Согласно [8, теорема 2 § 2 гл. XII, с. 448–449], случайная величина с законом распределения, соответствующим производящей функции (3), является собственной, если $\mathbf{E}V_2 \geqslant d+1$, и имеет конечное математическое ожидание, если $\mathbf{E}V_2 > d+1$. Очевидно, $\mathbf{E}V_2 = N$. Значит, $\sigma(1) = 1$ при $N \geqslant d+1$ и $\sigma'(1) = 1$ при $N \geqslant d+2$.

ЛИТЕРАТУРА

1. *Golic J. Dj.* Constrained embedding probability for two binary strings // SIAM J. Discrete Math. 1996. V. 9. No. 3. P. 360–364.
2. *Михайлов В. Г., Меженная Н. М.* Оценки для вероятности плотного вложения одной дискретной последовательности в другую // Дискретная математика. 2005. Т. 17. № 3. С. 19–27.
3. *Михайлов В. Г., Меженная Н. М.* Нижние оценки для вероятности вложения с произвольным допуском // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер. Естественные науки. 2012. № 2. С. 3–11.
4. *Donovan D. M., Lefevre J., and Simpson L.* A discussion of constrained binary embeddings with applications to cryptanalysis of irregularly clocked stream ciphers // R. Balakrishnan and C. V. Madhavan (eds.) Discrete Mathematics. Proc. Intern. Conf. on Discr. Math., Indian Institute of Science, Bangalore, December 2006. P. 73–86.
5. *Kholosha A.* Clock-controlled shift registers for key-stream generation // IACR Cryptology ePrint Archive 2001: 61 (2001). `http://eprint.iacr.org/2001/061.pdf`
6. *Меженная Н. М.* О проверке гипотезы о плотном вложении для дискретных случайных последовательностей // Вестник БГУ. Математика, Информатика. 2017. № 4. С. 9–20.
7. *Меженная Н. М.* Предельные теоремы в задачах о плотном вложении и плотных сериях в дискретных случайных последовательностях: дис. ... канд. физ.-мат. наук. Московский государственный институт электроники и математики. М., 2009.
8. *Феллер В.* Введение в теорию вероятностей и ее приложения: в 2 т. М.: Мир, 1984. Т. 2. 751 с.

УДК 519.7 DOI 10.17223/2226308X/11/4

НИЖНЯЯ ОЦЕНКА МОЩНОСТИ НАИБОЛЬШЕГО МЕТРИЧЕСКИ РЕГУЛЯРНОГО ПОДМНОЖЕСТВА БУЛЕВА КУБА[1]

А. К. Облаухов

Исследуются строго метрические регулярные подмножества булева куба. Представлены итеративные конструкции таких множеств. Получена формула для вычисления количества строго метрически регулярных множеств, получаемых с помощью данных конструкций. Построены специальные семейства метрически регулярных множеств и вычислены мощности множеств из этих семейств. Полученные значения дают нижнюю оценку мощности наибольших метрически регулярных множеств при фиксированном радиусе покрытия.

Ключевые слова: *метрически регулярное множество, метрическое дополнение.*

Рассмотрим $\mathbb{F}_2^n$ — пространство двоичных векторов длины n. *Расстояние Хэмминга* $\mathrm{d}(x, y)$ между двумя векторами $x, y \in \mathbb{F}_2^n$ равно количеству координат, в которых эти векторы различаются.

[1]Работа поддержана грантами РФФИ, проекты № 18-31-00479 и 17-41-543364.

Пусть $X \subseteq \mathbb{F}_2^n$ — произвольное множество, $y \in \mathbb{F}_2^n$ — произвольный вектор. Расстояние от y до X определяется как $\mathrm{d}(y, X) = \min\limits_{x \in X} \mathrm{d}(y, x)$. *Радиусом покрытия* множества X называется $\mathrm{d}(X) = \max\limits_{z \in \mathbb{F}_2^n} \mathrm{d}(z, X)$.

Рассмотрим множество $Y = \{y \in \mathbb{F}_2^n : \mathrm{d}(y, X) = \mathrm{d}(X)\}$ векторов, находящихся на максимальном расстоянии от X. Это множество называется *метрическим дополнением* [1] множества X и обозначается $\widehat{X}$. Если $\widehat{\widehat{X}} = X$, то множество X называется *метрически регулярным*.

Задача исследования максимальных и минимальных (по мощности) метрически регулярных множеств возникает на пути изучения *бент-функций*, множество которых является метрически регулярным [2]. Бент-функции часто используются в криптографии из-за высокой нелинейности [3], обеспечивающей повышенную устойчивость шифров к криптографическим атакам, однако многие связанные с ними задачи остаются открытыми. Например, неизвестно точное количество бент-функций в общем случае, а существующие верхняя и нижняя оценки значительно разнятся по порядку.

В работе изучается особый подкласс метрически регулярных множеств — строго метрически регулярные множества. Множества A, B, такие, что $\widehat{A} = B$, $\widehat{B} = A$ и $\mathrm{d}(A) = \mathrm{d}(B) = d$, называются *строго метрически регулярными*, если для любого вектора $x \in \mathbb{F}_2^n$ выполнено равенство $\mathrm{d}(x, A) + \mathrm{d}(x, B) = d$.

Получены итеративные конструкции строго метрически регулярных множеств.

Теорема 1. Пусть A, B — пара строго метрически регулярных множеств, являющихся метрическими дополнениями друг друга. Тогда $C = A \cup B$ также является строго метрически регулярным множеством.

Обобщение данной конструкции (теорема 2) позволяет получать больше строго метрически регулярных множеств с различными радиусами покрытия из известной пары строго метрически регулярных множеств A, B.

Теорема 2. Пусть A, B — пара строго метрически регулярных множеств, являющихся метрическими дополнениями друг друга с радиусом покрытия d. Обозначим $A_k = \{x \in \mathbb{F}_2^n : \mathrm{d}(x, A) = k\}$, $k = 0, 1, \ldots, d$. Пусть $i_1, \ldots, i_s$ — последовательность чисел, $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant d$. Тогда объединение $C = \bigcup\limits_{k=1}^{s} A_{i_k}$ является строго метрически регулярным множеством тогда и только тогда, когда существует число $r > 0$, такое, что выполняются все следующие условия:

1) для любого $k \in \{1, \ldots, s-1\}$ разница $(i_{k+1} - i_k)$ равна 1, $2r$ или $2r+1$;
2) для любого $k \in \{2, \ldots, s-1\}$ как минимум одна из разниц $(i_{k+1} - i_k), (i_k - i_{k-1})$ больше единицы;
3) i_1 равно либо r, либо 0, и если $i_1 = 0$ и $s > 1$, то $i_2 - i_1 = 2r$ или $2r+1$;
4) i_s равно либо $d - r$, либо d, и если $i_s = d$ и $s > 1$, то $i_s - i_{s-1} = 2r$ или $2r+1$.

Число r является радиусом покрытия множества C.

Получены формулы, позволяющие вычислить количество множеств, получаемых с помощью обобщённой конструкции.

Теорема 3. Пусть A, B — пара строго метрически регулярных множеств, являющихся метрическими дополнениями друг друга с радиусом покрытия d. Тогда количество $G_r(d)$ различных строго метрически регулярных множеств с радиусом покрытия r, которые можно получить с помощью теоремы 2 из пары A, B, вычисляется по следующим реккурентным формулам:

$$\begin{cases} G_r(d) = G_r(d-r) + G_r(d-r-1), \text{ если } d > r, \\ G_r(r) = 2, \\ G_r(d) = 0, \text{ если } 0 \leqslant d < r. \end{cases}$$

При помощи конструкции из теоремы 2, применённой к паре граней в пространствах соответствующих размерностей, построено семейство множеств $\{Y_n^d\}$ $(n \geqslant 2d)$, имеющих большую (относительно мощности всего пространства) мощность. Индекс n отражает размерность булева куба, в котором лежит соответствующее множество, а d — его радиус покрытия. На основе сферы радиуса d в пространстве $\mathbb{F}_2^{2d}$ построено семейство множеств $\{Z_n^d\}$ (также для $n \geqslant 2d$). Вычислив точные размеры множеств семейств (либо оценив их снизу), получаем нижнюю оценку на мощность наибольших метрически регулярных множеств.

Теорема 4. Пусть A — наибольшее метрически регулярное множество с радиусом покрытия d в булевом кубе размерности n $(n \geqslant 2d)$, r — остаток от деления $n+1$ на $2d+1$. Тогда $|A| \geqslant \max\left\{2^{n-2d}\binom{2d}{d},\ 2^n\left(\frac{2}{2d+1} - \frac{2}{\sqrt{n-r+1}}\right)\right\}$.

Заметим, что при достаточно больших d, n первое число приблизительно равно $1/\sqrt{\pi d}$ от мощности булева куба, второе — $2/(2d+1)$ от мощности булева куба.

ЛИТЕРАТУРА

1. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Т. 23. № 3. С. 93–106.
2. *Tokareva N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. No. 3. P. 666–670.
3. *Cusick T. W. and Stanica P.* Cryptographic Boolean Functions and Applications. Academic Press, 2017. 288 p.

УДК 519.1 DOI 10.17223/2226308X/11/5

УЛУЧШЕННАЯ ФОРМУЛА УНИВЕРСАЛЬНОЙ ОЦЕНКИ ЭКСПОНЕНТА ОРГРАФА[1]

В. М. Фомичев

Улучшена формула универсальной оценки экспонента n-вершинного примитивного орграфа, данная А. Далмэджем и Н. Мендельсоном (1964) с использованием множества контуров, длины которых взаимно простые. Предложенная формула использует в орграфе множество контуров $\hat{C}$ с множеством длин $L(\hat{C}) = \{l_1, \ldots, l_m\}$, где $d = (l_1, \ldots, l_m) \geqslant 1$, и множество длин кратчайших путей $\{r_{i,j}^{s/d}(\hat{C}) : s = 0, \ldots, d-1\}$ из вершины i в вершину j, проходящих через множество контуров $\hat{C}$ и образующих полную систему вычетов по модулю d. Показано, что $\exp\Gamma \leqslant 1 + \hat{F}\big(L(\hat{C})\big) + R(\hat{C})$, где $\hat{F}(L) = d \cdot F(l_1/d, \ldots, l_m/d)$; $F(a_1, \ldots, a_m)$ — число Фробениуса; $R(\hat{C}) = \max\limits_{(i,j)} \max\limits_{s} \{r_{i,j}^{s/d}(\hat{C})\}$. Указан класс орграфов с множеством вершин $\{0, \ldots, 2k-1\}$, $k > 2$, для которых предложенные оценки экспонентов лучше известных на величину $k-2$.

Ключевые слова: *число Фробениуса, примитивный орграф, экспонент орграфа.*

[1]Работа выполнена в соответствии с грантом РФФИ № 16-01-00226.