Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2

Пивень Н.А.

Ключевые слова: Квазигруппа, латинский квадрат, параметрическое задание, полиномиальная полнота, правильные семейства функций.

В работе анализируются всевозможные латинские квадраты порядка 4, порождаемые с помощью правильных семейств функций. Оказывается, что все такие квадраты задают квазигруппы, не являющиеся полиномиально полными. Предлагается обобщение конструкции, связанной с правильными семействами. В результате удается в 4 раза увеличить число порождаемых латинских квадратов и получить значительное число полиномиально полных квазигрупп.

1. Введение

В наши дни разрабатываются различные способы защиты информации, использующие квазигруппы и связанные с ними латинские квадраты. Это обусловлено например тем, что К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают свойством “совершенной секретности” ([1]). Примеры использования квазигрупп для решения различных задач криптографии можно найти в работах [2, 3, 4, 5].

С точки зрения криптографических приложений важную роль играет свойство полиномиальной полноты квазигрупп, так как задача распознавания разрешимости системы уравнений в полиномиально полной алгебре NP-полна ([6]). В работе [7] В. А. Артамоновым с соавторами в частности был получен критерий полиномиальной полноты квазигрупп порядка 4. Интересные результаты о полиномиальной полноте квазигрупп в более общем случае можно найти в работах [8, 9, 10].

В случае конечных квазигрупп квазигрупповая операция может быть задана таблицей Кэли, являющейся латинским квадратом. В. А. Носовым в работе [11] был предложен эффективный способ задания больших семейств латинских квадратов с помощью так называемых правильных семейств функций. Мы анализируем всевозможные латинские квадраты порядка 4, задаваемые правильными семействами функций. Оказывается, что, во-первых, таким образом порождается 60 из 576 квазигрупп, и, во-вторых, ни одна порождаемая квазигруппа не является полиномиально полной. Для устранения этого недостатка предлагается усиление конструкции В. А. Носова, названное перестановочной конструкцией. При ее использовании удается породить 240 латинских квадратов, 112 из которых задают полиномиально полные квазигруппы.

Дальнейшее изложение имеет следующую структуру. В разделе 2 даются основные определения. В разделе 3 анализируются латинские квадраты порядка 4, порождаемые правильными семействами функций. В разделе 5 вводится перестановочная конструкция и доказывается ее корректность. В разделе 6 анализируются латинские квадраты порядка 4, задаваемые перестановочной конструкцией. В приложении приводится список классов изоморизма построенных латинских квадратов.

Автор выражает благодарность А. Е. Панкратьеву и А. В. Галатенко за постановку задачи и внимание к работе.

2. Основные понятия

Определение 1. Конечной квазигруппой (Q, f_Q) называется множество Q, $|Q| < \infty$, на котором определена бинарная операция f_Q такая, что для любых элементов $a, b \in Q$ уравнения $f_Q(a, x) = b$ и $f_Q(y, a) = b$ однозначно разрешимы в Q.

В дальнейшем мы будем опускать слово “конечная”.

Определение 2. Латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n-элементного множества таким образом, что в каждой её строке и в каждом столбце все элементы различны.

Квазигрупповую операцию можно задавать табличным способом: для множества элементов $\{q_1, \ldots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица $m \times m$, такая что на пересечении i-ой строки и j-го столбца стоит $f_Q(q_i, q_j)$. Заметим, что построенная таким образом таблица, в связи с существованием и единственностью решения

уравнений $f_Q(a,x) = b$ и $f_Q(y,a) = b$, является латинским квадратом, который мы и называем латинским квадратом, связанным с квазигруппой.

Определение 3. Две квазигруппы (Q, f_Q) и (Q, f'_Q) называются изоморфными, если существует биекция $\varphi : Q \to Q$ такая, что для любых $a, b \in Q$ выполнено равенство $f'_Q(\varphi(a), \varphi(b)) = \varphi(f_Q(a,b))$. Функция φ называется изоморфизмом квазигрупп (Q, f_Q) и (Q, f'_Q).

Определение 4. Две квазигруппы (Q, f_Q) и (Q, f'_Q) называются изотопными, если существуют такие перестановки α, β и γ на множестве Q, что для любых $a, b \in Q$ справедливо равенство $f'_Q(a,b) = \gamma^{-1}(f_Q(\alpha(a), \beta(b)))$.

Понятие изотопности естественным образом переносится на латинские квадраты. Несложно увидеть, что матрица, изотопная латинскому квадрату, сама является латинским квадратом.

Пусть $n \in \mathbb{N} \cup \{0\}$, $\mathcal{O}_n$ — множество всех n-местных функций на множестве Q, $\mathcal{O} = \bigcup\limits_{n=0}^{\infty} \mathcal{O}_n$. На множестве $\mathcal{O}$ стандартным образом вводятся операции суперпозиции и замыкания ([12]). Замыкание множества $F \subseteq \mathcal{O}$ обозначается через $[F]$.

Определение 5. Квазигруппа (Q, f_Q) называется полиномиально полной, если $[\{f_Q\} \cup \mathcal{O}_0] = \mathcal{O}$.

Определение 6. Квазигруппа (Q, f_Q) называется простой, если операция f_Q не сохраняет ни одного нетривиального отношения эквивалентности на множестве Q.

Определение 7. Квазигруппа (Q, f_Q) называется аффинной, если на множестве Q может быть введена структура абелевой группы $(Q, +)$, такая что существуют автоморфизмы α, β группы $(Q, +)$, элемент $c \in Q$, и для любых $a, b \in Q$ справедливо равенство $f_Q(a,b) = \alpha(a) + \beta(b) + c$.

Несложно увидеть, что простота и аффинность сохраняются при изоморфизме.

Известно ([13]), что квазигруппа является полиномиально полной если и только если она простая и не аффинная. В случае $|Q| = 4$ в работе [7] установлено, что квазигруппа полиномиально полна тогда и только тогда, когда соответствующий латинский квадрат обладает следующими двумя свойствами:

I. среди строк и столбцов квадрата есть перестановка с 3-циклом (что обеспечивает простоту);

II. цикловая структура строк не является одной из этих трех (что обеспечивает не аффинность):

   1) четыре 3-цикла;

   2) два 4-цикла и две строки по два 2-цикла;

   3) одна тождественная перестановка и три строки по два 2-цикла.

Определение 8. Семейство булевых функций $\mathrm{F}=\{f_i\}_{i=1}^n$, $f_i = f_i(x_1, \ldots, x_n)$, называется правильным, если для любых различных значений аргументов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдется такой индекс $\alpha \in \{1, \ldots, n\}$, что $x'_\alpha \neq x''_\alpha$, $f_\alpha(x'_1, \ldots, x'_n) = f_\alpha(x''_1, \ldots, x''_n)$

Правильные семейства функций были введены В. А. Носовым в работе [11] для построения латинских квадратов порядка 2^n. Занумеруем элементы множества Q, $|Q| = 2^n$, числами от 0 до $2^n - 1$. Таким образом, каждому элементу $a \in Q$ можно сопоставить n-битный вектор $(a_1, \ldots, a_n)$, задающий двоичную запись номера. В результате квазигрупповая операция f_Q может быть представлена в векторной форме: записи $z = f_Q(x, y)$ и

$$\begin{aligned} z_1 &= f_Q^1(x_1, \ldots, x_n, y_1, \ldots, y_n), \\ &\vdots \\ z_n &= f_Q^n(x_1, \ldots, x_n, y_1, \ldots, y_n), \end{aligned}$$

где $f_Q^1, \ldots, f_Q^n$ — булевы функции, являющиеся компонентами вектор-функции, порожденной f_Q, эквивалентны.

Пусть $f_1, \ldots, f_n$ — булевы функции от n переменных, $\pi_1, \ldots, \pi_n$ — булевы функции от двух переменных. Рассмотрим следующее семейство функций от $2n$ переменных:

$$\begin{aligned} g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ &\vdots \\ g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{aligned} \tag{1}$$

где операция $\oplus$ означает сложение по модулю 2. В работе [11] показано, что семейство $G = \{g_1, \ldots, g_n\}$ задает латинский квадрат для любых функций $\pi_1, \ldots, \pi_n$ тогда и только тогда, когда семейство $F = \{f_1, \ldots, f_n\}$ правильное.

3. Латинские квадраты порядка 4, задаваемые правильными семействами

Рассмотрим латинские квадраты порядка 4, задаваемые всевозможными правильными семействами функций порядка 2 с помощью конструкции В. А. Носова. Известно ([14]), что в этом случае одна из функций правильного семейства является константой, а вторая фиктивно зависит от одноименной переменной.

Теорема 1. *С помощью правильных семейств порядка 2 порождается 60 различных латинских квадратов порядка 4, входящих в 8 различных классов изоморфизма. При этом все задаваемые квазигруппы не обладают свойством полиномиальной полноты.*

Доказательство. В силу структуры правильных семейств порядка 2, формулы для задания латинских квадратов принимают вид

$$\begin{aligned} z_1 &= x_1 \oplus y_1 \oplus f_1(\pi_2(x_2, y_2)) \\ z_2 &= x_2 \oplus y_2 \oplus f_2(\pi_1(x_1, y_1)). \end{aligned}$$

При этом возможны следующие случаи.

1) Обе функции f_1, f_2 являются константами. Несложно увидеть, что здесь возникает 4 различных латинских квадрата.

2) Ровно одна из функций f_1, f_2 являетсяя константой. Заметим, что выбор номера константной функции и выбор значения константы может быть выполнен четырьмя способами. Без ограничения общности рассмотрим случай, когда f_1 отлична от константы и f_2 тождественно равна 0. Значит, f_1 является тождественной функцией, либо отрицанием. Так как отрицание может быть опущено на переменную, множество латинских квадратов, задаваемых семейством, в котором $f_1(x) = x$, и семейством, в котором $f_1(x) = \overline{x}$, совпадают, и без ограничения общности можно считать, что $f_1(x) = x$. Заметим, что получаемые в этом случае латинские квадраты будут отличаться от латинских квадратов, учтенных в прошлом пункте, тогда и только тогда, когда функция π_2 отлична от константы. Таких функций 14. Очевидно, что различные функции π_2 задают различные латинские квадраты. Значит, общее число новых латинских квадратов, полученных в этом пункте, равно $14 \cdot 4 = 56$.

Таким образом, общее число латинских квадратов, порожденных правильными семействами порядка 2, равно $56 + 4 = 60$.

Заметим, что из приведенных выше рассуждений в частности следует, что число различных правильных семейств порядка 2 равно 12.

Все 60 латинских квадратов были перечислены явно, используя приведенные выше рассуждения. В работе мы ограничимся анализом классов изоморфизма. Представители классов и результаты анализа содержатся в таблице 1 в Приложении. Полиномиальная полнота устанавливалась в соответствии с упомянутым критерием из работы [7]. В четвертом столбце таблицы указан номер нарушенного необходимого условия полноты. □

4. Перестановочная конструкция

Усилим конструкцию, связанную с правильными семействами, следующим образом. Пусть $n \in \mathbb{N}$, $F = \{f_1, \ldots, f_n\}$ — правильное семейство булевых функций, $\alpha, \beta, \gamma \in S_n$ — перестановки на множестве $\{1, \ldots, n\}$. Наложим перестановки α, β, γ на индексы переменных x и y и номера функций g в представлении (1):

$$\begin{array}{rcl} g_{\gamma(1)} & = & x_{\alpha(1)} \oplus y_{\beta(1)} \oplus f_1(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})), \\ & \vdots & \\ g_{\gamma(n)} & = & x_{\alpha(n)} \oplus y_{\beta(n)} \oplus f_n(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})). \end{array} \quad (2)$$

Заметим, что исходное задание (1) получается из формул (2) при выборе тождественных перестановок в качестве α, β и γ.

Теорема 2. *При любых перестановках $\alpha, \beta, \gamma \in S_n$ и любых функциях от двух переменных $\pi_1, \ldots, \pi_n$ система функций $g_1, \ldots, g_n$ задает латинский квадрат.*

Доказательство. Так как любая перестановка может быть разложена в произведение транспозиций, наложение перестановок α, β и γ на систему (1) может быть сведено к цепочке наложения транспозиций, причем, как несложно увидеть, транспозиции, соответствующие разным перестановкам, коммутируют. Докажем утверждение теоремы индукцией по длине цепочек транспозиций.

Базис индукции: если длина всех цепочек равна 0, система (2) принимает вид (1), и утверждение теоремы следует из правильности семейства F.

Индуктивный переход: пусть утверждение верно для перестановок α', β', γ'. Покажем, что в этом случае к любой из этих перестановок можно применить произвольную транспозицию без нарушения условия теоремы. Достаточно доказать три утверждения.

1) Пусть α_0 — транспозиция, переставляющая переменные с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha_0 \cdot \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$. Тогда система (2) задает латинский квадрат.

2) Пусть β_0 — транспозиция, переставляющая переменные с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha'$, $\beta = \beta_0 \cdot \beta'$, $\gamma = \gamma'$. Тогда система (2) задает латинский квадрат.

3) Пусть γ_0 — транспозиция, переставляющая функции с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma_0 \cdot \gamma'$. Тогда система (2) задает латинский квадрат.

Для доказательства первого утверждения рассмотрим латинский квадрат LS, порожденный перестановками α', β', γ'. Дополнительно применим перестановку α_0. Порожденную новой системой матрицу обозначим LS'. Несложно заметить, что действие перестановки α_0 — это замена всех вхождений s-того разряда в номере строки на t-тый и наоборот. Это эквивалентно перестановке строк LS, при которой меняются местами строки с номерами вида $(a_1, \ldots, a_{s-1}, 0, a_{s+1}, \ldots, a_{t-1}, 1, a_{t+1}, \ldots, a_n)$ и $(a_1, \ldots, a_{s-1}, 1, a_{s+1}, \ldots, a_{t-1}, 0, a_{t+1}, \ldots, a_n)$. Следовательно матрица LS' получается применением изотопии к латинскому квадрату LS, то есть является латинским квадратом.

Второе утверждение доказывается аналогично, с заменой строк на столбцы.

Для доказательства третьего утверждения достаточно заметить, что транспозиция γ_0 действует как “перекодировка” элементов, меняя местами элементы, двоичное представление которых отличается только в позициях s и t. Следовательно, получающаяся матрица вновь изотопна исходному латинскому квадрату и, значит, сама является латинским квадратом.

В силу произвольности выбора функций $\pi_1, \ldots, \pi_n$ доказательство индуктивного перехода завершено. □

Расходы памяти на хранение перестановок α, β, γ невелики — они составляют $3n] \log n[$, что мало по сранению с памятью, требующейся для задания булевой функции от n переменных. В то же время возникающие новые латинские квадраты могут оказаться более предпочтительными с точки зрения приложений. В частности, в случае $n = 2$, как будет показано в следующем разделе, конструкция (2) позволяет получить значительное число полиномиально полных квазигрупп.

5. Латинские квадраты порядка 4, задаваемые перестановочной конструкцией

Теорема 3. *Перестановочная конструкция при $n = 2$ порождает 240 различных латинских квадрата, лежащих в 29 различных классах изоморфизма. При этом 112 полученных латинских квадрата задают полиномиально полные квазигруппы, лежащие в 14 различных классах изоморфизма.*

Доказательство. Порождаемые латинские квадраты были перечислены явно: к каждому из 60 функциональных заданий латинских квадратов, найденных в теореме 1, применялось по 8 перестановок (произвольных комбинаций транспозиций x_1 и x_2, y_1 и y_2, z_1 и z_2). В результате возникло 480 латинских квадратов, 240 из которых оказались попарно различными. В работе мы ограничимся анализом классов изоморфизма. Представители классов выписаны в Приложении. Результаты анализа содержатся в таблице 2 Приложения. Полиномиальная полнота устанавливалась в соответствии с критерием из работы [7]. В третьем столбце таблицы указано нарушенное необходимое условие полноты или поставлен прочерк, если квазигруппа полиномиально полна. □

6. Заключение

В работе проведено исследование латинских квадратов порядка 4, получаемых с помощью правильных семейств булевых функций порядка 2. Установлено, что все соответствующие квазигруппы не являются полиномиально полными. Предложено усиление конструкции правильных семейств, названное перестановочной конструкцией. Показано, что среди квазигрупп, связанных с новыми латинскими квадратами, имеется значительное число полиномиально полных.

Список литературы

[1] C. Shannon, “Communication theory of secrecy systems Bell System Techn. J., 28:4 (1949), 656–715

[2] М.М. Глухов, “О применениях квазигрупп в криптографии Прикладная дискретная математика, 2008, № 2, 28–32

[3] S. Markovski, D. Gligoroski, V. Bakeva, “Quasigroup String Processing: Part 1 Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci., XX: 1–2 (1999), 13–28

[4] S. Markovski, V. Kusacatov, “Quasigroup String Processing: Part 2 Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci., XXI: 1–2 (2000), 15–32

[5] V. Shcherbacov, “Quasigroup based crypto-algorithms arXiv:201.3016v1

[6] G. Horváth, C.L. Nehaniv, Cs. Szabó, “An assertion concerning functionally complete algebras and NP-completeness Theoret. Comput. Sci., 407 (2008), 591–595

[7] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, “On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts Quasigroups and Related Systems, 21:2 (2013), 117–130

[8] V.A. Artamonov, S. Chakrabarti, S.K. Pal, “Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations Discrete Applied Mathematics, 2016, 5–17

[9] V.A. Artamonov, S. Chakrabarti, S.K. Pal, “Characterizations of highly non-associative quasigroups and associative triples Quasigroups and Related Systems, 25 (2017), 1–19

[10] А.В. Галатенко, А.Е. Панкратьев, С.Б. Родин, “О полиномиально полных квазигруппах простого порядка Интеллектуальные системы. Теория и приложения, 20:3 (2016), 194–198

[11] В.А. Носов, “О построении классов латински хквадратов в булевой базе данных Интеллектуальные системы, 4:3–4 (1999), 307–320

[12] С.В. Яблонский, “Введение в дискретную математику Москва, Высшая школа, 2010

[13] J. Hagemann, C. Herrmann, “Arithmetically locally equational classes and representations of partial functions Colloq.Math.Sci. J. Bolyai., 29, 1982, 345–360

[14] V.A. Nosov, A.E. Pankratiev, “A generalization of the Feistel cipher Международная конференция “Мальцевские чтения”. Тезисы докладов., Новосибирск, 2015, 59

Приложение

Таблица 1

Номер	Мощность класса	Представитель класса	Нарушение полноты
1	4	0 1 2 3 1 0 3 2 2 3 0 1 3 2 1 0	I
2	8	0 3 2 1 3 2 1 0 2 1 0 3 1 0 3 2	I
3	8	2 3 0 1 1 2 3 0 0 1 2 3 3 0 1 2	I
4	8	0 3 2 1 1 2 3 0 2 1 0 3 3 0 1 2	I
5	8	2 1 0 3 3 2 1 0 0 3 2 1 1 0 3 2	I

Продолжение на следующей странице

Таблица 1, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
6	8	0 1 2 3 3 2 1 0 2 3 0 1 1 0 3 2	I
7	8	2 1 0 3 1 2 3 0 0 3 2 1 3 0 1 2	I
8	8	0 1 2 3 1 2 3 0 2 3 0 1 3 0 1 2	I

Таблица 1: Результаты анализа классов изоморфизма латинских квадратов, порожденных с помощью конструкции В. А. Носова правильными семействами булевых функций порядка 2

Таблица 2

Номер	Мощность класса	Представитель класса	Нарушение полноты
1	4	0 1 2 3 1 0 3 2 2 3 0 1 3 2 1 0	I
2	8	0 3 2 1 3 2 1 0 2 1 0 3 1 0 3 2	I
3	8	2 3 0 1 1 2 3 0 0 1 2 3 3 0 1 2	I

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
4	12	0 3 2 1 1 2 3 0 2 1 0 3 3 0 1 2	I
5	8	2 1 0 3 3 2 1 0 0 3 2 1 1 0 3 2	I
6	12	0 1 2 3 3 2 1 0 2 3 0 1 1 0 3 2	I
7	12	2 1 0 3 1 2 3 0 0 3 2 1 3 0 1 2	I
8	8	0 1 2 3 1 2 3 0 2 3 0 1 3 0 1 2	I
9	8	0 3 1 2 3 1 2 0 1 2 0 3 2 0 3 1	—
10	8	1 3 0 2 2 1 3 0 0 2 1 3 3 0 2 1	—
11	8	0 3 1 2 2 1 3 0 1 2 0 3 3 0 2 1	II.1

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
12	8	1 2 0 3 3 1 2 0 0 3 1 2 2 0 3 1	—
13	8	0 2 1 3 3 1 2 0 1 3 0 2 2 0 3 1	—
14	8	1 2 0 3 2 1 3 0 0 3 1 2 3 0 2 1	II.1
15	8	1 3 0 2 3 0 2 1 0 2 1 3 2 1 3 0	—
16	8	1 3 0 2 2 0 3 1 0 2 1 3 3 1 2 0	—
17	8	1 2 0 3 3 0 2 1 0 3 1 2 2 1 3 0	II.1
18	8	0 2 3 1 3 1 2 0 2 0 1 3 1 3 0 2	—
19	8	2 0 3 1 1 3 2 0 0 2 1 3 3 1 0 2	—

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
20	8	0 2 3 1 1 3 2 0 2 0 1 3 3 1 0 2	II.1
21	8	2 0 1 3 3 1 2 0 0 2 3 1 1 3 0 2	—
22	8	0 2 1 3 3 1 2 0 2 0 3 1 1 3 0 2	I
23	8	2 0 3 1 3 1 0 2 0 2 1 3 1 3 2 0	—
24	8	2 0 3 1 1 3 0 2 0 2 1 3 3 1 2 0	I
25	8	0 1 3 2 3 2 1 0 1 0 2 3 2 3 0 1	—
26	8	1 0 3 2 2 3 1 0 0 1 2 3 3 2 0 1	—
27	8	1 0 2 3 3 2 1 0 0 1 3 2 2 3 0 1	—

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
28	8	0 1 2 3 3 2 1 0 1 0 3 2 2 3 0 1	II.3
29	8	1 0 3 2 3 2 0 1 0 1 2 3 2 3 1 0	—

Таблица 2: Результаты анализа классов изоморфизма латинских квадратов, порожденных с помощью перестановочной конструкции правильными семействами булевых функций порядка 2

Investigations of quasigroups generated by proper families of boolean functions of order 2
Piven N.A.

Keywords: Quasigroup, Latin square, parametric assignment, polynomial completeness, proper families of functions

We analyze all Latin squares of order 4 generated by proper families of Boolean functions. It turns out that all these Latin squares define polynomially incomplete quasigroups. We propose a generalization of the construction based on proper families. As a result, the number of generated Latin squares grows four times, and an essential number of the corresponding quasigroups becomes polynomially complete.