О ДИАМЕТРЕ ГРАФА РАЗНОСТНЫХ ПЕРЕХОДОВ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Маслов А.С., БГУ, Минск

Пусть G — конечная группа в мультипликативной записи, e — единица G, $G^* = G \setminus \{e\}$ и $S(G)$ — множество всех подстановок, действующих на G. Пусть $s \in S(G)$, x_0, x_0' — различные элементы G, a_1, a_2, … — независимые случайные величины с равномерным на G распределением вероятностей и

$$x_t = s(x'_{t-1}a_t), \quad x_t = s(x'_{t-1}a_t), \quad \beta_t = x'_t x_t^{-1}, \quad t = 1,2,\ldots$$

Введённая последовательность (β_t) является траекторией однородной цепи Маркова с матрицей переходных вероятностей

$$P_s = (p_{\alpha\beta}), \quad p_{\alpha\beta} = \frac{1}{|G|}\sum_{x\in G}\mathbf{I}\{s(\alpha x) = \beta s(x)\}, \quad \alpha, \beta \in G^*, \tag{1}$$

где $\mathbf{I}\{E\}$ — индикатор наступления события E. Последовательность (β_t) принято называть последовательностью разностей подстановки s, поскольку в первоначальных работах [1, 2] рассматривались абелевы группы, и $p_{\alpha\beta}$ в этом случае характеризует вероятность перехода от входной разности $x' - x = \alpha$ к выходной разности $s(x'+a) - s(x+a) = \beta$. Обобщение понятия разности на случай произвольных групп было сделано в работе [3].

Графом разностных переходов подстановки $s \in S(G)$ назовём граф переходов цепи Маркова (1).

Теорема 1. Почти для всех подстановок из множества $S(G)$ диаметр графа разностных переходов равен 2.

Теорема означает, что для произвольных $\alpha, \beta \in G^*$ найдётся $\gamma \in G^*$ такое, что $p_{\alpha\gamma} > 0$ и $p_{\gamma\beta} > 0$, т.е. переход от состояния α к состоянию β можно осуществит за два шага.

Свойства цепи Маркова (1) связаны со свойствами группы $F_s \subseteq S(G)$, порождённой подстановками $f_a : x \mapsto s(xa)$, $x, a \in G$.

Теорема 2. Если граф разностных переходов является сильно связным, то группа F_s дважды транзитивна, т.е. для произвольных различных $x_1, x_2 \in G$ и произвольных различных $y_1, y_2 \in G$ найдётся $\sigma \in F_s$ такая, что $\sigma(x_i) = y_i$, i = 1,2. При этом σ может быть представлена в следующем виде

$$\sigma = f_{a_k} f_{a_{k-1}} \ldots f_{a_1}, \quad k \le d+1,$$

Где d – диаметр графа разностных переходов.

Литература

1. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. of Cryptology, vol. 4, pp. 3–72, 1991.

2. Biham E., Shamir A. Differential cryptanalysis of the full 16-round DES // Advances in Cryptology, CRYPTO'92, LNCS vol. 740, pp. 487–496, 1993.

3. Lai X., Massey J., Murphy S. Markov Ciphers and Differemtial Cryptanalysis // Advances in Cryptology, EUROCRYPT'91, pp. 17–38, 1991.