空间几何对象相对位置的新安全判定方法

赵 玉,易 磊
(安徽大学 计算机科学与技术学院,安徽 合肥 230039)

摘 要:针对空间几何对象相对位置判定问题提出一种新的解决方案,也就是运用矩阵秩的概念和一般矩阵求和的安全两方计算协议秘密判定空间几何对象相对位置问题。关于此问题,之前罗永龙教授设计了对应成比例判定协议,而文中则利用矩阵秩的概念和一般矩阵求和的安全两方计算协议设计了一些基础的空间几何对象相对位置安全判定协议。运用此协议解决了空间中的平面与平面位置关系问题、平面与直线位置关系问题和直线与直线位置关系问题。提出的新安全判定方法不久解决了空间几何对象相对位置判定问题,也将在其他安全多方计算问题中起到重要作用。

关键词:矩阵秩的概念;一般矩阵求和的安全两方计算协议;安全多方计算
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)05-0103-04

A New Secure Method for Determining Two Spatial Geometric Objects Related Position

ZHAO Yu, YI Lei
(School of Computer Science and Technology, Anhui University, Hefei 230039, China)

Abstract: Mainly aims at two spatial geometric objects related position judging problem proposes a kind of new solution, using the concept of matrix Zhi and the secure protocol for the sum of two matrices to judge two spatial geometric objects related position problem. As for this problem, professor Luo Yonglong also designed a protocol for determining whether two sets of data are proportional correspondingly, but this text uses the concept of matrix Zhi and the secure protocol for the sum of two matrices to design some secure protocols for determining two spatial geometric objects related position. Using these protocols to judge the problem of the flat surface and the flat surface related position in the space, to judge the problem of the flat surface and straight line related position in the space and to judge the problem of straight line and straight line related position in the space . In this paper, a new judging method is developed, it solves two spatial geometric objects related position judging problem, will also have important function in the other secure multi—party computation problems.

Key words: concept of matrix Zhi; secure protocol for the sum of two matrices; secure multi—party computation

0 引 言

安全多方计算(Secure Multi-Party Computation, SMC)[1]是研究一组互不信任的参与方在保护各自私有信息的前提下进行的合作计算问题,对解决网络环境下的信息安全具有重要价值。保护私有信息的计算几何[2]现已成为安全多方计算的一个重要分支,它是一类特殊的安全多方计算问题。虽然目前该问题已经有一些理论上的通用解决办法,但是在实际的计算效率上是不可行的,所以特殊问题需要特殊的解决办法。迄今为止,在保护私有信息的计算几何问题中,对于如何设计高效而安全的空间几何对象位置判定协议仍是一个极具挑战的研究课题,对于空间中的几何对象位置判定问题研究也是有限的,文献[3]中首次提出了一个秘密判定两组数据是否对应成比例判定协议,并基于该协议解决了点、直线、平面等空间几何对象之间的相对位置判定问题。笔者在前人的基础上,针对像平面、直线类空间几何对象之间的相对位置判定问题提出一种新的解决方案。就是运用矩阵秩的概念和一般矩阵求和的安全两方计算协议设计了一些基础的空间几何对象相对位置安全判定协议。并利用这些协议秘密判定了平面及直线间相对位置问题。平面及直线间相对位置判定问题也是研究任何空间几何对象位置判定问题的基础,对于研究安全的空间几何对象相对位置问题有着重要的指导意义。

收稿日期:2010-11-07;**修回日期**:2011-02-19
作者简介:赵 玉(1984-),女,硕士研究生,研究方向为网络与信息安全研究。

1 相关知识

1.1 矩阵秩的概念

引理1[4]:两个矩阵乘积的秩不大于每一因子的

秩。特别,当有一个因子是可逆矩阵时,乘积的秩等于另一因子的秩。

由矩阵的秩判断平面及直线间的相对位置[5~7]:

定理 1 设由空间两平面的方程组成的方程组为

$$\begin{cases} A_1x + B_1y + C_1z + D_1 = 0 (h1) \\ A_2x + B_2y + C_2z + D_2 = 0 (h2) \end{cases}$$

其系数矩阵和增广矩阵分别为

$$\boldsymbol{A1} = \begin{bmatrix} A_1B_1C_1 \\ A_2B_2C_2 \end{bmatrix} \quad \boldsymbol{A2} = \begin{bmatrix} A_1B_1C_1D_1 \\ A_2B_2C_2D_2 \end{bmatrix},$$

两平面 hi (i = 1,2) 相交的充要条件是 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 2$。

两平面 hi (i = 1,2) 平行的充要条件是 $r(\boldsymbol{A1}) = 1$, $r(\boldsymbol{A2}) = 2$。

两平面 hi (i = 1,2) 重合的充要条件是 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 1$。

定理 2 设空间两直线的一般方程分别为

$$\begin{cases} A_1x + B_1y + C_1z + D_1 = 0 \\ A_2x + B_2y + C_2z + D_2 = 0 \end{cases} \text{和}$$

$$\begin{cases} A_3x + B_3y + C_3z + D_3 = 0 \\ A_4x + B_4y + C_4z + D_4 = 0 \end{cases},$$

则组成的方程组

$$\begin{cases} A_1x + B_1y + C_1z + D_1 = 0 \\ A_2x + B_2y + C_2z + D_2 = 0 \\ A_3x + B_3y + C_3z + D_3 = 0 \\ A_4x + B_4y + C_4z + D_4 = 0 \end{cases}$$

的系数矩阵和增广矩阵分别为

$$\boldsymbol{A1} = \begin{bmatrix} A_1 B_1 C_1 \\ A_2 B_2 C_2 \\ A_3 B_3 C_3 \\ A_4 B_4 C_4 \end{bmatrix} \quad \boldsymbol{A2} = \begin{bmatrix} A_1 B_1 C_1 D_1 \\ A_2 B_2 C_2 D_2 \\ A_3 B_3 C_3 D_3 \\ A_4 B_4 C_4 D_4 \end{bmatrix}$$

两直线异面的充要条件是 $r(\boldsymbol{A1}) = 3$, $r(\boldsymbol{A2}) = 4$。

两直线相交的充要条件是 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 3$。

两直线平行的充要条件是 $r(\boldsymbol{A1}) = 2$, $r(\boldsymbol{A2}) = 3$。

两直线重合的充要条件是 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 2$。

定理 3 设空间有

一直线 L: $\begin{cases} A_1x + B_1y + C_1z + D_1 = 0 \\ A_2x + B_2y + C_2z + D_2 = 0 \end{cases}$

和一平面 H: $A_3x + B_3y + C_3z + D_3 = 0$,

则组成的方程组

$$\begin{cases} A_1x + B_1y + C_1z + D_1 = 0 \\ A_2x + B_2y + C_2z + D_2 = 0 \\ A_3x + B_3y + C_3z + D_3 = 0 \end{cases}$$

的系数矩阵和增广矩阵分别为

$$\boldsymbol{A1} = \begin{bmatrix} A_1 B_1 C_1 \\ A_2 B_2 C_2 \\ A_3 B_3 C_3 \end{bmatrix} \quad \boldsymbol{A2} = \begin{bmatrix} A_1 B_1 C_1 D_1 \\ A_2 B_2 C_2 D_2 \\ A_3 B_3 C_3 D_3 \end{bmatrix}$$

当 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 3$ 时,直线与平面相交。

当 $r(\boldsymbol{A1}) = r(\boldsymbol{A2}) = 2$ 时,直线在平面上。

当 $r(\boldsymbol{A1}) = 2$, $r(\boldsymbol{A2}) = 3$ 时,直线与平面平行。

1.2 不经意传输协议

不经意传输协议(Oblivious Transfer,简称 OT)[8] 指发送方 Alice 仅有一个秘密输入 m,他希望以 50% 的概率让接收方 Bob 获得 m,然而 Alice 不希望 Bob 知道他是否得到秘密 m。随后产生了很多 OT 的变种[9],文献[10]提出了 OT_2^1 的概念,描述为:Alice 有两个秘密输入 $m1$ 及 $m2$,希望根据 Bob 的选择让其获得其中的一个秘密,同样 Bob 不希望 Alice 知道其选择了哪一个。文献[11]将 OT_2^1 推广到 OT_n^1,它是指协议开始时发送方 Alice 有 n 个秘密输入 $m_1, m_2, \cdots, m_n$,协议结束时接收方 Bob 获得 n 个输入中的某个 m_i($1 \leqslant i \leqslant n$),同时保证 Bob 不能获得其他 $n-1$ 个输入并且 Alice 不能获得有关 i 的信息。

1.3 一般矩阵求和的安全两方计算协议

1.3.1 问题描述

假设 Alice 有一个 $m \times n$ 矩阵 A,Bob 有一个 $m \times n$ 矩阵 B,Alice 与 Bob 希望在不泄自身数据信息时协作计算 $A + B$ 的值。计算结束后,双方除知道各自的输出,不能得到对方数据的任何其它信息。只有当双方合作时才能同时得到 $A + B$ 的值[12]。

1.3.2 一般矩阵求和的安全两方计算协议(以下简称协议 1)

输入:Alice 有一个 $m \times n$ 矩阵 A, Bob 有一个 $m \times n$ 矩阵 B。

输出:Alice 得到 R_a,Bob 得到 R_b,满足 $R_aR_b = A + B$。

1) Alice 和 Bob 约定两个数值 P 和 m,让 P^m 足够大,使要计算 P^m 次加法是不可能的。

2) Alice 产生 m 个随机矩阵 $A_1, \cdots, A_m$, 使 $\boldsymbol{A} = \sum_{j=1}^{m} A_j$。

3) Bob 产生 m 个随机矩阵 $B_1, \cdots, B_m$, 使 $\boldsymbol{B} = \sum_{j=1}^{m} B_j$,生成一个 n 阶的可逆矩阵 R_b。

4) 对每一个 $j = 1, \cdots, m$,Alice 和 Bob 执行下面的子步骤。

a) Alice 产生一个秘密随机数 $l \leqslant k \leqslant P$;

b) Alice 发送 $H_1 \cdots H_p$ 到 Bob,其中 $H_k = A_j$,其余的 H_i 是随机矩阵,因为 k 是一个秘密数据,只有 Alice 知道,Bob 不能知道 H_i 哪一个是 A_j;

c)对所有的 $i=1,\cdots,P$,Bob 计算 $T_{j,i}=(H_i+B_j)R_b^{-1}$;

d)用不经意传输 OT_p^1 协议,Alice 取回 $T_j=T_{j,k}=(H_k+B_j)\ \boldsymbol{R}_b^{-1}=(A_j+B_j)\ \boldsymbol{R}_b^{-1}$

5) Alice 计算 $\boldsymbol{R}_a=\sum_{j=1}^{m}(A_j+B_j)\ \boldsymbol{R}_b^{-1}=(A+B)\ \boldsymbol{R}_b^{-1}$。

1.3.3　协议分析

1.3.3.1　协议1是正确的。

证明:因为 $\boldsymbol{A}+\boldsymbol{B}=(\boldsymbol{A}+\boldsymbol{B})\ \boldsymbol{R}_b^{-1}\boldsymbol{R}_b=[(\boldsymbol{A}+\boldsymbol{B})\ \boldsymbol{R}_b^{-1}]\ \boldsymbol{R}_b$即令 $\boldsymbol{R}_a=(\boldsymbol{A}+\boldsymbol{B})\ \boldsymbol{R}_b^{-1}$,则有 $\boldsymbol{R}_a\boldsymbol{R}_b=\boldsymbol{A}+\boldsymbol{B}$ 成立,因而协议正确。

1.3.3.2　协议1是保密的。

证明:

1) 在第4步中,对每一个 $J=l,\cdots,m$,Bob 猜对 A_j 的概率是 $1/P$,那么 Bob 猜对矩阵 $\boldsymbol{A}$ 的概率是 l/P^m,又因 P^m 是一个足够大的数,故 l/P^m 的值近似为零。

2) 在第4步中,基于不经意传输 OT_p^1 协议的安全性 Alice 只知道 $T_j=T_{j,k}=(H_k+B_j)\ \boldsymbol{R}_b^{-1}=(A_j+B_j)\ \boldsymbol{R}_b^{-1}$ $(j=l,\cdots,m)$ 而不知道其它的 $T_{j,i}=(H_i+B_j)\boldsymbol{R}_b^{-1}(j=l,\cdots,m,i=l,\cdots,p$ 且 $i\neq k)$. Alice 只知道 A_j 和 $T_j=(A_j+B_j)\ \boldsymbol{R}_b^{-1}(j=l,\cdots,m)$ 之间的关系。也就是说 Alice 知道 m 个方程,而这些方程中含有 $B_1,\cdots B_m$ 和 Rb 共 $m+1$ 个未知数,所以 Alice 不能由它掌握的据推出任何关于矩阵 $\boldsymbol{B}$ 的信息。

因此协议1是保密的。

2　一些基础的空间几何对象相对位置安全判定协议

2.1　平面与平面相对位置安全判定协议

2.1.1　问题描述

空间中两平面位置关系判定问题可以描述为:Alice 拥有一个平面 $h_1:A_1x+B_1y+C_1z+D_1=0$,Bob 拥有一个平面 $h_2:A_2x+B_2y+C_2z+D_2=0$,他们希望在不向对方泄露自己的信息时能判断出这两个平面的相对位置关系。

2.1.2　平面与平面相对位置安全判定协议

协议的主要思想是:首先利用两方平面方程的系数分别构建各自的系数矩阵和增广矩阵,然后通过上述的一般矩阵求和的安全两方计算协议秘密求解两方系数矩阵之和、增广矩阵之和。再根据上述的引理1,求解两方系数矩阵和的秩、两方增广矩阵和的秩。最后,由矩阵秩的相关概念判定两平面位置关系。协议设计如下:

输入:Alice 拥有一个平面 $h_1:A_1x+B_1y+C_1z+D_1=0$,Bob 拥有一个平面 $h_2:A_2x+B_2y+C_2z+D_2=0$

输出:Alice 和 Bob 在不泄露自己信息的情况下能安全地判断出这两个平面的相对位置关系。

1) Alice 在本地构造自己的系数矩阵和增广矩阵如下:

$$\boldsymbol{A}1=\begin{bmatrix}A_1 & B_1 & C_1\\ 0 & 0 & 0\end{bmatrix}\quad \boldsymbol{A}2=\begin{bmatrix}A_1 & B_1 & C_1 & D_1\\ 0 & 0 & 0 & 0\end{bmatrix}$$

2) Bob 在本地构造自己的系数矩阵和增广矩阵如下:

$$\boldsymbol{B}1=\begin{bmatrix}0 & 0 & 0\\ A_2 & B_2 & C_2\end{bmatrix}\quad \boldsymbol{B}2=\begin{bmatrix}0 & 0 & 0 & 0\\ A_2 & B_2 & C_2 & D_2\end{bmatrix}$$

3) Alice 和 Bob 协同执行两次协议1,协议执行后,Alice 获得 $Ra1=(\boldsymbol{A}1+\boldsymbol{B}1)\ Rb1^{-1}$ 和 $Ra2=(\boldsymbol{A}2+\boldsymbol{B}2)\ Rb2^{-1}$。

4) 根据上述的引理1,Alice 在本地计算 $T1=\mathrm{rank}(\boldsymbol{A}1+\boldsymbol{B}1)=\mathrm{rank}(\ Ra1\ Rb1\ )=\mathrm{rank}(\ Ra1\ )$ $T2=\mathrm{rank}(\boldsymbol{A}2+\boldsymbol{B}2)=\mathrm{rank}(\ Ra2Rb2\ )=\mathrm{rank}(\ Ra2)$,并将 $T1$ 和 $T2$ 传送给 Bob。

5) Alice 和 Bob 各自根据矩阵秩的相关概念判定两平面的位置关系,即如果 $T1=T2=2$ 两平面相交;如果 $T1=T2=1$ 两平面重合;如果 $T1=1,T2=2$ 两平面平行。

2.2　直线与平面相对位置安全判定协议

2.2.1　问题描述

空间直线与平面位置关系判定问题可以描述为:Alice 拥有一直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\ A_2x+B_2y+C_2z+D_2=0\end{cases}$,Bob 拥有一平面 $H:A_3x+B_3y+C_3z+D_3=0$,他们希望在不向对方泄露自己的信息时能判断出彼此的相对位置关系。

2.2.2　直线与平面相对位置安全判定协议

协议的主要思想是:首先利用两方直线跟平面方程的系数分别构建各自的系数矩阵和增广矩阵,然后通过上述的一般矩阵求和的安全两方计算协议秘密求解两方系数矩阵之和、增广矩阵之和。再根据上述的引理1,求解两方系数矩阵和的秩、两方增广矩阵和的秩。最后,由矩阵秩的相关概念判定直线跟平面位置关系。协议设计如下:

输入:

Alice 拥有一直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\ A_2x+B_2y+C_2z+D_2=0\end{cases}$,

Bob 拥有一平面 $H:A_3x+B_3y+C_3z+D_3=0$。

输出:Alice 和 Bob 在不泄露自己信息的情况下能安全地判断出彼此的相对位置关系。

1) Alice 在本地构造自己的系数矩阵和增广矩阵

如下：

$$A1=\begin{bmatrix}A_1 & B_1 & C_1\\ A_2 & B_2 & C_2\\ 0 & 0 & 0\end{bmatrix}\quad A2=\begin{bmatrix}A_1 & B_1 & C_1 & D_1\\ A_2 & B_2 & C_2 & D_2\\ 0 & 0 & 0 & 0\end{bmatrix}$$

2）Bob 在本地构造自己的系数矩阵和增广矩阵如下：

$$B1=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ A_3 & B_3 & C_3\end{bmatrix}\quad B2=\begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ A_3 & B_3 & C_3 & D_3\end{bmatrix}$$

3）Alice 和 Bob 协同执行两次协议 1，协议执行后，Alice 获得 Ra1 =（$A1$ + $B1$）$Rb1^{-1}$ 和 Ra2 =（$A2$ + $B2$）$Rb2^{-1}$。

4）根据上述的引理 1，Alice 在本地计算 $T1$ = rank（$A1$ + $B1$）= rank（Ra1 Rb1）= rank（Ra1）$T2$ = rank（$A2$ + $B2$）= rank（Ra2Rb2）= rank（Ra2），并将 $T1$ 和 $T2$ 传送给 Bob。

5）Alice 和 Bob 各自根据矩阵秩的相关概念判定直线与平面的位置关系，即如果当 $T1$ = $T2$ = 3 时，直线与平面相交；当 $T1$ = $T2$ = 2 时，直线在平面上；当 $T1$ = 2，$T2$ = 3 时，直线与平面平行。

2.3 直线与直线相对位置安全判定协议

2.3.1 问题描述

空间中两直线位置关系判定问题可以描述为：

Alice 拥有一直线 $L1$：$\begin{cases}A_1x+B_1y+C_1z+D_1=0\\ A_2x+B_2y+C_2z+D_2=0\end{cases}$，

Bob 拥有一直线 $L2$：$\begin{cases}A_3x+B_3y+C_3z+D_3=0\\ A_4x+B_4y+C_4z+D_4=0\end{cases}$

他们希望在不向对方泄露自己的信息时能判断出彼此的相对位置关系。

2.3.2 直线与直线相对位置安全判定协议

协议的主要思想是：首先利用两方直线方程的系数分别构建各自的系数矩阵和增广矩阵，然后通过上述的一般矩阵求和的安全两方计算协议秘密求解两方系数矩阵之和、增广矩阵之和。再根据上述的引理 1，求解两方系数矩阵和的秩、两方增广矩阵和的秩。最后，由矩阵秩的相关概念判定直线跟直线位置关系。协议设计如下：

输入：

Alice 拥有一直线 $L1$：$\begin{cases}A_1x+B_1y+C_1z+D_1=0\\ A_2x+B_2y+C_2z+D_2=0\end{cases}$

Bob 拥有一直线 $L2$：$\begin{cases}A_3x+B_3y+C_3z+D_3=0\\ A_4x+B_4y+C_4z+D_4=0\end{cases}$

输出：Alice 和 Bob 在不泄露自己信息的情况下能安全地判断出这两个直线的相对位置关系。

1）Alice 在本地构造自己的系数矩阵和增广矩阵如下：

$$A1=\begin{bmatrix}A_1 & B_1 & C_1\\ A_2 & B_2 & C_2\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}\quad A2=\begin{bmatrix}A_1 & B_1 & C_1 & D_1\\ A_2 & B_2 & C_2 & D_2\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}$$

2）Bob 在本地构造自己的系数矩阵和增广矩阵如下：

$$B1=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ A_3 & B_3 & C_3\\ A_4 & B_4 & C_4\end{bmatrix}\quad B2=\begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ A_3 & B_3 & C_3 & D_3\\ A_4 & B_4 & C_4 & D_4\end{bmatrix}$$

3）Alice 和 Bob 协同执行两次协议 1，协议执行后，Alice 获得 Ra1 =（$A1$ + $B1$）$Rb1^{-1}$ 和 Ra2 =（$A2$ + $B2$）$Rb2^{-1}$。

4）根据上述的引理 1，Alice 在本地计算 $T1$ = rank（$A1$ + $B1$）= rank（Ra1 Rb1）= rank（Ra1）$T2$ = rank（$A2$ + $B2$）= rank（Ra2Rb2）= rank（Ra2），并将 $T1$ 和 $T2$ 传送给 Bob。

5）Alice 和 Bob 各自根据矩阵秩的相关概念判定直线与直线的位置关系，即如果 $T1$ = 3，$T2$ = 4 两直线异面；如果 $T1$ = $T2$ = 3 两直线相交；如果 $T1$ = 2，$T2$ = 3 两直线平行；如果 $T1$ = $T2$ = 2 两直线重合。

3 结束语

秘密判定空间几何对象相对位置问题是一类特殊的安全多方计算问题。笔者在以前学者研究的基础上进一步研究了空间几何对象相对位置安全判定问题，并就此提出新的解决方案。由于直接运用了矩阵秩的一些基本概念和不经意传输协议，可能增加了协议的通信量。此问题将在以后的工作中进一步研究，以求设计出更好的协议。

参考文献：

[1] Yao A C. Protocols for secure computations[C]//In Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science. Chicago, USA: [s. n.], 1982: 160-164.

[2] Atallah J, Du Wenliang. Secure multi-party computational geometry[C]//The 7th Int'l Workshop on Algorithms and Data Structures(WADS 2001). Providence, Rhode Island, USA: [s. n.], 2001.

[3] 罗永龙，黄刘生. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展，2006，43(3)：410-416.

[4] 张禾瑞，郝鈉新. 高等代数[M]. 第 4 版. 北京：高等教育出版社，1999.

[5] 萧树铁. 大学数学——代数与几何[M]. 北京：高等教育出版社，2001.

（下转第 110 页）

大的提高,可知,遗传算法对初始权值的优化对BP神经网络以后的学习过程起到了正向作用。而Bagging集成算法的加入又大大提高了文中方法的准确率。

表1 不同算法的实验结果比较

算法名称	样本数目	预测准确数目	平均准确率
BP神经网络	168	119	70.8%
GA优化后的BP神经网络	168	142	84.5%
文中方法	168	159	94.6%

Bagging集成算法将数据集分成训练和测试两用,图3是文中算法的预测结果与实际负荷的比较图。

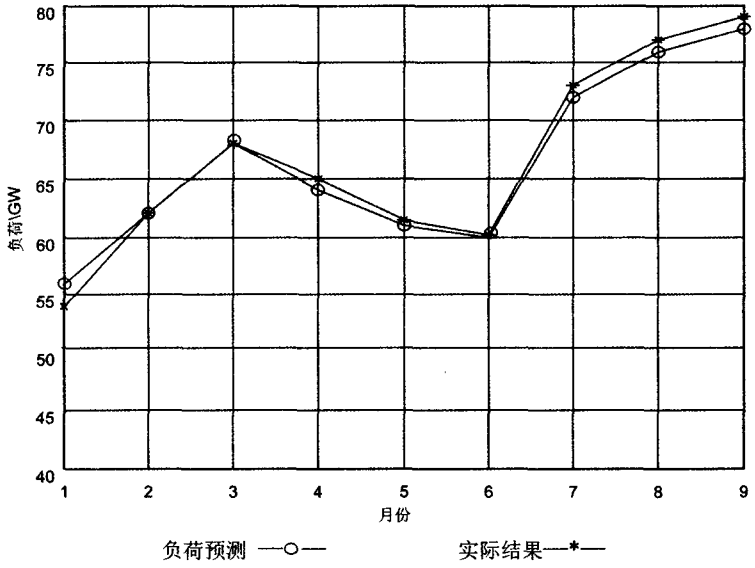

图3 基于Bagging算法集成遗传神经网络的负荷预测与实际结果的比较

4 结束语

提出基于Bagging算法集成遗传神经网络的负荷预测方法,是一种集各算法所长的新尝试。利用文中算法,首先用遗传算法可以得到全局最优解的特点,来克服BP神经网络易陷入局部极小值的缺点,再充分发挥BP神经网络很强的学习能力和训练能力,得到的预测结果,再经集成学习算法提高其准确率,从而获得更理想的结果,对电力负荷的预测具有实际意义。

参考文献:

[1] 邸凯昌.空间数据发掘与知识发现[M].武汉:武汉大学出版社,2000:5-38.

[2] 贺 蓉,曾 刚,姚建刚,等.天气敏感型神经网络在地区电网短期负荷预测中的应用[J].电力系统自动化,2001,25(17):32-35.

[3] 黎静华,粟 然,顾雪平,等.网格化的电力系统短期负荷预测的MDRBR模型[J].电力系统自动化,2005,29(24):27-31.

[4] 朱 明.数据发掘[M].合肥:中国科学技术大学出版社,2008:116-150.

[5] Chien-cheng,Yun-ching Tang. To improve the training time of BP neural Networks[C]//Info-tech and Info-net 2001 International Conferences.[s.l.]:[s.n.],2001:473-479.

[6] 王 蓓,刘 桥.优化BP神经网络的可靠性预测模型[J].计算机技术与发展,2007,17(9):102-105.

[7] Bergy Paul K, Ragsdale Cliff T, Hoskote Mangesh. A Simulated Annealing Genetic Algorithm for the Electrical Districting Problem[J]. Annals of Operations Research, 2003,9(5):33-35.

[8] 杨 超.基于遗传算法与神经网络的一卡通交易量预测[D].北京:北京邮电大学,2009:26-27.

[9] 陈 文,庞琳娜.GABP神经网络在交通流预测中的应用研究[J].人工智能,2009,25(5):245-247.

[10] 吴 斌,陈章潮,包海龙.基于人工神经元网络及模糊算法的空间负荷预测[J].电网技术,1999,23(11):1-4.

[11] Breiman L. Bagging predictors[J]. Machine Learning,1996,24(2):123-140.

[12] 朱红斌.基于Bagging算法和遗传神经网络的交通事件检测[J].计算机应用与软件,2010,27(1):234-236.

(上接第106页)

[6] Gruenberg K W,Weir A J. Linear Geometry[M]. New York Heidelberg Berlin:Spring-Verlag,1997.

[7] 安芹力.用矩阵的秩判断两空间直线及直线与平面的位置关系[J].高等数学研究,2005(3):54-55.

[8] Rabin M. How to exchange secrets by oblivious transfer[R].[s.l.]:Aiken Computation Laboratory,1981.

[9] Crepeau C. Equivalence between two flavors of oblivious transfers[C]//In Advances in Cryptology — CRYPTO 1987, Lecture Notes in Computer Science, volume 293.[s.l.]:Springer-Verlag,1988:350-354.

[10] Even S,Goldreich O, Lempel A. A randomized protocol for signing contracts[J]. Communications of the ACM,1985,28:637-64.

[11] Brassard S,Cr6peau C,Rovert J. All-or-noting disclosure of secrets[C]//In Advances inCryptology-Crypto86, Lecture Notes in Computer Science, Volume1987.[s.l.]:[s.n.],1986:234-238.

[12] 张 龙,闫 韬,柯品惠,等.关于矩阵的几个安全两方计算协议[J].齐齐哈尔大学学报,2009,25(3):64-67.