

进化神经网络在信用卡欺诈检测中的应用

凌晨添

(北京大学 计算语言所, 北京 100871)

摘 要: 自动信用卡欺诈检测是一个重要且有潜力的领域. 基于人工神经网络的欺诈检测系统虽能令人满意, 但具有良好结构的神经网络是很难构造的. 由此提出一种进化方法来自适应地生成用于欺诈检测的神经网络结构. 实验结果表明, 该进化神经网络可以有效地完成信用卡欺诈检测.

关键词: 欺诈检测; 神经网络设计; 进化编程

中图分类号: TP18

文献标识码: A

文章编号: 1000-7180(2011)10-0014-04

Evolutionary Neural Network for Credit Card Fraud Detection

LING Chen-tian

(Institute of Computational Linguistics, Peking University, Beijing 100871, China)

Abstract: Research on automatic credit card fraud detection is a significant and promising area. Generally, using artificial neural networks to construct fraud detectors can achieve satisfactory performance. However, it is difficult to design an appropriate architecture for a neural network. In this paper, we propose an evolutionary method to automatically generate the architecture for a neural fraud detector. Experimental results show that the evolutionary neural networks can efficiently perform credit card detection.

Key words: fraud detection; neural network design; evolutionary programming

1 引言

信用卡已经成为一种方便快捷的支付方式, 它不仅可以用于日常购物, 还有用于网上购物. 然而, 信用卡欺骗对信用卡发行者和持有者都造成了极大的经济损失. 因此, 高效的欺诈检测对信用卡持有人的利益和银行的收入保护具有重要意义. 我们可以基于人工神经网络来构造一个信用卡欺诈检测系统, 人工神经网络由一些类似人脑信息处理单元——神经元的单元结点进行驱动, 整个网络系统可以被看作是一个无参数分类器的黑盒, 可以应用于各种模式识别场景.

2 基于进化方法的全连通前馈网络优化

2.1 全连通前馈网络

全连通前馈网络有一个或多个隐含层. 图 1 显

示了一个全连通前馈网络的结构.

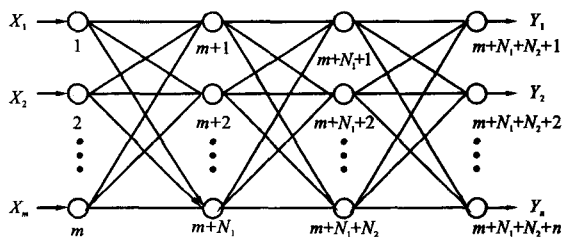


图 1 含有两个隐含层的全连通前馈网络

该网络由四层组成: 输入层、两个隐含层和输出层. 向量 $X = \{X_1, X_2, \dots, X_M\}$ 是网络的输入, 向量 $Y = \{Y_1, Y_2, \dots, Y_M\}$ 是网络的输出. 两个隐含层分别有 N_1 和 N_2 个神经元. 神经元 i 到神经元 j 的连接表示 i 以 j 的输出作为其输入. 我们把所有隐含神经元的总数记为 N , 把神经元 i 的输出记为 O_i , 那么整个网络的转换如下:

$$O_i = X_i, 1 \leq i \leq m;$$

$$O_i = f\left(\sum_{j=1}^m w_{ji} \cdot O_j\right), m+1 \leq i \leq m+N_1;$$

$$O_i = f\left(\sum_{j=m+1}^{m+N_1} w_{ji} \cdot O_j\right), m+N_1+1 \leq i \leq m+N_1+N_2;$$

$$O_i = f\left(\sum_{j=m+N_1+1}^{m+N} w_{ji} \cdot O_j\right), m+N+1 \leq i \leq m+N+n.$$

式中, w_{ji} 表示神经元 j 到神经元 i 的连接权重. f 是神经元转换函数. 我们以正切函数作为网络中所有神经元的转换函数.

训练过程需要一个样本集合. 在信用卡欺诈检测问题中, 样本集合就是过去的交易数据. 对于训练样本集中的数据, 我们已知每一笔交易是正常交易还是欺诈交易. 在训练过程中, 网络的权重被反复调整以最小化实际输出和期望输出的差距. 反向传播算法是最流行的训练算法, 是一种梯度下降算法.

由于隐含结点的非线性转换函数使得网络能够学习输入向量和输出向量之间的非线性或线性关系, 全连通神经网络能够应用于各种模式识别问题. 然而, 网络层数和每层结点数必须被正确的指定. 过多的神经元可能会导致一个过于复杂的系统. 在这种情况下, 训练网络需要大量的训练样本. 另一方面, 过于简单的网络可能没有足够的能力来解决检测问题.

2.2 编码方案和遗传操作

网络结构和连接权值的编码是同时进行的. 在本文设计的进化方法中没有交叉操作, 因此可以用实数进行编码. 由于网络是全连通的, 我们只对隐含层的数量以及每层的结点数进行编码. 记 N_i 为第 i 层的隐含结点数, 则可以用 $N_i \times N_j$ 的矩阵对第 i 层到第 j 层的连接权重进行编码.

图2中表示了本文设计的进化方法中的两种遗传算子, 分别是删除结点操作和增加结点操作. 在删除结点操作中, 结点 D 被删除, 从 A 到 D 的连接和从 B 到 D 的连接也被同时删除, 但其他连接的权重保持不变. 增加结点时, 在原有的网络中随机选择一个结点, 假设为 D . 然后该结点被分裂为两个新的结

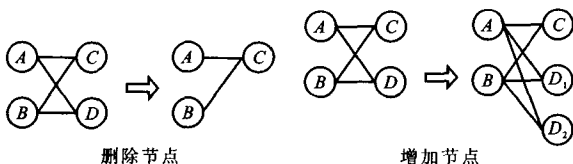


图2 两种遗传算子

点 D_1 和 D_2 . 分裂一个现有结点比随机增加一个结点的好处是前者可以保持原有的父结点和子结点之间的连接特征. 与 D_1 和 D_2 关联的边的权重计算采用了 Odri 等在文献[1]中提出的方法. 假设我们把结点 i 分裂为结点 i_1 和 i_2 , 那么权重更新过程如下 (其中 ∂ 是突变参数, 可以采取固定或随机值):

$$w_{ji_1} = w_{ji_2} = w_{ji}, i > j$$

$$w_{i_1 k} = (1 + \partial)w_{ik}, i < k$$

$$w_{i_2 k} = -\partial w_{ik}, i < k$$

2.3 适应度评价规则和选择机制

在本文设计的用于优化神经网络的进化方法中, 使用均方差 (Mean Squared Error) 的倒数来评价每个个体, 即每个神经网络结构的适应度:

$$\text{fitness} = \frac{1}{\text{MSE}} = \frac{1}{\frac{1}{Q} \sum_{k=1}^Q \sum_{i=1}^n (Y_i(k) - T_i(k))} \quad (1)$$

式中, Q 是训练样本数, n 是输出层结点数. $Y_i(k)$ 和 $T_i(k)$ 分别是第 k 个训练样本在第 i 个输出结点上的实际输出和期望输出.

另外, 进化方法的选择机制基于上述的适应度评价. 首先, 根据式(1) 计算每个个体的适应度, 然后根据适应度从高到低的顺序对 M 个个体进行排序.

3 进化方法的主要步骤

如流程图所示, 进化方法的主要步骤如图3所示.

3.1 步骤1—初始化

首先, 初始化种群数量 M , 最大进化代数 $G_{\max}$, 最大隐含层数量 $Nl_{\max}$, 每层最大结点数 $Nn_{\max}$. 然后在1和最大值之间生成一个均匀分布的随机数, 来初始化隐含层数量, 每层结点数. 同时, 连接权重也被初始化为在较小范围内均匀分布的随机数. 为了计算每一迭代中所有个体的适应值, 使用自适应学习率的反向传播算法来训练每个网络. 最后, 根据式(1) 来计算个体的适应值.

3.2 步骤2—终止判断

如果达到最大代数 $G_{\max}$, 就终止进化过程, 种群中适应度最优的网络即为进化过程的最终输出, 否则继续.

3.3 步骤3—选择

根据每个个体的适应度排序, 基于排序结果按概率选择一个个体进行以下两步突变操作.

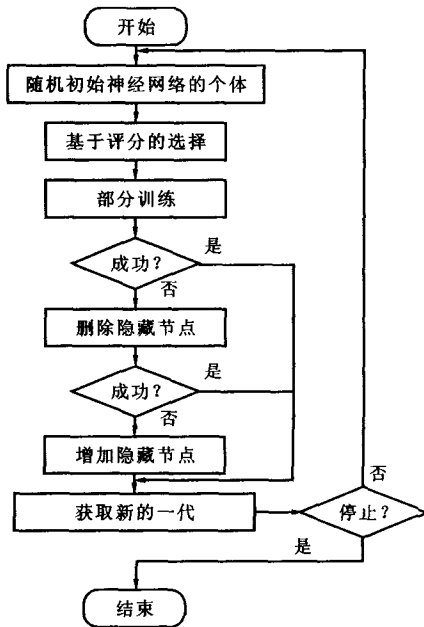


图3 算法流程图

3.4 步骤4—删除结点

随机生成一个介于1和用户指定的最大数量之间的数值 N_d . 如 Yao 在文献[2]中所述, N_d 的最大值通常很小, 大多数情况下都不超过3. 然后在步骤3中选择出来的个体中随机删除 N_d 个结点. 用反向传播算法训练删除结点后的网络. 如果训练后该网络的适应度比目前种群中适应度最差值好, 则用该网络替换目前适应度最差的个体, 并执行步骤2, 否则进入步骤5.

3.5 步骤5—增加结点

用步骤4中描述的方法生成一个数字 N_a , 并对步骤3中选择出来的个体进行增加结点操作, 随机选择并分裂 N_a 个结点来生成一个更大的网络. 然后用反向传播算法来训练增加结点后的网络, 并直接替换目前种族中适应度最差的个体, 最后返回步骤2.

4 实验

4.1 数据集

本文采用了一个基于计算机入侵的正常数据和异常数据混合的数据集. Barse 等^[3] 讨论了欺诈检测系统和入侵检测系统的共性和区别.

在该数据集中, 每笔交易均有41个属性, 包含了两种异常行为. 首先, 随机选择10 014个样本, 其中两种异常行为分别有129个和214个样本, 然后从中选择1 995个独立样本作为训练集. 训练集中的每笔交易都被标记为正常交易或异常交易. 训练集用于构建基于进化神经网络的欺诈检测系统. 最

后, 我们用训练集以外的样本, 即未标记的样本来评估进化神经网络的性能.

4.2 单层全连通前馈网络的实验结果

我们首先把神经网络的结构限制为单层全连通前馈网络. 有了这个限制, 可以清楚地观察到进化方法如何根据特定的检测问题找到一个最优网络结构.

在本实验中, 种群数量 M 为20, 每层的隐藏结点数最大值 $N_{\max}$ 为100. 为了观察到进化过程的收敛, 最大进化代数设置为400代.

如图4所示, 经过一定代数的进化, 算法收敛到类似的最优网络结构. 如文献[2]所述, 我们可以利用种群中每个个体携带的信息来选择一个更好的网络. 经过进化, 种群中所有个体可能有着近似的适应度, 但可能有差完全不同的网络结构. 在本例中, 一些网络已经对数据过度拟合. 所以我们另外选择了一个验证集来评价网络的性能, 并选择一个最好的作为最终输出^[4].

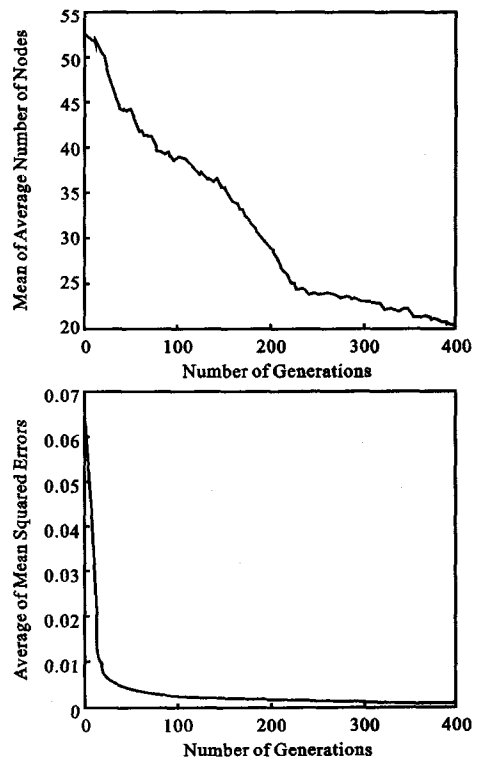


图4 在更大的搜索空间中, 单层全连通前馈网络的结构和准确度

使用这种方法, 我们构造一个三层前馈网络, 并在10 014个样例交易上进行测试^[5-6].

测试结果如表1所示. 定义检测正确率为系统判断为异常, 实际上也是异常交易的数量除以实际异常交易总数, 定义误报率为系统判断为异常, 但实际上是正常交易的数量除以实际异常交易总数. 检

测系统的目的是最大化正确率的同时减少误报率. 在本实验中,正确率为 96.2%,误报率为 2.9%.

表 1 最优单层前馈全连通网络的测试结果

		实际类型		
		正常	欺诈 A	欺诈 B
输出	正常	9 661	12	1
	欺诈 A	8	117	0
	欺诈 B	2	0	213

4.3 双层全连通前馈网络的实验

一般来说,多层前馈网络比单层前馈网络效果好. 进化方法也可以优化多层前馈网络的结构.

图 5 展示了双层前馈网络的进化过程,其中所有的网络都是全连通的. 在本实验中,种族数量 M 为 20,最大代数 G_{max} 为 400. 实验独立运行了 15 次. 显然在进化过程中,隐藏层结点数量和连接数量有着相似的特征.

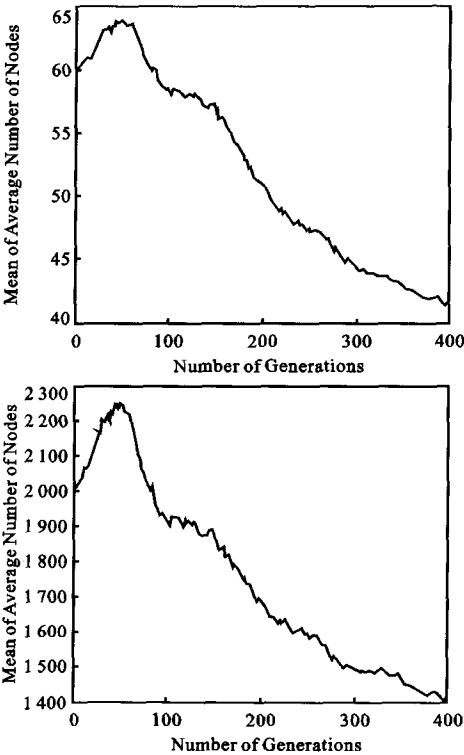


图 5 双层前馈网络的结构和准确度

我们在最终的种族中选择了最佳的个体,并在

测试集上进行测试,结果如表 2 所示. 正确率为 97.4%,误报率为 2.9%.

表 2 最优双层前馈全连通网络的测试结果

		实际类型		
		正常	欺诈 A	欺诈 B
输出	正常	9 661	9	1
	欺诈 A	8	120	0
	欺诈 B	2	0	214

5 结束语

近年来,信用卡欺诈越来越猖獗. 为了保障发卡机构和持有人的利益,本文提出了一种基于进化神经网络的信用卡欺诈检测技术,并展示了在特定的欺诈检测问题中,神经网络结构是如何通过进化算法得到自动化的优化选择. 然而,网络结构的进化过程需要较长的计算时间,因此如何通过更好的编码策略以及基因操作来优化进化效率需要进一步的研究.

参考文献:

[1] Odri S V, Petrovacki D P, Krstonosic G A. Evolutional development of a multilevel neural network[J]. Neural Networks, 1993,6(4):583-595.

[2] Yao X, Liu Y. A new evolutionary system for evolving artificial neural networks[J]. IEEE. Tran. Neural Networks, 1997(8):694-713.

[3] Barse E L, Kvarnstrom H, Jonsson E. Combining fraud and intrusion detection—meeting new requirements[C]// Proc. Nordic Workshop. Secure IT systems. Ireland: Cork, 2000.

[4] Barse E L, Kvarnstrom H, Jonsson E. A synthetic fraud data generation methodology[C]// Lecture Notes in Computer Science, ICICS 2002, Laboratories for Information Technology, Singapore, Springer Verlag, 2002.

[5] Margare H Dunham. Data mining introductory and advanced topics[M]. Boston: Prentice Hall, 2003.

[6] Yao X. A review of evolutionary artificial neural networks[J]. Int. J. Intell. Syst., 1993,8(4):539-567.

作者简介:

凌晨添 男,(1987—),硕士. 研究方向为信息检索与处理、机器学习.

(上接第 13 页)

[9] 李凡长,郑家亮. 基于 DFS 的专家数据库系统设计[J]. 计算机工程, 2001,27(3): 96-99.

[10] 刘芳,李凡长. DF 关系及其在数据聚类中的应用研究 [J]. 计算机工程与应用,2009,45(26): 138-146.

作者简介:

刘 芳 女,(1965—),硕士,副教授. 研究方向为数据库技术、动态模糊系统、智能软件.