# 基于模糊支持向量机的网络入侵检测研究

李 华 张简政
(重庆大学计算机学院 重庆 400044)

**摘 要** 模糊支持向量机理论属于统计学习理论,是支持向量机理论的推广,使支持向量机更好地运用到实际工作中。我们将其运用到网络入侵检测中,实验证明是可行的、高效的,有其特点和优势的。

**关键词** 网络入侵检测,支持向量机,模糊支持向量机,Libsvm

## Network Intrusion Detection Based on Fuzzy Support Vector Machine

LI Hua ZHANG Jian-Zheng
(School of Copmputer, Chongqing University, Chongqing 400044)

**Abstract** FSVM belongs to Statiscal Learning Theory, it exends SVM's application. We introduce it to network intrusion detection. The experiment results proves it is effective, efficient and preponderant.

**Keywords** Network intrusion detection, Support vector machine, Fuzzy support vector machine, Libsvm

## 1 引言

随着互联网络的飞速发展,网络安全正日益得到人们的关注,网络安全概念主要涵盖四个方面:保密性、完整性、可用性和认证。由于互联网络在设计实现和使用时候的种种安全问题,以上四个方面的安全无法得到根本保证,这使得入侵事件不断发生,也使入侵检测系统成为当前研究的热点。

根据入侵检测系统的分析数据的来源可以将入侵检测系统分为两大类:基于网络的入侵检测系统(Network-based IDS,简称 NIDS)和基于主机的入侵检测系统( Host-based IDS,简称 HIDS)。根据检测所使用的方法,IDS 还可以分为两种:误用检测和异常检测。误用检测需要建立入侵者的行为模式,异常检测需要建立正常用户的行为模式。由于各有各的优缺点,它们在不同的安全政策中有不同的应用。

入侵检测可以看作是一个分类问题,也就是对给定的审计数据进行分类:什么样的数据是正常的,什么样的数据是异常的。在有关文献中,Forrest[6] 等人把入侵检测看作是区分"自我"(也就是"正常")和"非自我"(也就是"异常")的过程,提出了基于免疫模型的入侵检测技术。Ghosh[7] 利用神经网络来提取特征和分类. W. Lee[8] 从数据挖掘技术的角度探讨了入侵检测的实现问题。以上方法都需要大量或者是完备的数据集才能达到比较理想的检测性能,并且训练时间长,对数据的规律性要求比较高。那么,如何在小样本,入侵特征呈现高维性的入侵检测中,取得更好的检测性能呢?

支持向量机(support vector machines, SVM)是一种建立在统计学习理论基础之上的机器学习方法。其主要的特点是根据 Vapnik[4] 结构风险最小化原则,尽量提高学习机的泛化能力,即由有限的训练集样本得到小的误差仍然能够保证对独立的测试集保持小的误差。另外,由于支持向量算法是一个凸优化问题,所以局部最优解一定是全局最优解。这是其他学习算法所不及的。

为了将支持向量机理论的进一步推广运用到实际中去,Chun-Fu Lin[1] 将模糊关系引入到支持向量机中,在分类问题上,更加注重异常数据的分类情况,进一步提高了检测异常数据的准确率。在理论上得到了验证,但在实际运用中还不够。本文首次将该算法引入到网络入侵检测中来,实验结果表明,该算法可行,有效,特点突出。

本文首先介绍了支持向量机,模糊支持向量机原理,在此基础上,将模糊支持向量机引入到网络入侵检测中,最后利用构造的数据集对模糊支持向量机算法进行实验,给出实验结果和分析。

## 2 支持向量机

支持向量机(SVM)是从线性可分情况下的最优分类面发展而来的,基本思想可用图 1 的二维情况说明。

图中,白色点和黑色点代表两类样本,$H$ 为分类线,$H1$,$H2$ 分别为过各类中离分类线最近的样本且平行于分类线的直线,它们之间的距离叫做分类间隔(margin)。所谓最优分类线就是要求分类线不但能将两类正确分开(训练错误率为 0),而且使分类间隔最大。分类线方程为 $x \cdot w+b=0$,我们可以对它进行归一化,使得对线性可分得样本集:

$$(x_i, y_i), i=1,\cdots,n, y\in\{+1,-1\} \quad (1)$$

李 华 副教授,硕士生导师,主要研究方向:网络和信息安全、综合网络信息技术;张简政 硕士,主要研究方向:网络安全。

## 参 考 文 献

1 何成武. 自动机理论及其应用. 北京:科学出版社,1990
2 秦志光,刘锦德. 安全系统的有限自动机. 电子科技大学学报,1996,25(1):71~75
3 宋荆汉,朱伟,等. HoneyPot 系统研究. Net Security Technologies and Application,2002. 1
4 赵伟峰,曾启铭. 一种了解黑客的有效手段——蜜罐(Honeypot). 计算机应用,2003
5 锁廷锋,马士尧. 网络欺骗技术. 信息网络安全,2003
6 Honeynet Project. http://www. honeynet. org

满足

$$y_i[(w\cdot x_i)+b]-1\geqslant 0, i=1,\cdots,n \quad (2)$$

此时分类间隔等于 $2/\|w\|$，使间隔最大等价于使 $\|w\|^2$ 最小，满足条件(2)且使 $\frac{1}{2}\|W\|^2$ 最小的分类面就叫做最优分类面，$H1$，$H2$ 上的训练样本点称作支持向量。

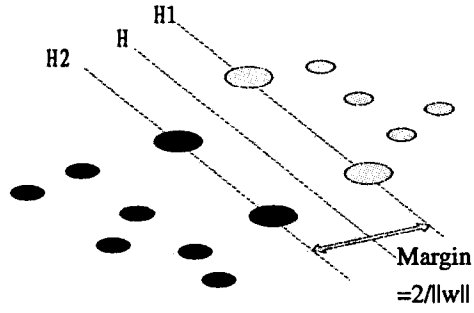


图 1　线性可分情况下的最优分类线

对线性问题，用 Lagrange 优化方法把最优分类面问题转化为对偶问题后，再解一个不等式约束下二次函数寻优的问题，即在约束条件

$$\sum_i^n y_i\alpha_i=0 \text{ 和 } \alpha_i\geqslant 0, i=1,\cdots,n \quad (3)$$

下对 $\alpha_i$ 求解下列寻优函数的最大值

$$Q(\alpha)=\sum_{i=1}^n\alpha_i-\frac{1}{2}\sum_{i,j=1}^n\alpha_i\alpha_j y_i y_j(x_i\cdot x_j) \quad (4)$$

$\alpha_i$ 为与每个样本对应得 Lagrange 乘子，这是一个不等式约束下二次函数寻优的问题。容易证明，解中将只有意部分(通常是少部分)$\alpha_i$ 不为零，对应得样本就是支持向量，解上述问题后得到最优的分类函数是

$$f(x)=\mathrm{sgn}\{(w\cdot x)+b\}=\mathrm{sgn}\{\sum_{i=1}^n a_i^* y_i(x_i\cdot x)+b^*\} \quad (5)$$

对非线性问题，可以通过非线性变换转化为某个高维空间中的线性问题，在变换空间中求最优分类面。这种变换可能比较复杂，因此这种思路在一般情况下不易实现。上述问题中，不论是寻优函数(4)还是分类函数(5)都只涉及训练样本之间的内积运算($X_i * X_j$)，这样，在高维空间实际上只需要进行内积运算，而这种内积运算时可以用原空间中的函数实现的，不必知道变换形式。根据泛函的有关理论，只要一种核函数 $K(X_i,X_j)$ 满足 Mercer 条件，它就对应某一变换空间中的内积。因此，在最优分类面中采用适当的内积函数 $K(X_i,X_j)$ 就可以实现某一非线性变换后的线性分类，而计算复杂度却没有增加，此时目标函数(4)变为

$$Q(\alpha)=\sum_{i=1}^n\alpha_i-\frac{1}{2}\sum_{i,j=1}^n\alpha_i\alpha_j y_i y_j K(x_i\cdot x_j) \quad (6)$$

而相应得分类函数也变为

$$f(x)=\mathrm{sgn}\{(w\cdot x)+b\}=\mathrm{sgn}\{\sum_{i=1}^n a_1^* y_i K(x_i\cdot x)+b^*\} \quad (7)$$

概括地说，支持向量机就是首先通过用内积函数定义的非线性变换将输入空间变换到一个高维空间，在这个空间中求(广义)最优分类面。

SVM 的核函数主要的有三类，主要采用的是 radial basis function(RBF)：

$K(x,x_i)=\exp\{-\frac{|x-x_i|^2}{\sigma^2}\}$，其中 $\sigma$ 为核参数。

## 3　模糊支持向量机

### 3.1　简介

SVM 是一个解决分类问题的强有力的工具，但其中存在不少缺陷，在很多实际问题中，数据集的作用是不同的，存在很多问题就是一部分数据明显比其他数据重要，我们更关注怎样把重要的数据进行正确的分类，哪些次要或没有意义的数据，我们没有必要过份关心其分类的情况。

也就是说，每一条数据不再精确属于两类中的哪一类，它可能 90%属于某一类，而 10%没有意义，也可能 20%属于某一类，而 80%没有意义。概括的讲，就是每条数据有一个模糊关系 $0<Si<1$ 在里面，这种模糊关系 Si 其实就是代表属于某一类的程度，那么$(1-Si)$就代表该数据无意义的程度，将扩展以后带有模糊关系的 SVM 称为 FSVM[1]。

### 3.2　SVM 重构

将(1)式加入模糊关系变为如下：

$$(x_i,y_i,s_i), i=1,\cdots,n, y\in\{+1,-1\} \quad (8)$$

每一个 $X_i$ 就有了一个模糊关系 $\sigma\leqslant S_i\leqslant 1$(其中 $i=1,\cdots n$，$\sigma$ 足够小但 $\sigma>0$)。

为了解决优化问题，模糊支持向量机作者构造了 Lagrangian

$$L(w,b,\xi,\alpha,\beta)=\frac{1}{2}w\cdot w+C\sum_{i=1}^l s_i\xi_i-\sum_{i=1}^l\alpha_i(y_i(w\cdot z_i+b)-1+\xi_i)-\sum_{i=1}^l\beta_i\xi_i \quad (9)$$

为了找到函数的 saddle point，这些参数必须满足如下条件：

$$\frac{\partial L(w,b,\xi,\alpha,\beta)}{\partial w}=w-\sum_{i=1}^l\alpha_i y_i z_i=0 \quad (10)$$

$$\frac{\partial L(w,b,\xi,\alpha,\beta)}{\partial w}=-\sum_{i=1}^l\alpha_i y_i=0 \quad (11)$$

$$\frac{\partial L(w,b,\xi,\alpha,\beta)}{\partial \xi_i}=s_i C-\alpha_i-\beta_i=0 \quad (12)$$

将上述三个条件应用于(9)中，那么最优超平面的问题就可以传化成即在约束条件(13)下

$$\sum_{i=1}^l y_i\alpha_i=0, 0\leqslant\alpha_i\leqslant s_i C, i=1,\cdots,l \quad (13)$$

求(14)式的最大值

$$W(\alpha)=\sum_{i=1}^l\alpha_i-\frac{1}{2}\sum_{i=1j=1}^l\sum^l\alpha_i\alpha_j y_i y_j K(x_i,x_j) \quad (14)$$

最终的决策函数跟(7)式一样，只是其中 $\alpha_i$ 的范围变成如下：

$$f(x)=\mathrm{sgn}\{(w\cdot x)+b\}=\mathrm{sgn}\{\sum_{i=1}^n a_1^* y_i K(x_i\cdot x)+b^*\}, \quad 0\leqslant\alpha_i\leqslant s_i C \quad (15)$$

## 4　基于模糊支持向量机的网络入侵检测实验

模糊支持向量机是支持向量机理论的推广，强调的是有意义的数据分类务必要正确。在网络入侵检测中，检测异常连接是其主要的工作，所以异常连接就是有意义的数据。这点上模糊支持向量机正好满足了着重检测异常连接的要求，将其运用到网络入侵检测，理论上是可行，有效的，我们进一步用实验来证明它。

本实验分为两个阶段：训练阶段和检测阶段。在训练阶段，根据已知的正常网路数据和异常数据按照式(13)(14)来训练模糊支持向量机，并根据式(2)得到模糊支持向量和相应的参数。在检测阶段，根据判决函数式(15)对测试数据进行分类，最后得到分类结果。

### 4.1　实验数据集介绍

数据集采用 Stolfo 等人在美国国防部高级研究计划局(DARPA)作 IDS 评测的原始数据集基础上恢复出来，并提取出入侵特征以后的连接记录集[5]。

DARPA 的数据集包含 7 个星期的网络流量，大约有 500 万条连接记录，其中包含 4 类的攻击：

DoS：拒绝服务攻击，如 SYN Flood，land 攻击；

R2L：远程权限获取，如：口令猜测；

U2R：各种权限提升，如：各种本地和远程 Buffer Overflow 攻击；

Probe：各种端口扫描和漏洞扫描 .

Stolfo 等人利用域知识提取出 4 类属性集共 41 个特征，分别为：

(1)基本属性集，如：连接的持续时间、协议、服务、发送字节数、接收字节数等；

(2)内容属性集，即用领域知识获得与信包内容相关的属性，如：连接中的 D-E 标志的个数、本连接中失败登录次数、是否成功登录等；

(3)流量属性集，即基于时间的与网络流量相关的属性，这类属性又分为两种集合，一种为 SameHost 属性集，即在过去 2s 内与当前连接具有相同目标主机的连接中，有关协议行为、服务等的一些统计信息，另外一种为 SameService 属性集，即在过去 2s 内与当前连接具有相同服务的连接中作出的一些统计信息。

(4)主机流量属性集，即基于主机的与网络流量相关的属性，这类属性是为了发现慢速扫描而设的属性，获取的办法是统计在过去的 100 个连接中的一些统计特性，如过去 100 个连接中与当前连接具有相同目的主机的连接数、与当前连接具有相同服务的连接所占百分比等。

属性可取值均不相同，这些属性的可取值详细说明如表 1 所示(C 代表连续属性，D 代表离散属性)。

表 1

| 基本属性集 | 内容属性集 | 流量属性集 | 主机流量属性集 |
|---|---|---|---|
| 1. duration:C | 10. hot:C | 23. count:C | 32. dst_host_count:C |
| 2. protocol_type:D | 11. num_failed_logins:C | 24. srv_count:C | 33. dst_host_srv_count:C |
| 3. service:D | 12. logged_in:D | 25. serror_rate:C | 34. dst_host_same_srv_rate:C |
| 4. flag:D | 13. num_compromised:C | 26. srv_serror_rate:C | 35. dst_host_diff_srv_rate:C |
| 5. src_bytes:C | 14. root_shell:C | 27. rerror_rate:C | 36. dst_host_same_src_port_rate:C |
| 6. dst_bytes:C | 15. su_attempted:C | 28. srv_rerror_rate:C | 37. dst_host_srv_diff_host_rate:C |
| 7. lang:D | 16. num_root:C | 29. same_srv_rate:C | 38. dst_host_serror_rate:C |
| 8. wrong_fragment:C | 17. num_file_creations:C | 30. diff_srv_rate:C | 39. dst_host_srv_serror_rate:C |
| 9. urgent:C | 18. num_shells:C | 31. srv_diff_host_rate:C | 40. dst_host_rerror_rate:C |
| | 19. num_access_files:C | | 41. dst_host_srv_rerror_rate:C |
| | 20. num_outbound_cmds:C | | |
| | 21. is_host_login:D | | |
| | 22. is_guest_login:D | | |

### 4.2 测试数据集构造

作者后面的工作考虑到要构建一个实用的智能网络入侵检测系统，故并没有对原始训练数据进行分类和调整比例，也考虑到一个智能入侵检测系统应该具有一定的发现新型攻击手段的能力，故训练数据中只有 27 种攻击手段，而在测试数据中增加了 14 种攻击手段，考虑到实验时间问题，笔者采用上述样本集的 1/10 来完成该实验！

由于我们采用模糊支持向量机算法，需要对数据集当中的异常数据和正常数据给定一个模糊关系，笔者采用的模糊关系如下：

$$s_i=\begin{cases}1, \text{if } y_i=1\\ 0.1, \text{if } y_i=-1\end{cases} \tag{16}$$

即异常连接取模糊关系 1，正常连接取模糊关系 0.1。

由于模糊支持向量机只能识别科学计数法的输入，故将选择数据集中的如协议类型，攻击类型等用固定数值替换，按上述提到的要求将数据改造成为模糊支持向量机软件能够识别的数据格式。

### 4.3 实验结果

我们采用传统的 C-FSVM(Cortes-Fuzzy Support Vector Machine，有监督的学习算法)算法进行学习和泛化，将 Libsvm 软件包按照式(8)(13)(14)(15)修改，使其成为模糊支持向量机的软件包。

实验中要统计与入侵检测性能相关的一些数据精度，时间等。

检测精度(Detection Precesion)＝被检测出来的异常数据样本数/异常样本总数

新型攻击检测率(Undiscovered Detection Rate)＝检测出的训练数据集中没有的攻击样本数/测试样本集中总的新型攻击样本数

误报率(False Positive)＝正常样本测出属于攻击样本数/正常样本数

检测时间(Detection Time)＝ 总的检测时间/总样本数

在试验过程中，libsvm 自带的 easy. py 脚本能够调整出最好 C，g(支持向量机中两个重要的参数，错分惩罚因子 C 和 RBF 核函数的控制因子 $1/\sigma^2$)的值，也可以自己设定参数进行测试。表 2 为基于 C-SVM 的入侵检测结果。

表 2

| C | g | 结果 |
|---|---|---|
| 128 | 0.25 | DP＝78.81% |
| | | UDR＝50.32% |
| | | FP＝2.11% |
| | | DT＝0.3ms |

### 4.4 实验结果分析

总体看，实验结果比较理想。

与 Wenke Lee[8] 等用数据挖掘应用于入侵检测作比较，如表 3。

表 3

| Class | Wenke Lee 等的新型攻击检测率结果 | 我们的检测结果 |
|---|---|---|
| DOS | 24.3% | |
| PROBING | 96.7% | |
| U2R | 81.8% | |
| R2L | 5.9% | |
| Overall | 37.7% | 50.32% |

与现在 Srinivas Mukkamala[3]等正在作将支持向量机用于入侵检测相比，如表 4。

与 Wenke Lee 等用数据挖掘作入侵检测的结果相比较，在检测新型攻击方式方面，效果更好，因为模糊支持向量机对需要着重分析的数据（攻击数据）进行了优化（参看 3.1），这也是模糊支持向量机用于入侵检测的特点和优势。

与 Srinivas Mukkamala 等的结果相比，差距不小，主要原因是他将各种攻击类型分类，然后再作检测，所以准确率非常高，但从实用的角度讲，不可能攻击会告诉你它是哪个攻击类型，所以我们运用的检测方式可以拿来实际运用。

表 4

| Class | Srinivas mukkamala 等的结果 | 我们的结果 |
|---|---|---|
| Normal | 99.55% | 78.81% |
| Probe | 99.70% | |
| DOS | 99.25% | |
| U2SU | 99.87% | |
| R2L | 99.78% | |

**下一步工作** 本文所做贡献主要是首次将模糊支持向量机引入网络入侵检测中，取得了理想的效果，检测新型攻击手段能力更强，也具有实用的价值，进一步推广了模糊支持向量机理论的实际应用。

下一步的工作是在一开源网络入侵检测系统 Bro 上，引入我们的 FSVM 检测模块，争取实现一实用的智能网络入侵检测系统。

## 参 考 文 献


1 Lin Chun-Fu. Fuzzy Support Vector Machines. IEEE TRANSACTIONS ON NUERAL NETWORKS, 2002, 13(2): 3

2 Vapnik V N. An Overview of Statistical Learning Theory. IEEE TRANSACTIONS O NEURAL NETWORKS, 1999, 10(5)

3 Mukkamala S, Sung A H. Artificial Intelligent Techniques for Intrusion Detection. 0-7803-7952-7/03 2003 IEEE

4 Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 1999

5 http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

6 Forrest S. Self-Nonself discrimination in a computer. CA: IEEE Computer Society Press, 1994

7 Ghosh AK. A real-time intrusion detection system based on learning program behavior. Recent Advances in Intrusion Detection (RAID 2000). Toulouse: Spinger-Verlag, 2000

8 Lee W, Stolfo SJ. A data mining framework for building intrusion detection model. CA: IEEE Computer Society Press, 1999

9 http://www.cert.org/stats/cert_stats.html

10 张学工. 关于统计学习理论与支持向量机. 自动化学报, 2000(1)


（上接第 74 页）

$T_i(i=1,2,\cdots,n)$的数量时，可以在执行算法 2.1 时改变输入 $t,n$ 的值，从而改变托管代理 $T_i$ 的数量。

3.2.5 计算量 在计算量上，主要集中在子密钥的产生。本密钥托管分配机制的子密钥产生采用的是基于状态树的$(t,n)$门限秘密共享方案，我们将此方案与现在广泛采用的基于 Shamir 的$(t,n)$门限秘密共享方案作一比较。

1. 基于 Shamir 的$(t,n)$限秘密共享方案

Shamir 秘密共享[5]是一个基于多项式插值的$(t, n)$门限秘密共享方案。首先选取有限域 $Z_q$ 中的 $n$ 个不同的非零元，记为 $x_i$，$1\leqslant i\leqslant n$，然后在 $Z_q$ 上随机选择一个次数为$(t-1)$的多项式 $f(x)=f_0+f_1x+\cdots+f_{t-1}x^{t-1}(\mathrm{mod}\ q)$，满足 $f(0)=f_0=d$。$f_1,f_2,\cdots,f_{t-1}$为 $Z_q$ 上的随机数，计算多项式 $d_i=f(x_i)(\mathrm{mod}\ q)$，$1\leqslant i\leqslant n$，$d_i$ 即为托管代理的影子（子密钥）。

从上面的计算过程看出：影子 $d_i$ 的计算共要进行 $n$ 次多项式 $f(x_i)$的计算，算法复杂度为 $t-1$ 次方阶 $o(n^{t-1})$。我们将 $f(x_i)$的模幂计算转化成模乘计算来考虑。多项式 $f(x_i)$的计算共需要$\frac{1}{2}t(t-1)$次模乘和$\frac{1}{2}t(t+1)$次模加运算。因此 $d_i$ 的计算总共需要$\frac{1}{2}t(t-1)\times n$次模乘和$\frac{1}{2}t(t+1)\times n$次模加运算。

2. 基于状态树的$(t,n)$门限秘密共享方案

基于状态树的$(t,n)$门限秘密共享方案的存取结构共$\binom{n}{t}$个，每一个存取结构需要进行 $t$ 次模加。因此影子 $d_i$ 的计算总共需要$t\binom{n}{t}$模加运算。算法为多项式复杂度。

从上述分析可以看出我们的方案比基于 Shamir 的$(t,n)$门限秘密共享方案的计算量要小得多。而且随着 $t$ 和 $n$ 的增大，基于状态树的$(t,n)$门限秘密共享的密钥分配机制比基于 Shamir 的$(t,n)$门限秘密共享效率高得多。

## 4 相关工作

目前，门限密钥托管方案所采用的秘密共享算法都是基于 Shamir 的$(t,n)$门限秘密共享，而本文提出的门限密钥托管方案是基于状态树的$(t,n)$秘密共享。由 3.2 节分析可知，无论在计算量上，还是在效率上，本文的方案均优于基于 Shamir 的$(t,n)$门限密钥托管方案。

**结束语** 本文基于 PKI(Public Key Infrastructure)提出了一个防欺诈的密钥托管方案，并提出了密钥托管分配机制。由于该方案的秘密共享采用基于状态树的$(t,n)$秘密共享，所以具有计算量小，效率高的特点。这个方案不仅有效地解决了用户欺诈的问题，而且托管用户可根据需要而改变托管代理的数量。本文在数字证书的发放与密钥托管之间建立了一种机制，把两者联系在一起，以真正实现密钥托管的目的。

下一步，我们将考虑门限密码系统的有效性研究，即在保证安全性的前提下，怎样使得共享密钥长度尽量小、计算速度尽量快。

## 参 考 文 献


1 National Institute of Standard and Technology (NIST). PKI technical specifications [DB/OL]. PartA: Requirements. Feb. 1996. http//csrc.ncsl.nist.gov/pki/fordrept.ps

2 Phoenix S J D. Cryptography, trusted third parties and escrow[J]. BT Technology Journal, 1997, 15(2): 45～62

3 徐秋亮，李大兴. 椭圆曲线密码体制. 计算机研究与发展，1999，36(11)：1281～1288

4 张险峰. 基于 ECC 的门限密码体制及其应用的研究：[博士论文]. 2003. 36～43

5 Shamir. How to share a secret[J]. Comm. of the ACM, 1979, 22(11): 612～613