4 举 例

在增强了反动作参数限制以后,ROAM 演算仍然具有类似 MA 和 SA 的很强的表达能力.我们以灰箱演算中经典的防火墙跨越(firewall-crossing)例子以及对多元异步π-演算的翻译来说明以上事实.

4.1 防火墙跨越

在文献[1,5]中多次使用防火墙跨越的例子,来说明灰箱演算在安全性上的描述能力.一个授权的代理(agent)可以正确地穿越一个防火墙(firewall)到达其内部.该防火墙(一个灰箱)的名字对外部完全保密,为了让授权的代理正确进入防火墙,防火墙首先送出一个向导灰箱,由于授权代理拥有预先约定好的密钥 k,k'和 k'',因此可以由向导灰箱带领进入防火墙内部.在 ROAM 中,防火墙跨越的例子表示为

$$\text{Agent}::=k'[\overline{\text{in}}\ k.\text{open}\ k.(x{:}W_w).\text{in}\ x.\ \overline{\text{open}}\ |k''[\ \overline{\text{open}}\ |Q]], \tag{8}$$

$$\text{Firewall}::=(vw)w[k[\text{out}.in\ k'.\ \overline{\text{open}}\ .\langle w\rangle|\ \overline{\text{out}}\ k.\ \overline{\text{in}}\ k'.\text{open}\ k'.\text{open}\ k''.P]. \tag{9}$$

在式(8)、式(9)中,进程 P 和 Q 可以是任意的.假设其类型分别为$\Gamma\vdash P{:}S_p\alpha_p\beta_p$,$\Gamma\vdash Q{:}S_q\alpha_q\beta_q$,则灰箱 w,k,k',k''以及 W_w 可分别赋予以下类型:

$$\Gamma\vdash w:Amb\ [S_p]\uparrow n \qquad \Gamma\vdash k:Amb[S_p]\uparrow 1 \qquad \Gamma\vdash k':Amb\ [S_p]\uparrow n$$

$$\Gamma\vdash k'':Amb\ [S_q]\alpha_q\beta_q \qquad W_w=Amb\ [S_p]\uparrow n$$

只要保证密钥 k,k',k''的保密性,授权代理利用密钥可顺利进入防火墙内部,并让其内部的进程 Q 在防火墙内部运行,我们可以得到以下结论:

$$(vk\ k'\ k'')(\text{Agent}\mid\text{Firewall})\approx(vw)w[P\mid Q].$$

这里关系"≈"是一种同余关系(congruence)(由于篇幅关系,在文中并未引入).无论将两个同余的进程放入什么上下文中,所得到的结果都表现出完全相同的外部特性.在 SA 中,防火墙跨越前后的同余性必须通过禁止上下文中存在某类动作来达到[6].ROAM 的鲁棒性表现在对任何存在恶意干扰的上下文,该同余性都成立.

4.2 翻译多元异步π-演算

对多元异步π-演算(polyadic asynchronous π-calculus)的翻译通常可以体现一套演算系统的表达能力.在多元异步π-演算中,通道(channel)n^π 的类型为 $Ch[W_1^\pi,\ldots,W_k^\pi]$,表示该通道所传递元组中第 i 个元素的类型为 W_i^π.类型判定使用 $\Gamma^\pi\vdash P^\pi$ 的形式,其中Γ^π为类型环境,P^π 为符合正确类型规则的π-进程.ROAM 演算对多元异步π-演算的一种翻译方案如下:

$$[[0^\pi]]::=0 \qquad [[P^\pi\mid Q^\pi]]::=[[P^\pi]]\mid[[Q^\pi]] \qquad [[!P^\pi]]::=![[P^\pi]] \qquad [[\Gamma^\pi\vdash P^\pi]]::=[[\Gamma^\pi]]\vdash[[P^\pi]]:Shh\uparrow n$$

$$[[\phi,\ n_1^\pi{:}W_1^\pi,\ldots,n_k^\pi{:}W_k^\pi]]::=\phi,\ n_1{:}[[W_1^\pi]],\ldots,n_k{:}[[W_k^\pi]]$$

$$[[Ch[W_1^\pi,\ldots,W_k^\pi]]]::=Amb[[[[W_1^\pi]]\times\ldots\times[[W_k^\pi]]]\uparrow n$$

$$[[(v^\pi n^\pi{:}Ch[W_1^\pi,\ldots,W_k^\pi])P^\pi]]::=(vn{:}[[Ch[W_1^\pi,\ldots,W_k^\pi]]])\ (n[!(\overline{in}\ n.\text{open}\ n)]\mid[[P^\pi]])$$

$$[[n^\pi\ (n_1^\pi{:}W_1^\pi,\ldots,n_k^\pi{:}W_k^\pi).P^\pi]]::=(vp{:}Amb[Shh]\uparrow n)(\text{open}\ p\mid n[in\ n.\ \overline{\text{open}}\ .(n_1{:}[[W_1^\pi]],\ldots,n_k{:}[[W_k^\pi]])$$
$$(p[\text{out}.\ \overline{\text{open}}\ .\ [[P^\pi]]\ ]\mid\overline{\text{out}}\ p)])$$

$$[[n^\pi\langle n_1^\pi,\ldots,n_k^\pi\rangle]]::=n[in\ n.\ \overline{\text{open}}\ .\langle n_1,\ldots,n_k\rangle]$$

这里,一个π-通道 n^π 表示为一个同名灰箱 n.该灰箱中的进程$!(\overline{in}\ n.\text{open}\ n)$不断地让试图在该通道上进行通信的灰箱进入,并将它们打开.在 n^π 上进行输入和输出操作被翻译为若干进入 n 并被打开的灰箱.输入和输出灰箱被相继打开以后,消息传递便在 n 中进行.消息传递完毕,得到输入的进程跳出 n 并继续运行.这样,在 n^π上进行元组通信被转化为在灰箱 n 中进行多元消息传递.

以上翻译方案对一个π-通道名只使用了一个灰箱名,既表示该π-通道,又代表进入该通道进行消息交换的输入输出灰箱.当然,可以分别再使用两个不同的灰箱名分别表示输入和输出灰箱,这样,每个灰箱的类型还可以定义得更加具体,如表示通道的灰箱还可更加明确.但是,上述简单方案足以说明 ROAM 的表达能力问题.

5 结论和进一步的工作

本文基于 MA 和 SA 的工作,提出了鲁棒灰箱演算系统——ROAM,进一步改进了 SA 中对 MA 强干扰的控制,克服了 SA 中存在的安全隐患.通过对防火墙跨越和多元异步π-演算的描述,表明 ROAM 与 MA 和 SA 类似,具有很强的描述能力.同时,本文提出了一套可以描述进程和能力的移动性和线程数两个属性的类型系统,并证明了该类型系统的归约一致性.针对 ROAM 的进一步工作有子类型系统的建立和证明、单线程进程的性质研究等.

References:

[1] Cardelli, L., Gordon, A.D. Mobile ambients. Lecture Notes in Computer Science, 1998,1378:140～155.

[2] Cardelli, L., Gordon A.D. Types for mobile ambients. In: ACM, ed. Proceedings of the POPL' 99, New York: ACM Press, 1999. 79～92.

[3] Cardelli, L., Ghelli, G., Gordon, A.D. Mobility types for mobile ambients. Lecture Notes in Computer Science, 1999,1644:230～239.

[4] Cardelli, L., Ghelli, G., Gordon, A.D. Ambient groups and mobility types. Lecture Notes in Computer Science, 2000,1872:333～347.

[5] Gordon, A.D., Cardelli, L. Equational properties of mobile ambients. Lecture Notes in Computer Science, 1999.1578:212～226.

[6] Levi, F., Sangiorgi, D. Controlling interference in ambients. In: Thomas, R., ed. Proceedings of the POPL 2000. New York:ACM Press, 2000. 352～364.

[7] Milner, R., Parrow, J.G., Walker, D.J. A calculus of mobile process. Information and Computation, 1992,100(1):1～77.

Further Control on the Grave Interference in Mobile Ambient[i]

GUAN Xu-dong, YANG Yi-ling, YOU Jin-yuan

(*Distributed Computing Technology Center*, *Department of Compuer Science and Engineering*, *Shanghai Jiaotong University*, *Shanghai* 200030, *China*)

E-mail: guan-xd@cs.sjtu.edu.cn; yang-yl@cs.sjtu.edu.cn; you-jy@cs.sjtu.edu.cn.ac.cn

http://dctc.sjtu.edu.cn

Abstract: In order to control the grave interference in mobile ambient (MA), Levi *et al.* proposed mobile safe ambients (SA). However, the coactions introduced in SA brought new security breaches. In this paper, robust ambients (ROAM) is proposed to eliminate those security breaches. In ROAM, coactions are still utilized to control the grave interference. In addition, the parameter of every coaction is explicitly specified to name the consumer of that coaction. This mechanism effectively eliminates the security breaches in SA. The firewall crossing example and the encoding of polyadic asynchronous π-calculus in ROAM show that ROAM still keeps the strong expressiveness of its ancestors. A fundamental type system for ROAM with both thread count and mobility attributes is also proposed and proved. The result in this paper shows that ROAM is a good candidate in the formalization of mobile computation.

Key words: process algebra; mobile ambient; mobile safe ambient; robust ambient; type

---

[i] Received June 9, 2000; accepted March 5, 2001
Supported by the Science and Technology Development Foundation of Shanghai of China under Grant No.995115014

基于支持向量机分类的回归方法*

陶 卿[1,2], 曹进德[3], 孙德敏[4]

[1](中国科学院 自动化研究所,北京 100080);
[2](中国人民解放军炮兵学院 一系,安徽 合肥 230031);
[3](东南大学 应用数学系,江苏 南京 210096);
[4](中国科学技术大学 自动化系,安徽 合肥 230027)

E-mail: q_tao@sohu.com; qing.tao@mail.ia.ac.cn

http://www.ia.ac.cn

摘要: 支持向量机(support vector machine,简称 SVM)是一种基于结构风险最小化原理的分类技术,也是一种新的具有很好泛化性能的回归方法.提出了一种将回归问题转化为分类问题的新思想.这种方法具有一定的理论依据,与 SVM 回归算法相比,其优化问题几何意义清楚明确.

关 键 词: 回归;分类;支持向量;最大边缘

中图法分类号: TP18 **文献标识码**: A

统计学习理论起源于 20 世纪 60 年代晚期[1,2],但在 1990 年以前,它仅仅是进行函数估计的理论分析工具.到了 90 年代中期,人们提出了理论严谨的结构风险最小化原理,并在此基础上创造性地产生出了一种新的机器学习算法——SVM(support vector machines)[3~5],SVM 的近期发展及成功应用使得统计学习理论已成为研究估计高维函数算法的理论和实用工具.

SVM 学习算法现已成为训练多层感知器、多项式和 RBF 神经网络的替代性方法[6].对线性可分(二分类)情形,SVM 算法最后归结为一个二次规划问题,这个规划问题具有一定的代表性和理论体系统一性.首先对线性不可分问题,只要对规划问题线性可分情形下的约束条件适当松弛,就可得到不可分情形下的线性分类器,这正是软边缘算法[5];而对非线性分类器的设计问题,可通过输入空间到特征空间的非线性映射将其转化为线性可分情形加以解决,而决定非线性分类器的优化问题正是线性可分情形时的适当变形,即将输入空间的欧氏内积变为核函数[6~8].基于结构风险最小化原理的思想同样被成功地应用于函数回归,出现了理论依据更好的回归方法[7].

从神经网络系统理论的发展来看[9],线性可分问题是最基本的,Rosenblatt 感知器(peceptron)的分类算法为三层前馈神经网络能以任意精度逼近 L^2 中的任意函数奠定了理论基础,而这种逼近能力正是前馈网络被广泛应用于建模预测和多种控制问题的理论依据.我们打算遵照前馈神经网络的理论体系对 SVM 进行研究.受 SVM 算法是最大边缘算法的启发,文献[10]对线性可分情形提出一种基于闭凸集间的距离优化的算法,而将线性不可分的情形,通过一种闭凸包收缩的方法,将其归结为线性可分情形.文献[10]的优化问题集可分性判断和解分类超平面于一体,其中支持向量的几何意义非常清晰.

分类问题的样本点明确地属于某一类,而回归问题样本点属于的类别事先是不知道的,这正是分类问题与

* 收稿日期: 2000-09-15; 修改日期: 2001-04-17

基金项目: 国家自然科学基金资助项目(60175023);中国博士后科学基金资助项目(5030436);安徽省自然科学基金资助项目(01042304);安徽省优秀青年基金资助项目

作者简介: 陶卿(1965－),男,安徽长丰人,博士,副教授,主要研究领域为神经网络,支持向量机;曹进德(1963－),男,安徽和县人,博士,教授,主要研究领域为应用数学,神经网络;孙德敏(1939－),男,辽宁新民人,教授,博士生导师,主要研究领域为模式识别与智能系统,控制理论及其应用.

回归问题的区别所在.本文通过对样本点集的适当变换,提出一种将回归问题转化为二分类问题的新思想,从而可用文献[10]的方法求解,一方面这与前馈神经网络的理论体系相一致,另一方面也使得回归问题中支持向量的几何意义更明显,为分类问题的研究成果应用于回归问题奠定了理论基础.

1 SVM 回归方法

本节将简介基于结构风险最小化原理的 Support Vector 回归方法[7,11].

考虑下列线性回归问题:

$$(y_1, x_1),...,(y_l, x_l),\ x_i \in R^n,\ y_i \in R,\ i = 1,2,...,l,$$

求回归线性函数

$$f(x) = \langle w, x \rangle + b,$$

其中 $w \in R^n$, $b \in R$.

基于 Support Vector 的最优回归函数是指满足结构风险最小化原理,即极小化

$$\Phi(w) = \frac{1}{2}\|w\|^2 + C \cdot R_{emp}[f], \tag{1}$$

其中 C 是预先指定的常数, $R_{emp}[f]$ 是经验风险.

对于 $R_{emp}[f]$,可以采用不同的代价函数来描述,如二次函数、Huber 函数和 e -insensitive 函数,其中 Vapnik 提出的 e -insensitive 函数具有很好的性质[7].当回归测度函数为 e -insensitive 代价函数:

$$|x|_e = \begin{cases} 0 & \text{if } |x|_e \le e \\ |x| - e & \text{otherwise} \end{cases}$$

时,式(1)可表示为

$$\Phi(w) = \frac{1}{2}\|w\|^2 + \frac{1}{l}\sum_{i=1}^{l}|y_i - f(x_i)|_e. \tag{2}$$

特别地,当 $|y_i - \langle w, x_i \rangle - b| \le e$, $i = 1,2,...,l$ 满足时,式(2)显然等价于

$$\min \frac{1}{2}\|w\|^2, \tag{3}$$

$$\text{subject to } \begin{cases} y_i - \langle w, x_i \rangle - b \le e \\ \langle w, x_i \rangle + b - y_i \le e \end{cases}.$$

当优化问题式(2)的约束条件不满足时,它显然是无解的.为了克服这一缺陷,用类似于 Cortes 的松弛方法[5]来处理式(3),此时式(2)变为

$$\min \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{l}(x_i + x_i^*), \tag{4}$$

$$\text{subject to } \begin{cases} y_i - \langle w, x_i \rangle - b \le e + x_i \\ \langle w, x_i \rangle + b - y_i \le e + x_i^* \\ x_i, x_i^* \ge 0 \end{cases}.$$

松弛回归方法的几何意义如图 1 所示.对优化问题式(4),通过采用数学规划中的对偶方法,可得到最优回归线性函数的 w 和支持向量[7,11].

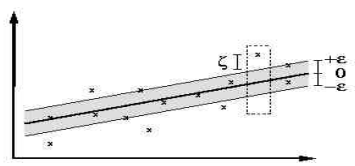

Fig.1 The relaxation method for regression

图 1 松弛回归方法

2 基于分类的回归方法

本节首先将回归问题转化为线性可分情形下的分类问题,进而用文献[10]的方法加以解决.

受图 1 的启发,选取 $e>0$,第 1 节中的回归问题显然可以转化为 $Q_1=\{(x_i,y_i+e),i=1,...,l\}$ 和 $Q_2=\{(x_i,y_i-e),i=1,...,l\}$ 的线性分类问题.下面来分析这种转化的合理性.

首先,当选取的 e 充分大时,Q_1 和 Q_2 总是线性可分的;其次,当 Q_1 和 Q_2 线性可分时,根据线性可分情形下的 SVM 理论[3,6,7],Q_1 和 Q_2 的最大边缘分类超平面 $\langle\hat{w},z\rangle+\hat{b}=0$ 中的 $\hat{w}=(\hat{w}_1,\hat{w}_2)$ 由下列优化问题决定:

$$\min \frac{1}{2}\|\hat{w}\|^2, \tag{5}$$

$$\text{subject to } \begin{cases}\langle\hat{w},z_i\rangle+\hat{b} & >0 \quad z_i\in Q_1\\ \langle\hat{w},z_i\rangle+\hat{b} & <0 \quad z_i\in Q_2\end{cases}.$$

按照超平面的函数表示习惯,令 $\hat{w}_2=-1$.此时,优化问题式(5)和优化问题式(3)等价,这种等价性表明,当 $|y_i-\langle w,x_i\rangle-b|\le e$, $i=1,2,...,l$ 满足时,回归问题和转化后分类问题的解是一致的.

根据以上的分析和文献[10],可用闭凸集间距的方法来求解第 1 节中的回归问题:

$$\begin{cases}\min\|l_1p_1+l_2p_2+...+l_lp_l-b_1q_1-b_2q_2-...-b_lq_l\|^2\\ l_1+l_2+...+l_l=1,\ b_1+b_2+...+b_l=1\\ l_i\ge 0,b_j\ge 0,i=1,2,...,l\end{cases}, \tag{6}$$

其中 $p_i=(x_i,y_i+e)$, $q_i=(x_i,y_i-e)$, $i=1,2,...,l$.与优化问题式(5)相比,式(6)总是有解的,从解的结果还可以判断 Q_1 和 Q_2 的线性可分性.设 $l_1^*,l_2^*,...,l_l^*,\ b_1^*,b_2^*,...,b_l^*$ 是式(6)的一组解,则 Q_1 和 Q_2 的最大边缘线性分类器为过 $l_1^*p_1+l_2^*p_2+...+l_l^*p_l$ 和 $b_1^*q_1+b_2^*q_2+...+b_l^*q_l$ 连线中点且与这条连线垂直的超平面,可用点法式求得其方程.对应于 $l_1^*,l_2^*,...,l_n^*,\ b_1^*,b_2^*,...,b_m^*$ 中非零数的向量称为相应回归问题的支持向量.

最后,我们讨论一下 e 的选取问题.首先 e 不能选取得过大,尽管选取充分大的 e 可保证 Q_1 和 Q_2 的线性可分,但它同时导致 Q_1 和 Q_2 的范围过大,从而使分类集合 VC 维的上界增大[3,6,7],与结构风险最小化原理相矛盾.如果规划问题式(6)目标函数的最优值为 0,表明 Q_1 和 Q_2 线性不可分,这说明 e 选取得过小,这时可用文献[10]中闭凸集收缩的方法来解决.

3 方法应用举例

例 1:考虑下列线性回归问题[7].

x	y
1.0	−1.6
3.0	−1.8
4.0	−1.0
5.6	1.2
7.8	2.2
10.2	6.8
11.0	10.0
11.5	10.0
12.9	10.0

取 $e=5$,得 $l_5=1$,其余 $l_i=0$, $b_1=0.0276$, $b_7=0.9724$,其余 $b_i=0$. $w=(2.9237,-2.5205)$, $b=-12.1083$.分类结果如图 2 和图 3 所示.