ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 29 МАТЕМАТИКИ Выпуск 2
2022

В. С. Домрачев (Москва, Лаб. ТВП). **О влиянии различных пороговых заданий классов функций k-значной логики на их свойства в схеме фильтрующего генератора.**

УДК 004.421.5 DOI https://doi.org/10.52513/08698325_2022_29_1_1

Резюме: Произведено сравнение свойств выходных v-грамм в схеме фильтрующего генератора с позиции запретов и полузапретов функции усложнения k-значной логики полиэдрального класса, построенного на основе различных заданий порождающей для класса булевой функции. Получены оценки значности логики k для гарантированного наличия в полиэдральных классах равновероятных функций.

Ключевые слова: Запрет функции, полузапрет функции, фильтрующий генератор, равновероятная функция.

Настоящие тезисы в целом посвящены изучению свойств выходных v-грамм фильтрующего генератора ([1–3]) в зависимости от порогового задания классов k-значных функций усложнения. В частности, невозможность появления v-граммы на выходе схемы фильтрующего генератора говорит о ее запретности.

В данных тезисах рассматривается метод растяжения для построения классов k-значных функций с определенными свойствами выходных v-грамм, описанный в работе [4], исходя из соответствующих свойств для порождающих булевых функций. Показано, что запрет для порождающей булевой функции может стать полузапретом первого или второго рода (при которых локализируется число решений [5]) или остаться запретом для построенных классов k-значной логики. Данный вопрос изучался в работах [5, 6], но был рассмотрен только для одного вида задания исходной булевой функции — с минимальным вхождением переменных в неравенства ([7]). В данной работе исследуются свойства выходных v-грамм при других пороговых заданиях: минимальным количеством неравенств и с поточечным отсечением вершин («поточечное»), и производится их сравнение с изученным заданием с минимальным вхождением переменных в неравенства.

Наряду со свойством запретности в работе сравниваются оценки значности логики k, при которых в полученном методом растяжения полиэдральном классе гарантированно будут содержаться равновероятные функции. Методика оценки значности логики, использованная в исследовании, была предложена в работе [4]. Разные задания исходной булевой функции порождают разные полиэдральные классы k-значной логики, что отражается на различных оценках k.

В каталоге Н. В. Никонова [7] представлены доказательства запретности v-грамм для всех булевых функций от 3-х переменных в случае задания минимальным вхождением переменных в неравенства, и для класса функций с графом 3.1 (одна компонента связности с тремя связными вершинами) указана оценка значности логики $k \geqslant 7$. При этом все полученные с помощью метода растяжения v-граммы в k-значной области становятся запретами.

Из проведенных для класса функций с графом 3.1 доказательств в случае задания их одним пороговым неравенством следует, что v-грамма в k-значной области не

всегда становится запретом. Так, для функций 3.1.2.1, 3.1.4.1-3.1.7.1 v-грамма становится полузапретом второго рода, для функций 3.1.1.1 и 3.1.3.1 при $k = 2t + 1$, $t \geqslant 7$ становится запретом, а при $k = 2t$, $t \geqslant 8$ — полузапретом первого рода. Оценка значности логики k для всех функций класса с графом 3.1 одинакова: $k \geqslant 15$, что уступает оценке из каталога.

Для «поточечного» задания удалось снизить оценку ($k \geqslant 6$), но полиэдральное доказательство для этих функций провести не удалось, что говорит о нетривиальной связи задания функции и доказательства запретности v-граммы.

Таким образом, сравнивая три описанных выше вида задания функции на примере класса функций от 3-х переменных с графом 3.1, можно сделать следующие выводы. Наиболее простыми представляются доказательства для задания, характеризующегося минимальным вхождением переменных в неравенства. При этом все запретные v-граммы в k-значной области становятся также запретами. Наилучшую оценку значности логики k гарантированного наличия в полученном полиэдральном классе равновероятных функций удается получить для «поточечного» задания. Для задания минимальным количеством неравенств, с одной стороны, проще проводятся доказательства запретности v-граммы, но, с другой стороны, не для всех значений k v-грамма остается запретом, и оценка k содержания равновероятных функций значительно хуже оценки, приведенной в каталоге.

СПИСОК ЛИТЕРАТУРЫ

1. Словарь криптографических терминов. Под ред. Погорелова Б. А., Сачкова В. Н. М.: МЦНМО, 2006, 92 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. // *Sumarokov S. N.* Prohibitions of binary functions and reversibility for a class of coding devices. — OPPM Surv. Appl. Ind. Math., Moscow, 1994, v. 1, is. 1, p. 33–55. (In Russian).
3. *Golic J. D.* On the security of nonlinear filter generators. FSE'96. Lect. Notes Comput. Sci. 1996, v. 1039, p. 173–188.
4. *Никонов Н. В.* Метод растяжения в построении классов равновероятных k-значных функций с запретом. — Обозрение. прикл. и промышл. матем., 2006, т. 13, в. 6, с. 961–974. // *Nikonov N. V.* An extension method in the construction of classes of equiprobable k-valued functions with interdiction. — OPPM Surv. Appl. Ind. Math., Moscow, 2006, v. 13, is. 6, p. 961–974. (In Russian)
5. *Никонов Н. В.* Полиэдральные классы функций k-значной логики с обобщенными запретами и полузапретами. — Математические вопросы криптографии. 2012, т. 3, в. 1, с. 53–69. // *Nikonov N. V.* Polyhedral classes of k-valued logic functions with generalized filter taboo and semitaboo. — Mathematical Aspects of Cryptography, Moscow, 2012, v. 3, is. 1, p. 53–69. (In Russian)
6. *Домрачев В. С.*, *Никонов Н. В.* О свойствах обобщенных выходных v-грамм полиэдральных классов функций k-значной логики. — Обозрение. прикл. и промышл. матем., 2020, т. 27, № 2, с. 138–140. // *Domrachev V. S.*, *Nikonov N. V.* On properties of generalized output sequences of polyhedral k-valued logic functions. — OPPM Surveys Appl. Industr. Math., Moscow, 2020, v. 27, is. 2, p. 138–140. (In Russian.)
7. *Никонов Н. В.* О классификации всех булевых функций от 3-х переменных с обобщенными запретами. — Ж. Вестник МГУЛ «Лесной вестник», 2004, № 5 (36), с. 177–188. // *Nikonov N. V.* Classification of all Boolean functions in 3 variables with generalized taboo tuples. — Forestry Bulletin, 2004, v. 5 (36), p. 177–188. (In Russian.)

UDC 004.421.5

Domrachev V. S. (Moscow, TVP Laboratories)**. On influence of various threshold classes structures of k-valued logic functions on their properties in the filter generator.**

Abstract: The study aims to investigate the properties of the output v-tuples in the filter generator from the position of taboos and semitaboos of k-valued logic filter functions from polyhedral classes, constructed on the basis of various structures of generating Boolean function. The article presents estimates of logic value k for the guaranteed presence of balanced functions in polyhedral classes.

Keywords: Function taboo, function semitaboo, filter generator, balanced function.