布尔函数最优连续化

洪 洁[1]，范修斌[2]，方 刚[2]，路晓峰[2]

(1. 成都电子机械高等专科学校 成都 610031; 2. 中国科学院数学与系统科学研究院 北京 100080)

【摘要】针对求取SP网络结构中布尔函数最优连续化在一定情况下是一个组合优化的问题。通过概率论和运筹学相结合的方法，将布尔函数连续化的问题转化为连续函数的线性和非线性规则问题，得到了布尔函数最优连续化函数的存在性和唯一性的证明。

关 键 词 布尔函数; 互信息; 存在性; 唯一性

中图分类号 O224 文献标识码 A

Continuous Optimization of Boolean Functions

Hong Jie[1]，Fan Xiubin[2]，Fang Gang[2]，Lu Xiaofeng[2]

(1. Chengdu Electronmachanical college Chengdu 610031;

2. Academy of Mathematics and system Sciencel Chinese Academy of sciences Beijing 100080)

Abstract To seek for Boolean continuous optimization function in the sp netwoork strueture, in certauin cases, is a combinational optimal problem. Using the method integrating probability theory with operationed research and analysis, the problem is tansformed into the solution of linear and nonlinear programming of continuous functions. As result, the proof of existemce and uniqueness of Booleoon continuous optimizetion funetion is proposed in this paper.

Key words Boolean functions; inter-information; existence; uniqueness

在离散密码学函数连续化的基础上，文献[1]给出了若干利用极大似然估计方法分析密码问题的结论,而利用极大似然估计方法求取布尔函数的过程是非线性函数的全局极大值的求解过程。众所周知DES、AES等密码算法大都采用SP网络迭代技术，感兴趣的读者可参阅文献[2, 3]中给出的Fly算法也采用SP网络迭代技术，并对SP网络迭代技术给出了一定的密码学分析。而若利用文献[1]中给出的极大似然估计方法对SP网络迭代技术进行相关的密码学分析，必须对SP网络迭代技术中所使用的布尔函数进行连续化处理。

一般来说，同一个布尔函数存在多个不同的连续化函数，而不同形式的连续化函数在将组合优化问题转化为非线性连续最优化问题时对信息提取能力、对非线性规划问题的求解性质有很大的影响。故此时对布尔函数的连续化方法提出了要求，需要信息提取能力强的布尔函数的连续化方法。

1 布尔函数最优连续化的提出

定义 1 设 F 是一定义域为 $[0,1]^n$，值域为 $[0,1]$ 上的 n 元连续函数，f 是一 n 元布尔函数，若 F 的定义域由 $[0,1]^n$ 限制在 $\{0,1\}^n$，值域由 $[0,1]$ 限制在 $\{0,1\}$ 时，即为 f 函数，则称 F 函数是布尔函数 f 的一个连续化函数。显然布尔函数存在多种连续化函数。

例1 对于布尔函数 $f(x,y)=x\oplus y$，有6个函数 $F_i(x,y),\ (i=1,2,\cdots,6)$ 为 f 的连续化函数：

收稿日期：2004 – 06 – 23
作者简介：洪 洁(1968 –)，女，在职硕士生，主要从事网络安全方面的研究.

1) $F_1(x,y)=x+y-2xy$；2) $F_2(x,y)=\frac{1}{2}-\frac{1}{2}|x+y-1|+\frac{1}{2}|x-y|$；3) $F_3(x,y)=(x-y)^2$；

4) $F_4(x,y)=|x-y|$；5) $F_5(x,y)=1-(x+y-1)^2$；6) $F_6(x,y)=1-|x+y-1|$。

直接验证可得知上述六种连续化函数，当定义域由 $[0,1]^n$ 限制在 $\{0,1\}^n$，值域由 $[0,1]$ 限制在 $\{0,1\}$ 时，都为布尔函数 $f(x,y)=x\oplus y$，因此满足定义1。

引理 1 设 F 和 G 都是布尔函数 f 的连续化函数，则对任意 $l\in[0,1]$，$\hat{F}=lF+(1-l)G$，也是 f 的连续化函数。

证明 因为 F 和 G 都是 n 元布尔函数 f 的连续化函数，所以根据定义1，$\forall a\in F_2^n$，则 $F(a)=G(a)=f(a)$。$\hat{F}(a)=lF(a)+(1-l)G(a)=(l+1-l)f(a)=f(a)$，故命题成立。

由引理得知同一个布尔函数的不同的连续化函数的凸组合仍然是一个连续化函数。在例1中 $F_1(x,y)=\frac{1}{2}F_3(x,y)+\frac{1}{2}F_5(x,y)$，$F_2(x,y)=\frac{1}{2}F_4(x,y)+\frac{1}{2}F_6(x,y)$，即 $F_1(x,y)$ 是 $F_3(x,y)$ 与 $F_5(x,y)$ 的凸组合；$F_2(x,y)$ 是 $F_4(x,y)$ 与 $F_6(x,y)$ 凸组合。从以上的分析得知，对任意的布尔函数，存在许多不同的连续化函数。哪个是密码学意义下最优的连续化函数？在SP网络多层迭代的连续化处理过程中，得到的中间结果应与层函数的输入变量分布律一致，才能具有优化的信息提取能力。为此，给出如下定义：

定义2 设 $F(x_1,x_2,\cdots,x_n)$ 是 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 的一连续化函数，若满足：$P(f(X_1,\cdots,X_n)=1)\equiv F(p_1,\cdots,p_n)$，其中，$p_i=P(X_i=1)$，并且 $X_1,\cdots,X_n$ 是相互独立的二元随机变量，则称 $F(x_1,x_2,\cdots,x_n)$ 是 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 密码学意义下的最优连续化函数。以信息论的观点分析定义2的合理性。

引理 2[4] 设 $X_1,X_2,\cdots,X_n$ 是取值于 F_2 且分布律分别为 $p_i=P(X_i=1),\ i=1,2,\cdots,n$ 的随机变量，并且 $X_1,\cdots,X_n$ 是相互独立，$f(x_1,x_2,\cdots,x_n)$ 为任一 n 元布尔函数，$Y\overset{\Delta}{=}f(X_1,X_2,\cdots,X_n)$ 是由 $X_1,X_2,\cdots,X_n$ 以及 $f(x_1,x_2,\cdots,x_n)$ 诱导出的二元随机变量，则 $X_1,X_2,\cdots,X_n$ 与 Y 的互信息为

$$I((X_1,X_2,\cdots,X_n);Y)=\sum_{(x_1x_2\cdots x_n)\in F_2^n}\sum_{y\in F_2}p(x_1x_2\cdots x_n,y)\log_2\frac{p(x_1x_2\cdots x_n,y)}{p(x_1x_2\cdots x_n)p(y)} \tag{1}$$

由引理2可以看出：当 $f(x_1,x_2,\cdots,x_n)$ 的连续化函数 $F(x_1,x_2,\cdots,x_n)$ 满足定义2时，即

$$\begin{cases}P(Y=1)=P(f(X_1,\cdots,X_n)=1)\equiv F(p_1,\cdots,p_n),\\ P(Y=0)=P(f(X_1,\cdots,X_n)=0)\equiv 1-F(p_1,\cdots,p_n)\end{cases} \tag{2}$$

式中 利用 $F(x_1,x_2,\cdots,x_n)$ 代替 $f(x_1,x_2,\cdots,x_n)$，满足 $X_1,X_2,\cdots,X_n$ 与 Y 的互信息量。故定义2中的连续化函数是信息论意义下最优的连续化函数。

2 布尔函数最优连续化函数的存在性与唯一性

定理 1 对于任一 n 元布尔函数 $f(x_1,\cdots,x_n)$ 其最优连续化函数是存在且唯一的 。

证明 由定义2，令 $P(f(X_1,\cdots,X_n)=1)=H(p_1,\cdots,p_n),\ \forall p_i\in[0,1],i=1,2,\cdots,n.$ 即 H 是关于 $p_i,i=1,2,\cdots,n$ 的 n 元实函数。又由于 $f(x_1,\cdots,x_n)$ 是布尔函数，故得知 H 是关于 $p_i,i=1,2,\cdots,n$ 的连续函数，从而存在性可证。

又设 $P(f(X_1,\cdots,X_n)=1)\equiv H_1(p_1,\cdots,p_n)$，由于 p_i 的任意性，故 $H=H_1$，唯一性得证。

例2 求 $f(x_1,x_2)=x_1\oplus x_2$ 的最优连续化函数。

$$P(f(X_1,X_2)=1)=P(X_1\oplus X_2=1)=P(X_1=1,X_2=0)+P(X_1=0,X_2=1)=$$
$$p_1(1-p_2)+(1-p_1)p=p_1+p_2-2p_1p_2$$

故 $F(x_1,x_2)=x_1+x_2-2x_1x_2$ 是 $f(x_1,x_2)=x_1\oplus x_2$ 的最优连续化函数。同时，例2也给出了一般布尔函数的最优连续化函数的求取方法。

(下转第626页)

量；$\boldsymbol{v}_m$，$\boldsymbol{V}_M$，$\boldsymbol{a}_m$，$\boldsymbol{a}_M$ 分别表示物体与地球相对惯性系的速度和加速度，则存在如下关系

$$m\boldsymbol{v}_m = M\boldsymbol{V}_M\text{，}\quad m\boldsymbol{a}_m = M\boldsymbol{a}_M\text{，}$$

即

$$\frac{\boldsymbol{v}_m}{\boldsymbol{V}_M} = \frac{M}{m}\text{，}\quad \frac{\boldsymbol{a}_m}{\boldsymbol{a}_M} = \frac{M}{m}\text{，}$$

对该问题，也可取与地球相连的参照系来讨论。由于地球相对于惯性系有加速度 $\boldsymbol{a}_M$，故地球参照系是一个平动加速的非惯性系(简称地球系)。在地球上观察，物体的动量为 $m(\boldsymbol{v}_m + \boldsymbol{V}_M) = (M+m)\boldsymbol{V}_M$ (因 $\frac{\boldsymbol{v}_m}{\boldsymbol{V}_M} = \frac{M}{m}$)，这也是物体地球系统的总动量。另一方面，对地球系，作用于物体地球系统的相互作用外力之和等于零，但此时须考虑系统所受的惯性力。作用在物体上的惯性力为 $m\boldsymbol{a}_M$，作用在地球上的惯性力为 $M\boldsymbol{a}_M$，这两力之和等于 $(M+m)\,\boldsymbol{a}_M$。根据式(7)，在地球参照系中可列出方程

$$\frac{\mathrm{d}}{\mathrm{d}t}[(M+m)\boldsymbol{V}_M] = (M+m)\boldsymbol{a}_M$$

上式表明：物体地球系统总动量的导数等于惯性力作用之和。在这里可看到，系统的动量变化是由于惯性力的作用获得的，惯性力起着与外力相同的作用效果。

参 考 文 献

[1] 郭士堃. 理论力学(上册)[M]. 北京：人民教育出版社，1982
[2] 王均能. 非惯性系力学概论[M]. 成都：电子科技大学出版社，1993

编 辑 刘文珍

(上接第622页)

3 结 束 语

本文之所以要讨论布尔函数的连续化问题，是因为在许多密码算法的设计中，随着SP网络迭代层数的增加，一般布尔函数的连续化函数，由于不是信息论意义之下最优的连续化函数，使得目标函数的信息衰减太大，又加之SP网络迭代的密码学意义之一就是使明码信息迅速扩散，故一般连续化函数构造的目标函数，其优化算法的求解能力相对较差，所以布尔函数的最优连续化的问题，已成为有待进一步讨论的问题之一。

本文部分研究结果得到了中国科学院数学与系统科学研究院章祥荪研究员、袁亚湘研究员、刘木兰研究员及刘德刚副研究员的指导与帮助，在此表示感谢。

参 考 文 献

[1] Andelmen D. Maximum likelihood estimation applied to cryptanalysisp[D]. A Dissertation Submitted to the Department of Electrical Engineering and the Committee on Graduate Studies of Stanford University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy . Stan ford, 1979.
[2] Daemen J, Vincent R J. The design of rijndael[M], New York: Springer-Verlag, 2002
[3] 吕述望, 范修斌, 周玉洁. 序列密码的设计与分析[M]. 北京：中软电子出版社，2003
[4] Thomas M. Cover, Joy A. Thomas, elements of information theory [M]. Chichester VSA: John Wiley & Sons, Inc., 1991
[5] Kullback S. Information theory and statistics [M]. New York: Wiley, 1959

编 辑 刘文珍