

Алгебраические свойства квазигрупп,
порождаемых правильными семействами булевых функций

II Международная научная конференция
«Актуальные вопросы математики и физики»

К. Д. Царегородцев

МГУ им. М.В. Ломоносова

24.09.2025, Волгоград

Квазигруппа

Множество Q с заданной на нём бинарной операцией $\circ: Q \times Q \rightarrow Q$, со следующим свойством: для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что:

$$a \circ x = b, \quad y \circ a = b.$$

Denes и Keedwell, *Latin squares and their applications (2nd edition)*; Белоусов, *Основы теории квазигрупп и луп*.



Криптография на квазигруппах: примеры

■ Симметричные примитивы: шифры¹, хэш-функции².

¹Gligoroski, Markovski и Knapskog, «The stream cipher Edon80»; Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

²Gligoroski, Markovski и Kocarev, «Edon-R, An Infinite Family of Cryptographic Hash Functions»; Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'».

³Катышев, Виктор Тимофеевич Марков и Александр Александрович Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей».

⁴Gribov, Zolotych и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring»; В. Т. Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

⁵Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups»; Gligoroski, Ødegård, Jensen и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».



Криптография на квазигруппах: примеры

- Симметричные примитивы: шифры¹, хэш-функции².
- Асимметричные примитивы: аналоги протокола Диффи-Хеллмана³, гомоморфное шифрование⁴, шифрование с лазейкой⁵ и многое другое.

¹Gligoroski, Markovski и Knapskog, «The stream cipher Edon80»; Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

²Gligoroski, Markovski и Kocarev, «Edon-R, An Infinite Family of Cryptographic Hash Functions»; Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'».

³Катышев, Виктор Тимофеевич Марков и Александр Александрович Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей».

⁴Gribov, Zolotych и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring»; В. Т. Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

⁵Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups»; Gligoroski, Ødegård, Jensen и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».



Криптографически релевантные свойства квазигрупп

- Малое число $a(Q)$ ассоциативных троек

$$a(Q) = |\{(a, b, c) \in Q^3 \mid (a \circ b) \circ c = a \circ (b \circ c)\}|$$



Криптографически релевантные свойства квазигрупп

- Малое число $a(Q)$ ассоциативных троек

$$a(Q) = |\{(a, b, c) \in Q^3 \mid (a \circ b) \circ c = a \circ (b \circ c)\}|$$

- Полиномиальная полнота квазигрупп (любое отображение $f: Q^n \rightarrow Q$ задается с помощью композиции констант и операции умножения).



Криптографически релевантные свойства квазигрупп

- Малое число $a(Q)$ ассоциативных троек

$$a(Q) = |\{(a, b, c) \in Q^3 \mid (a \circ b) \circ c = a \circ (b \circ c)\}|$$

- Полиномиальная полнота квазигрупп (любое отображение $f: Q^n \rightarrow Q$ задается с помощью композиции констант и операции умножения).
- Отсутствие подквазигрупп, т.е. подмножеств $Q' \subset Q$, которые замкнуты относительно умножения.



Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; для практических приложений $|Q| \approx 2^{64}$, это много.

⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

⁷Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

⁸В. Т. Марков, Михалёв и А. А. Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

⁹Snášel и др., «Hash functions based on large quasigroups».



Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; для практических приложений $|Q| \approx 2^{64}$, это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого, компактно задаваемого класса⁶.

⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

⁷Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

⁸В. Т. Марков, Михалёв и А. А. Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

⁹Snášel и др., «Hash functions based on large quasigroups».



Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; для практических приложений $|Q| \approx 2^{64}$, это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого, компактно задаваемого класса⁶.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)⁷.

⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

⁷Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

⁸В. Т. Марков, Михалёв и А. А. Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

⁹Snášel и др., «Hash functions based on large quasigroups».



Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; для практических приложений $|Q| \approx 2^{64}$, это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого, компактно задаваемого класса⁶.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)⁷.
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой⁸, модульное вычитание⁹).

⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

⁷Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

⁸В. Т. Марков, Михалёв и А. А. Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

⁹Snášel и др., «Hash functions based on large quasigroups».



Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; для практических приложений $|Q| \approx 2^{64}$, это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого, компактно задаваемого класса⁶.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)⁷.
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой⁸, модульное вычитание⁹).
- Различные способы функционального задания квазигруппы.

⁶Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

⁷Gligoroski, Ødegård, Mihova и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

⁸В. Т. Марков, Михалёв и А. А. Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

⁹Snášel и др., «Hash functions based on large quasigroups».



Правильное семейство

Семейство функций

$$f_i: Q^n \rightarrow Q, \quad 1 \leq i \leq n,$$

называется правильным, если для любых двух наборов $x \neq y$ найдется такая координата i , что $x_i \neq y_i$, но $f_i(x) = f_i(y)$.

Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups»; Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом», «Построение классов латинских квадратов в булевой базе данных»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».



Правильное семейство

Семейство функций

$$f_i: Q^n \rightarrow Q, \quad 1 \leq i \leq n,$$

называется правильным, если для любых двух наборов $x \neq y$ найдется такая координата i , что $x_i \neq y_i$, но $f_i(x) = f_i(y)$.

Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups»; Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом», «Построение классов латинских квадратов в булевой базе данных»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

При росте n число булевых правильных семейств растет достаточно быстро.

Размер n	Число булевых правильных семейств
$n = 2$	$\approx 2^{3.58}$
$n = 3$	$\approx 2^{9.54}$
$n = 4$	$\approx 2^{22.4}$
$n = 5$	$\approx 2^{49.18}$

Пусть \mathcal{F}, \mathcal{G} — два правильных семейства функций размера n над группой $(G^n, +)$.
Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию \circ следующим образом:

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}).$$



Пусть \mathcal{F}, \mathcal{G} — два правильных семейства функций размера n над группой $(G^n, +)$.
Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию \circ следующим образом:

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}).$$

Об индексах ассоциативности

- Операция \circ является квазигрупповой.
- Индексы ассоциативности квазигрупп, построенных по паре $(\mathcal{F}, \mathcal{G})$ и по паре $(\mathcal{G}, \mathcal{F})$, совпадают.
- Для $G = \mathbb{Z}_2$ индексы ассоциативности квазигрупп, построенных по паре $(\mathcal{F}, \mathcal{G})$ и по паре $(\mathcal{F} \oplus \alpha, \mathcal{G} \oplus \alpha)$, совпадают.
- Для $G = \mathbb{Z}_2$ количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, четно.



Ассоциативность, $n = 2$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

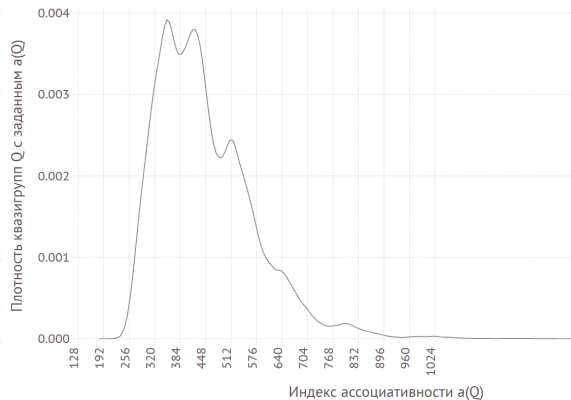
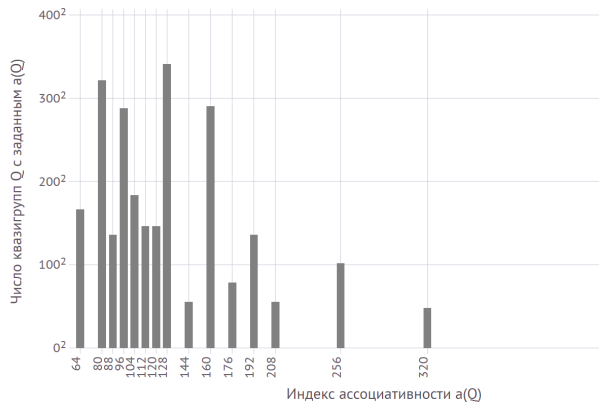
$a(Q)$	Кол-во Q
16	32
32	96
64	16

Ассоциативность, $n = 3$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

$a(Q)$	КОЛ-ВО Q	$a(Q)$	КОЛ-ВО Q
64	27648	144	3072
80	103424	160	84480
88	18432	176	6144
96	82944	192	18432
104	33792	208	3072
112	21504	256	10368
120	21504	320	2304
128	116352	512	64

Ассоциативность, $n = 4$



Подстановки, порождаемые правильными семействами

Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное, (Q, \circ) — квазигруппа. Тогда отображение

$$\sigma_{\mathcal{F}}(x): x \rightarrow x \circ \mathcal{F}(x), \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \rightarrow \begin{bmatrix} x_1 \circ f_1(x_1, \dots, x_n) \\ \vdots \\ x_n \circ f_n(x_1, \dots, x_n) \end{bmatrix}$$

является подстановкой: $\sigma_{\mathcal{F}} \in Perm(Q^n)$.



Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок»

Если $(Q, +)$ — группа (т.е., операция $+$ ассоциативна), то семейство $\mathcal{G}: Q^n \rightarrow Q^n$, определенное равенством

$$\mathcal{G}(x) = (-x) + \sigma_{\mathcal{F}}^{-1}(x)$$

также является правильным.



Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок»

Если $(Q, +)$ — группа (т.е., операция $+$ ассоциативна), то семейство $\mathcal{G}: Q^n \rightarrow Q^n$, определенное равенством

$$\mathcal{G}(x) = (-x) + \sigma_{\mathcal{F}}^{-1}(x)$$

также является правильным.

Т.е., если \mathcal{F} — правильное, то существует правильное семейство \mathcal{G} со свойством

$$\sigma_{\mathcal{F}}^{-1}(x) = \sigma_{\mathcal{G}}(x).$$



Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок»

Если $(Q, +)$ — группа (т.е., операция $+$ ассоциативна), то семейство $\mathcal{G}: Q^n \rightarrow Q^n$, определенное равенством

$$\mathcal{G}(x) = (-x) + \sigma_{\mathcal{F}}^{-1}(x)$$

также является правильным.

Т.е., если \mathcal{F} — правильное, то существует правильное семейство \mathcal{G} со свойством

$$\sigma_{\mathcal{F}}^{-1}(x) = \sigma_{\mathcal{G}}(x).$$

Таким образом, множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).



О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.



О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.

Транзитивность действия

Замыкание $\mathcal{S}^{\text{prop}}$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).



О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.

Транзитивность действия

Замыкание $\mathcal{S}^{\text{prop}}$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).

Булев случай

При $Q = \mathbb{E}_2$ замыкание $\sigma_{\mathcal{F}}$ порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

Schurr, «Unique sink orientations of cubes».



О подстановках, порождаемых правильными семействами-3

Пусть \mathcal{F} — правильное семейство булевых функций.

Четность числа элементов в прообразе

Для любого $\alpha \in \{0, 1\}^n$ число решений уравнения $\mathcal{F}(x) = \alpha$ всегда четно.



О подстановках, порождаемых правильными семействами-3

Пусть \mathcal{F} — правильное семейство булевых функций.

Четность числа элементов в прообразе

Для любого $\alpha \in \{0, 1\}^n$ число решений уравнения $\mathcal{F}(x) = \alpha$ всегда четно.

Количество неподвижных точек $\sigma_{\mathcal{F}}$

У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.



Простота и неаффинность, $n = 2$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

Свойства	Аффинная	Неаффинная
Не простая	112	0
Простая	32	0



Простота и неаффинность, $n = 3$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

Свойства	Аффинная	Неаффинная
Не простая	30784	231936
Простая	9216	281600



- Рассмотрены некоторые релевантные с точки зрения криптографии свойства квазигрупп, порождаемых правильными семействами.



- Рассмотрены некоторые релевантные с точки зрения криптографии свойства квазигрупп, порождаемых правильными семействами.
- Доказан ряд утверждений про индекс ассоциативности получаемых квазигрупп, проведен вычислительный эксперимент для $n = 2, 3, 4$.









- Рассмотрены некоторые релевантные с точки зрения криптографии свойства квазигрупп, порождаемых правильными семействами.
- Доказан ряд утверждений про индекс ассоциативности получаемых квазигрупп, проведен вычислительный эксперимент для $n = 2, 3, 4$.
- Доказан ряд утверждений про подстановки, порождаемые правильными семействами функций; проведен вычислительный эксперимент для проверки простоты и неаффинности для $n = 2, 3$.



Спасибо за внимание!








Список литературы I

-  Chen, Y., S. J. Knapskog и D. Gligoroski. «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity». *АНГЛ. В: Submitted to ISIT 2010 (2010)*, с. 14.
-  Denes, J. и A. Keedwell. *Latin squares and their applications (2nd edition)*. *АНГЛ.* Elsevier, 2015.
-  Galatenko, A. V., V. A. Nosov и A. E. Pankratiev. «Latin squares over quasigroups». *АНГЛ. В: Lobachevskii Journal of Mathematics 41.2 (2020)*, с. 194—203.
-  Gligoroski, D., S. Markovski и S. J. Knapskog. «A public key block cipher based on multivariate quadratic quasigroups». *АНГЛ. В: arXiv preprint arXiv:0808.0247 (2008)*.
-  — . «The stream cipher Edon80». *АНГЛ. В: New stream cipher designs*. Springer, 2008, с. 152—169.
-  Gligoroski, D., S. Markovski и L. Kocarev. «Edon-R, An Infinite Family of Cryptographic Hash Functions». *АНГЛ. В: International Journal of Security and Networks 8.3 (2009)*, с. 293—300.








Список литературы II

-  Gligoroski, D., R. S. Ødegård, R. E. Jensen и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme». Англ. В: *International Conference on Trusted Systems*. Springer. 2011, с. 184—203.
-  Gligoroski, D., R. S. Ødegård, M. Mihova и др. «Cryptographic hash function Edon-R'». Англ. В: *2009 Proceedings of the 1st International Workshop on Security and Communication Networks*. IEEE. 2009, с. 1—9.
-  Gribov, Aleksei Viktorovich, Pavel Andreevich Zolotykh и Aleksandr Vasil'evich Mikhalev. «A construction of algebraic cryptosystem over the quasigroup ring». В: *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]* 1.4 (2010), с. 23—32.
-  Schurr, I. «Unique sink orientations of cubes». Англ. Дис. ... док. ETH Zurich, 2004.
-  Snášel, V. и др. «Hash functions based on large quasigroups». Англ. В: *Computational Science-ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I* 9. Springer. 2009, с. 521—529.







Список литературы III

-  Tiwari, S. K. и др. «INRU: A Quasigroup Based Lightweight Block Cipher». Англ. В: *arXiv preprint arXiv:2112.07411* (2021).
-  Белоусов, В. Д. *Основы теории квазигрупп и луп*. М.: Наука, 1967.
-  Грибов, А. В. «Алгебраические неассоциативные структуры и их приложения в криптографии». Дис. ... док. Московский государственный университет им. М. В. Ломоносова, 2015.
-  Катышев, Сергей Юрьевич, Виктор Тимофеевич Марков и Александр Александрович Нечаев. «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей». В: *Дискретная математика* 26.3 (2014), с. 45—64.
-  Марков, В. Т., А. В. Михалёв и Е. С. Кислицын. «Неассоциативные структуры в гомоморфной криптографии». В: *Фундаментальная и прикладная математика* 23.2 (2020), с. 209—215.



Список литературы IV

-  Марков, В. Т., А. В. Михалёв и А. А. Нечаев. «Неассоциативные алгебраические структуры в криптографии и кодировании». В: *Фундаментальная и прикладная математика* 21.4 (2016), с. 99—124.
-  Носов, В. А. «Критерий регулярности булевского неавтономного автомата с разделенным входом». В: *Интеллектуальные системы. Теория и приложения* 3.3-4 (1998), с. 269—280.
-  — . «Построение классов латинских квадратов в булевой базе данных». В: *Интеллектуальные системы. Теория и приложения* 4.3-4 (1999), с. 307—320. ISSN: 2075-9460; 2411-4448.
-  Носов, В. А. и А. Е. Панкратьев. «Латинские квадраты над абелевыми группами». В: *Фундаментальная и прикладная математика* 12.3 (2006), с. 65—71.

