УДК 519.143

А. В. Назарок, асп. (Ин-т математики АН Украины, Киев)

Построение ортогональных стартеров и его следствия

Предложен метод построения системы $\frac{v-1}{2}$ попарно ортогональных стартеров порядка v для $v \equiv 6k+1 \equiv 7 \pmod{12} \equiv p \equiv \frac{n^2+n+1}{t}$ таких, что одним из первообразных корней поля Галуа простого порядка p является число 3 (k — простое, $k \neq 2$, n и t — целые положительные числа). При этом стартеры, входящие в данную систему, удовлетворяют некоторым дополнительным условиям. Следствием этого результата явилось построение ряда комбинаторных конструкций, в том числе ранее неизвестных.

Запропоновано метод побудови системи $\frac{v-1}{2}$ попарно ортогональних стартерів порядку v для $v \equiv 6k+1 \equiv 7 \pmod{12} \equiv p \equiv \frac{n^2+n+1}{t}$ таких, що одним із первісних коренів поля Галуа простого порядку p є число 3 (k — просте, $k \neq 2$, n і t — цілі додатні числа). При цьому стартери, що входять в дану систему, задовольняють деякі додаткові умови. Наслідком цього результату є побудова ряду комбінаторних конструкцій, в тому числі раніше невідомих.

Системы s попарно ортогональных стартеров порядка v ($POS\ (v, s)$) являются важным инструментом в исследовании многих проблем, связанных с s-мерными кубами Рума и Киркмана, рамками, графами, схемами Хауэлла, симметричными и разделяемыми неполными латинскими квадратами, уравновешенными турнирными схемами, блок-схемами и другими конфигурациями [1—9].

Вопрос о числе попарно ортогональных стартеров порядка v ($N\ (v)$) является чрезвычайно сложным и поэтому малоизученным. За исключением некоторых результатов, полученных для ряда конкретных значений v [6, 10, 11], в этой области можно отметить лишь результат Динитца [10]: $N\ (v) \geqslant t$, если $v = 2^k \cdot t + 1$, где k — целое, t — нечетное, v — простое число.

В настоящей статье предложен метод построения системы $\frac{v-1}{2}$ попарно ортогональных стартеров порядка v для $v \equiv 6k+1 \equiv 7 \pmod{12} \equiv$ $\equiv p \equiv \frac{n^2+n+1}{t}$, таких, что одним из первообразных корней поля Галуа простого порядка $p\ (GF\ (p))$ является число 3 (k — простое, $k \neq 2$, n и t — целые положительные числа). При этом стартеры, входящие в систему $POS\left(v, \frac{v-1}{2}\right)$ (за исключением паттерн-стартера), являются косыми, уравновешенными и погружаемыми, а паттерн-стартер — только уравновешенным.

Следствием этого результата явилось построение $\frac{v-1}{2}$-кубов Рума порядка v и $\frac{v-3}{4}$-кубов Киркмана порядка $2v+1$, систем $\frac{v-1}{2}$ попарно ортогональных симметричных латинских квадратов (квазигрупп) порядка v $\Big($и, следовательно, систем $\frac{v-1}{2}$ попарно ортогональных разделяемых неполных латинских квадратов типа $1^v\Big)$, косых рамок Рума типа $1^v \cdot 2^1$, а также уравновешенных турнирных схем, допускающих разбиения, порядка $v+1$ для некоторых v.

Необходимые для дальнейшего изложения результатов определения стартера (в том числе интранзитивного, сильного, уравновешенного, косого, погружаемого) и косого аддера приведены в работах [5, 10—12]. В известных определениях ортогональных стартеров $S_1 = \{\{s_i, t_i\}\}$ и $S_2 = \{\{u_i, v_i\}\}$ [10] потребуем, кроме того, выполнения условия

$$u_i - s_i + u_j - s_j \neq v \quad \forall i \neq j. \tag{1}$$

Именно такие стартеры S_1 и S_2 будем далее называть ортогональными.

В 1897 г. Хеффтер [13] поставил свою первую разностную проблему: можно ли разделить множество чисел $K = \{1, 2, \ldots, 3k\} \subset \mathbb{Z}^+$ на k троек $S = \{\{a(i), b(i), c(i)\} \mid 1 \leqslant i \leqslant k\}$ так, чтобы для любого i выполнялось условие $a(i) + b(i) + c(i) \equiv 0 \pmod{6k+1}$ или $a(i) + b(i) \equiv c(i) \pmod{6k+1}$? Он показал, что решение первой разностной проблемы Хеффтера (ПРПХ) служит базовыми блоками циклической системы троек Штейнера порядка $6k+1$ ($CSTS\,(6k+1)$), т. е. блок-схемы $(v, 3, 1)$-$BIBD$ с циклическим автоморфизмом $i \to i+1 \pmod{6k+1}$.

Пусть $G = \{0, 1, \ldots, v-1\}$, а $S = \{\{a, b, a+b\}\}$ ($|S| = k$) является решением ПРПХ (здесь и далее суммирование и вычитание осуществляются по модулю v). Пусть $b > a$. Представим множество S в виде $S = \bigcup_{j=1}^{k} S_j$, $\bigcap_{j=1}^{k} S_j = \{\varnothing\}$. Рассмотрим множество $S_j = (a, b, a+b)$ при фиксированном j. Пусть $\sigma = \begin{pmatrix} a & b & a+b \\ b-a & 2b+a & 2a+b \end{pmatrix}$ — подстановка множества $G \setminus \{0\}$, а τ — перестановка трех элементов a, b и c такая, что $\tau(a, b, c) = (a, c, b)$. Тогда из множества S_j (далее индекс j будет опущен) можно образовать последовательность

$$S \equiv S_{1,1} \to S_{1,2} \to S_{1,3} \to S_{1,4} \to S_{2,1} \to S_{2,2} \to S_{2,3} \to S_{2,4} \to S_{3,1} \to \ldots S_{3,4} \to \ldots$$
$$\ldots S_{q,1} \to S_{q,2} \to S_{q,3} \to S_{q,4} \to \ldots, \tag{2}$$

где $S_{1,2} = \sigma S$, $S_{1,3} = \tau\sigma S$, $S_{1,4} = \sigma\tau\sigma S$, $S_{2,1} = \tau\sigma\tau\sigma S$, $S_{2,2} = \sigma\tau\sigma\tau\sigma S$ и т. д.

Ясно, что

$$S_{q,1} = (3^{q-1} \cdot a, 3^{q-1} \cdot b, 3^{q-1} \cdot (a+b)), \quad S_{q,2} = (3^{q-1} \cdot (b-a), 3^{q-1} \cdot (2b+a), 3^{q-1} \cdot (2a+b)),$$

$$S_{q,3} = (3^{q-1} \cdot (b-a), 3^{q-1} \cdot (2a+b), 3^{q-1} \cdot (2b+a)), S_{q,4} = (3^q \cdot a, 3^q \cdot (a+b), 3^q \cdot b)), \quad q \in \mathbb{Z}^+.$$

Рассмотрим числа вида $v = 6k+1$, для которых выполняются следующие условия:

1) $v \equiv p$;
2) $k \equiv p_2$ ($p_2 \neq 2$);
3) $v \equiv (n^2 + n + 1)/t$, $\{n, t\} \subset \mathbb{Z}^+$, p, p_2 — простые числа;
4) одним из первообразных корней $GF(p)$ является число 3.

Обозначим через V множество чисел, которые удовлетворяют этим условиям. Тогда $V = \{7, 19, 31, 43, 79, \ldots\}$.

Замечание 1. Для проверки условия 4 необходимо и достаточно [14], чтобы число 3 не удовлетворяло ни одному из следующих сравнений: $3^{\frac{p-1}{2}} \equiv 1 \pmod p$, $3^{\frac{p-1}{3}} \equiv 1 \pmod p$, $3^{\frac{p-1}{k}} \equiv 1 \pmod p$.

Учитывая, что по определению число 3 является первообразным корнем $GF(p)$, из теоремы Вильсона [14] следует $3^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Покажем, что для чисел $v \in V$ k-множество $\overline{X} = \{S_{1,1}, S_{1,3}, S_{2,1}, S_{2,3}, \ldots, S_{\frac{k-1}{2},1}, S_{\frac{k-1}{2},3}, \ldots, S_{\frac{k+1}{2},1}\}$ является решением ПРПХ. Без потери общности можно считать, что в множестве $S_{1,1} = \{a, b, a+b\}$ $a \equiv 3^0 \equiv 1$.

Положим $b = n$. Так как $a + b = n + 1 = -n^2$, то $b - a = n - 1$,

$2a + b = 1 - n^2$, $2b + a = n - n^2$. Как отмечалось выше, действия производятся по модулю v.

С одной стороны, для чисел $v \in V$ можно считать, что задана аддитивная циклическая группа простого порядка $\mathbb{Z}_p$, которую, в свою очередь, можно разложить на классы вычетов, например, по модулю k, т.е. $\mathbb{Z}_p = \bigcup_{i=0}^{k-1} R_i$, $\bigcap_{i=0}^{k-1} R_i = \{\varnothing\}$, $R_i \equiv i \pmod k$. С другой стороны, первообразный корень 3 для $GF(p)$ порождает мультипликативную циклическую группу $G = \{3\}$. Следовательно, группу G можно представить в виде

$$G = \bigcup_{i=0}^{k-1} G_i, \quad \bigcap_{i=0}^{k-1} G_i = \{\varnothing\}, \quad G_i = 3^{R_i}.$$

Теперь определим такое r, что $3^r \equiv n$. Для этого необходимо решить сравнение типа $x^m \equiv n \pmod p$ или, пользуясь критерием Эйлера, сравнения $n^{\frac{p-1}{m}} \equiv 1 \pmod p$ $\forall m \mid p-1$. В рассматриваемом случае $m \in \{1, 2, 3, k, 2k, 3k\}$.

Легко видеть, что $1 \left(\mathrm{mod}\, \dfrac{n^2+n+1}{t}\right) \equiv 1 \pmod{n^3 - 1} \equiv n^{3 \cdot 2^\alpha}$, где $\alpha \in \mathbb{Z}$. Поэтому n является вычетом степеней k или $2k$, т. е. $n \in \{3^k, 3^{2k}, 3^{4k}, 3^{5k}\}$. С учетом этого и тождеств $-1 \equiv 3^{3k}$ и $1 \equiv 3^0 \equiv 3^{6k}$ запишем выражения для чисел $a + b$, $b - a$, $2a + b$ и $2b + a$:

$$a + b = \begin{cases} 3^{5k} \text{ при } n = 3^k; \\ 3^k \text{ при } n = 3^{2k}; \\ 3^{5k} \text{ при } n = 3^{4k}; \\ 3^k \text{ при } n = 3^{5k}, \end{cases} \qquad b - a = \begin{cases} 3^k (1 + 3^{2k}) \text{ при } n = 3^k; \\ 3^{2k} (1 + 3^k) \text{ при } n = 3^{2k}; \\ 3^{3k} (1 + 3^k) \text{ при } n = 3^{4k}; \\ 3^{5k} (1 - 3^k) \text{ при } n = 3^{5k}, \end{cases}$$

$$2a + b = \begin{cases} 1 - 3^{2k} \text{ при } n = 3^k; \\ 1 + 3^k \text{ при } n = 3^{2k}; \\ 3^{5k} (1 + 3^k) \text{ при } n = 3^{4k}; \\ 3^k (1 - 3^{2k}) \text{ при } n = 3^{5k}, \end{cases} \qquad 2b + a = \begin{cases} 3^k (1 - 3^k) \text{ при } n = 3^k; \\ 3^k (1 + 3^k) \text{ при } n = 3^{2k}; \\ 3^{4k} (1 + 3^k) \text{ при } n = 3^{4k}; \\ 3^k (1 - 3^k) \text{ при } n = 3^{5k}. \end{cases}$$

Из приведенных выражений видно, что $n \neq 3^k$ и $n \neq 3^{5k}$, поскольку множество элементов, образующих решение ПРПХ, не должно содержать повторяющихся элементов.

В случае простых чисел $v \in V$ из тождества $3^{\frac{p-1}{2}} \equiv -1 \pmod p$ следует, что образующее решение ПРПХ множество элементов должно представлять собой совокупность $3k$ подряд идущих степеней числа 3. При этом возможны два случая: 1) все $3k$ степеней положительны (это множество $3k$ степеней обозначим X); 2) часть степеней отрицательна, остальная часть степеней положительна (это множество $3k$ степеней обозначим Y). Под отрицательной степенью понимается запись этой степени в форме левой части тождества $-3^i \equiv 3^{i+3k}$.

Пусть $a = 3^0$, $b = 3^u$, $a + b = 3^z$, $b - a = 3^w$, $2a + b = 3^x$, $2b + a = 3^y$. Тогда множество элементов X, образующих множество $\overline{X}$, имеет вид

$$X = \{3^0, 3^1, \ldots, 3^{\frac{k-1}{2}}, 3^u, 3^{u+1}, \ldots, 3^{u+\frac{k-1}{2}}, 3^z, 3^{z+1}, \ldots, 3^{z+\frac{k-1}{2}}, 3^w, 3^{w+1}, \ldots$$
$$\ldots, 3^{w+\frac{k-3}{2}}, 3^x, 3^{x+1}, \ldots, 3^{x+\frac{k-3}{2}}, 3^y, 3^{y+1}, \ldots, 3^{y+\frac{k-3}{2}}\}.$$

Покажем, что для каждого из оставшихся случаев $n = 3^{2k}$ и $n = 3^{4k}$ выполняется условие $3^k + 1 = 3^{\frac{k+1}{2}}$. Действительно, в случае $n = 3^{2k}$ имеем $3^k = 1 + n$, но $1 + n = (n+2)^2 - 2(n+1)$. Тогда $3(n+1) = (n+2)^2$, откуда следует $3^k = \frac{1}{3}(n+2)^2$, т. е. $3^{\frac{k+1}{2}} = n + 2$. Но и $3^k + 1 = n + 2$. Следовательно, $3^k + 1 = 3^{\frac{k+1}{2}}$.

В случае $n = 3^{4k}$ имеем $3^k = -n$, но $-n = (1-n)^2 + 2n$. Тогда $-n = \frac{1}{3}(1-n)^2$, откуда $3^k = \frac{1}{3}(1-n)^2$, т. е. $3^{\frac{k+1}{2}} = 1 - n$. Но и $3^k + 1 = 1 - n$. Следовательно, и в этом случае $3^k + 1 = 3^{\frac{k+1}{2}}$.

В случае $n = 3^{2k}$ $3^k - 1 = n = 3^{2k}$, а в случае $n = 3^{4k}$ $3^k - 1 = -(n+1) = 3^{2k}$. Кроме того, в случае $n = 3^{2k}$ имеем $3^{\frac{k-1}{2}}(n-1) = -1$, $3^{\frac{k-1}{2}}(n+2) = n+1$, $3^{\frac{k-1}{2}}(2n+1) = n$. В случае же $n = 3^{4k}$ имеем $3^{\frac{k-1}{2}}(n-1) = n$, $3^{\frac{k-1}{2}}(n+2) = 1, 3^{\frac{k-1}{2}}(2n+1) = n+1$. Следовательно, для чисел $v \in V$ в случаях $n = 3^{2k}$ и $n = 3^{4k}$ в ряду (2) через $2k$ шагов образуется $2k$ троек таких, что первая и последняя из них будут одинаковыми с точностью до порядка следования их элементов.

В случае $n = 3^{4k}$ из приведенных выше тождеств $3^{\frac{k-1}{2}}(n-1) = n$, $3^{\frac{k-1}{2}}(n+2) = 1$ и $3^{\frac{k-1}{2}}(2n+1) = n+1$ вытекают тождества $n - 1 = -3^{\frac{k+1}{2}}$, $n + 2 = 3^{\frac{k+1}{2}} \cdot (n+1)$ и $2n + 1 = 3^{\frac{k+1}{2}} \cdot n$, а в случае $n = 3^{2k}$ из тождеств $3^{\frac{k-1}{2}} \cdot (n-1) = -1$, $3^{\frac{k-1}{2}} \cdot (n+2) = n+1$ и $3^{\frac{k-1}{2}}(2n+1) = n$ вытекают тождества $n - 1 = 3^{\frac{k+1}{2}} \cdot n$, $n + 2 = 3^{\frac{k+1}{2}}$, $2n + 1 = 3^{\frac{k+1}{2}} \cdot (n+1)$.

Следовательно, в случае $n = 3^{2k}$ множество X имеет вид

$$X = \{3^0, 3^1, \ldots, 3^{\frac{k-1}{2}}, 3^{2k}, 3^{2k+1}, \ldots, 3^{\frac{5k-1}{2}}, 3^k, 3^{k+1}, \ldots, 3^{\frac{3k-1}{2}}, 3^{\frac{5k+1}{2}}, 3^{\frac{5k+3}{2}}, \ldots$$
$$\ldots, 3^{3k-1}, 3^{\frac{k+1}{2}}, 3^{\frac{k+3}{2}}, \ldots, 3^{k-1}, 3^{\frac{3k+1}{2}}, 3^{\frac{3k+3}{2}}, \ldots, 3^{2k-1}\} = \{3^0, 3^1, 3^2, \ldots, 3^{3k-1}\},$$

а в случае $n = 3^{4k}$ —

$$X = \{3^0, 3^1, \ldots, 3^{\frac{k-1}{2}}, 3^{4k}, 3^{4k+1}, \ldots, 3^{\frac{9k-1}{2}}, 3^{5k}, 3^{5k+1}, \ldots, 3^{\frac{11k-1}{2}}, 3^{\frac{7k+1}{2}}, 3^{\frac{7k+3}{2}}, \ldots$$
$$\ldots, 3^{4k-1}, 3^{\frac{11k+1}{2}}, 3^{\frac{11k+3}{2}}, \ldots, 3^{6k-1}, 3^{\frac{9k+1}{2}}, 3^{\frac{9k+3}{2}}, \ldots, 3^{5k-1}\} =$$
$$= \{3^{4k}, 3^{4k+1}, \ldots, 3^{\frac{k-1}{2}}\}.$$

Таким образом, как в случае $n = 3^{2k}$, так и в случае $n = 3^{4k}$ множество $\overline{X}$ является решением ПРПХ.

З а м е ч а н и е 2. С учетом замечания 1 число n определяется однозначно.

Заменив в тройках множества $\overline{X} = \{\{a, b, a+b\}\} = \left\{F_i : F_{2\nu+1} = S_{\nu+1,3},\ F_{2\nu} = S_{\nu+1,1} \mid i = 0, 1, \ldots, k-1,\ \nu = 0, 1, \ldots, \frac{k-1}{2}\right\}$ элементы вида $a + b$

на элементы вида $-(a+b)$, составим множество $\overline{Y}=\{\{a, b, -(a+b)\}\}=\{F_i' \mid i=0, 1, \ldots, k-1\}$, и из него — множество $\overline{U}=\{(-3)^i \cdot F_0'\}$. Здесь и далее запись типа $\text{const}\cdot\{a, b, c\}$ означает тройку $\{\text{const}\cdot a, \text{const}\cdot b, \text{const}\cdot c\}$. Нетрудно проверить, что множество $\overline{Y}$ является решением ПРПХ для случаев $n=3^{2k}$ и $n=3^{4k}$. Следовательно, множество $\overline{U}$ также является решением ПРПХ, причем в обоих случаях множество элементов U, образующих решение $\overline{U}$, можно представить в виде $U=U_+=\{3^j \mid j=0, 2, \ldots, 6k-2\}$.

Построим множество

$$U_-=\{3^{j+f} \mid j=0, 2, \ldots, 6k-2, f\in\{1, 3, \ldots, 6k-1\}\}=\{3^f \mid f=1, 3, \ldots, 6k-1\}.$$

Тогда множества $W_f=\{U_+, U_-\}=\{\{3^j, 3^{j+f}\} \mid j=0, 2, \ldots 6k-2, f\in\{1, 3, \ldots, 6k-1\}\}$ являются системой $POS\left(v, \dfrac{v-1}{2}\right)$ поскольку, во-первых, $U_+\cup U_-=G\setminus\{0\}$, во-вторых, множества $W_1, W_3, \ldots, W_{6k-1}$ являются стартерами, так как $\forall f\in\{1, 3, \ldots, 6k-1\}$

$$\bigcup_{\substack{j=0,\\ j\equiv 0 \pmod 2}}^{6k-2} (3^{j+f}-3^j)=\bigcup_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{6k-2} 3^{j+\text{const}}=\begin{cases}U_+, & \text{если } \text{const}\equiv 0 \pmod 2;\\ U_-, & \text{если } \text{const}\equiv 1 \pmod 2,\end{cases}$$

и, наконец, в-третьих, стартеры $W_1, W_3, \ldots, W_{6k-1}$ являются попарно ортогональными.

Докажем последнее утверждение. Пусть $R(f_r)=\bigcup\limits_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{6k-2} (3^{j+f_r}-3^j)$, $r=1, 2, f_1, f_2\in\{1, 3, \ldots, 6k-1\}$, $f_1\neq f_2$. Тогда возможны следующие случаи: 1) $R(f_1)=U_+$, $R(f_2)=U_+$; 2) $R(f_1)=U_+$, $R(f_2)=U_-$; 3) $R(f_1)=U_-$, $R(f_2)=U_+$; 4) $R(f_1)=U_-$, $R(f_2)=U_-$.

В случае 1 в стартере W_{f_2} переставим пары элементов так, чтобы в стартерах W_{f_1} и W_{f_2} на местах с одинаковым порядковым номером находились пары элементов, разность которых одинакова. Тогда $W_{f_1}=\{\{3^j, 3^{j+f_1}\}\}$, а $W_{f_2}=\{\{3^{j+m}, 3^{j+m}+3^{j+f_1}-3^j \mid m\in\{0, 2, \ldots, 6k-2\}\}$ и, следовательно, $\bigcup\limits_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{6k-2} (3^{j+m}-3^j)=\begin{cases}U_+\\ U_-\end{cases}$, т. е. в любом случае стартеры W_{f_1} и W_{f_2} ортогональны. В случае 2 проделаем ту же операцию, что и в случае 1, предварительно поменяв местами элементы пар в стартере W_{f_2}. Получим тот же результат. Случаи 3 и 4 аналогичны случаям 1 и 2.

Кроме того, ясно, что $3k+f\equiv 0 \pmod 2$ и стартер

$$W_{-f}=\{\{-3^j, -3^{j+f}\} \mid j=0, 2, \ldots, 6k-2, f\in\{1, 3, \ldots, 6k-1\}\}=W_{6k-f}.$$

Таким образом, система $POS\left(v, \dfrac{v-1}{2}\right)$ для $v\in V$ состоит из множества стартеров $\{W_{\pm f} \mid f=1, 3, \ldots, 3k\}$, причем $W_{3k}=W_{-3k}$ (стартер $P=W_{3k}=\{\{x, -x\} \mid x\in G\setminus\{0\}\}$ называется паттерн-стартером [10]).

Согласно [11, 12] стартеры $W_1, W_3, \ldots, W_{3k-2}, W_{3k+2}, \ldots, W_{6k-1}$ являются косыми (а значит, и сильными), уравновешенными и погружаемыми, а стартер P является только уравновешенным.

На основании изложенного выше сформулируем следующую теорему.

Теорема. *Для чисел вида* $v=p=6p_2+1\equiv 7 \pmod{12}\equiv\dfrac{n^2+n+1}{t}$ *таких, что число* 3 *является первообразным корнем* $GF(p)$ (p, p_2 *— простые,* n *и* t *— целые положительные числа*), $N(v)=(v-1)/2$. *При этом стартеры, входящие в систему* $POS(v, (v-1)/2)$ (*за исключением паттерн-стартера*), *являются косыми, уравновешенными и погружаемыми, а паттерн-стартер — только уравновешенным.*

Примеры. 1. $v=19$; $\overline{U}=\{\{1,7,11\},\ \{16,17,5\},\ \{9,6,4\}\}$.

2. $v=43$; $\overline{U}=\{\{1,6,36\},\ \{40,25,21\},\ \{9,11,23\},\ \{16,10,17\},\ \{38,35,13\},\ \{15,24,4\},\ \{41,14,31\}\}$.

Из полученных результатов следует возможность построения ряда комбинаторных конструкций, в том числе ранее неизвестных. Определения таких комбинаторных объектов, как кубы Рума и Киркмана, системы попарно ортогональных разделяемых неполных латинских квадратов (квазигрупп), кратно разрешимых блок-схем, рамок, уравновешенных турнирных схем и схем Хауэлла, можно найти в работах [6—8, 10, 11].

Из полученного решения ПРПХ для чисел $v\in V$ следует и решение проблемы построения $CSTS\ (v)$.

Гросс, Маллин и Уоллис [15] предположили, что число попарно ортогональных симметричных латинских квадратов $V(v)\leqslant\frac{v-1}{2}$ для любых нечетных $v\geqslant 7$. В данной работе показано, что для всех $v\in V$ $N(v)=\frac{v-1}{2}$, причем на условие ортогональности стартеров наложено дополнительное условие (1). Как известно [10], система $POS\ (v,\ s)$ эквивалентна системе s идемпотентных симметричных попарно ортогональных латинских квадратов порядка v (или системе s попарно ортогональных квазигрупп $Q\ (\cdot)$, $Q\ (\bigcirc)$, $Q\ (\otimes)$, заданных на v-элементном множестве Q, в каждой из которых верны следующие тождества : $a\bigvee b=b\bigvee a$ и $a\bigvee a=a$, где $\bigvee\in\{\cdot,\ \circ,\ \otimes\}$ и $a,\ b\in Q$), а также s-кубу Рума. Другими словами, система $POS\ (v,\ s)$ эквивалентна системе s попарно ортогональных разделяемых неполных латинских квадратов типа 1^v. Таким образом, в рассматриваемом случае для чисел $v\in V$, когда $v\ (v)=s=(v-1)/2$, неравенство Гросса — Маллина — Уоллиса превращается в равенство.

Известно [7, 11], что квадрат Киркмана $KS_k\ (v;\ 1,\ \lambda)$ эквивалентен дважды разрешимой блок-схеме $DR\ (v,\ k,\ \lambda)$-$BIBD$, а следовательно, $KS_2\ (v;\ 1,1)$ эквивалентен квадрату Рума порядка v ($RS\ (v)$), схеме Хауэлла со стороной $2v-1$ и порядка $2v$ ($H\ (2v-1,\ 2v)$) и косой рамке Рума типа 1^v ($RSF\ (1^v)$).

Выше отмечалось, что стартеры $W_1, W_3, \ldots, W_{6k-1}$ являются погружаемыми. Исходя из каждой пары стартеров W_f и W_{-f} ($f\in\{1,3,\ldots,3k-1\}$), легко может быть построен квадрат Киркмана $KS_3\,(2v+1;\ 1,\ 1)$ $(v\neq 7)$ [11]. Таким же образом могут быть построены все $\left(\frac{v-1}{2}-1\right)/2=(v-3)/4$ квадртов Киркмана $KS_3\,(2v+1;\ 1,\ 1)$, т. е. $\frac{v-3}{4}$-куб Киркмана, каждая 2-мерная проекция которого является квадратом Киркмана $KS_3\,(2v+1;\ 1,\ 1)$. Построим, например, ранее неизвестный $KS_3\,(87;\ 1,\ 1)$ из стартеров W_1 и W_{-1} порядка 43 на $\mathbb{Z}_v\times\{0,\ 1\}\cup\{\infty\}$:

$$W_1=\{\{1,2\},\ \{6,12\},\ \{36,29\},\ \{40,37\},\ \{25,7\},\ \{21,42\},\ \{9,18\},\ \{11,22\},\ \{23,3\},\ \{16,32\},\ \{10,20\},\ \{17,34\}\ \{38,33\},\ \{35,27\},\ \{13,26\},\ \{15,30\},\ \{24,5\},\ \{4,8\},\ \{41,39\},\ \{14,28\},\ \{31,19\}\},$$

$$W_{-1}=\{\{41,42\},\ \{31,37\},\ \{14,7\},\ \{6,3\},\ \{36,18\},\ \{1,22\},\ \{25,34\},\ \{21,32\},\ \{40,20\},\ \{11,27\},\ \{23,33\},\ \{9,26\},\ \{10,5\},\ \{16,8\},\ \{17,30\},\ \{13,28\},\ \{38,19\},\ \{35,39\},\ \{4,2\},\ \{15,29\},\ \{24,14\}\}.$$

Пусть $n=3^{4k}$, $a\equiv 1, b\equiv n$. Нетрудно проверить, что, исходя из ранее доказанных тождеств $3^k+1=3^{\frac{k+1}{2}}$ и $3^k-1=3^{2k}$, множества пар элементов S и T, где

$$S=\{\overline{Y},3^k\overline{Y}\}=\{\{1,-n\},\{n,n+1\},\{-(n+1),-1\},$$

$$\{-3^{\frac{k+1}{2}}, -3^{\frac{k+1}{2}}(n+1)\}, \{3^{\frac{k+1}{2}}(n+1), 3^{\frac{k+1}{2}}n\}, \{-3^{\frac{k+1}{2}}n, 3^{\frac{k+1}{2}}\},$$

$$\{3, -3n\}, \{3n, 3(n+1)\}, \{-3(n+1), -3\}, \ldots$$

$$\ldots, \{3^{\frac{k-1}{2}}, -3^{\frac{k-1}{2}}n\}, \{3^{\frac{k-1}{2}}n, 3^{\frac{k-1}{2}}(n+1)\}, \{-3^{\frac{k-1}{2}}(n+1), -3^{\frac{k-1}{2}}\}\}$$

и

$$T = \{3^k\overline{Y}, 3^{k+\frac{k+1}{2}}\overline{Y}\} = \{\{-n, -3^{\frac{k+1}{n}}n\}, \{n+1, 3^{\frac{k+1}{2}}(n+1)\},$$

$$\{-1, -3^{\frac{k+1}{2}}\}, \{-3^{\frac{k+1}{2}}(n+1), -3(n+1)\},$$

$$\{3^{\frac{k+1}{2}}n, 3n\}, \{3^{\frac{k+1}{2}}, 3\}, \{-3n, -3^{\frac{k+3}{2}}n\}, \{3(n+1), 3^{\frac{k+3}{2}}(n+1)\},$$

$$\{-3, -3^{\frac{k+3}{2}}\}, \ldots, \{-3^{\frac{k-1}{2}}n, -3^k n), \{3^{\frac{k-1}{2}}(n+1), 3^k(n+1)\},$$

$$\{-3^{\frac{k-1}{2}}, -3^k\}\},$$

являются ортогональными стартерами. Если в стартере T элементы $-n$ и 1 (а следовательно, в стартере S элементы 1 и $3^{\frac{k-1}{2}}(n+1)$ соответственно) заменить элементами α и β, то образуется интранзитивный стартер для $G \cup \{\alpha, \beta\}$. Тогда согласно [5] может быть построена косая рамка Рума типа $1^v \cdot 2^1$. Аналогичный результат может быть получен и в случае $n = 3,^{2k}$ $a \equiv n$, $b \equiv 1$.

Пример. $v = 7$; $S = \{\{\alpha, 5\}, \{2, 3\}, \{4, \beta\}\}$, $R = \{1, 5\}$, $T = P = \{\{\alpha, 2\}, \{3, 4\}, \{6, \beta\}\}$, $C = \{6, 1\}$.

Покажем, что для чисел $v \in V$ таких, что число $2 \in \{3^f \mid f = 1, 3, 5, \ldots, 6k-1\}$, можно построить уравновешенную турнирную схему, допускающую разбиения ($PBTD\,(v+1)$). Построим, например, $PBTD$ (44), существование которой до сих пор оставалось не доказанным [6, 8].

Пусть одна из ячеек (s, t) или (t, s) косой рамки Рума типа 1^v ($(s, t) \in G \times G \setminus \bigcup_{i=1}^{v} (G_i \times G_i)$, где $\{G_1, G_2, \ldots, G_v\}$ — разбиение множества G), построенной с помощью приведенных выше стартеров S и T, пуста, а другая заполнена неупорядоченной парой элементов $\{x, y\}$ $(x, y \in G)$. Заполним пустую ячейку неупорядоченной парой элементов $\{x+v, y+v\}$, а главную диагональ — неупорядоченной парой элементов $\{\{i, i+v\} \mid i = 0, 1, \ldots, v-1\}$. В результате получим схему Хауэлла $H_1(v, 2v)$. Воспользуемся тем фактом, что часть пар элементов вида $\{x, y\}$ и $\{x+v, y+v\}$ может быть заменена на пары элементов вида $\{x, y+v\}$ и $\{x+v, y\}$ без нарушения латинскости строк и столбцов $H_1(v, 2v)$, и произведем такую частичную замену. Заменим далее пары элементов вида $\{x+i, y+i\}$ и $\{p+i, q+i\}$, $p, q \in G$, соответственно на $\{x+i, \alpha\}$ (или $\{y+i, \alpha\}$) и $\{p+i, \beta\}$ (или $\{q+i, \beta\}$) так, чтобы образовалась схема Хауэлла $H_1(v+1, 2(v+1))$, в которой в последней строке (столбце) находилась бы совокупность пар $\{\{x+i, y+i\}\}$, а в последнем столбце (строке) — совокупность пар $\{\{p+i, q+i\}\}$ (в ячейке $(v+1, v+1)$ находится пара элементов $\{\alpha, \beta\}$). Такая замена всегда возможна, поскольку, как показано выше, стартеры S и T образуют интранзитивный стартер для $G \cup \{\alpha, \beta\}$.

Поскольку число $2 = 3^{f^*} \in \{3^f \mid f = 1, 3, \ldots, 6k-1\}$, то среди $3k$ попарно ортогональных стартеров $W_1, W_3, \ldots, W_{6k-1}$ будет и стартер W_{f^*}. Кроме стартера W_{f^*} выберем из этой совокупности стартеров такой, чтобы, во-первых, в схеме Хауэлла $H_2(v, 2v)$, полученной из косой рамки Рума типа 1^v (образованной, в свою очередь, с помощью этого стартера и стартера W_{f^*}), можно было произвести замену парами элементов вида $\{x, y+v\}$ и $\{x+v, y\}$ тех пар элементов вида $\{x, y\}$ и $\{x+v, y+v\}$, которые не были заменены в $H_1(v, 2v)$, и, во-вторых, совокупность пар элементов, находящихся в последней строке $H_2(v+1, 2(v+1))$, была такой же, как и в последней строке (столбце) $H_1(v+1, 2(v+1))$, что может быть достигнуто путем замены пар элементов $\{\{i, i+v\}\}$ и $\{\{x+i, 2x+i\}\}$ на $\{\beta, i+v\}$ и $\{\alpha, 2x+i\}$ соответственно. В $H_2(v+1, 2(v+1))$, как и в $H_1(v+1, 2(v+1))$, ячейка $(v+1, v+1)$ содержит пару элементов $\{\alpha, \beta\}$. Этим требованиям удовлетворяет, в частности, паттерн-стартер P.

Таким образом, образуются две схемы Хауэлла $H_1(v+1, 2(v+1))$ и $H_2(v+1, 2(v+1))$ с общей строкой, т. е. $PBTD(v+1)$. Отметим, что $PBTD(v)$ эквивалентна квадрату Рума с максимально пустым подквадратом порядка v и имеет тесную связь с факторизацией графов Котзига [8].

Пример. $PBTD$ (44). ($2 = 3^{27}$, $\bar{i} = i + v\ \forall i \in G$)

$$W_{27} = \{\{\overline{0}, \beta\}, \{\alpha, 30\}, \{\overline{26},\overline{13}\}, \{14, \overline{14}\}, \{34,\overline{34}\}, \{21,\overline{21}\}, \{4,8\}, \{\overline{24},\overline{5}\},$$
$$\{25,\overline{25}\}, \{6,12\}, \{42,\overline{42}\}, \{36,29\}, \{\overline{27},\overline{35}\}, \{19, \overline{19}\}, \{33,38\}, \{20,\overline{20}\}, \{7,\overline{7}\},$$
$$\{37,\overline{37}\}, \{41,\overline{41}\}, \{18,\overline{18}\}, \{\overline{1}, \overline{2}\}, \{16,\overline{16}\}, \{31,\overline{31}\}, \{1, 2\}, \{32,\overline{32}\}, \{17,\overline{17}\},$$
$$\{9,\overline{9}\}, \{11,\overline{11}\}, \{22,\overline{22}\}, \{\overline{33},\overline{38}\}, \{40,\overline{40}\}, \{27,35\}, \{\overline{36},\overline{29}\}, \{23,\overline{23}\}, \{\overline{6}, \overline{12}\},$$
$$\{28,\overline{28}\}, \{24,5\}, \{\overline{4},\overline{8}\}, \{39,\overline{39}\}, \{3,\overline{3}\}, \{10,\overline{10}\}, \{26,13\}, \{\overline{15},\overline{30}\}\},$$

$$P = \{\{\overline{0},\beta\}, \{\alpha,29\}, \{\overline{28},\overline{15}\}, \{11,\overline{11}\}, \{30,\overline{30}\}, \{16,\overline{16}\}, \{41,2\}, \{\overline{31},\overline{12}\}, \{17,\overline{17}\}$$
$$\{40,3\}, \{32,\overline{32}\}, \{25,18\}, \{\overline{39},\overline{4}\}, \{6,\overline{6}\}, \{19,24\}, \{5,\overline{5}\}, \{34,\overline{34}\}, \{20,\overline{20}\},$$
$$\{23,\overline{23}\}, \{42,\overline{42}\}, \{\overline{21},\overline{22}\}, \{38,\overline{38}\}, \{9,\overline{9}\}, \{21,22\}, \{8,\overline{8}\}, \{35,\overline{35}\}, \{26,\overline{26}\},$$
$$\{27,\overline{27}\}, \{37,\overline{37}\}, \{\overline{19},\overline{24}\}, \{10,\overline{10}\}, \{39,4\}, \{\overline{25},\overline{18}\}, \{33,\overline{33}\}, \{\overline{40},\overline{3}\}, \{36,\overline{36}\},$$
$$\{31,12\}, \{\overline{41},\overline{2}\}, \{1,\overline{1}\}, \{7,\overline{7}\}, \{13,\overline{13}\}, \{28,15\}, \{\overline{14},\overline{29}\}\},$$
$$R = \{0,15\},\ C = \{0,14\},$$

$$S = \{\{0,\overline{0}\}, \{39,\overline{39}\}, \{\overline{29},\overline{31}\}, \{\overline{18},\overline{21}\}, \{15,\overline{15}\}, \{8,\overline{8}\}, \{19,\overline{19}\}, \{35,\overline{35}\},$$
$$\{30,\overline{30}\}, \{\overline{11},\overline{20}\}, \{26,16\}, \{\overline{23},\overline{34}\}, \{\overline{2},\overline{14}\}, \{7,\overline{7}\}, \{12,\beta\}, \{24,\overline{24}\}, \{33,17\},$$
$$\{\alpha,10\}, \{\overline{22},\overline{40}\}, \{6,\overline{6}), \{9,32\}, \{3,25\}, \{\overline{3},\overline{25}\}, \{\overline{9},\overline{32}\}, \{4,\overline{4}\}, \{22,40\}, \{\overline{27},\overline{10}\},$$
$$\{\overline{33},\overline{17}), \{36,\overline{36}\}, \{\overline{12},\overline{41}\}, \{5,\overline{5}\}, \{2,14\}, \{23,34\}, \{\overline{26},\overline{16}\}, \{11,20\}, \{42,\overline{42}\},$$
$$\{28,\overline{28}\}, \{13,\overline{13}\}, \{37,\overline{37}\}, \{1,\overline{1}\}, \{18,21\}, \{29,31\}, \{38,\overline{38}\}\},$$

$$T = \{\{0, \overline{0}\}, \{38,\overline{38}\}, \{\overline{31},\overline{33}\}, \{\overline{21},\overline{24}\}, \{11,\overline{11}\}, \{3,\overline{3}\}, \{13,\overline{13}\}, \{28,\overline{28}\},$$
$$\{22,\overline{22}\}, \{\overline{20},\overline{29}\}, \{16,6\}, \{\overline{34},\overline{2}\}, \{\overline{14},\overline{26}\}, \{37,\overline{37}\}, \{41,\beta\}, \{9,\overline{9}\}, \{17,1\}, \{\alpha,36\},$$
$$\{\overline{40},\overline{15}\}, \{30,\overline{30}\}, \{32,12\}, \{25,4\}, \{\overline{25},\overline{4}\}, \{\overline{32},\overline{12}\}, \{23,\overline{23}\}, \{40,15\}, \{\overline{10},\overline{36}\},$$
$$\{\overline{17},\overline{1}\}, \{8,\overline{8}\}, \{23,\overline{23}\}, \{18,\overline{18}\}, \{14,26\}, \{34,2\}, \{\overline{16},\overline{6}\}, \{20,29\}, \{7,\overline{7}\}, \{35,\overline{35}\},$$
$$\{19,\overline{19}\}, \{42,\overline{42}\}, \{5,\overline{5}\}, \{21,24\}, \{31,38\}, \{39,\overline{39}\}\},$$
$$R = \{41,27\},\ C = \{27,10\}.$$

1. *Wallis W. D., Street A. P., Wallis J. S.* Combinatorics: Room squares, sum-free sets, Hadamard matrices.— Berlin: Springer, 1972.— 322 p.
2. *Stinson D. R.* Some results concerning frames, Room squares, and subsquares // Austral. Math. Soc. Ser. A.— 1981.— **31**.— P. 376—384.
3. *Mendelsohn E., Rosa A.* One-factorizations of the complete graph-a survey // J. Graph Theory.— 1985.— **9**.— P. 43—65.
4. *Rosa A., Stinson D. R.* One factorizations of regular graphs and Howell designs of small order // Util. math.— 1986.— **29**.— P. 99—124.

5. *Stinson D. R.* On the existence of skew Room frames of type 2^n // Ars Combinatoria.— 1987.— **24**.— P. 115—128.
6. *Lamken E. R.* A note on partitioned balanced tournament designs // Ibid.— P. 5—16.
7. *Lamken E. R.* On classes of doubly resolvable $(v, 3,2)$-*BIBDs* from balanced tournament designs // Ibid.— P. 85—91.
8. *Lamken E. R., Vanstone S. A.* Balanced tournament designs and related topics // Discrete Math.— 1989.— **77**.— P. 159—176.
9. *Lamken E. R.* A note on indecomposable Kirkman squares //Ars Combinatoria.— 1990.— **29**.— P. 161—167.
10. *Dinitz J. H.* Room *n*-cubes of low order // J. Austral. Math. Soc. Ser. A.— 1984.— **36**, N 2.— P. 237—252.
11. *Stinson D. R., Vanstone S. A.* A Kirkman square of order 51 and block size 3// Discrete Math.— 1985.— 55, N 1.— P. 107—111.
12. *Du Ding-Zhu, Hsu F. D.* Partitionable starters for twin prime power type // Ibid.— 1991.— **87**, N 1.— P. 23—28.
13. *Heffter L.* Uber tripelsysteme // Math. Ann.— 1987.— **49**.— P. 101—112.
14. *Виноградов И. М.* Основы теории чисел.— М. : Наука, 1965.— 172 с.
15. *Gzoss K. B., Mullin R. C., Wallis W. G.* The number of pairwise orthogonal symmetric latin squares // Util. math.— 1973.— **4**.— P. 239 — 251.

Получено 28.11.91