◎研究、探讨◎

线性有限自动机输入输出集的性质

谢正卫[1],郭 振[2]
XIE Zheng-wei[1],GUO Zhen[2]

1.江苏技术师范学院 数理学院,江苏 常州 213001
2.信阳师范学院 计算机与信息技术学院,河南 信阳 464000
1.School of Mathematics and Physics,Jiangsu Teachers University of Technology,Changzhou,Jiangsu 213001,China
2.School of Computer and Information Technology,Xinyang Normal University,Xinyang,Henan 464000,China
E-mail:xiezhengwei@jstu.edu.cn

XIE Zheng-wei,GUO Zhen.Character of input and output of linear finite automata.Computer Engineering and Applications,2009,45(35):28-30.

Abstract: This paper proves that the compound automata of two linear finite automata has the character of homogeneous input and output,and builts equality relation between the input number of the compound automata of two weakly invertible linear finite automata with delay 1 and the input number of the two automata.

Key words: linear finite automata;compound;input;output;weakly invertible

摘 要:证明了两个线性有限自动机化合而得到的自动机具有输入输出均匀的性质,建立了由两个延迟1步弱可逆线性有限自动化合后得到的自动机的输入集个数与化合前自动机输入集个数的等式关系。

关键词:线性有限自动机;化合;输入;输出;弱可逆
DOI:10.3778/j.issn.1002-8331.2009.35.009 **文章编号:**1002-8331(2009)35-0028-03 **文献标识码:**A **中图分类号:**TP301.1

1 引言

有限自动机是一门新兴的交叉学科,近几十年来,人们用数学的方法对有限自动机进行了广泛的研究[1-8],有限自动机理论已成为密码学、控制论、神经网络、生物等学科的重要研究工具。有限自动机理论有很大的实用背景,在数字通信中有广泛的应用,特别是在一种基于身份的密码体制和数字签名方面显示出了它的优势和潜力[4-8],在双钥和基于身份的密码体制的构造中,有限自动机的化合成为一种基本手段[3]。而线性自动机是线性系统和一般离散系统的交叉点,所以研究线性有限自动机对于研究有限自动机有重要的意义[12-15]。文献[9-11]对非线性有限自动机的输入输出集的性质进行了讨论,文献[8]对线性有限自动机的输入输出集在密码学上的应用进行了讨论,主要讨论了两个线性有限自动机的化合而得到的自动机具有输入输出均匀的性质,建立了由两个延迟1步弱可逆线性有限自动化合后得到的自动机输入集个数与化合前自动机输入集个数的等式关系,即化合后自动机的长为2的输入集个数用化合前自动机长为1的输入集个数表示,这对研究复杂自动机的性质具有较高的参考价值。

2 基本概念与记号

定义1 一个有限自动机是一个五元组 $M=<X,Y,S,\delta,\lambda>$,其中非空有限集 X、Y 和 S 分别是输入、输出和状态字母表;δ 是一个从 $S\times X$ 到 S 的单值映射,λ 是一个从 $S\times X$ 到 Y 的单值映射,分别称为下一状态函数和输出函数,称 X、Y 和 S 中的元素分别为 M 的输入字母、输出字母和状态,称 $X^*\cup X^\omega$ 和 $Y^*\cup Y^\omega$ 中的元素分别为 M 的输入序列和输出序列。

δ 可唯一扩充为 $S\times X^*$ 到 S 的单值映射:

$\delta(s,\Lambda)=s,\delta(s,\alpha x)=\delta(\delta(s,\alpha),x),s\in S,\alpha\in X^*,x\in X$

同样,λ 可唯一扩充为 $S\times(X^*\cup X^\omega)$ 到 $Y^*\cup Y^\omega$ 的单值映射,满足条件:

$\lambda(s,\Lambda)=\Lambda,\lambda(s,x\alpha)=\lambda(s,x)\lambda(\delta(s,x),\alpha),s\in S,\alpha\in X^*\cup X^\omega,x\in X$

分别对 α 和 β 的长进行归纳,有 $\delta(s,\alpha\beta)=\delta(\delta(s,\alpha),\beta)$

$\lambda(s,\alpha\gamma)=\lambda(s,\alpha)\lambda(\delta(s,\alpha),\gamma),s\in S,\alpha\beta\in X^*,\gamma\in X^*\cup X^\omega$

定义2 设 X,Y 和 S 分别是域 $GF(q)$ 上 l,m 和 n 维向量空间,δ 是笛卡儿积空间 $S\times X$ 到空间 S 的线性映射,λ 是空间 $S\times$

基金项目:江苏省高校自然科学研究指导性计划项目(No.07KJD1100043);江苏技术师范学院青年科研基金(No.KYY08043)。
作者简介:谢正卫(1979-),男,讲师;郭振(1978-),男,讲师。
收稿日期:2009-08-26 **修回日期:**2009-10-09

X 到空间 Y 的线性映射，则称有限自动机 $M=<X,Y,S,\delta,\lambda>$为一个 $GF(q)$线性有限自动机，并称 l,m,n 为 M 的结构参数。

定义 3 设 $M_1=<X,Y,S_1,\delta_1,\lambda_1>$和 $M_2=<Y,Z,S_2,\delta_2,\lambda_2>$为两有限自动机，定义 $M_1\cdot M_2=<X,Z,S_1\times S_2,\delta,\lambda>$，其中对任意$<s_1,s_2>\in S_1\times S_2,x\in X$ 有

$\delta(<s_1,s_2>,x)=<\delta_1(s_1,x),\delta_2(s_2,\lambda_1(s_1,x))>$

$\lambda(<s_1,s_2>,x)=\lambda_2(s_2,\lambda_1(s_1,x))$，则称 $M_1\cdot M_2$ 为 M_1 与 M_2 的化合。

定义 4 设 $M=<X,Y,S,\delta,\lambda>$是一个有限自动机，且 $s\in S$，t 是正整数，则记 $Out_M(s,t)=\{y_1y_2\cdots y_t\in Y^t|$存在 $\alpha\in X^t$，使得 $\lambda(s,\alpha)=y_1y_2\cdots y_t\}$，并且记 $O_M(s,t)=|Out_M(s,t)|$。$Out_M(s,t)$是以 s 为初始状态 M 所有可能的 t 长输出所组成的集合，$Out_M(s,t)\subseteq Y^t$。$O_M(s,t)$是以 s 为初始状态 M 所有可能的 t 长输出的个数。

定义 5 设 $M=<X,Y,S,\delta,\lambda>$是一个有限自动机，且 t 是正整数，$\forall s,s'\in S$ 都有 $O_M(s,t)=O_M(s',t)$，则记 $O_M(t)=O_M(s,t)$。

定义 6 设 $s\in S$，$\forall y_1y_2\cdots y_t\in Out_M(s,t)$，记 $In_M(s,y_1y_2\cdots y_t)=\{x_1x_2\cdots x_t\in X^t|\lambda(s,x_1x_2\cdots x_t)=y_1y_2\cdots y_t\}$，$In_M(s,y_1y_2\cdots y_t)$是以 s 为初始状态，使得 M 输出为 $y_1y_2\cdots y_t$的所有的 t 长输入的集合。

引理 1[8] 设 $M=<X,Y,S,\delta,\lambda>$是一个线性 FA，$\forall s\in S,y_1y_2\cdots y_t,y_1'y_2'\cdots y_t'\in Out_M(s,t)$，有$|In_M(s,y_1y_2\cdots y_t)|=|In_M(s,y_1'y_2'\cdots y_t')|$，这时记 $I_M(s,t)=|In_M(s,y_1y_2\cdots y_t)|$，$y_1y_2\cdots y_t\in Out_M(s,t)$。

引理 2[8] 设 $M=<X,Y,S,\delta,\lambda>$是一个线性 FA，$\forall s,s'\in S$，有 $I_M(s,t)=I_M(s',t)$。

引理 3[8] 设 $M=<X,Y,S,\delta,\lambda>$是输入输出均匀的，则有 $O_M(t)\cdot I_M(t)=|X|^t$，其中$|X|$表示 X 的元素的个数。

定义 7 如果一个自动机满足引理 1 和引理 2 的后半部分条件，则记 $I_M(t)=|In_M(s,y_1y_2\cdots y_t)|$，$y_1y_2\cdots y_t\in Out_M(s,t)$。

定义 8 设 $M=<X,Y,S,\delta,\lambda>$是一个有限自动机，则称 M 是延迟 τ 步弱可逆的，若对 $\forall s\in S,a,a'\in X,\alpha,\alpha'\in X^*$，$|\alpha|=|\alpha'|=\tau$ 都有 $\lambda(s,a\alpha)=\lambda(s,a'\alpha')$推出 $a=a'$。

3　关于线性有限自动机输入输出集的一些结果

命题 1 设 $M_1=<X,X,S_1,\delta_1,\lambda_1>$，$M_2=<X,X,S_2,\delta_2,\lambda_2>$分别是 $GF(q)$上两个线性有限自动机，记 $M=M_1\cdot M_2=<X,X,S_1\times S_2,\delta,\lambda>$，则 $\forall s,s'\in S=S_1\times S_2$，都有 $O_M(s,t)=O_M(s',t)$。

证明 $\forall s\in S$，记 $s=\langle s_1,s_2\rangle$，$s_1\in S_1,s_2\in S_2$，并记 X,S 的零向量 x_0,s_0，记 S_1,S_2的零向量 s_0^1,s_0^2，记长度为 t 的 x_0 输入序列 x_0^t。由于 λ_1,λ_2 为线性映射，则对 $\forall x_1,x_2,\cdots,x_t\in X$，$\lambda(s,x_1x_2\cdots x_t)=\lambda(\langle s_1,s_2\rangle,x_1x_2\cdots x_t)=\lambda_2(s_2,\lambda_1(s_1,x_1x_2\cdots x_t))=\lambda_2(s_0^2+s_2,\lambda_1(s_1,x_1x_2\cdots x_t)+\lambda_1(s_0^1,x_0^t))=\lambda_2(s_0^2,\lambda_1(s_1,x_1x_2\cdots x_t))+\lambda_2(s_2,\lambda_1(s_0^1,x_0^t))=\lambda_2(s_0^2+s_0^2,\lambda_1(s_0^1,x_1x_2\cdots x_t)+\lambda_1(s_1,x_0^t))+\lambda_2(s_2,\lambda_1(s_0^1,x_0^t))=\lambda_2(s_0^2,\lambda_1(s_0^1,x_1x_2\cdots x_t))+\lambda_2(s_0^2,\lambda_1(s_1,x_0^t))+\lambda_2(s_2,\lambda_1(s_0^1,x_0^t))=\lambda_2(s_0^2,\lambda_1(s_0^1,x_1x_2\cdots x_t))+\lambda_2(s_0^2+s_2,\lambda_1(s_1,x_0^t)+\lambda_1(s_0^1,x_0^t))=\lambda(\langle s_0^1,s_0^2\rangle,x_1x_2\cdots x_t)+\lambda_2(s_2,\lambda_1(s_1,x_0^t))=\lambda(\langle s_0^1,s_0^2\rangle,x_1x_2\cdots x_t)+\lambda(\langle s_1,s_2\rangle,x_0^t)=\lambda(s_0,x_1x_2\cdots x_t)+\lambda(s,x_0^t)$。

即 $\forall s\in S$，$\lambda(s,x_1x_2\cdots x_t)=\lambda(s_0,x_1x_2\cdots x_t)+\lambda(s,x_0^t)$，由于 x_0^t为零输入数列，$\lambda(s,x_0^t)$为常输出序列，状态 s,s_0的输出一一对应，因此 $O_M(s,t)=O_M(s_0,t)$，有 s 的任意性，故结论成立。

命题 2 设 $M_1=<X,Y,S_1,\delta_1,\lambda_1>$，$M_2=<X,X,S_2,\delta_2,\lambda_2>$分别是 $GF(q)$上两个线性有限自动机，记 $M=M_1\cdot M_2=<X,X,S_1\times S_2,\delta,\lambda>$，则对任意$\langle s_1,s_2\rangle\in S_1\times S_2$，$s_1\in S_1,s_2\in S_2$，$\forall y_1y_2\cdots y_t\in Out_M(\langle s_1,s_2\rangle,t)$都有

$$\left|In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)\right|=\left|In_M(\langle s_0^1,s_0^2\rangle,x_0^t)\right|$$

证明 $\forall x_1x_2\cdots x_t,x_1'x_2'\cdots x_t'\in In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)$，即 $\lambda(\langle s_1,s_2\rangle,x_1x_2\cdots x_t)=\lambda(\langle s_1,s_2\rangle,x_1'x_2'\cdots x_t')=y_1y_2\cdots y_t$，则有 $\lambda_2(s_2,\lambda_1(s_1,x_1x_2\cdots x_t))=\lambda_2(s_2,\lambda_1(s_1,x_1'x_2'\cdots x_t'))\Rightarrow\lambda_2(s_2-s_2,\lambda_1(s_1,x_1x_2\cdots x_t)-\lambda_1(s_1,x_1'x_2'\cdots x_t'))=x_0^t\Rightarrow\lambda_2(s_0^2,\lambda_1(s_0^1,x_1x_2\cdots x_t-x_1'x_2'\cdots x_t'))=x_0^t$，即 $\lambda(\langle s_0^1,s_0^2\rangle,x_1x_2\cdots x_t-x_1'x_2'\cdots x_t')=x_0^t$。从而 $x_1x_2\cdots x_t-x_1'x_2'\cdots x_t'\in In_M(\langle s_0^1,s_0^2\rangle,x_0^t)$，并且易知 $x_0^t\in In_M(\langle s_0^1,s_0^2\rangle,x_0^t)$，故有$\left|In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)\right|\leqslant\left|In_M(\langle s_0^1,s_0^2\rangle,x_0^t)\right|$。

另一方面 $\forall x_1x_2\cdots x_t\in In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)$及 $x_1'x_2'\cdots x_t'\in In_M(\langle s_0^1,s_0^2\rangle,x_0^t)$则有 $x_1x_2\cdots x_t+x_1'x_2'\cdots x_t'\in In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)$。

这是因为

$$\begin{aligned}&\lambda(\langle s_1,s_2\rangle,x_1x_2\cdots x_t)+\lambda(\langle s_0^1,s_0^2\rangle,x_1'x_2'\cdots x_t')=\\&\lambda_2(s_2,\lambda_1(s_1,x_1x_2\cdots x_t))+\lambda_2(s_0^2,\lambda_1(s_0^1,x_1'x_2'\cdots x_t'))=\\&\lambda_2(s_2+s_0^2,\lambda_1(s_1,x_1x_2\cdots x_t)+\lambda_1(s_0^1,x_1'x_2'\cdots x_t'))=\\&\lambda_2(s_2,\lambda_1(s_1,x_1x_2\cdots x_t+x_1'x_2'\cdots x_t'))=\\&\lambda_2(\langle s_1,s_2\rangle,x_1x_2\cdots x_t+x_1'x_2'\cdots x_t'))\end{aligned}$$

故有$\left|In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)\right|\geqslant\left|In_M(\langle s_0^1,s_0^2\rangle,x_0^t)\right|$。

综上，$\left|In_M(\langle s_1,s_2\rangle,y_1y_2\cdots y_t)\right|=\left|In_M(\langle s_0^1,s_0^2\rangle,x_0^t)\right|$，再由$\langle s_1,s_2\rangle$的任意性和 $y_1y_2\cdots y_t$的任意性知结论成立。

由命题 1、2 知两个输入输出集相同的线性有限自动机的化合后得到的自动机是输入输出均匀的。

命题 3 设 $M=<X,X,S,\delta,\lambda>$是 $GF(q)$上延迟一步线性有限自动机，则对 $s\in S$，$\forall y\in Out_M(s,1)$，记 $In_M(s,y)=\{x_1,x_2,\cdots,x_m\}$，$s$ 的 m 个后继 $\delta(s,x_1),\delta(s,x_2),\cdots,\delta(s,x_m)$的输出集相交为空，并集为 X。

证明 M 是线性有限自动机，由文献[8]的定理 1 知 M 的每个状态长为 1 的输出集有 $O_M(1)$个元素，特别地 s 的 m 个后继

长为1的输出集有$O_M(1)$个元素。

假设$\delta(s,x_i)$与$\delta(s,x_j)(i\neq j)$的输出集相交,则存在$x,x'\in X$使$\lambda(\delta(s,x_j),x)=\lambda(\delta(s,x_j),x')=y'$,故有$\lambda(s,x_jx)=\lambda(s,x_jx')=yy'$,由于$M$是延迟1步弱可逆,则有$x_i=x_j$矛盾,故$s$的$m$个后继输出集不相交。

又由引理1、2知$|In_M(s,y)|=I_M(1)=m$,故这些状态的输出集的个数为$I_M(1)\times O_M(1)$,又由引理3知$I_M(1)\times O_M(1)=|X|$,综上知结论成立。

定理1 设$M_1=<X,X,S_1,\delta_1,\lambda_1>,M_2=<X,X,S_2,\delta_2,\lambda_2>$分别是$GF(q)$上两个延迟一步弱可逆线性有限自动机,记$M=M_1\cdot M_2=<X,X,S_1\times S_2,\delta,\lambda>$,则$I_M(2)=I_{M_1}(1)\times I_{M_2}(1)$。

证明 由命题2知$I_M(2)=|In_M(\langle s_0^1,s_0^2\rangle,x_0^2)|$,下面讨论$In_M(\langle s_0^1,s_0^2\rangle,x_0^2)$中元素的个数。

$x_0\in Out_M(\langle s_0^1,s_0^2\rangle,1)$,由$\lambda$得定义及$\lambda_2$为线性有限自动机,至少存在$x_0\in Out_{M_1}(s_0^1,1)$使$\lambda_2(s_0^2,x_0)=x_0$,对$x_0$(看成$Out_{M_1}(s_0^1,1)$中的元素),由引理1及引理2知存在$I_{M_1}(1)$个元素$x_1x_2\cdots x_{m_1}$(其中$m_1=I_{M_1}(1)$,有一个为$x_0$)使$\lambda_1(s_0^1,x_i)=x_0$,$1\leqslant i\leqslant m_1$。对$s_0=\langle s_0^1,s_0^2\rangle$的$m_1$个后继分别记为$\delta(s_0,x_1),\delta(s_0,x_2),\cdots,\delta(s_0,x_{m_1})$,即为$\langle\delta_1,(s_0^1,x_1),\delta_2(s_0^2,\lambda_1(s_0^1,x_1))\rangle,\langle\delta_1,(s_0^1,x_2),\delta_2(s_0^2,\lambda_1(s_0^1,x_2))\rangle,\cdots,\langle\delta_1,(s_0^1,x_{m_1}),\delta_2(s_0^2,\lambda_1(s_0^1,x_{m_1}))\rangle$,即为$\langle\delta_1,(s_0^1,x_1),\delta_2(s_0^2,x_0)\rangle,\langle\delta_1,(s_0^1,x_2),\delta_2(s_0^2,x_0)\rangle\cdots\langle\delta_1,(s_0^1,x_{m_1}),\delta_2(s_0^2,x_0)\rangle$。由于$M_1$是线性有限自动机,由文献[8]的定理1知$M_1$的每个状态长为1的输出集都有$O_{M_1}(1)$个元素。由$M_2$是线性有限自动机,则$\delta_2(s_0^2,x_0)=s_0^2$长为1的输出集都有$O_{M_2}(1)$个元素,在开始已经取定一个为$x_0$。

下面证明$|In_M(\langle s_0^1,s_0^2\rangle,x_0^2)|=I_M(2)=I_{M_1}(1)\times I_{M_2}(1)$。由$M_2$是线性有限自动机,$|In_{M_2}(\delta_2\langle s_0^2,x_0\rangle,x_0)|=|In_{M_2}(s_0^2,x_0)|=In_{M_2}(1)$(这里用到$\delta_2\langle s_0^2,x_0\rangle=s_0^2$)。由命题3知$\delta_1(s_0^1,x_1),\delta_1(s_0^1,x_{m_1}),\cdots,\delta_1(s_0^1,x_{m_1})$的输出集不相交,并且并集为$X$,从而可以保证$\lambda_2$的输入可以全部取到。对于$In_{M_2}(\delta_2\langle s_0^2,x_0\rangle,x_0)$中的元素$y$,在上述状态中有且只有一个状态$s'$使得$y$是$s'$的输出元,并且在$X$中存在$I_{M_1}(1)$个元素使得$\lambda_1(s',x)=y$,因此当$M$的状态是$\langle s_0^1,s_0^2\rangle$时有$I_{M_1}(1)\times I_{M_2}(1)$个长为2的输入序列使$\lambda(\langle s_0^1,s_0^2\rangle,\alpha)=x_0x_0$。

另一方面假设X中有x'使$\lambda(\langle s_0^1,s_0^2\rangle,x')=\lambda_2(s_0^2,\lambda_1(s_0^1,x'))=\lambda_2(s_0^2,y_1)=x_0$,并且$x_0$是$\langle s_0^1,s_0^2\rangle$的后继$\langle\delta_1(s_0^1,x'),\delta_2(s_0^2,y_1)\rangle$的输出集中的一个元素,由$\lambda$的定义,那么必存在$y_2\in X$使得$\lambda_2(\delta_2(s_0^2,y_1),y_2)=x_0$,因此有$\lambda_2(s_0^2,y_1y_2)=x_0x_0$,又存在$y^*\in In_{M_2}(\delta_2\langle s_0^2,x_0\rangle,x_0)$使得$\lambda_2(s_0^2,x_0y^*)=x_0x_0$,由$M_2$延迟1步弱可逆,故有$y_1=x_0$,从而$\lambda_1(s_0^1,x')=x_0$,这就说明$x'$在集合$\{x_1,x_2,\cdots,x_{m_1}\}$中,综上可得$I_M(2)=|In_M(\langle s_0^1,s_0^2\rangle,x_0^2)|=I_{M_1}(1)\times I_{M_2}(1)$,从而结论成立。

4 结论

综上讨论,证明了两个线性有限自动机的化合而得到的自动机是输入输出均匀的,还建立了两个延迟1步弱可逆线性有限自动化合后得到的自动机的输入集个数与化合前自动机输入集个数的等式关系,即化合后自动机的长为2的输入集个数用化合前自动机长为1的输入集个数表示,这对研究复杂自动机的性质具有较高的参考价值。对于更一般的情况,延迟2步以上弱可逆化合后的长度大于2的自动机输入集个数与化合前自动机输入集个数的关系有待进一步研究。

参考文献:

[1] 陶仁骥.自动机引论[M].北京:科学出版社,1986.

[2] 陶仁骥.有限自动机的可逆性[M].北京:科学出版社,1979.

[3] 鲍丰.弱可逆有限自动机的化合与分解[J].中国科学:A辑,1995,23(7):759-765.

[4] Tao Renji,Chen Shihua.Two varieties of finite automata public key cryptosystem and digitial signature[J].J of Computer Science and Technology,1986,1(1):9-18.

[5] 陶仁骥,陈世华.基于身份的密码体制和数字签名的有限自动机公开钥密码实现[C]//密码学进展—CHINACRYPT'92.北京:科学出版社,1992:87-104.

[6] Tao Renji,Chen Shihua,Chen Xuemei.FAPKC3:A new finite automaton public key cryptosystem[J].Computer Science and Technology,1997,4(12):289-305.

[7] Tao Renji,Chen Shihua.Input-trees of finite automata and application to cryptanalysis[J].Computer science and Technology,2000,15(4):305-325.

[8] 鲍丰.线性有限自动机的递增秩与FA公开钥密码体制的复杂性[J].中国科学:A辑,1994,24(2):193-200.

[9] Tao Renji,Chen Shihua.Structure of weakly invertible semi-input-memory finite automata with delay 1[J].Computer Science and Technology,2002,17(4):369-376.

[10] Tao Renji,Chen Shihua.Structure of weakly invertible semi-input-memory finite automata with delay 2[J].Computer Science and Technology,2002,17(6):682-688.

[11] 姚刚.有限自动机可逆性的若干结果[D].中国科学院研究生院,2003.

[12] 陈世华.关于弱可逆线性有限自动机的弱逆结构[J].计算机学报,1981(6):409-419.

[13] 吕书志.环上线性有限自动机的可逆性的一些结果[J].计算机学报,1991(8):570-578.

[14] 谢正卫,邓培民,易忠.线性有限自动机的同步序列及其生成算法[J].计算机工程与应用,2006,42(24):34-38.

[15] 谢正卫,邓培民,易忠.线性有限自动机的UIO序列及其生成算法[J].计算机工程与应用,2007,43(2):49-52.