密模态算子的公理和规则。

定理 8:基本信念逻辑的公理系统(表 5)是可靠且强完全的。证明见《动态认知逻辑》①。

根据定理 8 可知在表 5 中引入关于秘密的归约公理 (S) 则可得到带有秘密算子 S 的逻辑语言 $\mathcal{L}_{BS}$ 的公理系统,其可靠性与强完全性则可从定理 8 中证得。

命题 9:在 $\mathcal{L}_{BS}$ 语言中,对任意的公式 φ 以及个体 a 而言,都有$\models S_a\varphi\rightarrow B_aS_a\varphi$。

证明:令 M 为任意信念模型,w 为 M 中的任意世界。假设 $M,w\models S_a\varphi$,则根据归约公理 (S) 有 $M,w\models\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a\neg B_b\varphi$。则根据 B_a 算子满足(4)公理、(T)公理以及对合取算子满足分配律$\models B_a(\varphi\wedge\psi)\leftrightarrow(B_a\varphi\wedge B_a\psi)$可算得 $M,w\models B_a\varphi \wedge B_aB_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_aB_a\neg B_b\varphi$,进一步则可算出 $M,w\models B_a(\varphi \wedge B_a\varphi \wedge \wedge_{b\in Agt\setminus\{a\}}B_a\neg B_b\varphi)$,即有 $M,w\models B_aS_a\varphi$。

命题 10:表 5 中的公理是有效的,规则是保持有效性的。

证明:令 M 为任意信念模型,w 为 M 中的任意世界。

○ 对于(K)公理,假设 $M,w\models S_a(\varphi\rightarrow\psi)\wedge S_a\varphi$,只需证 $M,w\models S_a\psi$。从 $M,w\models S_a(\varphi\rightarrow\psi)$ 中可得 $M,w\models\wedge_{b\in Agt\setminus\{a\}}B_a\neg B_b(\varphi\rightarrow\psi)$,又因为$\models\neg B_b(\varphi\rightarrow\psi)\rightarrow(\neg B_b\neg\varphi\wedge\neg B_b\psi)$,故易得 $M,w\models\wedge_{b\in Agt\setminus\{a\}}B_a(\neg B_b\neg\varphi\wedge\neg B_b\psi)$,从而有

①van Ditmarsch, H., et al. *Completeness. Dynamic Epistemic Logic*. Springer, 2008, p. 178.

$\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_b\psi$。又从 $M,w\models S_a(\varphi\rightarrow\psi)\wedge S_a\varphi$ 中可得 $M,w\models B_a(\varphi\rightarrow\psi)\wedge B_a\varphi\wedge\varphi$,则 $M,w\models\psi\wedge B_a\psi$。从而有 $M,w\models\psi\wedge B_a\psi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_b\psi$,即 $M,w\models S_a\psi$,故(K)公理得证。

○ 对于(T)公理的证明可从归约公理(S)中直接得证。

○ 对于(C)公理的证明可从归约公理(S)以及$\models B_a(\varphi\wedge\psi)\leftrightarrow(B_a\varphi\wedge B_a\psi)$中直接得证。

○ (D)公理则是(T)公理的推论。

○ ($\top$)公理可从 $\models B_a\top$ 以及关于 B_a 的必然化规则中得证。

○ ($\bot$)公理是(T)公理的例示。

○ 从归约公理(S)中易证等值替换规则(RE)是保持有效性的。(Nnec)与(Dnec)规则可使用(RE)规则结合($\top$)公理和($\bot$)公理推导出来。

○ 对于(4)公理$\models S_a\varphi\rightarrow S_aS_a\varphi$ 的证明,根据归约公理(S),即证$\models(\varphi\wedge B_a\varphi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_b\varphi)\rightarrow(S_a\varphi\wedge B_aS_a\varphi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_bS_a\varphi)$。令 M 为任意信念模型,w 为 M 中的任意世界使得 $M,w\models\varphi\wedge B_a\varphi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_b\varphi$,即有 $M,w\models S_a\varphi$。再根据命题 8,从 $M,w\models B_a\varphi$ 有 $M,w\models B_aS_a\varphi$,因此只需证明 $M,w\models\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_bS_a\varphi$ 即可。根据 $M,w\models\varphi\wedge B_a\varphi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_b\varphi$ 的语义定义有:

① $M,w\models\varphi$;

②对所有 $w'\in W$, 若 wR_aw', 则 $M,w'\models\varphi$;

③对所有 $w'\in W,b\in Agt\setminus\{a\}$,若 wR_aw',则(存在 $u\in W$,使得 $w'R_bu$ 并且 $M,u\models\neg\varphi$)。

(反证法)假设存在 $b\in Agt\setminus\{a\}$ 使得 $M,w\models\neg B_a\neg B_bS_a\varphi$。因此,存在点 $w'\in W$ 使得 wR_aw'(③的前件被满足)并且 $M,w'\models B_bS_a\varphi$。所以,对所有 $v\in W$,若 $w'R_bv$ 则 $M,v\models S_a\varphi$(④)。执行③的后件可知存在 $u\in W$ 使得 $w'R_bu$,故根据④有 $M,u\models S_a\varphi$,因而有 $M,u\models\varphi$,这与③矛盾,故必有 $M,w\models\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_bS_a\varphi$。综上,$M,w\models(S_a\varphi\wedge B_aS_a\varphi\wedge\wedge_{b\in Agt\setminus\{a\}} B_a\neg B_bS_a\varphi)$,根据归约公理($S$)则有 $M,w\models S_aS_a\varphi$,从而有(4)公理得证。

表 6　秘密信念系统

关于 S_a 算子的公理:		
(**K**)	$\models S_a(\varphi\rightarrow\psi)\rightarrow(S_a\varphi\rightarrow S_a\psi)$	秘密的分配性
(**T**)	$\models S_a\varphi\rightarrow\varphi$	秘密的真值性
(**4**)	$\models S_a\varphi\rightarrow S_aS_a\varphi$	秘密的正自省性
(**C**)	$\models(S_a\varphi\wedge S_a\psi)\rightarrow S_a(\varphi\wedge\psi)$	秘密的组合性
(D)	$\models S_a\varphi\rightarrow\neg S_a\neg\varphi$	秘密的持续性
($\top$)	$\models\neg S_a\top$	永真不是秘密
($\bot$)	$\models\neg S_a\bot$	矛盾不是秘密
关于 S_a 算子的规则:		
(**RE**)	从$\models(\varphi\leftrightarrow\psi)$,得$\models(S_a\varphi\leftrightarrow S_a\psi)$	等值替换规则
(Nnec)	从$\models\varphi$,得$\models\neg S_a\varphi$。	否定的必然化规则
(Dnec)	从$\models\varphi$,得$\models\neg S_a\neg\varphi$	可能必然化规则
关于 S_a 与 S_b 算子间的交互公理:		
(Ns)	$\neg S_aS_b\varphi$	无秘密之秘密

注:$\mathcal{L}_S$ 语言中秘密模态词的公理、规则及重要定理(ECKT4 系统的扩张),其中主体 $a\neq b$。加粗的公理或规则称为核心公理或规则,其他未加粗的公理和规则可从加粗的公理或规则中推导出来。

从表 3 与表 6 中可知,不管是在认知模型中还是在信念模型中,我们关于秘密算子的两个归约公理(S)与(S)使得我们关于单主体的秘密模态算子 S_a 与 S_a 都满足 ECKT4 系统,准确而言它们都是 ECKT4 加上$\top$公理的扩张。当然在信念逻辑的语义下,我们有如下性质。

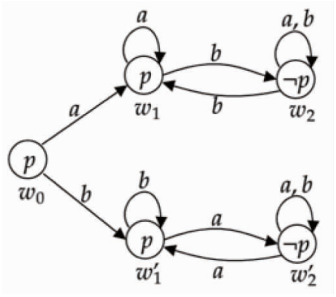

图 2　信念模型 M_1

注:信念模型 M_1,圆代表具体的世界,其满足的原子命题及其否定写在了圆内,带有标签的箭头代表着对应主体的可及关系。

命题 11:表 4 中无效的推理和公式在信念逻辑语义下依然是无效的,并且当 $a \neq b$ 时,如下公式也是无效的:

$\models S_a\varphi \rightarrow \neg S_b\varphi$	秘密非独占性
$\models S_a \neg S_a\varphi \rightarrow \neg S_b \neg S_b\varphi$	嵌套非独占性
$\models \neg S_a \neg S_b\varphi$	非秘密可秘性

证明:根据所有的认知模型都是信念模型的特殊形式,因而所有在认知模型上不保持有效性的公式或推理在信念模型上也不保持。因而根据命题 5 的证明可知将表 4 中的 S 算子换成 S 算子后,其在信念逻辑语义下依旧是无效的。

对于$\models S_a\varphi \rightarrow \neg S_b\varphi$ 与$\models S_a \neg S_b\varphi \rightarrow \neg S_b \neg S_b\varphi$ 的证明见图 2 这个反模型。令 $Agt=\{a,b\}$,$\varphi=p$,易见 $M,w_0 \models S_ap \wedge S_bp$。现只需证明$\models S_a \neg S_b\varphi \rightarrow \neg S_b \neg S_b\varphi$,令 $Agt=\{a,b\}$,$\varphi=\neg p$,我们证明 $M,w_0 \models S_a \neg S_b \neg p \wedge S_b \neg S_b \neg p$。首先因为 $M,w_0 \models \neg p$,故根据 S_a 的语义有 $M,w_0 \models \neg S_a \neg p$。同理 $M,w_1 \models \neg S_a \neg p$。因为在 w_2 上有$\neg B_b \neg p$ 和$\neg p$ 成立,且对 a 而言只有 $w_2R_aw_2$,所以 $M,w_2 \models B_a \neg B_b \neg p \wedge B_a \neg p \wedge \neg p$,即 $M,w_2 \models S_a \neg p$。因而根据 $w_1 R_b w_2$,有 $M,w_1 \models \neg B_b \neg S_a \neg p$。在 w_0 上只有 w_1 是 R_a 可及的,故 $M,w_0 \models B_a \neg B_b \neg S_a \neg p$。从而我们证明了 $M,w_0 \models \neg S_a \neg p \wedge B_a \neg S_a \neg p \wedge B_a \neg B_b \neg S_a \neg p$,又因为只有 a,b 两个不同的个体,故根据归约公理有 $M,w_0 \models S_a \neg S_a \neg p$。同理,可根据 w_0,w'_1,w'_2 间的关系证得 $M,w_0 \models S_b \neg S_b \neg p$ 成立。故 $M,w_0 \models S_a \neg S_b \neg p \wedge S_b \neg S_b \neg p$ 得证,$S_a \neg S_b\varphi \rightarrow \neg S_b \neg S_b\varphi$ 不是有效式。

对于$\models \neg S_a \neg S_b\varphi$ 的证明见图 3 这个反模型。令 $Agt=\{a,b\}$,$\varphi=p$。因为 $M,w \models \neg p$,故 1)$M,w \models \neg S_bp$。因为在 u 点上 b 的信念关系只有 $u R_b u$ 且 a 的信念关系只有 uR_aw,故易见 $M,u \models p \wedge B_bp \wedge B_b \neg B_ap$,根据归约公理($S$)有 $M,u \models S_b\varphi$,根据主体 b 在 w 上只有 $w R_b u$ 有 $M,w \models B_bS_b\varphi$,根据($D$)公理有 $M,w \models \neg B_b \neg S_b\varphi$。又因为主体 a 在 w 上只有 wR_aw,故 $M,w \models B_a \neg B_b \neg S_b\varphi$ 且根据 1)还有 $M,w \models B_a \neg S_bp$,从而有 $M,w \models \neg S_bp \wedge B_a \neg S_bp \wedge B_a \neg B_b \neg S_b\varphi$,根据归约公理($S$)有 $M,w \models S_a \neg S_b\varphi$,故$\models \neg S_a \neg S_b\varphi$ 得证。

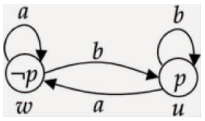

图 3　信念模型 M_2

注:信念模型 M_2,圆代表具体的世界,其满足的原子命题及其否定写在了圆内,带有标签的箭头代表着对应主体的可及关系。

图 3 中的模型反映了现实生活中一种非常典型的现象①。比如 p 表示命题“鬼神是存在的”,则在 w 世界上“主体 a 相信鬼神是不存在的”($B_a \neg p$),而“主体 b 相信鬼神是存在的”(B_bp)。不仅如此,我们还有$B_bB_a \neg p$ 与B_aB_bp 在 w 世界成立。在 w 世界上“主体 a 知道$\neg p$”($\neg p \wedge B_a \neg p$),但主体 b 不知道知道$\neg p$,不仅如此,主体 b 在 w 世界上也不知道 p(因为$\neg p$ 为真)。因而在 w 世界上“p 不是主体 b 的秘密”($\neg S_bp$),而又因为在 u 世界上我们已证得“p 是主体 b 的秘密”(S_bp),故在 w 世界上“主体 b 相信 p 是主体 b 的秘密”(B_bS_bp,蕴涵$\neg B_b \neg S_bp$),从而有“主体 b 不知道 p 不是自己的秘密”($\neg K_b \neg S_bp$,即$\neg(\neg S_bp \wedge B_b \neg S_bp)$),故在 w 世界上“p 不是主体 b 的秘密”本身不是主体 b 的秘密,即$\neg S_b \neg S_bp$ 在 w 世界上真。更进一步而言,因为在 w 世界上有$\neg K_b \neg S_bp$ 与$\neg S_bp$,故“p 不是主体 b 的秘密”是主体 a 的秘密($S_a \neg S_bp$)。也就是说,在 w 世界上“鬼神是存在不是主体 b 的秘密”这个信息只有主体 a 知道,它是主体 a 的秘密。

①即两个人相信的东西是完全相反的,并且也都“知道”对方相信的东西与自己是不同的。图 3 则回答了在这样的模型中有什么样的秘密。

结语

本文分别给出了“秘密”这一概念在知识逻辑与信念逻辑上的定义及与其对应的归约公理,并分别给出了一个可靠且完全的带有秘密算子的知识逻辑与信念逻辑的公理系统。进一步,本文分别从知识逻辑语义与信念逻辑语义分析了纯秘密逻辑系统的语义特征,并探讨了其公理系统。发现无论是在知识逻辑语义还是在信念逻辑语义下,纯秘密逻辑系统都是一个非正规的逻辑系统(ECKT4 系统的扩张),它们的完全性目前都还是一个开问题。它们虽然对秘密语义解释不同,但在单主体的条件下满足的公理与规则是一样的。在多主体的条件下,信念逻辑语义下的秘密算子允许不同主体拥有相同的秘密,这一点更符合现实情境。如将“$K_a\varphi$”用信念逻辑定义为“$(\varphi \wedge B_a\varphi)$”(为真的信念),则知识逻辑中的秘密算子 S_a 则可用信念逻辑中的秘密算子 S_a 来翻译。但不管是在哪一种系统中,秘密算子都是 ECKT4 系统上引入(⊤)公理的扩张,它们都不满足“负自省公理”(即 5 公理)。该研究结论有助于我们弄清网络信息中“信息保密”的逻辑特性,以及“网络结构”与“信息保密”间的内在规律,并为加强“信息保密”工作提供理论借鉴。

On the Logical Semantics of “Secret”

XIONG Zuo-jun[1] & ZHANG Yu-zhi[2]

(1. Institute of Logic and Intelligence, Southwest University, Chongqing 400715, China;
2. School of Political Science and Public Administration, Qufu Normal University, Rizhao 276825, China)

Abstract: “Secret” is an important notion for knowledge and belief, and an important object discussed by information network privacy and security. We analyze the logical semantics of “secret” from Epistemic Logic and Deontic Logic, and offer its reduction axioms and axiomatization systems respectively. To capture the logical properties of the notion “secrets”, we further analyze and discuss its axioms and rules of “a pure logic system of secret” from the semantics of Epistemic Logic and Deontic Logic, and find that “the logic system of secret” from the semantics of Epistemic Logic is the same as from the semantics of Deontic Logic under the single-agent system (satisfying the same axioms and rules). In particular, pure systems of secrets generated by different semantics are all non-normal modal logics, they are extensions of the ECKT4 system. An important difference for the two systems rests in interactions among multiple agents, the completeness results of these two systems are still open problems.

Key words: secret; epistemic logic; doxastic logic; non-normal modal logic

(责任校对　游星雅)