对称逻辑公式在经典逻辑度量空间中的分布

胡明娣[1],王国俊[1,2]
(1.陕西师范大学数学研究所,陕西西安 710062; 2.上海市高可信计算重点实验室,华东师范大学,上海 200062)

摘 要: 将密码学中对称布尔函数的概念引入到计量逻辑学理论之中,定义了对称逻辑公式和准对称逻辑公式.指出二值逻辑公式与布尔函数既密切相关,又有重要区别.证明了 n 元对称公式占全体 n 元逻辑公式的比例随 n 的增大而趋向于零,然而全体对称公式的真度之集却在[0,1]中稠密.最后从拓扑学的观点证明了全体对称公式之集在经典逻辑度量空间中无处稠密.

关键词: 对称逻辑公式; 真度; 稠密; 经典逻辑度量空间; 无处稠密
中图分类号: O159 **文献标识码:** A **文章编号:** 0372-2112 (2011) 02-0419-05

Distribution of the Symmetrical Logic Formulas in the Classical Logic Metric Space

HU Ming-di[1], WANG Guo-jun[1,2]
(1. *Institute of Mathematics, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai* 200062, *China*)

Abstract: The concept of symmetric Boolean functions treated in cryptology is transplanted into quantitative logic, and the concepts of symmetric logic formulas and pseudo-symmetric logic formulas are introduced. It is pointed out that logic formulas in two valued logic are closely related to Boolean functions while they have crucial differences. It is proved that the ratio of the number of symmetric formulas with n atoms over the number of all formulas with n atoms converges to zero when n tends to infinite. It is proved that the set of truth degrees of symmetric logic formulas is dense in [0,1]. It is proved from the viewpoint of topology that the set consisting of all symmetric logic formulas is a nowhere dense set in the classical logic metric space.

Key words: symmetric logic formula; truth degree; dense; classical logic metric space; nowhere dense

1 引言

现实世界中的命题是多种多样的,其中有大量的具体命题是不能简单地用"真"和"伪"对其可信性作二值判断的,而应当对它们的可信性程度进行量化判断.正是基于这种考虑,本文第二作者将程度化思想引入到了数理逻辑之中,建立起了计量逻辑学的基本理论[1~6].此后又与概率逻辑学相结合,将随机化思想引入到了经典的推理模式中[7,8].如今已在包括 Lukasiewicz, £ *, Gödel,和 Goguen 等多种命题逻辑系统中构造出了相应的逻辑度量空间,从而将近似推理引入到了素以严格的形式化推理为特征的各种命题逻辑系统之中.值得注意的是,除了个别零星的结果而外[9,10],可以说对于逻辑度量空间自身构造的研究还远未开始.由于对于二值命题逻辑而言,逻辑公式的真度完全由其诱导的布尔函数所决定,而在密码学中已经对布尔函数有了非常深刻的研究[11],所以如果能设法将那里有关布尔函数的各种性质引入到数理逻辑之中,必将会有力地促进计量逻辑学的发展.基于这种考虑,作为第一步,本文将密码学中对称布尔函数的概念引入到了二值计量逻辑学理论之中,定义了对称逻辑公式和准对称逻辑公式.同时指出二值逻辑公式与布尔函数既密切相关,又有重要区别(参看本文第三节).证明了对称公式的两种截然相反的性态,即,n 元对称公式只占全体 n 元逻辑公式的很小一部分,其比例随 n 的增大而趋向于零;然而从另一角度看,n 元对称公式却又很多,因为可以证明对称逻辑公式的真度之集像全体逻辑公式之集一样,是在[0,1]中稠密的.最后,我们从拓扑学的观点出发,证明了全体对称公式之集在经典逻辑度量空间中的分布是稀疏的,即,是无处稠密的.

2 基本概念

定义 1[11] 称映射 $f:\{0,1\}^n\to\{0,1\}$ 为 n 元布尔函数.设 $\alpha=(x_1,x_2,\cdots,x_n)\in\{0,1\}^n$,若 $f(\alpha)=1$,则称 α

稿日期:2009-09-16;修回日期:2010-04-27
基金项目:国家自然科学基金(No.10771129);陕西师范大学研究生培养创新基金(No.2009CXB006)

为 f 的特征向量;称 α 中 1 的个数为 α 的重量.若一旦 $\{0,1\}^n$ 中某重量为 k 的向量是 f 的特征向量,那么 $\{0,1\}^n$ 中全部重量为 k 的向量都是 f 的特征向量($0\leqslant k\leqslant n$),则称 f 为对称的布尔函数.以下用 $N(f)$ 记 f 的特征向量的个数,显然

$$N(f)=|f^{-1}(1)| \tag{1}$$

(**注 1** 上面关于 f 对称性的表述并非文献[11]中的原始定义,但易证本文的定义和文献[11]中的定义是等价的.)

定义 2[11] 称

$$f(x)=\sum_{k=0}^{n}\alpha_k\sigma_{k,n},(\alpha_k=0,1) \tag{2}$$

为 n 元对称布尔函数 f 的基本表示形式,其中

$$\sigma_{k,n}=\sum_{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant n}x_{i_1}\cdots x_{i_k}.$$

注 2 定义 2 中采用的是 f 的多项式表示,由于不影响本文的推导,为节省篇幅起见,我们对什么是多项式表示不作介绍.

定义 3[4] 设 $S=\{p_1,p_2,p_3,\cdots\}$,$F(S)$ 是由 S 生成的$(\neg,\vee,\rightarrow)$型自由代数,称 S 中的元为原子公式,称 $F(S)$ 中的元为合式公式,简称公式.

设$\{0,1\}$是最简单的布尔代数,其中

$$\neg a=1-a,a\vee b=\max\{a,b\},a\rightarrow b=1\text{ 当且仅当 }a\leqslant b \tag{3}$$

则$\{0,1\}$也是$(\neg,\vee,\rightarrow)$型代数.

定义 4[4] 设 $A(p_1,p_2,\cdots p_n)$ 是含有原子公式 p_1,$p_2,\cdots p_n$ 的逻辑公式,用 x_i 取代 $p_i(i=1,2,\cdots,n)$,并按式(3)理解逻辑连接词 $\neg,\vee,\rightarrow$,则得一布尔函数 f_A:$\{0,1\}^n\rightarrow\{0,1\}$,称为 A 所诱导的布尔函数.称 $N(f_A)/2^n$ 为公式 A 的真度,记为 $\tau(A)$.设 A,B 为 $F(S)$ 中的两个公式,称

$$\xi(A,B)=\tau((A\rightarrow B)\wedge(B\rightarrow A)) \tag{4}$$

为 A 与 B 之间的相似度.再令

$$\rho(A,B)=1-\xi(A,B),\ A,B\in F(S) \tag{5}$$

是 $F(S)$ 上的伪距离,称$(F(S),\rho)$为逻辑度量空间.

已知两个逻辑公式逻辑等价当且仅当它们之间的相似度为 1,或等价地,它们之间的伪距离为 0[4].

注 3 (1)定义 4 中公式真度的定义并非文献[4]中的原始定义,但由式(1)可见二者是等价的.

(2)公式 A 中的原子公式的标号未必是从 1 到 n 的连续编号,但设其中最大编号为 n,令 $B=A\vee(p_1\wedge\neg p_1)\vee\cdots\vee(p_n\wedge\neg p_n)$,则 B 与 A 逻辑等价,B 中原子公式的标号就是从 1 到 n 的连续编号了,所诱导的布尔函数也就可写为 $f(x_1,\cdots,x_n)$ 的形式了.以下凡提到含有 n 个原子公式的逻辑公式 A,恒假定 A 中的原子公式的标号是从 1 到 n 的连续编号.

(3)当 A 与 B 相似(即 $\xi(A,B)=1$)时 $\rho(A,B)=0$,这时 A 和 B 可以是不同的公式,可见$(F(S),\rho)$不是度量空间,只是伪度量空间.但由于逻辑等价关系 $\approx$ 是 $F(S)$ 上的$(\neg,\vee,\rightarrow)$型同余关系,这里 $A\approx B$ 当且仅当 $\rho(A,B)=0$,所以 ρ 自然地在 Lindenbaum 商代数$[F(S)]=F(S)/\approx$上诱导一个真正的度量,仍记为 ρ .这时$([F(S)],\rho)$就是一个度量空间.

3 对称逻辑公式与准对称逻辑公式

定义 5 设 A 是含有 n 个原子公式的逻辑公式.如果 A 所诱导的布尔函数是对称布尔函数,则称 A 为 n 元对称逻辑公式.容易看出,如果两个逻辑公式诱导的布尔函数相同,则此二公式逻辑等价,但反过来,逻辑等价的公式未必诱导出相同的布尔函数.

例 1 设 $A=p_1\wedge p_2,B=(p_1\wedge p_2)\vee(p_3\wedge\neg p_3)$,则 A 与 B 逻辑等价,但它们所诱导的布尔函数分别是 2 元布尔函数和 3 元布尔函数,显然是不同的.值得注意的是,前者的特征向量只有一个,即,(1,1),后者的特征向量有两个,即,(1,1,1)和(1,1,0).所以由定义 1 看出,前者是对称函数,而后者不是对称函数.因此我们得出结论:

命题 1 如果一个逻辑公式是对称公式,则和它逻辑等价的公式未必是对称公式.

命题 1 反映出了二值逻辑公式与布尔函数既密切相关,又有明显区别.

命题 2 设 A 与 B 含有同样的 n 个原子公式,则 A 与 B 逻辑等价当且仅当 A 与 B 诱导同样的布尔函数.

证明 设 A 与 B 含有同样的 n 个原子公式,且 A 与 B 逻辑等价.这时二者之间的相似度等于 1,那么由式(4)得 $\tau((A\rightarrow B)\wedge(B\rightarrow A))=1$,即,$(A\rightarrow B)\wedge(B\rightarrow A)$是重言式.分别用 f 和 g 表示 A 和 B 所诱导的布尔函数,则$(A\rightarrow B)\wedge(B\rightarrow A)$所诱导的布尔函数可写为$(f\rightarrow g)\wedge(g\rightarrow f)$,这里的运算由式(3)确定.由$(A\rightarrow B)\wedge(B\rightarrow A)$是重言式知每个 n 维 0-1 向量都是$(f\rightarrow g)\wedge(g\rightarrow f)$的特征向量,所以 f 和 g 的特征向量必相同.那么 f 与 g 也就是相同的布尔函数.可见 A 与 B 诱导同样的布尔函数.反过来,当 A 与 B 诱导同样的布尔函数时,由定义 4 知 A 与 B 逻辑等价.

注 4 当含有同样的 n 个原子公式的公式 A 与 B 诱导同样的布尔函数时,除了可能有的原子公式的排序而外,A 与 B 是没有区别的,如,$A=(p_4\wedge p_1)\vee(p_2\wedge p_3),B=(p_2\wedge p_3)\vee(p_1\wedge p_4)$.以下认为这两种逻辑公式是同一个逻辑公式.

定义 6 设逻辑公式 $B(p_1,\cdots,p_n)$ 与对称逻辑公式 $A(p_1,\cdots,p_m)$ 逻辑等价,则称 B 为准对称逻辑公式.

例 2 在例 1 中,B 是准对称逻辑公式.又,对称逻

辑公式自然也是准对称逻辑公式.所以准对称逻辑公式之集包含了对称逻辑公式之集.

命题 3　设 $B(p_1,\cdots,p_n)$与对称逻辑公式 $A(p_1,\cdots,p_m)$逻辑等价,且 $B(p_1,\cdots,p_n)$不是对称逻辑公式,则 $m<n$.

证明　由命题 2 知 $m\neq n$.设 $m>n$,令 $C=B\vee(p_{n+1}\wedge\neg p_{n+1})\vee\cdots\vee(p_m\wedge\neg p_m)$,则 C 与 B 逻辑等价,从而 C 也与 A 逻辑等价.所以由命题 2 知 C 诱导的布尔函数 h 是对称布尔函数.用 g 表示 B 诱导的布尔函数.由 g 不是对称布尔函数知存在重量为 k 的两个 n 维 0-1 向量 α 和 β 使 $g(\alpha)\neq g(\beta)$.分别令 α 和 β 的第 $n+1$ 到第 m 个坐标全为 0,就得到布尔函数 h 的两个重量为 k 的向量 α^* 和 β^* 使 $h(\alpha^*)\neq h(\beta^*)$.这与 h 是对称布尔函数相矛盾!所以 $m<n$.

命题 4　设二对称逻辑公式 $A(p_1,\cdots,p_m)$与 $B(p_1,\cdots,p_n)$逻辑等价,且 A 与 B 不是重言式,也不是矛盾式,则 $m=n$.

证明　分别用 $f(x_1,\cdots,x_m)$与 $g(x_1,\cdots,x_n)$表示 A 与 B 所诱导的布尔函数,设 $m\neq n$,不放假定 $m<n$.这时重言式$(A\rightarrow B)\wedge(B\rightarrow A)$诱导的布尔函数$(f\rightarrow g)\wedge(g\rightarrow f)$恒等于 1,这里的运算由式(3)确定.那么 $f(x_1,\cdots,x_m)$与 $g(x_1,\cdots,x_n)$恒相等.因为 A 不是重言式,也不是矛盾式,所以 $\{0,1\}^m$ 中存在重量为 k 的向量 α 和重量为 $k+1$ 的向量 β 使 $f(\alpha)$和 $f(\beta)$不相等$(0\leqslant k<m)$.不妨设 $f(\alpha)=0,f(\beta)=1$.则 g 也有重量为 $k+1$ 的 n 维特征向量 β^*,因为只需在 β 后补充 $n-m$ 个 0 就得到这种向量 β^*.但在 α 后补充 1 个 1 和 $m-n-1$ 个 0 又得到一个重量为 $k+1$ 的 n 维向量 α^*.这时 g 在两个重量为 $k+1$ 的向量上取不同的值,与 g 是对称布尔函数相矛盾!所以 $m=n$.

命题 5　设 $B(p_1,\cdots,p_n)$是准对称逻辑公式,且 B 不是重言式,也不是矛盾式,则存在唯一的对称逻辑公式与 B 逻辑等价.

证明　如果有两个对称逻辑公式 A 和 C 都与 B 逻辑等价,则 A 和 C 是逻辑等价的对称公式,所以由命题 4 知 A 和 C 含有同样多的原子公式.再由命题 2 和注 4 知 A 和 C 是相同的逻辑公式.

4　对称逻辑公式集在逻辑度量空间中的分布

定理 1　n 元对称逻辑公式占全体 n 元逻辑公式的比例随 n 的增大而趋向于零.

证明　设 A 是 n 元对称逻辑公式,则 f_A 是 n 元对称布尔函数.由式(2)知随着 α_k 在$\{0,1\}$中各种可能的选取,不同的 n 元对称布尔函数共有 2^{n+1}个,n 元对称逻辑公式也就共有 2^{n+1}个.但全体 n 元布尔函数共有 2^{2^n}个,全体 n 元逻辑公式也就共有 2^{2^n}个.显然 2^{n+1}与 2^{2^n}之比随 n 的增大而趋向于 0.所以 n 元对称逻辑公式占全体 n 元逻辑公式的比例随 n 的增大而趋向于零.

由定理 1 看出,n 元对称逻辑公式只是全体 n 元逻辑公式中的极少一部分.但有趣的是,从另一个角度看 n 元对称公式却又表现出截然相反的性质.事实上,我们有下面的

定理 2　对称逻辑公式的真度之集像全体逻辑公式的真度之集一样,是在[0,1]中稠密的.

为了证明定理 2,我们需要一个引理.

引理 1　二项展开式的系数具有如下性质:

(1) $C_{2n}^0, C_{2n}^1,\cdots, C_{2n}^n$是递增数列, $C_{2n}^{n+1}, C_{2n}^{n+2},\cdots, C_{2n}^{2n}$是递减数列, C_{2n}^n是最大值.

(2) $\lim\limits_{n\to\infty}C_{2n}^n/2^{2n}=0$.

证明　(1)设 $k<n$,则

$$\frac{C_{2n}^k}{C_{2n}^{k+1}}=\frac{(2n)!}{k!\ (2n-k)!}\Big/\frac{(2n)!}{(k+1)!\ (2n-k-1)!}=\frac{k+1}{2n-k}<1.$$

所以(1)中的前一个结论成立.其它类似可证.

(2)由斯特林公式得

$$\lim_{m\to\infty}m!\ /\sqrt{2\pi m}\left(\frac{m}{e}\right)^m=1.$$

由此可得

$$C_{2n}^n/2^{2n}=\frac{(2n)!}{(n!)^2}\Big/2^{2n}\doteq\left(\frac{\sqrt{4\pi n}(2n/e)^{2n}}{(\sqrt{2\pi n}(n/e)^n)^2}\right)\Big/2^{2n}=\frac{1}{\sqrt{\pi n}}.$$

这就证明了(2).

现在证明定理 2.

证明　设 $Q\subset[0,1]$.如果对任意给定的正数 ε,Q 有有限子集,其成员由小到大依次为:

$$\tau(0),\tau(1),\cdots,\tau(m),$$

满足条件 $\tau(0)=1/2^m,\tau(m)=1$ 和 $\tau(k+1)-\tau(k)<\varepsilon$ $(k=0,1,\cdots,m-1)$,则 Q 在[0,1]中稠密.现在用 Q 记全体对称逻辑公式的真度之集,以下只需证明 Q 满足上述条件即可.事实上,设 ε 是任意给定的正数,由引理 1 知可取 $2n$ 充分大,使 $C_{2n}^n/2^{2n}<\varepsilon$.取 $2n$ 元对称布尔函数 f_k,使其特征向量之集为 $\bigcup\limits_{i=0}^{k}D(i)$,这里 $D(i)$是全体重量为 i 的 $2n$ 维 0-1 向量之集,则由 $|D(i)|=C_{2n}^i$知诱导出对称布尔函数 f_k 的逻辑公式 A_k 的真度等于 $\sum\limits_{i=0}^{k}(C_{2n}^i/2^{2n})$.这时令

$$\tau(0)=C_{2n}^0/2^{2n}=1/2^{2n},\cdots,\tau(2n)=\sum_{i=0}^{2n}(C_{2n}^i/2^{2n})=1,$$

且由引理 1 知

$$\tau(k+1)-\tau(k)=C_{2n}^{k+1}/2^{2n}\leqslant C_{2n}^n/2^{2n}<\varepsilon,$$

$$(k=0,1,\cdots,2n-1).$$

所以满足所需要的条件,定理 2 证毕.

推论 1 准对称逻辑公式的真度之集像全体逻辑公式的真度之集一样,是在[0,1]中稠密的.

证明 因为准对称逻辑公式之集包含了对称逻辑公式之集,所以由定理 2 即得本推论.

以下我们从拓扑的观点讨论对称逻辑公式之集在逻辑度量空间中的分布.

定义 7[12] 设$(X,\cup)$是拓扑空间,E 是 X 的子集.如果 E 在$(X,\cup)$中的闭包不含内点,则称 E 是无处稠密集.

引理 2 设(X,ρ)是(伪)度量空间,E 是 X 的子集.如果①E 自身不含内点;②E 的补集中每个点都和 E 有正距离.则 E 是 X 中的无处稠密集.

证明 设 E 不是无处稠密集,则 E 的闭包 clE 有内点 a,即,存在正数 ε 使以 a 为中心以 ε 为半径的实心球 $B(a,\varepsilon)$包含于 clE 之中.但由①知 E 不含内点,所以 $B(a,\varepsilon)$中有点 b 不属于 E.那么由②知 $\rho(b,E)=\delta>0$.从而 b 不是 E 的聚点,即,b 不属于 clE,这与 $b\in B(a,\varepsilon)\subset clE$ 相矛盾! 所以 E 是无处稠密集.

定理 3 全体对称逻辑公式之集是逻辑度量空间中的无处稠密集.

证明 只需证明全体准对称逻辑公式之集 E 是逻辑度量空间中的无处稠密集,因为 E 包含了全体对称逻辑公式之集,且无处稠密集的子集是无处稠密集.设 A 是准对称逻辑公式,我们证明在 A 的任一小的邻域中都存在非准对称逻辑公式,从而 E 不含内点.因为准对称公式与某对称逻辑公式逻辑等价,从而二者之间的距离为 0,所以不妨设 A 是对称公式,A 所诱导的布尔函数为$f(x_1,\cdots,x_n)$.设 ε 是任意给定的正数,将 A 诱导的布尔函数等价扩充为

$$f^*(x_1,\cdots,x_n,x_{n+1},\cdots,x_{n+k})=f(x_1,\cdots,x_n)\vee(x_{n+1}\wedge\neg x_{n+1})\vee\cdots\vee(x_{n+k}\wedge\neg x_{n+k}) \quad (6)$$

则诱导出式(6)的逻辑公式 B 与 A 逻辑等价.取 k 充分大,使$\frac{1}{2^{n+k}}<\varepsilon$.

(1)如果 A 是矛盾式,任取仅有 1 个重量为 n 的特征向量的 $n+k$ 元布尔函数 g,则由定义 4 知诱导出 g 的逻辑公式 C 与 A 之间的距离为 $1/2^{n+k}<\varepsilon$,且可证 C 不是准对称公式.事实上,$n+k$ 元对称布尔函数一旦有重量为 n 的特征向量,就有 $C_{n+k}^n>1$ 个这种向量,不会仅有 1 个,所以 C 不是对称公式.又,由非对称的准对称公式诱导的布尔函数的构造知:改变 $n+k$ 维 0-1 向量的最后一个坐标不会影响该布尔函数的值,它一旦有重量为 n 的特征向量,就至少有两个这种向量,所以 C 也不是准对称公式.

(2)如果 A 是重言式,则取仅有 1 个重量为 n 的 $n+k$ 维 0-1 向量不是特征向量的 $n+k$ 元布尔函数 h,则由定义 4 知诱导出 h 的逻辑公式 D 与 A 之间的距离为 $1/2^{n+k}<\varepsilon$,且用和(1)中类似的分析可证 D 不是准对称逻辑公式.

(3)现在设 A 既不是矛盾式也不是重言式,则布尔函数 f 既可取值 0 又可取值 1.由命题 4 和 $n+k>n$ 知 B 不是对称逻辑公式.现在任选一个 $n+k$ 维 0-1 向量 α,则由式(6)知对每个前 n 个坐标和 α 的前 n 个坐标相同的向量 β 而言,恒有 $f^*(\alpha)=f^*(\beta)$.取 $n+k$ 维 0-1 向量 γ,改变它的最后一个坐标得另一个 $n+k$ 维 0-1 向量 λ.作 $n+k$ 元布尔函数 g^* 使 $g^*(\lambda)\neq f^*(\lambda)$,而在其余 $n+k$ 维 0-1 向量处 g^* 与 f^* 的值都相等.以 H 记诱导出布尔函数 g^* 的逻辑公式,则可证 H 不是准对称逻辑公式.由 g^* 的作法和定义 4 知 $\rho(A,H)=1/2^{n+k}<\varepsilon$.

综上所述知准对称公式集 E 不含内点,所以引理 2 中的条件①成立.以下只需证明引理 2 中条件②也成立.

事实上,设 C 不是准对称逻辑公式,C 所诱导的布尔函数为$h(x_1,\cdots,x_n)$.任取 n 元对称逻辑公式 A,设 A 诱导的布尔函数为$f(x_1,\cdots,x_n)$.则由 A 和 C 不等价和定义 4 知 $\rho(C,A)\geqslant 1/2^n=\delta>0$.再设 G 是任一对称逻辑公式,G 所诱导的布尔函数为 $\eta(x_1,\cdots,x_m)$.如果 $m\leqslant n$,把 η 等价扩充为 n 元布尔函数,并设 Q 为相应的逻辑公式,则 Q 是准对称公式而 C 不是准对称公式,所以 $\rho(C,G)=\rho(C,Q)\geqslant 1/2^n=\delta>0$.最后设 $m>n$,$m=n+k$.将 h 等价扩充为

$$h^*(x_1,\cdots,x_m)=h(x_1,x_2,\cdots,x_n)\vee(x_{n+1}\wedge\neg x_{n+1})\vee\cdots\vee(x_m\wedge\neg x_m)$$

由 C 不是准对称公式知存在重量为 r 的不同的 n 维 0-1 向量 α 和 β 使 $h(\alpha)=0$ 且 $h(\beta)=1$ 或 $h(\alpha)=1$ 且 $h(\beta)=0$.不妨设 $h(\alpha)=0$ 且 $h(\beta)=1$.因为重量为 n 或 0 的 n 维向量只有一个,所以由 α 与 β 不相等知 $1<r<n$.在向量 α 的后面任意添加 k 维 0-1 向量,共可得出 2^k 个 $n+k$ 维 0-1 向量,布尔函数 h^* 在这些向量处的值都等于 0.我们称这些向量为 0 值向量.同样地,在向量 β 的后面任意添加 k 维 0-1 向量,共可得出 2^k 个 $n+k$ 维 0-1 向量,布尔函数 h^* 在这些向量处的值都等于 1.我们称这些向量为 1 值向量.这些向量(包括 0 值向量和 1 值向量)的重量等于从 r 到 $r+k$ 的各个值.其中重量等于 $r+i$ 的向量有 C_k^i 个($i=0,1,\cdots,k$).对称布尔函数 η 在上述重量等于 $r+i$ 的 0 值向量处的值若等于 0,则 η 与 h^* 在 C_k^i 个 1 值向量处的值都不同;若 η 在上述重量等于 $r+i$ 的 0 值向量处的值等于 1,则 η 与 h^* 在 C_k^i 个 0 值向量处的值都不同.这一事实对从 0 到 k 的 i 都成立,所以 η 与 h^* 一共在 2^k 个 $n+k$ 维

0 – 1向量处的值不同.以 C^* 记诱导出 h^* 的逻辑公式,则由定义 4 知

$$\rho(C,G)=\rho(C^*,G)\geqslant 2^k\times(1/2^{n+k})=1/2^n=\delta>0.$$

又,设 P 是任意准对称公式,则 P 与某对称逻辑公式 Q 的距离为 0,从而由以上所证知 $\rho(C,P)\geqslant\delta>0$.所以 $\rho(C,E)\geqslant\delta>0$.可见引理 2 中的条件②也成立.这就证明了定理 3.由以上证明有

推论 2　全体准对称逻辑公式之集是逻辑度量空间中的无处稠密集.

5　结论

本文将密码学中对称布尔函数的概念引入到计量逻辑学理论之中,定义了对称逻辑公式和准对称逻辑公式.指出二值逻辑公式与布尔函数既密切相关,又有重要区别.较仔细地研究了对称逻辑公式在逻辑度量空间中的分布.密码学中布尔函数的研究成果非常丰硕,借鉴这些成果并将其引入到计量逻辑学之中必将丰富和促进其发展,同时也可反过来从某种角度补充密码学中布尔函数的研究.本文只是在这方面的迈出的第一步.如何将布尔函数更深入的性质,如线性点、对偶性、相关免疫性等一系列性质[11,13]引入计量逻辑学的研究之中是很值得探索的研究课题.又,布尔函数的基本性质已经有在多值情形的推广[13],计量逻辑学也已在多值乃至连续值命题逻辑中展开,所以将类似于布尔函数的多值函数的性质与计量逻辑学作相互联系的研究也就是顺理成章的了.关于这些课题,我们将于后续的研究中进行讨论.

参考文献:

[1] 王国俊.计量逻辑学(I)[J].工程数学学报,2006,23(2):191 – 215.
Wang G J.Quantitative logic(I)[J].Chinese Journal of Engineering Mathematics,2006,23(2):191 – 215.(in Chinese)

[2] 王国俊,宋建社.命题逻辑中的程度化方法[J].电子学报,2006,34(2):252 – 257.
Wang G J,Song J S.Graded method in propositional logic[J].Acta Electronica Sinica,2006,34(2):252 – 257.(in Chinese)

[3] Wang G J,Fu L,Song J S.Theory of truth degrees of propositions in two valued propositional logic[J].Science in China,ser.A,2002,45(9):1106 – 1116.

[4] 王国俊.数理逻辑引论与归结原理(2 版)[M].北京:科学出版社,2006:204 – 219.
Wang G J.Introduction to Mathematical Logic and Resolution Principle(2nd.Ed)[M].Beijing:Science in China press,2006.204 – 219.(in Chinese)

[5] Wang G J,Zhou H J.Introduction to Mathematical Logic and Resolution Principle[M].Science Press,Beijing & Alpha Science International Limited,Oxford,U.K.,2009.258 – 276.

[6] Wang G J.Zhou H J.Quantitative logic[J].Information Sciences,2009,179(3):226 – 247.

[7] 王国俊,惠小静.概率逻辑学基本定理的推广[J].电子学报,2007,35(7):801 – 812.
Wang G J,Hui X J.Generalization of fundamental theorem of probability logic[J].Acta Electronica Sinica,2007,35(7):801 – 812.(in Chinese)

[8] Wang G J,Hui X J.Randomization of classical inference patterns and its application[J].Science in China,ser.F,2007,50(6):867 – 877.

[9] Wang G J,She Y H.A topological characterization of consistency of logic theories in propositional logic[J].Mathematical Logic Quarterly,2006,52(5):470 – 477.

[10] 胡明娣,王国俊.经典逻辑度量空间中的反射变换[J].陕西师范大学学报:自然科学版,2009,37(6):1 – 4.
Hu M D,Wang G J.Reflexive transform in classical logic metric space[J].Journal of Shaanxi Normal University:Natural Science Edition,2009,37(6):1 – 4.(in Chinese)

[11] 温巧燕,钮心忻,杨义先.现代密码学中的布尔函数[M].北京:科学出版社,2000.1 – 31.
Wen Q Y,Niu X X,Yang Y X.Boolean Functions in Current Cryptology[M].Beijing:Science in China Press,2000.1 – 31.(in Chinese)

[12] R Engelking.General Topology[M].Berlin:Heldmann Verlag,1978.25.

[13] 冯登国,肖国镇.布尔函数的对偶性和线性点[J].通信学报,1996,17(1):46 – 50.
Feng D G,Xiao G Z.Duality and linear points of Boolean functions[J].Journal of Chins Institute of Communications,1996,17(1):46 – 50.(in Chinese)

[14] 郭锦辉,李世取.满足阶严格雪崩准则的多值函数的谱特征[J].中国工程科学,2005,7(12):45 – 48.
Guo J H,Li S Q.The strict avalanche criterion of order k spectral properties of m-valued logical functions[J].Engineering Science,2005,7(12):45 – 48.(in Chinese)

作者简介:

胡明娣　女,1972 年生于陕西安康.陕西师范大学数学与信息科学学院博士生,副教授.研究方向为不确定推理、计算智能.
E-mail:humingdiwww@163.com

王国俊　男,1935 年生于北京.陕西师范大学教授,博士生导师.研究方向为不确定推理、计算智能.　E-mail:gjwang@snnu.edu.cn