

Н. В. Н и к о н о в (Москва, ТВП). **О существовании запрета у пороговой функции.**

Рассмотрим фильтрующий генератор (см. [1]) с функцией $f(\vec{x}) = f(x_1, \dots, x_n) \in \Phi_n$, где Φ_n — класс булевых функций, крайние переменные которых x_1, x_n — существенные. На выходе генератора формируется последовательность знаков $\{\gamma_j\}$, $j \in \mathbf{N}$, связанных соотношениями

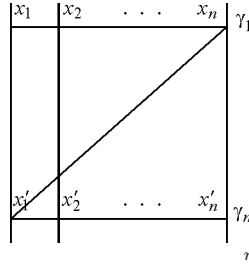
$$f(x_{1+i}, \dots, x_{n+i}) = \gamma_{1+i}, \quad i = 0, 1, \dots \quad (1)$$

При этом последовательность $\gamma_1, \dots, \gamma_N$ называется *запретом функции $f(\vec{x})$ длины N* , если соответствующая система вида (1) несовместна ($i = 0, 1, \dots, N-1$). Данное определение было введено С. Н. Сумароковым в работе [2], в которой был доказан критерий отсутствия у функции запрета. Согласно критерию, функция $f(\vec{x}) \in \Phi_n$ не имеет запрета тогда и только тогда, когда все ν -граммы $\gamma_1, \dots, \gamma_\nu$ на выходе фильтрующего генератора с функцией $f(\vec{x})$ имеют равномерное распределение для любого $\nu \in \mathbf{N}$. Отсюда в частности следует, что все неравновероятные функции имеют запрет.

Основной результат настоящего доклада заключается в том, что пороговые функции из Φ_n не относятся к классу функций без запрета. Напомним, что функция $\pi(\vec{x}) = \pi(x_1, \dots, x_n)$ называется *пороговой*, если существует такая линейная форма $l(\vec{x}) = a_1x_1 + \dots + a_nx_n$, $a_i \in \mathbf{R}$ и $b \in \mathbf{R}$, что $\pi(\vec{x}) = 1 \Leftrightarrow l(\vec{x}) \geq b$, $\pi(\vec{x}) = 0 \Leftrightarrow l(\vec{x}) < b$.

Теорема. *Любая пороговая функция $\pi(\vec{x}) \in \Phi_n$ имеет запрет.*

Доказательство теоремы базируется на том наблюдении, что для произвольной пороговой функции $\pi(\vec{x}) \in \Phi_n$ всегда существует некоторая неравномерно распределенная ν -грамма длины, не превосходящей n , что говорит, исходя из критерия Сумарокова, о существовании запрета.



Действительно, рассмотрим n -граммы вида $\overbrace{\gamma_1 \dots \gamma_n}^{n-1}$ (см. рис.). Вероятность появления таких n -грамм равна

$$\begin{aligned} \mathbf{P} \{ \overbrace{\gamma_1 \dots \gamma_n}^{n-1} \} &= \frac{1}{2} \left[\mathbf{P} \{ \pi(\vec{x}) = \gamma_1 | x_n = 0 \} \mathbf{P} \{ \pi(\vec{x}') = \gamma_n | x'_1 = x_n = 0 \} \right. \\ &\quad \left. + \mathbf{P} \{ \pi(\vec{x}) = \gamma_1 | x_n = 1 \} \mathbf{P} \{ \pi(\vec{x}') = \gamma_n | x'_1 = x_n = 1 \} \right]. \end{aligned} \quad (2)$$

В силу того, что пороговая функция $\pi(\vec{x})$ является полностью монотонной (см. [3], [4]) и лежит в классе Φ_n , заведомо выполняются следующие неравенства:

$$\begin{aligned} \mathbf{P} \{ \pi(\vec{x}) = 0 | x_i = 0 \} &> \mathbf{P} \{ \pi(\vec{x}) = 0 | x_i = 1 \}, \\ \text{либо } \mathbf{P} \{ \pi(\vec{x}) = 0 | x_i = 0 \} &< \mathbf{P} \{ \pi(\vec{x}) = 0 | x_i = 1 \}; \end{aligned} \quad (3)$$

$$\begin{aligned} \mathbf{P} \{ \pi(\vec{x}) = 1 | x_i = 0 \} &> \mathbf{P} \{ \pi(\vec{x}) = 1 | x_i = 1 \}, \\ \text{либо } \mathbf{P} \{ \pi(\vec{x}) = 1 | x_i = 0 \} &< \mathbf{P} \{ \pi(\vec{x}) = 1 | x_i = 1 \}, \end{aligned} \quad (4)$$

$i \in \{1, n\}$. Для равновероятных функций имеем $\mathbf{P}\{\pi(\vec{x}) = \gamma | x_i = \varepsilon\} = 1/2 \pm \delta_i$, $\gamma, \varepsilon \in \{0, 1\}$, $\delta_i > 0$, $i \in \{1, n\}$. Исходя из (2), получаем, что $\mathbf{P}\{\overbrace{\gamma_1 \dots \gamma_n}^{n-1}\} = 1/4 \pm \delta_1 \delta_n$, в силу чего можно гарантировать существование у функции $\pi(\vec{x})$ неравномерно распределенной n -граммы $\gamma_1, \gamma_2, \dots, \gamma_n$.

Здесь отметим, что существуют пороговые функции, все ν -граммы которых имеют равномерное распределение вплоть до $\nu = n - 1$ (см. [5]).

Класс функций с запретами, описываемых условиями (3) и (4), намного шире класса пороговых функций. В другой интерпретации, условия (3) и (4) могут быть заменены на следующие:

$$w_{x_i=0}(f(\vec{x})) \neq w_{x_i=1}(f(\vec{x})), \quad i \in \{1, n\}, \quad (5)$$

где $w_{x_i=\varepsilon}(f(\vec{x}))$ — вес функции $f(\vec{x})$ при фиксации $x_i = \varepsilon$, $\varepsilon \in \{0, 1\}$, $i \in \{1, n\}$.

Заметим, что приведенные рассуждения верны и для случая, когда информация с регистра сдвига фильтрующего генератора поступает на функцию $f(\vec{x})$ не с подряд идущих ячеек, а с ячеек, расположенных на расстояниях $l_1, l_2, \dots, l_{n-1}$, что говорит о наличии у функции $f(\vec{x})$ со свойством (5) составного обобщенного запрета (совокупности запретов при любых l_j , $j = 1, \dots, n - 1$).

В докладе отмечается, что приведенная теорема и дальнейшие рассуждения справедливы и для пороговых функций k -значной логики (см. [4]).

Работа выполнена при поддержке гранта Президента РФ НШ-4.2008.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Фомичев В. М.* Дискретная математика и криптология М.: Диалог Мифи, 2003, 397 с.
2. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств. — Обозрение прикл. и промышл. матем., 1994, т. 1, в. 1, с. 33–55.
3. *Дертоузос М.* Пороговая логика. М.: Мир, 1967, 343 с.
4. *Никонов В. Г., Никонов Н. В.* Особенности пороговых представлений k -значных функций. — Труды по дискретной математике, 2008, т. 11, в. 1 (принята к публикации).
5. *Никонов Н. В., Усанов Д. В.* Запреты и вероятностные свойства ν -грамм булевых функций от 3-х переменных. — Вестник МГУЛ «Лесной вестник». М.: МГУЛ, 2006, № 6 (48), с. 146–158.