一类约化梯阵的 R_aR_b 表示*

王 浩

(中国科学院软件研究所 北京 100080)

摘要 本文首先阐明线性 R_aR_b 变换之间的关系,并提出了算法 MR_{ab},再引用标准线性 R_aR_b 变换,证明了 R_aR_b 变换与算法 MR_{ab} 求解方程组的能力是等价的. 然后讨论 MR_{ab} 与算法 ALT 之间的关系,进而说明受 ALT 攻击的那些有限自动机包含在线性 R_aR_b 类中.

关键词 算法,有限自动机,约化梯阵,线性 R_aR_b 变换.

中图法分类号 TP301.1

文献[1]详细讨论了线性及非线性 R_aR_b 变换,用于一类有限自动机(FA)的弱可逆性的判定及求弱逆. FAPKC3[2]作为一种公开钥密码体制,在具体实现时,密钥生成器(Key Generator)中有检测过程(Check Process),用于把可由线性 R_aR_b 方法求弱逆的 FA(本文称所有这样的 FA 之集为线性 R_aR_b 类)筛出去.

文献[3]提出了一个密码攻击算法 ALT,用于分析有限自动机公开钥密码体制. 该算法基于一种矩阵类型的约化梯阵形式.

基于自然形式系数矩阵的约化梯阵形式,本文提出了算法 MR_{ab}. 在阐明不同线性 R_aR_b 变换之间的关系的基础上,用文献[4]中的标准线性 R_aR_b 变换的术语,证明了 R_aR_b 变换与算法 MR_{ab} 求解方程组的能力是等价的. 然后讨论 ALT 与 MR_{ab} 的关系,进而说明 ALT 攻击的那些 FA 包含在线性 R_aR_b 类中.

1 一些准备

我们是在有限域 $GF(q)$ 上进行讨论. 设 A 为一个矩阵,对 A 的任一非零行,第 1 个非零元称为该行的首元(Leading Entry of the Row). 若 A 的前 r 行非零,其它行全零,且第 $1\sim r$ 行的首元所在的列 $t_1,\ldots,t_r$ 满足 $t_1<\ldots<t_r$,则称 A 为梯阵(Echelon Matrix). 进而,如果每个首元为 1,且每个首元 1 所在的列的其它元全零,则称这样的 A 为约化梯阵(Reduced Echelon Matrix).[5]

引理 1.[5] 任何矩阵可经有限次初等行变换化为约化梯阵. 且约化梯阵是唯一的.

设 X 和 Y 分别为 $GF(q)$ 上 l 和 m 维向量空间. 考虑 (h,k) 阶存储 FA M,其输出 y_i 由

---

* 本文研究得到国家自然科学基金和中国科学院"八五"重点科研项目基金资助. 作者王浩,1963 年生,博士,主要研究领域为计算机科学理论,密码学及其应用,软件系统和工程.

本文通讯联系人:王浩,北京 100038,海淀区羊坊店西路 5 号国家税务总局信息中心

本文 1996-11-15 收到修改稿

$eq_0(i)$:　　$f_0(x_i,\ldots,x_{i-h},y_i,\ldots,y_{i-k})=0$

决定. 而 $f_0(i)=f_0(x_i,\ldots,x_{i-h},y_i,\ldots,y_{i-k})$ 展开后的矩阵形式为

$$f_0(i)=\sum_{j=0}^{h}B_{j0}\psi(x_{i-j},\ldots,x_{i-j-h'})+\sum_{j=0}^{k}A_{j0}\varphi(y_{i-j},\ldots,y_{i-j-k'})+C_{00} \tag{1}$$

其中 $0\leqslant h'\leqslant h, 0\leqslant k'\leqslant k$, $x_{-h-1},\ldots,x_{-h-k}$ 及 $y_{-k-1},\ldots,y_{-k-k'}$ 为哑变元. C_{00} 为 m 维列向量. $\psi(x_{i-j},\ldots,x_{i-j-h'})$ 是由 $x_{i-j},\ldots,x_{i-j-h'}$ 的分量的所有可能的单项式(至少含有 x_{i-j} 的某个分量)组成的 L 维列向量. $\varphi(y_{i-j},\ldots,y_{i-j-k'})$ 是由 $y_{i-j},\ldots,y_{i-j-k'}$ 的分量的所有可能的单项式(至少含有 y_{i-j} 的某个分量)组成的 L' 维列向量. B_{i0} 和 A_{j0} 分别是 $m\times L$ 和 $m\times L'$ 阶矩阵. $i=0,\ldots,h, j=0,\ldots,k$.

对 $c=0,1,\ldots$, 分别记 $f_c(i)=f_c(x_i,\ldots,x_{i-h},y_{i+c},\ldots,y_{i-k})$ 和 $f'_c(i)=f'_c(x_i,\ldots,x_{i-h},y_{i+c},\ldots,y_{i-k})$ 为

$$f_c(i)=\sum_{j=0}^{h}B_{jc}\psi(x_{i-j},\ldots,x_{i-j-h'})+\sum_{j=-c}^{k}A_{jc}\varphi(y_{i-j},\ldots,y_{i-j-k'})+C_{0c} \tag{2}$$

和　　$f'_c(i)=\sum_{j=0}^{h}B'_{jc}\psi(x_{i-j},\ldots,x_{i-j-h'})+\sum_{j=-c}^{k}A'_{jc}\varphi(y_{i-j},\ldots,y_{i-j-k'})+C'_{0c}$　　(3)

而记矩阵方程 $eq_c(i)$ 和 $eq'_c(i)$ 分别为 $f_c(i)=0$ 和 $f'_c(i)=0$. 如果 $eq'_c(i)$ 是由可逆矩阵 P_c 左乘方程 $eq_c(i)$ 两边所得, 使 B'_{0c} 的前 r_c 行线性无关, 且后 $m-r_c$ 行为 0, 则称 $eq_c(i)$ 经一次线性 R_a 变换得 $eq'_c(i)$, 并称 $eq'_c(i)$ 经一次线性 R_b 变换得 $eq_{c+1}(i)$: $\begin{bmatrix}E'_cf'_c(i)\\E''_cf'_c(i+1)\end{bmatrix}=0$. 其中 E'_c 和 E''_c 分别为 m 阶单位矩阵 E_m 的前 r_c 行和后 $m-r_c$ 行子矩阵. 此时, 我们称 $eq_c(i)$ 经一次线性 R_aR_b 变换得 $eq_{c+1}(i)$. 并记为

$$eq_c(i)\overset{R_a[P_c]}{\rightarrow}eq'_c(i)\overset{R_b[r_c]}{\rightarrow}eq_{c+1}(i).$$

已知FA M 在状态 $s=[x_{i-1},\ldots,x_{i-h},y_{i-1},\ldots,y_{i-k}]^T$ 下有输出 $y_i\ldots y_{i+\tau}$, 则输入变元 $x_i,\ldots,x_{i+\tau}$ 满足方程组

$$\begin{cases}eq_0(i+\tau)\\\ldots\\eq_0(i)\end{cases} \tag{4}$$

设

$$eq_0(i)\overset{R_a[P_0]}{\rightarrow}eq'_0(i)\overset{R_b[r_0]}{\rightarrow}eq_1(i)\rightarrow\ldots\rightarrow eq_\tau(i)\overset{Ra[P_\tau]}{\rightarrow}eq'_\tau(i)\overset{R_b[r_\tau]}{\rightarrow}eq_{\tau+1}(i) \tag{5}$$

为任意线性 R_aR_b 变换序列, 则文献[1]中性质(g)给出

引理 2.[1] 方程组(4)等价于方程组

$$\begin{cases}E'_0eq'_0(i+\tau)\\\ldots\\E'_\tau eq'_\tau(i)\\E''_\tau eq'_\tau(i)\\\ldots\\E''_0eq'_0(i)\end{cases} \tag{6}$$

2 不同线性 R_aR_b 变换之间的关系

令
$$\Gamma=\begin{bmatrix} B_{00} & \cdots & \cdots & B_{h0} & & A_{00} & \cdots & \cdots & A_{h0} & & C_{00} \\ & \ddots & & & \ddots & & \ddots & & & \ddots & \vdots \\ & & B_{00} & \cdots & \cdots & B_{h0} & & A_{00} & \cdots & \cdots & A_{h0} & C_{00} \end{bmatrix} \tag{7}$$

$$Z=[\psi(x_{i+\tau},\ldots,x_{i+\tau-h'}),\ldots,\psi(x_{i-h},\ldots,x_{i-h-h'}),\varphi(y_{i+\tau},\ldots,y_{i+\tau-k'}),\ldots,\varphi(y_{i-k},\ldots,y_{i-k-k'}),1]^T \tag{8}$$

其中转置符号 T 表示 Z 是按各分量顺序排放的列向量. 于是方程组(4)可写为

$$\Gamma Z=0$$

令 $\Gamma'=$

$$\begin{bmatrix} E'_0B'_{00} & \cdots & \cdots & \cdots & E'_0B'_{h0} & & & E'_0A'_{00} & \cdots & \cdots & E'_0A'_{h0} & & E'_0C'_{00} \\ & \ddots & & & & \ddots & & \vdots & & & & \ddots & \vdots \\ & & E'_\tau B'_{0\tau} & E'_\tau B'_{1\tau} & \cdots & \cdots & E'_\tau B'_{h\tau} & E'_\tau A'_{-\tau,\tau} & \cdots & \cdots & \cdots & \cdots & E'_\tau A'_{h\tau} & E'_\tau C'_{0\tau} \\ & & E''_\tau B'_{1\tau} & \cdots & \cdots & E''_\tau B'_{h\tau} & E''_\tau A'_{-\tau,\tau} & \cdots & \cdots & \cdots & \cdots & E''_\tau A'_{h\tau} & E''_\tau C'_{0\tau} \\ & & \vdots & & & \vdots & & \ddots & & & & \vdots & \vdots \\ & & E''_0B'_{10} & \cdots & \cdots & E''_0B'_{h0} & & & E''_0A'_{00} & \cdots & \cdots & E''_0A'_{h0} & E''_0C'_{00} \end{bmatrix} \tag{9}$$

则方程组(6)可写为 $\Gamma' Z=0$

且 Γ' 是由 Γ 经一系列初等行变换所得. 而对 Γ' 再施行初等行变换可化为约化梯阵 Γ'',具体地说,可选取 $m(\tau+1)$ 阶可逆矩阵

$$P=\begin{bmatrix} P_{00} & \cdots & P_{0\tau} & P_{0,\tau+1} \\ & \ddots & \vdots & \vdots \\ & & P_{\tau\tau} & P_{\tau,\tau+1} \\ & & & P_{\tau+1,\tau+1} \end{bmatrix} \tag{10}$$

使
$$\Gamma''=P\Gamma' \tag{11}$$

为 Γ 的约化梯阵,其中 P_{cc} 为 r_c 阶可逆矩阵,使 $P_{cc}E'_cB'_{0c}$ 为约化梯阵,r_c 为 E'_c 的行数,$c=0,\ldots,\tau$. 而 $P_{\tau+1,\tau+1}$ 为 $\Sigma_{c=0}^{\tau}(m-r_c)\times\Sigma_{c=0}^{\tau}(m-r_c)$ 阶可逆矩阵.

由引理 1 知,Γ 无论经过怎样的初等行变换,其约化梯阵是唯一的,都是 Γ''. 于是有引理 2 的一个简单推论.

推论 1. 设 FA M 在一个线性 R_aR_b 变换下对应的 E'_c 行数为 r_c,而在另一个线性 R_aR_b 变换下对应的 $\bar{E}'_c$ 的行数为 $\bar{r}_c$,则 $r_c=\bar{r}_c, c=0,\ldots,\tau$.

一般地,考虑到 τ 是任取的非负整数,也称 r_τ 为 FA M 的 τ 次约化秩[6]或第 τ 个递增秩[7],$\tau=0,1,\ldots$.

设 I 是矩阵 Γ 的行指标集$\{1,2,\ldots,m(\tau+1)\}$的一个子集,则 Γ 的对应于 I 的所有行构成的子矩阵记为 $\Gamma_{I,*}$,本文也简记为 Γ_I. 由引理 2,并考虑到 $E'_ceq'_c(0), c=0,\ldots,\tau$ 中不含变元 $x_i,\ldots,x_{i+\tau}$,则得

引理 3. 设 M 是(h,k)阶存储 FA,其输出 y_i 由 $eq_0(i)$决定. 已知 FA M 在状态 $s=[x_{i-1},\ldots,x_{i-h},y_{i-1},\ldots,y_{i-k}]^T$ 下有输出 $y_i\ldots y_{i+\tau}$. 则对任意线性 R_aR_b 变换序列(5),

(a) $E''_cf'_c(i)\equiv 0$,这里 $f'_c(i)$为 $eq'_c(i)$的左端,$c=0,\ldots,\tau$.

(b) 输入变元 $x_i,\ldots,x_{i+\tau}$适合方程组(4)当且仅当 $x_i,\ldots,x_{i+\tau}$适合方程组

$$\begin{cases} E'_0 eq'_0(i+\tau) \\ \cdots \\ E'_\tau eq'_\tau(i) \end{cases} \tag{12}$$

引理 4. 设
$$I=\left\{\sum_{c=0}^{\tau-1} r_c+i; i=1,\ldots,r_\tau\right\} \tag{13}$$

$$J=\left\{\sum_{c=0}^{\tau} r_c+i; i=1,\ldots,m(\tau+1)-\sum_{c=0}^{\tau} r_c\right\} \tag{14}$$

而 Γ'，Γ''和 J 分别见(9)、(10)和(14)，则存在 $r_\tau\times\Sigma_{c=0}^{\tau}(m-r_c)$阶矩阵 $P_{\tau,\tau+1}$及 r_τ 阶可逆矩阵 $P_{\tau\tau}$，使
$$\Gamma''_I=P_{\tau\tau}\Gamma'_I+P_{\tau,\tau+1}\Gamma'_J \tag{15}$$
特别在引理 3 的条件下，　$\Gamma''_I Z=P_{\tau\tau}\Gamma'_I Z=P_{\tau\tau}E'_\tau f'_\tau(i)$

定理 1. 设 $eq'_\tau(i)$及$\overline{eq}'_\tau(i)$都是由 $eq_0(i)$经线性 R_aR_b 变换所得，$f'_\tau(i)$和 $\overline{f}'_\tau(i)$分别为 $eq'_\tau(i)$和$\overline{eq}'_\tau(i)$的左端，则存在 r_τ 阶可逆矩阵 Q 及函数 g，使
$$E'_\tau f'_\tau(i)-Q\cdot E'_\tau\overline{f}'_\tau(i)=g(x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k})$$
且在引理 3 的条件下，　$g(x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k})\equiv 0$

证明：根据引理 4 的(15)式，分别存在 r_τ 阶可逆矩阵 $P_{\tau\tau}$和 $\overline{P}_{\tau\tau}$及 $r_\tau\times\Sigma_{c=0}^{\tau}(m-r_c)$阶矩阵 $P_{\tau,\tau+1}$和 $\overline{P}_{\tau,\tau+1}$，使 $\Gamma''_I=P_{\tau\tau}\Gamma'_I+P_{\tau,\tau+1}\Gamma'_J$　　$\Gamma''_I=\overline{P}_{\tau\tau}\overline{\Gamma}'_I+\overline{P}_{\tau,\tau+1}\overline{\Gamma}'_J$
这里 Γ''是 Γ 的唯一约化梯阵，取 $Q=P_{\tau\tau}^{-1}\overline{P}_{\tau\tau}$，则 $\Gamma'_I-Q\overline{\Gamma}'_I=-P_{\tau\tau}^{-1}P_{\tau,\tau+1}\Gamma'_J+P_{\tau\tau}^{-1}\overline{P}_{\tau,\tau+1}\overline{\Gamma}'_J$. 故 $E'_\tau f'_\tau(i)-Q\cdot E'_\tau\overline{f}'_\tau(i)=\Gamma'_I Z-Q\overline{\Gamma}'_I Z=-P_{\tau\tau}^{-1}P_{\tau,\tau+1}\Gamma'_J Z+P_{\tau\tau}^{-1}\overline{P}_{\tau,\tau+1}\overline{\Gamma}'_J Z$. 上式右边是 $x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k}$的函数，记为 $g(x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k})$. 且在引理 3 的条件下，$g(x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k})\equiv 0$.

3　改进的算法 MR_{ab}及其输出的 R_aR_b 表示

为了考察算法 ALT[3]的攻击能力，我们先给出并考察算法 MR_{ab}.

算法 MR_{ab}. 对方程组(4)的系数矩阵 Γ 施行初等行变换化为约化梯阵 Γ''，并输出 Γ''_I，其中 I 见(13)式.

由算法 MR_{ab}的输出 Γ''_I 构作的方程组为 $\Gamma''_I Z=0$.

设 Γ'，Γ''，I 和 J 分别见公式(9)、(11)、(13)和(14)，则实际上，Γ'_I 和 Γ''_I 分别是 Γ'和 Γ''的这样的子矩阵，由 Γ'和 Γ''的第 $1\sim\tau L$ 列全零且第 $\tau L+1\sim(\tau+1)L$ 列非零的元所在的行构成. Γ'_J 和 Γ''_J 分别是 Γ'和 Γ''的这样的子矩阵，由 Γ'和 Γ''的第 $1\sim(\tau+1)L$ 列全零的行构成. 于是由引理 1 和引理 2 容易证得：

引理 5. 设 FA M 的第 τ 个递增秩为 r_τ，记 $\Gamma''_I=[0\ldots0\ B''_{0\tau}\ldots B''_{h\tau}A''_{-\tau,\tau}\ldots A''_{k\tau}C''_{0\tau}]$，其中 Γ''_I 的前 τL 列为零矩阵，则秩 $B''_{0\tau}=r_\tau$. 即对方程组(4)的系数矩阵 Γ 施行初等行变换所导出的含且只含变元 x_i 及参数 $x_{i-1},\ldots,x_{i-h},y_{i+\tau},\ldots,y_{i-k}$的全体方程组的系数矩阵的秩为 r_τ.

我们使用文献[4]中的标准线性 R_aR_b 变换的术语. 对 $c=0,1,\ldots$，设 $eq_c(i)\xrightarrow{R_a[P_c]}eq'_c(i)\xrightarrow{R_b[r_c]}eq_{c+1}(i)$为一次线性 R_aR_b 变换，如果 $eq'_c(i)$的系数矩阵$[B'_{0c}\ldots B'_{hc}A'_{-cc}\ldots A'_{kc}C'_{0c}]$为

约化梯阵，则称所用的线性 R_aR_b 变换为标准线性 R_aR_b 变换（见文献[4]），并记为 $EQ_c(i)\xrightarrow{R_a[P_{c^-}]}EQ'_c(i)\xrightarrow{R_b[r_c]}EQ_{c+1}(i)$，$c=0,1,\ldots$，其中 $EQ_0(i)$ 就是 $eq_0(i)$；$f_0(i)=0$，这里 $f_0(i)$ 见(1)式.

用标准线性 R_aR_b 变换的术语重述引理2，即方程组(4)等价于方程组

$$\begin{cases} E'_0EQ'_0(i+\tau) \\ \cdots \\ E'_\tau EQ'_\tau(i) \\ E''_\tau EQ'_\tau(i) \\ \cdots \\ E''_0EQ'_0(i) \end{cases} \tag{16}$$

并把方程组(16)也写成矩阵形式　　$\overline{\Gamma}Z=0$

其中 $\overline{\Gamma}$ 形如(9)式，$\overline{\Gamma}_IZ=E'_\tau F'_\tau(i)$，且在引理3的条件下，$\overline{\Gamma}_JZ\equiv 0$. 对 $\overline{\Gamma}$ 再施行初等行变换所得约化梯阵仍为 Γ''，见(11)式. 且存在可逆矩阵 $\overline{P}$ 形如(10)式，只是把(10)式中的 P_{ij} 替换为 $\overline{P}_{ij}$，$i,j=0,\ldots,\tau+1$，且 $i\leqslant j$，使　　$\Gamma''=\overline{P}\overline{\Gamma}$

因 $E'_\tau EQ'_c(\tau-c)$ 中 $\psi(x_{\tau-c},\ldots,x_{\tau-c-K})$ 的系数矩阵已为约化梯阵，故可取 $\overline{P}_{cc}=E_{r_c}$，取 r_c 为 E'_c 的行数，则 r_c 为 M 的第 c 个递增秩，$c=0,1,\ldots,\tau$. 于是由(15)式得：

引理6. 算法 MR_{ab} 的输出为　　$\Gamma''_I=\overline{\Gamma}_I+\overline{P}_{\tau,\tau+1}\overline{\Gamma}_J$　　(17)

其中 $\overline{P}_{\tau,\tau+1}$ 为 $r_\tau\times\sum_{c=0}^{\tau}(m-r_c)$ 阶矩阵.

定理2. 条件同引理3，由算法 MR_{ab} 的输出构作的方程组可由标准线性 R_aR_b 变换得到. 即

$$\Gamma''_IZ=E'_\tau F'_\tau(i)$$

其中 $F'_\tau(i)$ 为 $EQ'_\tau(i)$ 的左端.

证明：由引理6，MR_{ab} 的输出为(17)式，于是 $\Gamma''_IZ=\overline{\Gamma}_IZ+\overline{P}_{\tau,\tau+1}\overline{\Gamma}_JZ=\overline{\Gamma}_IZ=E'_\tau F'_\tau(i)$.

4　算法 MR_{ab} 与线性 R_aR_b 变换的等价性

定理3. 条件同引理3，设 $f'_\tau(i)$ 为方程 $eq'_\tau(i)$ 的左端，则存在 r_τ 阶可逆矩阵 Q，使 $\Gamma''_IZ-Q\cdot E'_\tau f'_\tau(i)\equiv 0$.

证明：对 $eq_0(i)$ 经标准线性 R_aR_b 变换得到的 $EQ'_\tau(i)$，设 $F'_\tau(i)$ 为 $EQ'_\tau(i)$ 的左端，由定理1知，存在可逆矩阵 Q，使　　$E'_\tau F'_\tau(i)-Q\cdot E'_\tau f'_\tau(i)\equiv 0$

由定理2，$\Gamma''_IZ-Q\cdot E'_\tau f'_\tau(i)=E'_\tau F'_\tau(i)-Q\cdot E'_\tau f'_\tau(i)\equiv 0$.

综合定理2和定理3可知，对FA M，由算法 MR_{ab} 输出的关于变元 x_i 的方程组与线性 R_aR_b 变换所得的关于 x_i 的有效方程之间仅仅相差一个可逆矩阵. 它们关于变元 x_i 的求解能力是一致的.

5　算法 ALT 与 MR_{ab} 的比较

本节在有限域 $GF(2)$ 上讨论，并设 $m=l=8$. 文献[3]中的算法 ALT 所处理的 FA 形如

$$y_i=\sum_{j=1}^{k}A_jy_{i-j}+\sum_{j=1}^{h}B_jx_{i-j}+\sum_{j=1}^{h}\overline{B}_jx_{i-j}x_{i-j-1}\quad i=0,1,\ldots \tag{18}$$

且 $\overline{B}_0=\overline{B}_h=0$，$x_{-h-1}$ 为哑变元. 而 $x_{i-j}x_{i-j-1}$ 表示 2 个向量 x_{i-j} 和 x_{i-j-1} 的逐分量相乘所得的列向量. 从时刻 i 开始到时刻 $i+\tau$，共得 $\tau+1$ 个方程，并由此求解 x_i. 文献[3]把这些方程表述为以下的矩阵形式

$$[C\ D]\overline{X}=0 \tag{19}$$

其中 $C=\begin{bmatrix} B_0 & & & \overline{B}_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ B_\tau & \cdots & B_0 & \overline{B}_\tau & \cdots & \overline{B}_0 \end{bmatrix}$

为 $8(\tau+1)\times 8(2\tau+2)$ 阶矩阵，而 $D=$

$$\begin{bmatrix} A_h & \cdots & \cdots & A_1 & E & & B_h & \cdots & \cdots & \cdots & B_1 & \overline{B}_h & \cdots & \cdots & \cdots & \overline{B}_1 \\ & \ddots & & & \ddots & \ddots & & \ddots & & & \vdots & & \ddots & & & \vdots \\ & & A_h & \cdots & \cdots & A_1 & E & & B_h & \cdots & B_{\tau+1} & & & \overline{B}_h & \cdots & \overline{B}_{\tau+1} \end{bmatrix}$$

为 $8(\tau+1)\times 8(2h+\tau+k+1)$ 阶矩阵，且

$$\overline{X}=[x_i,\ldots,x_{i+\tau},x_ix_{i-1},\ldots,x_{i+\tau}x_{i+\tau-1},y_{i-k},\ldots,y_{i+\tau},x_{i-h},\ldots,x_{i-1},x_{i-h}x_{i-h-1},\ldots,x_{i-1}x_{i-2}]^T$$

为 $8(3\tau+2h+k+3)$ 维列向量. 令　　$K=\{1,\ldots,8\}$

则算法 ALT[3]是对方程组(19)的系数矩阵 $[C\ D]$ 施行初等行变换化为约化梯阵 $[C''\ D'']$，并输出 D'' 的前 8 行 D''_K. 由此输出构作的方程组为 $[C''\ D'']_K\overline{X}=0$.

根据文献[3]中定理 1 的证明，ALT 所处理的形如(18)的 FA 具有如下性质：

$$C''_K=[E\ 0\ \ldots\ 0] \tag{20}$$

其中 C''_K 中共有 $2\tau+1$ 个 8×8 零矩阵 0.

今用 MR_{ab} 也来处理形如(18)的 FA，则可令

$$\Gamma=\begin{bmatrix} B_0 & \overline{B}_0 & \cdots & B_h & \overline{B}_h & & E & A_1 & \cdots & \cdots & A_h & & \\ & \ddots & & & \ddots & & & \ddots & \ddots & & & \ddots & \\ & B_0 & \overline{B}_0 & \cdots & B_h & \overline{B}_h & & & E & A_1 & \cdots & \cdots & A_h \end{bmatrix}$$

$$Z=[x_{i+\tau},x_{i+\tau}x_{i+\tau-1},\ldots,x_{i-h},x_{i-h}x_{i-h-1},y_{i+\tau},\ldots,y_{i-k}]^T$$

定理 4. 对形如(18)且满足性质(20)的 FA，由 ALT 的输出构作的方程组也可由 MR_{ab} 的输出构作.

证明：设存在 $8(\tau+1)$ 可逆矩阵 Q，使 $Q[C\ D]=[C''\ D'']$ 为约化梯阵，且

$$[C''\ D'']_K=[E\ 0\ \ldots\ 0\ A_h^*\ldots\ A_{-\tau}^*\ B_h^*\ldots\ B_1^*\ \overline{B}_h^*\ldots\ \overline{B}_1^*]$$

记 $Q=\begin{bmatrix} Q_{00} & \cdots & Q_{0\tau} \\ \vdots & \cdots & \vdots \\ Q_{\tau 0} & \cdots & Q_{\tau\tau} \end{bmatrix}$

其中 Q_{ij} 为 8 阶矩阵，$i,j=0,\ldots,\tau$. 令

$$Q'=\begin{bmatrix} Q_{\tau\tau} & \cdots & Q_{\tau 0} \\ \vdots & \cdots & \vdots \\ Q_{0\tau} & \cdots & Q_{00} \end{bmatrix}$$

注意到 Γ 与 $[C\ D]$ 的特点，把 $Q'\Gamma$ 的后 8 行记为 $(Q'\Gamma)_{-K}$，则

$$(Q'\Gamma)_{-K}=[0\ \ldots\ 0\ E\ 0\ B_1^*\ \overline{B}_1^*\ldots\ B_h^*\ \overline{B}_h^*\ A_{-\tau}^*\ldots\ A_k^*]$$

由引理 5，仅由初等行变换可把 $Q'\Gamma$ 化为梯阵 Γ'，使

$$\Gamma'_I=(Q'\Gamma)_{-K}$$

且 $$\Gamma'_J Z\equiv 0$$

再由初等行变换把 Γ' 化为约化梯阵 Γ''，则存在 $8\times\Sigma_{c=0}^{r}(8-r_c)$ 阶矩阵 $P_{r,r+1}$ 使

$$\Gamma''_I=\Gamma'_I+P_{r,r+1}\Gamma'_J$$

于是 $\Gamma''_I Z=\Gamma'_I Z+P_{r,r+1}\Gamma'_J Z=\Gamma'_I Z=(Q'\Gamma)_{-K}Z=[C''\ D'']_K\overline{X}$. 从而 $[C''\ D'']_K\overline{X}=\Gamma''_I Z$.

对一般的FA，定理4之逆非真. 为叙述方便，选取 $l=m=3$，且考虑1阶输入存储FA M

$$y_i=[B_0\ \overline{B}_0\ B_1\ \overline{B}_1]\begin{bmatrix}x_i\\ \psi(x_i)\\ x_{i-1}\\ \psi(x_{i-1})\end{bmatrix},i=0,1,\ldots$$

其中 $x_i=[a_1,a_2,a_3]^T$，$\psi(x_i)=[a_1a_2,a_2a_3,a_3a_1]^T$，$B_0=\begin{bmatrix}1&0&1\\ &0&0\\ &&0\end{bmatrix}$，$\overline{B}_0=0$，$B_1=\begin{bmatrix}0&0&1\\ &1&1\\ &&0\end{bmatrix}$，

$\overline{B}_1=\begin{bmatrix}0&&\\0&0&\\1&1&1\end{bmatrix}$.

先用标准线性 R_aR_b 变换来判定和求弱逆. 这里

$$E'_0EQ'_0(i):[101\ 000\ 001\ 000\ 100][x_i,\psi(x_i),x_{i-1},\psi(x_{i-1}),y_i]^T=0$$

$$E'_1EQ'_1(i):\begin{bmatrix}1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\ &1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\ &&&1&1&1&0&0&0&0&0&0&0&0&1&0&0&0\end{bmatrix}\begin{bmatrix}x_i\\ \psi(x_i)\\ x_{i-1}\\ \psi(x_{i-1})\\ y_{i+1}\\ y_i\end{bmatrix}=0$$

且 $r_0=1,r_1=3$. 可直接验证，对任何参数 x_{i-1},y_{i+1} 和 y_i，$E'_1EQ'_1(i)$ 的左端关于 x_i 为双射，从而关于 x_i 有且只有一个解. 于是 M 延迟1步弱可逆. 并可由 $E'_1EQ'_1(i)$ 求出其延迟1步弱逆 M^*（具体方法见文献[1]）：$M^*=(Y,X,S^*,\delta^*,\lambda^*)$，其中 $Y=X=GF(2)^3$，$S^*=Y\times X\times\{0,1\}$，对任意 $x_{-1}\in\hat{X}$，$y_{-1},y_0\in Y$，$c=0,1$，有 $\delta^*(\langle y_{-1},x_{-1},0\rangle,y_0)=\langle y_0,x_{-1},1\rangle$，

$\delta^*(\langle y_{-1},x_{-1},1\rangle,y_0)=\langle y_0,x_0,1\rangle$，$\lambda^*(\langle y_{-1},x_{-1},c\rangle,y_0)=x_0$，$x_0=\begin{bmatrix}0&0&1\\ &0&1\\ &&1\end{bmatrix}x_{-1}$

$$\cdot\begin{bmatrix}0&1&0\\0&1&0\\0&1&0\end{bmatrix}y_0+\begin{bmatrix}1&&\\1&0&\\1&0&0\end{bmatrix}y_{-1}\cdot\begin{bmatrix}0&1&0\\0&1&0\\0&1&0\end{bmatrix}y_0+\begin{bmatrix}0&0&1\\ &1&1\\ &&1\end{bmatrix}y_0+\begin{bmatrix}1&&\\0&0&\\0&0&0\end{bmatrix}y_{-1}$$

$$+\begin{bmatrix}0&0&1\\ &0&0\\ &&0\end{bmatrix}x_{-1}$$，其中“·”表示两向量的对应分量之积.

再用 MR_{ab} 来处理. 令 $r=1$

$$\Gamma=\begin{bmatrix} B_0 & \overline{B}_0 & B_1 & \overline{B}_1 & & & E & \\ & & B_0 & \overline{B}_0 & B_1 & \overline{B}_1 & & E \end{bmatrix}$$

$$Z=[x_{i+1},\psi(x_{i+1}),x_i,\psi(x_i),x_{i-1},\psi(x_{i-1}),y_{i+1},y_i]^T$$

对 Γ 施行初等行变换化为约化梯阵

$$\Gamma''=\begin{bmatrix} 1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\ &&&&&&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\ &&&&&&&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\ &&&&&&&&&1&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\ &&&&&&&&&&&&1&1&0&0&0&0&0&0&1&0\\ &&&&&&&&&&&&&&1&1&1&0&0&0&0&0&1 \end{bmatrix}$$

于是 $r_0=1,r_1=3$. 且 $I=\{2,3,4\}$，由 MR_{ab} 的输出构作的方程组

$$0=\Gamma''_1Z=\begin{bmatrix} 1&0&1&0&\\ &1&1&0&0\\ &&0&1&1&1 \end{bmatrix}\begin{bmatrix} x_i\\ \psi(x_i) \end{bmatrix}+\begin{bmatrix} 0&&1&0&\\ &0&&&0\\ &&0&&&0 \end{bmatrix}\begin{bmatrix} x_{i-1}\\ \psi(x_{i-1}) \end{bmatrix}$$

$$+\begin{bmatrix} 0&&&1&\\ &1&&&0\\ &&1&&&0 \end{bmatrix}\begin{bmatrix} y_{i+1}\\ y_i \end{bmatrix}=E'_1F'_1(0)$$

同理也可判定 M 延迟 1 步弱可逆，并由此方程组可求出

$$x_i=\begin{bmatrix} 0&0&1\\ &0&1\\ &&1 \end{bmatrix}x_{i-1}\cdot\begin{bmatrix} 0&1&0\\ 0&1&0\\ 0&1&0 \end{bmatrix}y_{i+1}+\begin{bmatrix} 1&&\\ 1&0&\\ 1&0&0 \end{bmatrix}y_i\cdot\begin{bmatrix} 0&1&0\\ 0&1&0\\ 0&1&0 \end{bmatrix}y_{i+1}$$

$$+\begin{bmatrix} 0&0&1\\ &1&1\\ &&1 \end{bmatrix}y_{i+1}+\begin{bmatrix} 1&&\\ 0&0&\\ 0&0&0 \end{bmatrix}y_i+\begin{bmatrix} 0&0&1\\ &0&0\\ &&0 \end{bmatrix}x_{i-1}$$

最后，如果用文献[3]中的算法 ALT 来处理. 这时 $r=1$.

$$[C\ D]=\begin{bmatrix} B_0&0&\overline{B}_0&0&E&0&B_1&\overline{B}_1\\ B_1&B_0&\overline{B}_1&\overline{B}_0&0&E&0&0 \end{bmatrix}$$

$$\overline{X}=[x_i,x_{i+1},\psi(x_i),\psi(x_{i+1}),y_i,y_{i+1},x_{i-1},\psi(x_{i-1})]^T$$

对$[C\ D]$施行初等行变换化为约化梯阵

$$[C''\ D'']=\begin{bmatrix} 1&0&0&1&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0\\ &1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\ &&1&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\ &&&&&&1&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\ &&&&&&&&&&&&1&0&0&0&0&0&1&1&0&0&0\\ &&&&&&&&&&&&&1&0&0&0&0&0&0&1&1&1 \end{bmatrix}$$

由 ALT 的输出构作的方程组为

$$[C''\ D'']_K\overline{X}=0$$

即

$$x_i+\begin{bmatrix} 1&0&1\\ 1&0&1\\ 1&0&1 \end{bmatrix}x_{i+1}+\begin{bmatrix} 1&&\\ &0&\\ &&0 \end{bmatrix}y_i+\begin{bmatrix} 1&&\\ 1&1&\\ 1&0&0 \end{bmatrix}y_{i+1}+\begin{bmatrix} 0&0&1\\ &0&0\\ &&0 \end{bmatrix}x_{i-1}=0$$

不能由 x_{i-1}, y_{i+1}, y_i 求解唯一的 x_i 的值.

致谢 本文的写作过程得到陶仁骥和陈世华老师的悉心指导和极大帮助,并和陈小明、冯培荣、隆永红及李建宝同志进行过有益的讨论,谨此表示衷心地感谢.

参考文献

1 Tao Renji, Chen Shihua. Generating a kind of nonlinear finite automata with invertibility by transformation method. Technical Report No. ISCAS-LCS-95-05, Laboratory for Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing, June 1995.

2 Tao Renji, Chen Shihua, Chen Xuemei. FAKKC3: a new finite automaton public key cryptosystem. Technical Report No. ISCAS-LCS-95-07, Laboratory for Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing, June 1995.

3 覃中平,张焕国. 分析有限自动机公开钥密码. 密码学进展——CHINACRYPT'96,北京:科学出版社,1996. 75~86.

4 王浩. 关于一类有限自动机的可逆性. 密码学进展——CHINACRYPT'96,北京:科学出版社,1996. 95~102.

5 Birkhoff G, MacLane S. A survey of modern algebra. Forth edition, New York: Macmillan Publishing Co. Inc., 1977. 183~187.

6 戴宗铎. 不变量与线性有限自动机的可逆性. 密码学进展——CHINACRYPT'94,北京:科学出版社,1994. 127~134.

7 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. 中国科学(A 辑),1994,24(2):193~200.

THE R_aR_b REPRESENTATION OF A CLASS OF THE REDUCED ECHELON MATRICES

WANG Hao

(*Institute of Software The Chinese Academy of Sciences Beijing* 100080)

Abstract The relations between different linear R_aR_b transformations are described. Based on the reduced echelon matrix, an algorithm MR_{ab} is proposed. By using the standard linear R_aR_b transformations, the equivalence of the output equation system of MR_{ab} to the image equation system of linear R_aR_b transformations is proved. After discussion about the relations between the algorithm MR_{ab} and ALT, the following conclusion is obtained: it is unnecessary for the finite automaton public key cryptosystem FAPKC3 to include another check process in the key generator to seive out a finite automaton of which a weak inverse can be obtained by ALT.

Key words Algorithm, finite automaton, reduced echelon matrix, the linear R_aR_b transformation.

Class number TP301.1