Теоретико-автоматные методы в криптографии

Верхняя оценка степени различимости связных перестановочных автоматов с заданным диаметром

Известна достижимая оценка степени различимости R конечного автомата с числом состояний |S|

$$R \leq |S| - 1.$$

Почти все автоматы имеют степень различимости асимптотически равную

$$\log_{|X|} \log_{|Y|} |S|,$$

Для связного перестановочного автомата с диаметром D мной доказано

$$R \le (l_0 + 1)(D + 1) + \left[\frac{|S|}{2^{l_0+1}}\right] - 1,$$

$[\nu]$ – целая часть числа ν,

l_0 – максимальное l, если оно существует, при котором

$$\left[\frac{|S|}{2^{l}}\right] - \left[\frac{|S|}{2^{l+1}}\right] > D + 1,$$

в противном случае $l_0 = -1$.

Данная оценка достижима для следующих параметров перестановочного связного автомата Мура:

1) $D=1, \quad |S|=3\cdot 2^m, \; m\in N_0$;

2) $D=1, \quad |S|=5\cdot 2^m, \; m\in N_0$;

3) $D=2, \quad |S|=5\cdot 2^m, \; m\in N_0$.

Обозначим $A(|S|, D)$ - класс приведенных связных перестановочных автоматов Мура с числом состояний |S|, выходным алфавитом Y, |Y|=2 и диаметром D.

Доказано,

1) для любого автомата с $|S| = 2(n+1)+1$,

R<|S|-1

тогда и только, когда

$$D < n+1.$$

2) если $|S| = 4(n+1)$, R<|S|-1, то $D < 2(n+1)$,

3) если $|S| = 4(n+1)+2$ и $R = 4(n+1)+1$, то

$$D \geq 2(n+1)+2,$$

- Обозначим через **θ(J)** и назовем **полнотой последовательности** *J* элементов алфавита X максимальное k, если оно существует, при котором все возможные *k*-граммы алфавита X встречаются в последовательности J.

Назовем входные слова $J,J' \in X^k$ автомата A **вероятностно неотличимыми** относительно A, если для любого $y \in Y^k$ при случайном и равновероятном выборе начального состояния $s \in S$ вероятности $P(A(s,J)=y)$, $P(A(s,J')=y)$ событий $A(s,J)=y$ и $A(s,J')=y$ совпадают.

Обозначим через Q_A и назовем **степенью вероятностной неотличимости** автомата A максимальное k, если оно существует, при котором любая пара слов из X^k вероятностно неотличима относительно A, в противном случае, полагаем $Q_A=\infty$.

ТЕОРЕМА 3. Пусть $|S'|$ - простое число, $\theta(A`(s`))>Q_{A``}$. Тогда число классов неотличимых состояний автономного последовательного соединения $A' \to A''$ ограничено снизу величиной $|S'|$, (период $W_{A` \to A``}$ внешнего функционирования автомата $A' \to A''$ кратен $|S'|$).

ТЕОРЕМА 4. Пусть $|S'|$ - простое число, $A'' = \left(X'', V_n, F_q, (h_x)_{x \in X''}, (f_x)_{x \in X''}\right)$ - векторный перестановочный неавтономный автомат и $q^n < \theta(A'(s'))$. Тогда число классов неотличимых состояний автомата $A' \to A''$ ограничено снизу величиной $|S'|$, (а его период внешнего функционирования кратен $|S'|$).

ТЕОРЕМА 5. Пусть $|S'|$ - простое число, $A'' = (X'', V_n, F_q, (\alpha_x)_{x \in X''}, (c_x)_{x \in X''})$ - векторный линейный перестановочный неавтономный автомат и $n < \theta(A'(s'))$. Тогда число классов неотличимых состояний автомата $A' \to A''$ ограничено снизу величиной $|S'|$, а его период внешнего функционирования кратен $|S'|$.

Будем говорить, что множество входных слов $\Im_1,\ldots,\Im_t$ одинаковой длины автомата A **сильно различимо (относительно A)**, если при любой правой части **y** система уравнений $A(s,\Im_j)=\mathbf{y}$, $j\in\{1,\ldots,t\}$ не имеет решения в множестве начальных состояний автомата A. В противном случае, данное множество входных слов автомата A называется **слабо неотличимым** множеством (относительно A). Максимальное k, если таковое существует, при котором все k-граммы входного алфавита автомата A слабо неотличимы обозначим через σ_A и назовем степенью слабой автономности автомата A. В противном случае, полагаем $\sigma_A=\infty$.

•

ТЕОРЕМА 9. Пусть $\theta(A(s^A)) > \sigma_B$. Тогда периоды выходных последовательностей автомата $A \to B$ больше единицы. Если $|S^A|$ - простое число, то

1) периоды выходных последовательностей автомата $A \to B$ кратны $|S^A|$,

2) мощности классов неотличимых состояний автомата $A \to B$ ограничены сверху величиной $|S^B|$.

- СЛЕДСТВИЕ 9. Пусть выходная последовательность автомата A содержит пару сильно различимых, относительно автомата B, мультиграмм. Тогда периоды выходных последовательностей автомата $A \to B$ больше единицы. Если $|S^A|$ - простое число, то

1) периоды выходных последовательностей автомата $A \to B$ кратны $|S^A|$,

мощности классов неотличимых состояний автомата $A \to B$ ограничены сверху величиной $|S^B|$.

Пусть $A=(S,Y,\delta,\lambda)$ – автономный автомат выходным алфавитом Y которого являетс некоторая конечная группа G.

Состояния $s,s'\in S$ назовем G–неотличными, есл найдется неединичный элемент $g\in G$, при котором

$$A(s)=y_1,y_2,\ldots \quad , A(s')=y'_1,y'_2,\ldots, \quad y'_j=gy_j ,$$

$j\in[1, 2, . .)$.

-

Справедливо утверждение. Если для полноциклового приведенного автомата $A=(S,Y,\delta,\lambda)$, где $Y=G$ – некоторая конечная группа,

$$(|G|,|S|)=1,$$

то A является G–приведенным автоматом.

•

Пусть $A_1=(S_1, Y, h^{(1)}, \lambda^{(1)})$ – полноцикловый автомат, $A_2=(X, S_2, (h_x^2)_{x\in X})$ – перестановочный коммутирующий (т.е. $h_x^2 h_{x'}^2=h_{x'}^2 h_x^2$, при любых x $x' \in X$) автомат без выхода,

$Y=X$, а G – некоторая конечная группа и $\lambda: S_1 \times S_2 \to G$ отображение вида

$$\lambda(s_1,s_2)=f(s_1)\cdot\nu(s_2),$$

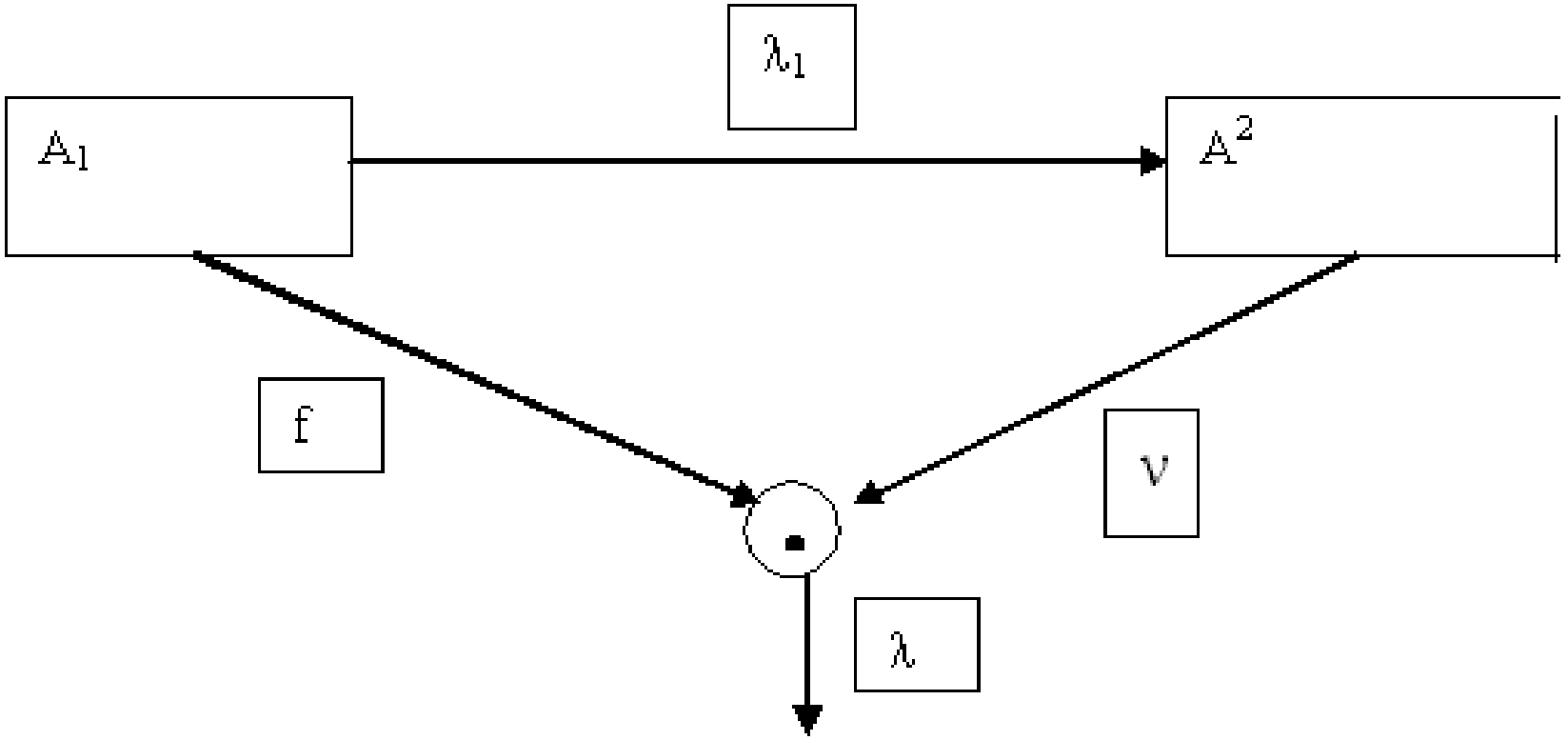
где $f: S_1 \to G$, $\nu: S_2 \to G$.

- Рассмотрим последовательное соединение $A=A_1 \to A_2$ автоматов A_1, A_2 с выходной функцией λ, $A=A_1 \to A_2=(S_1 \times S_2, G, \delta, \lambda)$

$\delta(s_1,s_2)=(h^{(1)}(s_1), h^{(2)}_{s_1}(s_2))$, $\lambda(s_1,s_2)=f(s_1)\cdot\nu(s_2)$

умножение $\cdot$ - операция в группе G.

- Автомат A имеет вид



Обозначим через A_f автономный автомат отличающийся от A_1 лишь функцией выхода $A_f=(S_1, Y, \delta, f)$, а через $A_П=(S_2, Y, П, \nu)$ - автономный автомат с множеством состояний S_2 функцией перехода

$$П=h^2_{x(|S_1|)}h^2_{x(|S_1|-1)}\dots h^2_{x(1)},$$

Где $A_1(s_1)=x(1),x(2),\dots,x(|S_1|),\dots$ - выходная последовательность автомата A_1 с некоторого состояния $s_1 \in S_1$.

Теорема 5. Пусть $A_1=(S_1, Y, \delta^{(1)}, \lambda^{(1)})$ и $A_2=(X, S_2, (h_x^2)_{x\in X})$ – перестановочный коммутирующий автомат, $Y=X$, G – некоторая конечная группа λ $S_1\times S_2\to G$ отображение вида

$$\lambda(s_1,s_2)=f(s_1)\cdot \nu(s_2),$$

где $f:S_1\to G$, $\nu:S_2\to G$. Пусть также автоматы $A_f=(S_1, Y, \delta, f)$, $A_\Pi=(S_2, Y, \Pi, \nu)$ G-приведенные. Тогда, если автомат $A=A_1\to A_2$ полноцикловый, то он G-приведен.

- Спасибо за внимание