4. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
5. *Luo G., Cao X., and Mesnager S.* Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. 2019. V. 11. No. 6. P. 1261–1273.
6. *Li Y., Kan H., Mesnager S., et al.* Generic constructions of (Boolean and vectorial) bent functions and their consequences // IEEE Trans. Inform. Theory. 2022. V. 68. No. 4. P. 2735–2751.
7. *Wolfmann A.* Special bent and near-bent functions // Adv. Math. Commun. 2014. V. 8. No. 1. P. 21–33.
8. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.
9. *Canteaut A. and Charpin P.* Decomposing bent functions // IEEE Trans. Inf. Theory. 2003. V. 49. No. 8. P. 2004–2019.
10. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions // LNCS. 1990. V. 473. P. 161–173.
11. *Kutsenko A.* Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.

УДК 519.7 DOI 10.17223/2226308X/15/8

ГЕНЕРАЦИЯ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С НЕВЫРОЖДЕННЫМИ КООРДИНАТНЫМИ ФУНКЦИЯМИ

И. А. Панкратова, Е. А. Рубан, С. В. Чикалова

Предложен алгоритм генерации обратимой векторной булевой функции, все координатные функции которой существенно зависят от всех переменных.

Ключевые слова: *векторные булевы функции, подстановки, существенная зависимость функции от переменной.*

Обозначим через $P_2(n)$ множество всех булевых функций от n переменных. Говорят, что переменная x_i, $1 \leqslant i \leqslant n$, *существенная для функции* $f(x_1, \ldots, x_n) \in P_2(n)$ (f *существенно зависит от переменной* x_i), если найдётся пара наборов $a, b \in \mathbb{Z}_2^n$, соседних по i-й координате, такая, что $f(a) \neq f(b)$; будем называть такую пару наборов *доказывающей существенность переменной* x_i *для функции* f (или просто *доказывающей парой*, если из контекста ясно, о каких переменной и функции идёт речь). Переменная, от которой функция не зависит существенно, называется *фиктивной для этой функции*; функции, существенно зависящие от всех переменных, — *невырожденными*.

Векторной булевой функцией $((n, m) -)$ называется отображение $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. Такую функцию можно рассматривать как упорядоченный набор из m булевых функций f_i, $i = 1, \ldots, m$, которые называются *координатными функциями*: $F = (f_1 \ldots f_m)$.

Оценим вероятность того, что случайно сгенерированная векторная булева функция невырожденная. По формуле включений и исключений определим D_n — количество функций в $P_2(n)$, имеющих фиктивные переменные:

$$D_n = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} 2^{2^{n-i}}.$$

Вероятность того, что булева функция от n переменных невырожденная, равна

$$\mathsf{P}_n = 1 - D_n / 2^{2^n}. \tag{1}$$

Вычисления по формуле (1) показывают, что $\mathsf{P}_n \approx 1$ при $n \geqslant 5$. Для случайной (n, m)-функции получаем вероятность невырожденности

$$\mathsf{P}_{n,m} = \mathsf{P}_n^m = \left(1 - D_n/2^{2^n}\right)^m. \tag{2}$$

Рассмотрим случай, когда $n = m$ и F обратима, т. е. является подстановкой на $\mathbb{Z}_2^n$. Подстановки используются во многих криптосистемах, в частности в криптосистемах с функциональными ключами [1, 2]. Для обеспечения стойкости криптосистем функции в них должны обладать определёнными свойствами; одно из таких свойств — существенная зависимость всех координат от всех переменных (т. е. их невырожденность). Векторную булеву функцию назовём *невырожденной*, если все её координатные функции невырожденные.

Для подстановок не удалось найти или получить формулу, аналогичную (2), но проведённые эксперименты дают тот же результат: начиная с $n = 5$, почти все случайно сгенерированные подстановки оказываются невырожденными. Тем не менее считаем, что задача генерации невырожденной подстановки не теряет своей значимости; например, в некоторой криптосистеме могут использоваться не любые подстановки, а из какого-то класса, для которого доля невырожденных подстановок в нём может оказаться другой (не близкой к 100 %).

Ранее в [3] предложен алгоритм генерации невырожденных подстановок с помощью n независимых транспозиций из тождественной подстановки или из такой, все координатные функции которой имеют ровно одну существенную переменную; обозначим классы подстановок, доставляемых этим алгоритмом, через $\mathcal{K}_n$ и $\mathcal{K}'_n$ соответственно. В [4, 5] описаны свойства функций этих классов, некоторые из них оказались неудовлетворительными с точки зрения криптографической стойкости. Кроме того, алгоритм в [3] не обладает свойством полноты, т. е. не может получить *любую* невырожденную подстановку. В данной работе эта проблема решена.

Докажем вспомогательные утверждения для булевых функций.

Утверждение 1. Пусть $f \in P_2(n)$, $f \neq \mathrm{const}$ и x_i — фиктивная переменная для f. Выберем два произвольных набора $a, b \in \mathbb{Z}_2^n$, таких, что $f(a) \neq f(b)$, и построим функцию $g \in P_2(n)$ так: $g(a) = f(b)$, $g(b) = f(a)$, $g(c) = f(c)$ для всех $c \in \mathbb{Z}_2^n \setminus \{a, b\}$. Тогда функция g существенно зависит от переменной x_i.

Доказательство. Пусть c — набор, соседний с a по i-й координате. Заметим, что $c \neq b$, так как x_i — фиктивная переменная для f и $f(a) \neq f(b)$. Получим

$$g(c) = f(c) = f(a) \neq f(b) = g(a),$$

т. е. x_i — существенная переменная для g. ■

Замечание 1. Поскольку выбор наборов a, b в утверждении 1 не зависит от номера фиктивной переменной, все переменные, фиктивные для f, являются существенными для построенной функции g.

Обозначим через $\mathbf{e}_i$, $1 \leqslant i \leqslant n$, булев вектор длины n с единственной единицей в i-й координате; $\mathrm{w}(f)$ — вес функции f.

Утверждение 2. Пусть $f \in P_2(n)$, $n \geqslant 3$, f уравновешенная и имеет фиктивную переменную. Тогда для каждой её существенной переменной найдётся не менее трёх доказывающих пар.

Доказательство. Пусть x_i — существенная и x_j — фиктивная переменные для функции f. Тогда $f(y) \neq f(y \oplus \mathbf{e}_i)$ для некоторого $y \in \mathbb{Z}_2^n$. В силу фиктивности переменной x_j можем записать, что

$$f(y \oplus \mathbf{e}_j) = f(y) \neq f(y \oplus \mathbf{e}_i) = f(y \oplus \mathbf{e}_i \oplus \mathbf{e}_j),$$

т. е. имеем две доказывающие пары: $\langle y, y \oplus \mathbf{e}_i \rangle$ и $\langle y \oplus \mathbf{e}_j, y \oplus \mathbf{e}_i \oplus \mathbf{e}_j \rangle$.

Разобьём множество $\mathbb{Z}_2^n$ на четвёрки наборов вида $\langle x, x \oplus \mathbf{e}_i, x \oplus \mathbf{e}_j, x \oplus \mathbf{e}_i \oplus \mathbf{e}_j \rangle$; одна из них (при $x = y$) содержит две доказывающие пары, а функция f на наборах этой четвёрки дважды принимает значение 0 и дважды 1.

Предположим, что больше доказывающих пар нет, тогда ввиду $f(x \oplus \mathbf{e}_j) = f(x) = f(x \oplus \mathbf{e}_i) = f(x \oplus \mathbf{e}_i \oplus \mathbf{e}_j)$ на наборах из каждой четвёрки (кроме случая $x = y$) функция f принимает одно и то же значение; пусть это значение равно 1 на k четвёрках. Получаем

$$\mathrm{w}(f) = 2 + 4k = 2^{n-1};$$

второе равенство должно выполняться в силу уравновешенности f, но оно невозможно при $n \geqslant 3$. ■

Следствие 1. Пусть для функции f выполнены условия утверждения 2. Тогда функция g, построенная способом, описанным в утверждении 1, невырожденная.

Доказательство. Если переменная фиктивная для функции f, то она является существенной для g (см. замечание 1).

Если переменная x_i существенная для функции f, то по утверждению 2 для неё существует не менее трёх доказывающих пар. Функция g отличается от функции f на двух наборах, поэтому независимо от того, как будут выбраны эти наборы, хотя бы одна пара, доказывающая существенность переменной x_i для функции g, останется. ■

На основании следствия 1 с учётом того, что координаты любой подстановки на $\mathbb{Z}_2^n$ уравновешены, получаем следующие два утверждения.

Утверждение 3. Пусть $n \geqslant 3$; $a, b \in \mathbb{Z}_2^n$ — произвольные взаимно инверсные наборы; G — подстановка на $\mathbb{Z}_2^n$, такая, что $G(a) = b$, $G(b) = a$, $G(c) = c$ для всех $c \in \mathbb{Z}_2^n \setminus \{a, b\}$. Тогда G невырожденная.

Утверждение 4. Пусть $n \geqslant 3$; F — подстановка на $\mathbb{Z}_2^n$, каждая координата которой имеет хотя бы одну фиктивную переменную; $F(x) = a$ и $F(y) = b$, где $a, b \in \mathbb{Z}_2^n$ — произвольные взаимно инверсные наборы. Построим подстановку G на $\mathbb{Z}_2^n$ так: $G(x) = b$, $G(y) = a$, $G(c) = F(c)$ для всех $c \in \mathbb{Z}_2^n \setminus \{a, b\}$. Тогда G невырожденная.

Оба утверждения имеют недостатки — функция G в утверждении 3 близка к тождественной, а в утверждении 4 строится из «особой» подстановки F, которую ещё надо как-то получить. Оба недостатка преодолены в алгоритме 1.

Полнота алгоритма 1 обеспечивается выбором любой подстановки на шаге 1.

Корректность алгоритма следует из того, что для функций f_i, которые меняются на шаге 6, выполнены условия следствия 1, следовательно, после обмена $F(x) \leftrightarrow F(y)$ они станут невырожденными. Остальные координатные функции F невырожденные уже с шага 1.

Для выполнения шага 1 в алгоритме 2 можно адаптировать на случай векторной функции алгоритм из [6, разд. 6.2].

Алгоритм 1. Генерация невырожденной подстановки на $\mathbb{Z}_2^n$

Вход: $n \in \mathbb{N}$, $n \geqslant 3$.

Выход: подстановка $F = (f_1 \dots f_n) : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, такая, что функции f_i существенно зависят от всех переменных, $i = 1, \dots, n$.

1: Построить случайную подстановку $F = (f_1 \dots f_n)$ на $\mathbb{Z}_2^n$ любым известным алгоритмом (например, методом тасования Фишера — Йетса [7]).
2: Построить вектор $v = (v_1 \dots v_n) \in \mathbb{Z}_2^n$, такой, что $v_i = 1 \Leftrightarrow f_i$ имеет фиктивную переменную, $i = 1, \dots, n$ (см. алгоритм 2).
3: **Если** $v = 0 \dots 0$, **то**
   выход, ответ — F.
4: Выбрать любой набор $x \in \mathbb{Z}_2^n$.
5: Найти $y \in \mathbb{Z}_2^n$, такой, что $F(y) = F(x) \oplus v$.
6: Поменять местами значения $F(x)$ и $F(y)$.
7: Выход, ответ — F.

Алгоритм 2. Анализ вырожденности векторной булевой функции

Вход: функция $F = (f_1 \dots f_m) : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$.

Выход: вектор $v = (v_1 \dots v_m) \in \mathbb{Z}_2^m$, такой, что $v_i = 1 \Leftrightarrow f_i$ имеет фиктивную переменную, $i = 1, \dots, m$.

1: Выполнить преобразование Мёбиуса $G = (g_1 \dots g_m) = \mu(F)$, где $g_i(a_1, \dots, a_n) = 1 \Leftrightarrow$ моном $x_1^{a_1} \dots x_n^{a_n}$ входит в АНФ функции f_i.
2: **Для всех** $i = 1, \dots, m$:
3: вычислить $c := \bigvee\limits_{a \in \mathbb{Z}_2^n : g_i(a) = 1} a$;
4: **Если** $c = 1, \dots, 1$, **то**
   $v_i := 0$,
5: **иначе**
6: $v_i := 1$.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
3. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
4. *Карпова Л. А., Панкратова И. А.* Свойства координатных функций одного класса подстановок на $\mathbb{F}_2^n$ // Прикладная дискретная математика. Приложение. 2017. № 10. С. 38–40.
5. *Панкратова И. А.* Свойства компонент некоторых классов векторных булевых функций // Прикладная дискретная математика. 2019. № 44. С. 5–11.
6. *Панкратова И. А.* Булевы функции в криптографии. СПб., М., Краснодар: Лань, 2019.
7. *Кнут Д. Э.* Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е изд. М.: Вильямс, 2007.