

模糊推理中蕴涵运算的信息度约束^{*}

Information Measure Requirement of Implication Operator in Fuzzy Reasoning

陈丹 何华灿 王晖

(西北工业大学计算机科学与工程系 西安710072)

Abstract This paper has comprehensively classified implication operations, and proposed information measure requirement of all implication operators by using Yager's specificity measure. Finally, Some typical implication operators are discussed to see if they satisfy the information measure requirement.

Keywords Fuzzy implication, Information inhibition

1 引言

模糊推理中蕴涵运算的选择是很重要的,国内外学者对于蕴涵运算进行了大量的研究^[2~5,8],研究内容涉及到蕴涵运算的性质、新的运算形式、不同蕴涵运算的比较等方面,通常对于蕴涵运算的选择在于该蕴涵算子能够满足哪些由二值蕴涵扩展而来的性质^[6],如: $I(1,b)=1; I(0,a)=1$; 如果 $a < b$, 则 $I(a,c) < I(b,c)$; 连续性等等。

对于蕴涵运算应满足的性质,除连续性外,大部分都是针对蕴涵运算在定义域中某一点上的性质,这在模糊命题逻辑中,并没有什么不妥之处。但是,在模糊推理中,输入和输出都是以模糊子集的形式出现,如:

规则: IF A THEN B
已知: C
推理得到 D

由于 A, B, C, D 都是模糊子集,这使得考虑蕴涵运算的性质应从整个子集上出发,而不应仅限于蕴涵运算在某点处的运算性质,因为对模糊推理结果的语义解释依赖模糊集上的每一点在值域上的取值^[1]。本文将讨论蕴涵运算在模糊推理中的信息度约束。

2 对现有模糊蕴涵运算的归纳

我们将模糊蕴涵运算分成两类,一类是从二值蕴涵运算扩展而来的(即满足 $I(0,1)=1, I(1,1)=1, I(0,0)=1, I(1,0)=0$),一类是由二值逻辑与连接词扩展而来的(即满足 $I(1,0)=0, I(1,1)=1, I(1,0)=0, I(0,0)=0$)。

由二值蕴涵运算扩展而来的模糊蕴涵通常有两种:1) $I(a,b)=\sup\{x \in [0,1] | T(a,x) \leq b\}$, 通常称为 R 蕴涵; 2) 由二值逻辑演化而来的: $I(a,b)=S(N(a),$

$b)$, 通常称为 S 蕴涵。这里, T 和 S 分别为任意 T 范数和 S 范数, N 为否定。

二值蕴涵运算扩展而来的模糊蕴涵运算除上述两种之外,还有一些性质较好的蕴涵运算如 Yager 的 $I(a,b)=b^{a+1}$, 并不能被这两类运算所包括,为此文[2]提出 A 蕴涵运算,它是由一组公理定义的运算,由二值逻辑与连接词扩展而来的蕴涵包括了 T 范数和约束蕴涵(Force Implication)^[13]。分类的框图如图1所示。

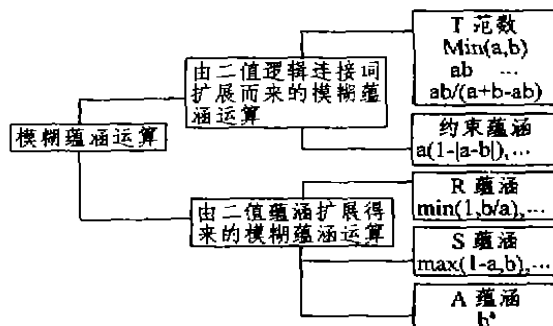


图1 蕴涵运算的分类

3 特征测度和模糊蕴涵运算的信息度约束

模糊推理包括三个元素: IF-THEN 规则, 输入数据和结果。容易得到的结束就是: 从模糊推理过程得到的结果所包含的信息度应不大于 IF-THEN 规则后所包含的信息度。

令 $\text{Inf}(A)$ 来表示模糊集 A 的信息度。对于引言中所提到的模糊推理, 我们可以得到: $\text{Inf}(D) \leq \text{Inf}(B)$ 。Yager 提出了一种特征测度(Specificity Measure)用来描述包含在可能性分布中的信息度^[6], 假定 X 是一

^{*} 本课题得到了国家教委博士学科点专项基金(98069923)和陕西省自然科学基金(98X15)的资助。

个有限集, A 是 X 的一个模糊子集, a_i 是集合 A 的第 i 个最大的隶属函数值, 特征测定的定义如下:

$Sp: [0, 1]^n \rightarrow [0, 1]$ 如果满足以下性质: 1) $Sp(A) = 1$, 当且仅当 A 是一个单元素集合; 2) $Sp(\emptyset) = 0$; 3) $(\partial Sp(A)/\partial a_1) > 0$, 对于 $j \geq 2$, $(\partial Sp(A)/\partial a_j) \leq 0$; 则它是特征测度.

Yager 给出的特征测度公式^[1]如下:

$$Sp(A) = a_1 - \sum_{j=2}^n w_j a_j \quad (1)$$

其中, $0 \leq w_j \leq 1$, $\sum_{j=2}^n w_j = 1$, 当 $j < i$, $w_j \geq w_i$.

以下根据上述特征测度来推导在模糊推理中蕴涵运算满足信息度约束的条件. Yager 曾在文[7]中针对基于相似度的模糊推理中 S 蕴涵运算讨论了信息度约束, 然而 S 蕴涵仅是蕴涵运算的一部分, 且由于基于推理合成运算的模糊推理在模糊推理运算中更常用, 因此本文对一般蕴涵运算 $I(a, b)$ 在基于推理合成运算的模糊推理中进行讨论.

考虑如下的规则:

IF x is A THEN y is B

在此规则中, B 是一个在空间 $Y = \{y, y_1, \dots, y_n\}$ 的模糊集合. 用 $B(y)$ 表示 B 的隶属函数. 假设 Y 中的元素被标号使得对于 $i < j$, $B(y_i) \geq B(y_j)$.

在模糊推理中, 通常已知为如下的集合:

$$\mu_C(x) = \begin{cases} 1 & x = x_0 \\ 0 & \text{其它} \end{cases}$$

利用 $\sup$ - τ 作为推理合成运算 (CRI), 可得到:

$$\mu_D(y) = \sup_x \tau(\mu_C(x), I(\mu_A(x), \mu_B(y))) = I(\mu_A(x_0), \mu_B(y))$$

这里 $\mu_A(x_0)$ 反映了输入与模糊控制规则前件的匹配程度. 假设对于输入 C_1 得到匹配度 $\mu_{C_1}(x_0) = a_1$, 推理结果为 D_1 ; 输入 C_2 得到匹配度 $\mu_{C_2}(x_0) = a_2$, 推理结果为 D_2 , 则有:

$$D_1(y) = I(a_1, B(y)), D_2(y) = I(a_2, B(y))$$

$$D_1(y_i) = I(a_1, B(y_i)), D_2(y_i) = I(a_2, B(y_i))$$

$D(y)$ 表示集合 D 的隶属函数. 进一步简化, 将 $D_1(y_i)$ 表示为 D_{1i} , $D_2(y_i)$ 表示为 D_{2i} , $B(y_i)$ 表示为 b_i . 由于对于 $i < j$, 有 $B(y_i) \geq B(y_j)$, 根据 I 运算的单调性可得:

$$\text{对于 } j < i, \text{ 有 } D_{1i} \geq D_{1j}, D_{2i} \geq D_{2j}$$

利用式 (1) 的测度公式可得:

$$\text{Inf}(D_1) = D_{10} - \sum_{j=1}^n w_j D_{1j}$$

$$\text{Inf}(D_2) = D_{20} - \sum_{j=1}^n w_j D_{2j}$$

假设 $a_1 > a_2$, 即 C_1 比 C_2 更好地与 A 匹配, 因此从 D_1 推理得到的结果比 D_2 所得的结果的信息量更大, 即 $\text{Inf}(D_1) > \text{Inf}(D_2)$

于是得到:

$$D_{10} - \sum_{j=1}^n w_j D_{1j} \geq D_{20} - \sum_{j=1}^n w_j D_{2j}$$

推出:

$$D_{10} - D_{20} - \sum_{j=1}^n w_j (D_{1j} - D_{2j}) \geq 0$$

由于 $\sum_{j=1}^n w_j = 1$, 可得到:

$$\sum_{j=1}^n w_j (D_{10} - D_{20} - (D_{1j} - D_{2j})) \geq 0$$

$$D_{10} - D_{20} - (D_{11} - D_{21}) \geq 0$$

即: $I(a_1, B_0) - I(a_2, B_0) \geq I(a_1, B_1) - I(a_2, B_1)$

对于所有 $a_1 \geq a_2, B_0 \geq B_1$

$$I(a_1, B_0) - I(a_1, B_1) \geq I(a_2, B_0) - I(a_2, B_1)$$

对于 $a_2 = 0$, 可得: $I(a_1, B_0) - I(a_1, B_1) \geq 0$

对于 $a_1 = 1$, 由 $I(1, b) = b$ 可得: $B_0 - B_1 \geq I(a_2, B_0) - I(a_2, B_1)$

这一不等式可由图2所示.

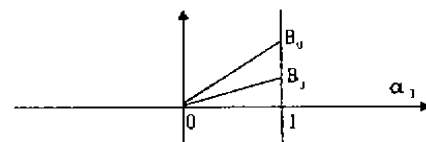


图2 满足信息度约束的运算的性质

对以上的推导进行归纳, 得到以下的结论:

模糊蕴涵运算 I 若满足 $I(v, a) - I(v, b) = D(v)$, 对于所有 $a > b$, $D(v)$ 是 v 的非减函数, 则可以保证其满足信息度约束.

4 各种蕴涵运算的信息度约束分析

利用蕴涵运算的信息度约束, 针对几种典型的蕴涵运算进行讨论.

(1) $\min(1, b/a)$

$D(v) = I(v, a) - I(v, b) = \min(1, a/v) - \min(1, b/v)$. 若 $a > b > v$, $D(v) = 0$; 若 $a > v > b$, $D(v) = 1 - b/v$; 若 $v > a > b$, $D(v) = (a - b)/v$

由于 $(a - b)/v$ 是一个减函数, 因此 $\min(1, b/a)$ 并不能满足信息量约束.

(2) $\min(1, 1 - a + b)$

$D(v) = I(v, a) - I(v, b) = \min(1, 1 - v + a) - \min(1, 1 - v + b)$. 若 $v > a > b$, $D(v) = a - b$; 若 $a > v > b$, $D(v) = v - b$; 若 $a > b > v$, $D(v) = 0$.

$D(v)$ 是 v 的非减函数, 因此 $\min(1, 1 - a + b)$ 满足信息度约束. 对于不同蕴涵运算的讨论见表1所示.

由上表可以得出以下几点结论:

(下转第62页)

②非标准的加密方式,即加密方式是除公开密钥和对称密钥加密外的其他加密方式。如 Hash 函数等。

③消息中包含长期秘密项,如主体的私钥。

我们将用于若干次密码协议运行的数据项,如主体的公开密钥、秘密密钥等定义为长期项;而将主体在一次协议运行中引入的临时数据项,如一次性随机数、短期密钥等定义为短期项。长期项和短期项是不同类型的数据项。若协议消息中包含主体私钥这样的长期秘密项,目前所得到的模型检测技术的理论结果,也无法分析这种密码协议的安全性。

结束语 模型检测技术分析密码协议,开启了模型检测技术新的应用领域,并且取得了公认的成功,并使密码协议的形式分析跨越了 BAN 类逻辑所存在的缺陷,向前进了一大步。但模型检测技术分析密码协议仍然存在着不少问题,这些问题仍然有待于我们继续进行研究。目前关键的问题在于模型检测只能分析有限状态系统,这势必对可以分析的密码协议有所要求。未来的研究趋势是如何扩大模型检测技术可分析密码协议的种类并和定理证明技术相结合,从而扩大可分析密码协议的种类,进而解决密码协议安全性分析问题。

参考文献

- 1 Burrows M, Abadi M, Needham R. A Logic of Authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18~36
- 2 Boyd C, Mao W. On a Limitation of BAN Logic. In: EU-

- ROCRYPT'93. Berlin: Springer-Verlag, 1993. 240~247
- 3 张玉清, 李继红, 肖国镇. 密码协议分析工具——BAN 逻辑及其缺陷. 西安电子科技大学学报, 1999, 26(3): 376~378
- 4 Lowe G. Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR. In: Proc. of TACAS'96. Berlin: Springer Verlag, 1996. 147~166
- 5 Hoare C A R. Communicating Sequential Processes. Prentice-Hall, 1985
- 6 Dang Z, Kemmerer R. Using the ASTRAL Model Checker for Cryptographic Protocol Analysis. In: DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997. Available at: URL: <http://dimacs.rutgers.edu/Workshops/Security/program2/program.html>
- 7 Marrero W, Clarke E, Jha S. A Model checker for Authentication Protocols. In: DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997. Available at: URL: <http://dimacs.rutgers.edu/Workshops/Security/program2/program.html>
- 8 Mutehell J, Mutehell M, Stern U. Automated Analysis of Cryptographic Protocols using Murφ. In: Proc. of the IEEE Symposium on Security and Privacy. USA: IEEE Computer Society Press, 1997. 141~151
- 9 SMV. Available at: URL: <http://www.cs.cmu.edu/~modelcheck/>
- 10 Zhang Yuqing, Xiao Guozhen. Breaking and fixing the Helsinki protocol using SMV. ELECTRONICS LETTERS, 1999, 35(15): 1239~1240
- 11 张玉清, 王磊, 肖国镇, 等. Needham-Schroeder 公钥协议的模型检测分析. 软件学报, 2000, 11(10): 1348~1352
- 12 Lowe G. Towards a Completeness Result for Model Checking of Security Protocols. Journal of Computer Security, 1999, 7(2~3): 89~146
- 13 Abadi M, Needham R. Prudent Engineering Practice for Cryptographic Protocols. IEEE Transactions on Software Engineering, 1996, 22(1): 6~15

(上接第 125 页)

1) 对于 S 蕴涵 $S(1-a, b)$, 不是对于所有的 S 范数都满足信息度约束, 如 $S(a, b) = a + b - ab$ 就不能使 S 蕴涵满足信息度约束。

表 1 不同蕴涵运算的信息度约束分析

蕴涵算子	种类	是否满足信息度约束
$a(1- b-a)$	约束蕴涵	否
b^a	A 蕴涵	是
$\min(a, b)$	T 范数	是
ab	T 范数	是
$\max(1-a, b)$	S 蕴涵	是
$1-a+b-(1-a)b$	S 蕴涵	否
$\min(1, b/a)$	R 蕴涵	否
$\min(1, 1-a+b)$	R 蕴涵	是

2) 不是对于所有的 R 蕴涵都满足信息度约束。

3) T 范数 $\min$ 运算虽然与二值蕴涵运算不相容, 但由于其满足信息度约束, 因此在实际应用中通常用 $\min$ 运算作为蕴涵运算而能得到较好的性质。

结论 本文利用 Yager 的特征测度, 推出了在基

于推理合成算法的模糊推理中, 模糊蕴涵运算满足信息度约束的条件。在选用模糊蕴涵运算时, 应从模糊子集的角度考虑它的信息度约束, 而不只局限于模糊蕴涵运算在定义域上单点处的性质。

参考文献

- 1 Yager R. R. Measures of information in Generalized constraints. Int. j. uncertainty, fuzziness and knowledge-based systems, 1998, 6: 519~532
- 2 Fernandez F G, Kreinovich V. Fuzzy Implication Can be Arbitrarily Complicated: A Theorem. Int. J. Intelligent Systems, 1998, 13: 445~451
- 3 Turksen I B, Kreinovich V, Yager R R. A new class of fuzzy implications. Axioms of fuzzy implication revisited. Fuzzy Sets and Systems, 1998, 100: 262~272
- 4 陈丹, 何华灿, 王晖. 模糊蕴涵和模糊推理研究. 计算机科学, 2000. 7
- 5 Dujat C, Vincent, N. Force implication: A new approach to human reasoning. Fuzzy Sets and Systems, 1995, 69: 53~63
- 6 Yager R R. Default knowledge and measures of specificity. Information Sciences, 1992, 61: 1~44
- 7 Yager R R. On the global requirement for the implication operators in fuzzy modus ponens. Fuzzy Sets and Systems, 1993, 106: 3~10
- 8 Klir G J, Bo Y. Fuzzy Sets and Fuzzy Logic: Theory and Application, Prentice-Hall, NJ, 1995