Quasigroups and Related Systems **9** (2002), 1 – 17

Quasigroup power sets and cyclic S–systems

Galina B. Belyavskaya

Abstract

We give new constructions of power sets of quasigroups (latin squares) based on pairwise balanced block designs and complete cyclic S-systems of quasigroups.

1. Introduction

Let L be a fixed latin square of order n with elements of the set $Q = \{0, 1, \ldots, n-1\}$ and $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ be an ordered set of permutations $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, where row i of L is the image of $(0, 1, \ldots, n-1)$ under the permutation α_i, $0 \leqslant i \leqslant n-1$. We write $L = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$. If $R = (\beta_0, \beta_1, \ldots, \beta_{n-1})$ is another latin square of order n, then the product square LR is defined as $(\alpha_0\beta_0, \alpha_1\beta_1, \ldots \ \ldots, \alpha_{n-1}\beta_{n-1})$, where $\alpha_i\beta_i$ denotes the usual product of the permutation α_i on β_i.

Let L be a latin square of order n and m a positive integer greater than one. If $L^2, L^3, \ldots, L^m$ are all latin squares, then $\{L, L^2, \ldots, L^m\}$ is called a *latin power set of size* m. This concept was introduced explicitly in [7] and implicitly in [13]. In this case the latin squares $L, L^2, \ldots, L^m$ are pairwise orthogonal [15], Theorem 1.

The authors of [7] conjectured that for all $n \neq 2, 6$ there exists a latin power set consisting of at least two $n \times n$ latin squares. This problem was also put by J. Dénes in [5]. A proof of this conjecture would provide

2000 Mathematics Subject Classification: 20N05, 20N15

Keywords: latin square, latin power set, S-system of quasigroups, block design, quasigroup.

Acknowledgment: The research described in this publication was made possible in part by Award No. MM2-3017 of the Moldovan Research and Development Association (MRDA) and U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

a new disproof of the Euler conjecture (if $n = 4k + 2$, then there is no pair of orthogonal latin squares of order n). A construction in [7], based on Mendelsohn designs, gives infinitely many counterexamples to the Euler conjecture but unfortunately the construction does not work when $n \equiv 2 \pmod 6$. In [7] it was proved that for $7 \leqslant n \leqslant 50$ and for all larger n except possibly those of the form $6k + 2$ there exists a latin power set containing at least two latin squares of order n.

In [8] J. Dénes and P.J. Owens gave a new construction of power sets of $p \times p$ latin squares for all primes $p \geqslant 11$ not based on group tables. Such latin power sets of prime order can be used to obtain latin power sets of a composite order by the known methods.

The main construction of [8] is based on a circular Tuscan square.

As is noted in [8], for both theoretical and practical reasons it is important to find latin power sets that are not based on group tables (the sets given in [8] are constructed by using rearrangements of rows of a group table). It is important, for example, for a ciphering device, whose algorithm is based on latin power sets [9]. It is obvious that latin power sets based on non-group tables are preferable to those based on group tables because the greater irregularity makes the cipher safer.

In this article we use an algebraic approach to latin power sets. In Section 1 some necessary information from [1, 2, 3] concerning S-systems of quasigroups is given. In Section 2 we use cyclic S-systems (they are a particular case of latin power sets) and pairwise balanced block designs of index one ($BIB(v, b, r, k, 1)$) for the construction of quasigroup power sets of different sizes.

The suggested construction, in particular, is used to obtain power sets of quasigroups of all orders $n = 12t + 8 = 6(2l + 1) + 2$, $t, l \geqslant 1$, i.e. for any $n = 6k + 2$ where k is an odd number, $k \geqslant 3$.

In Section 3, there is described a composite method of constructing quasigroup (latin) power sets based on pairwise balanced block designs of index one of type $(v; k_1, k_2, \ldots, k_m)$ ($BIB(v; k_1, k_2, \ldots, k_m)$). At the end of this section the sizes of quasigroup power sets are given that can be constructed using some known block designs and cyclic S-systems by means of the suggested methods.

2. Cyclic S-systems as quasigroup power sets

Let $Q(A)$ and $Q(B)$ be groupoids. *Mann's (right) multiplication* $B \cdot A$ of the operation B on A is defined in the following way [14]:

$$B \cdot A(x, y) = B(x, A(x, y)), \quad x, y \in Q.$$

The operation $(\cdot)$ on the set of all operations defined on the set Q is associative, i.e. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. If $Q(A)$ and $Q(B)$ are quasigroups and L, R are the latin squares corresponding to them, then

$$B \cdot A(x, y) = \beta_x \alpha_x y,$$

where $\beta_x y = B(x, y)$, $\alpha_x y = A(x, y)$ and β_x (α_x) is row x of R (L).

Thus, Mann's (right) multiplication of quasigroups corresponds to the product of the respective latin squares and conversely.

Let $A = B$, then we get

$$A \cdot A = A^2, \quad A \cdot A \cdot A = A^3, \quad \ldots, \quad \underbrace{A \cdot A \cdot \cdots \cdot A}_{m} = A^m.$$

If $A, A^2, \ldots, A^m$ are quasigroups, then $\{A, A^2, \ldots, A^m\}$ is called a *quasigroup power set* (briefly QPS), $\{L, L^2, \ldots, L^m\}$ is the latin power set corresponding to this QPS.

Let $\Sigma = \{A, B, C, \ldots\}$ be a system of binary operations given on Q.

Definition 1. [1] A system of operations $Q(\Sigma)$ is called an *S–system* if

1. Σ contains the unit operations F and E $(F(x, y) = x, \ E(x, y) = y$ $\forall x, y \in Q)$ and the remaining operations define quasigroups,
2. $A \cdot B \in \Sigma'$ for all $A, B \in \Sigma'$, where $\Sigma' = \Sigma \setminus F$,
3. $A^* \in \Sigma$ for all $A \in \Sigma$, where $A^*(x, y) = A(y, x)$.

An S-system $Q(\Sigma)$ is finite if Q is a finite set. In finite $Q(\Sigma)$ for any $A \in \Sigma$ is defined A^{-1} as the solution of the equation $A(a, x) = b$, i.e. $A^{-1}(a, b) = x$. Then $A^{-1} = A^k \in \Sigma$ for some natural k, because the set of all invertible to the right operations on Q forms a finite group with respect to the right multiplication of operations. In this group E is the unit and $A^{-1} \cdot A = A \cdot A^{-1} = E$.

We remind the reader that two binary operations A and B defined on Q are said to be orthogonal if the pair of equations $A(x, y) = a$ and $B(x, y) = b$ has a unique solution for any elements $a, b \in Q$.

All operations of an S-system $Q(\Sigma)$ are pairwise orthogonal and the following properties of finite S-systems are also important:

1. Σ' is a group with respect to the (right) multiplication of operations, E is the unit of this group and A^{-1} is the inverse element of A.

2. All the quasigroups of $Q(\Sigma)$ are idempotent, if $|\Sigma| \geqslant 4$, where $|\Sigma|$ is the number of operations of $Q(\Sigma)$.

Theorem 1. (Theorem 4.3 in [1]) *Let $Q(\Sigma)$ be an $S-$system, $|Q| = n$, $|\Sigma| = k$, then $k-1$ divides $n-1$ and $r = \frac{n-1}{k-1} \geqslant k$ or $r = 1$.*

In [1] the number r is called an *index* of the S-system $Q(\Sigma)$. The number k is called *order* of $Q(\Sigma)$.

An S-system is called *complete* if $r = 1$ (in this case $n = k$). It then contains $n-2$ quasigroups.

A characterization for a finite complete S-system was given in [1], Theorem 4.6.

Definition 2. [3] An S-system $Q(\Sigma)$ of order k is called *cyclic* if $\Sigma'(\cdot)$, where $\Sigma' = \Sigma \setminus F$ and $(\cdot)$ represents composition of operations (called Mann's multiplication above), is a cyclic group.

By Corollary 1 of [3] a complete S-system $Q(\Sigma)$ is cyclic iff it is an S-system over a field $Q(\cdot, +)$, i.e. iff every operation of Σ has the form

$$A_a(x, y) = (1 - a)x + ay, \quad a, x, y \in Q, \tag{1}$$

where 1 is the unit of the multiplicative group of the field.

Remark 1. *If $Q(\Sigma)$, $\Sigma = \{F, E, A, A^2, \ldots, A^{k-2}\}$, is a complete cyclic $S-$system of order k, then*

$$A(x, y) = (1 - a)x + ay,$$

where the element a is a generating element of the multiplicative (cyclic) group of a field. Indeed, it is easy to prove that

$$A^l(x, y) = (1 - a^l)x + a^l y, \quad l = 1, 2, \ldots, k-2,$$

and $A^{k-1} = E$ iff $a^{k-1} = 1$.

Conversely, if an element a is a generating element of the multiplicative group of a field, then the quasigroup A_a of (1) generates a complete cyclic $S-$system.

Every cyclic S-system of order k and index r corresponds to a quasigroup power set of size $k-2$ and consists of quasigroups of order $n = rk - r + 1$.

From the results of [2, 3], the description of an arbitrary cyclic S-system by means of a field and an incomplete balanced block design can be obtained. First we need the following definitions.

Definition 3. [6] A *balanced incomplete block design* (or $BIB(v, b, r, k, \lambda)$) is an arrangement of v elements $a_1, a_2, \ldots, a_v$ by b blocks such that

1. every block contains exactly k different elements;

2. every element appears in exactly r different blocks;

3. every pair of different elements (a_i, a_j) appears in exactly λ blocks.

Definition 4. [2] A $BIB(v, b, r, k, 1)$ is called an $S(r, k)-$*configuration* if k is a prime power, i.e. $k = p^\alpha$.

It is known that the parameters of a $BIB(v, b, r, k, 1)$ satisfy the following equalities

$$v = rk - r + 1, \qquad b = \frac{rk - r + 1}{k} r \, .$$

In accordance with Theorem 1 of [2] a cyclic S-system of index r and order k exists iff there exists an $S(r, k)$-configuration.

Let us give a construction of an S-system of order k and index r for the case of a cyclic S-system.

Let an $S(r, k)$-configuration be given on a set Q, where $|Q| = v = rk - r + 1$, and let $Q_1, Q_2, \ldots, Q_b$ be its blocks. Let $H(+, \cdot)$ be a field of order k (such a field exists as k is a prime power) and let $H(\tilde{\Sigma})$, $\tilde{\Sigma} = \{F, E, A_1, A_2, \ldots, A_{k-2}\}$, be a complete cyclic S-system over this field.

1. On the block Q_i $(i = 1, 2, \ldots, b)$ we define a quasigroup $Q_i(A_j^{(i)})$, $j = 1, 2, \ldots, k-2$, isomorphic to the quasigroup $H(A_j)$ of the S-system $H(\tilde{\Sigma})$:

   $$A_j^{(i)}(x, y) = \alpha_i^{-1} A_j(\alpha_i x, \alpha_i y) = A_j^{\alpha_i}(x, y),$$

   where α_i is an arbitrary one-to-one mapping of the set Q_i upon H, $i = 1, 2, \ldots, b$.

2. Then, on the set Q, we define the operations B_j, $j = 1, 2, \ldots, k-2$, in the following way:

$$B_j(x,y) = \begin{cases} A_j^{(i)}(x,y), & \text{if} \quad x,y \in Q_i,\ x \neq y, \\ x, & \text{if} \quad x = y. \end{cases}$$

By Theorem 1 of [2] the system $Q(\Sigma)$, $\Sigma = \{F, E, B_1, \ldots, B_{k-2}\}$, is an S-system of index r and order k. It is called an *$S-$system over the field $H(+,\cdot)$ and the $S(r,k)-$configuration*. Moreover, by Theorem 3 of [3] such an S-system is cyclic and any S-system over a field and an $S(r,k)$-configuration is cyclic.

If $\tilde{\Sigma} = \{F, E, A, A^2, \ldots, A^{k-2}\}$, then by (1) and Remark 1

$$A_j(u,v) = A^j(u,v) = (1-a^j)u + a^j v, \quad j = 1, 2, \ldots, k-2,$$

$u, v \in H$, where the element a is a generating element of the multiplicative group of the field $H(+,\cdot)$.

Hence,

$$\begin{aligned} A_j^{(i)}(x,y) &= \alpha_i^{-1}((1-a^j)\alpha_i x + (a^j \cdot \alpha_i y)) = \alpha_i^{-1} A^j(\alpha_i x, \alpha_i y) \\ &= (A^j)^{\alpha_i}(x,y) = (A^{\alpha_i})^j(x,y), \qquad x,y \in Q_i, \end{aligned}$$

since it is easy to see that $(A \cdot B)^\alpha = A^\alpha \cdot B^\alpha$ if α is an isomorphism, $(A \cdot B)^\alpha(x,y) = \alpha^{-1}[(A \cdot B)(\alpha x, \alpha y)]$. Then

$$B^j(x,y) = B_j(x,y) = \begin{cases} (A^{\alpha_i})^j(x,y), & \text{if} \quad x,y \in Q_i,\ x \neq y, \\ x, & \text{if} \quad x = y \end{cases}$$

and $\Sigma = \{F, E, B, B^2, \ldots, B^{k-2}\}$.

In an Appendix we give an illustrative example of this construction.

3. Direct product of quasigroup power sets

Let $Q_1(A_1)$, $Q_2(A_2)$ be two binary groupoids. On the set $Q_1 \times Q_2$ which consists of all pairs (a_1, a_2), where $a_i \in Q_i$, $i = 1, 2$, define the direct product $A_1 \times A_2$ of the operations A_1 and A_2:

$$(A_1 \times A_2)((x_1,x_2),(y_1,y_2)) = (A_1(x_1,y_1), A_2(x_2,y_2)).$$

If A_1, A_2 are quasigroup operations, then $A_1 \times A_2$ also is a (binary) quasigroup operation.

Proposition 1. $(A_1 \times A_2)^m = A_1^m \times A_2^m$ *for any natural number* m.

Proof. Let $m = 2$, then

$$\begin{aligned}(A_1 \times A_2)^2((x_1, x_2), (y_1, y_2)) = \\ &= (A_1 \times A_2)((x_1, x_2), (A_1 \times A_2)((x_1, x_2), (y_1, y_2))) = \\ &= (A_1 \times A_2)((x_1, x_2), (A_1(x_1, y_1), A_2(x_2, y_2))) = \\ &= (A_1(x_1, A_1(x_1, y_1)), A_2(x_2, A_2(x_2, y_2))) = \\ &= (A_1^2(x_1, y_1), A_2^2(x_2, y_2)) = (A_1^2 \times A_2^2)((x_1, x_2), (y_1, y_2)) .\end{aligned}$$

Hence,

$$(A_1 \times A_2)^2 = A_1^2 \times A_2^2 .$$

But then

$$(A_1 \times A_2)^3 = (A_1 \times A_2)(A_1 \times A_2)^2 = (A_1 \times A_2)(A_1^2 \times A_2^2)$$

since the Mann's multiplication $(\cdot)$ of operations is associative. Using that we can similarly show that

$$(A_1 \times A_2)^3 = A_1^3 \times A_2^3 .$$

Hence, by induction on the integer m, we may deduce that Proposition 1 is true. □

Let $Q_1(A_1), Q_2(A_2), \ldots, Q_n(A_n)$ be binary groupoids. On the set $Q_1 \times Q_2 \times \cdots \times Q_n$ define the direct product of the operations $A_1, \ldots, A_n$

$$\begin{aligned}(A_1 \times A_2 \times \cdots \times A_n)((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)) = \\ = (A_1(x_1, y_1), A_2(x_2, y_2), \ldots, A_n(x_n, y_n)).\end{aligned}$$

Proposition 1 at once implies

Corollary 1. $(A_1 \times A_2 \times \cdots \times A_n)^m = A_1^m \times A_2^m \times \cdots \times A_n^m$.

Now let us consider the following n QPSs:

$$Q_i(\Sigma_i), \qquad \Sigma_i = \{A_i, A_i^2, \ldots, A_i^{m_i}\}, \qquad i = 1, 2, \ldots, n,$$

and on the set $Q_1 \times Q_2 \times \cdots \times Q_n$ define the set

$$\begin{aligned}\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_n = \{(A_1 \times A_2 \times \cdots \times A_n), \\ (A_1^2 \times A_2^2 \times \cdots \times A_n^2), \ldots, (A_1^m \times A_2^m \times \cdots \times A_n^m)\},\end{aligned}$$

where $m = \min\{m_1, m_2, \dots m_n\}$. By Corollary 1

$$\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_n = \{(A_1 \times A_2 \times \cdots \times A_n), \\ (A_1 \times A_2 \times \cdots \times A_n)^2, \dots, (A_1 \times A_2 \times \cdots \times A_n)^m\},$$

and $(Q_1 \times Q_2 \times \cdots \times Q_n)(\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_n)$ is a QPS of size m which consists of quasigroups of order $|Q_1| \cdot |Q_2| \cdot \ldots \cdot |Q_n|$. We call this QPS the direct product of QPSs $Q_i(\Sigma_i),\ i = 1, 2, \dots, n$.

Theorem 2. *Let $n = p_1^{u_1} p_2^{u_2} \dots p_s^{u_s}$, where for all $i = 1, \dots, s$, the p_i are prime numbers, the u_i are natural numbers and $m = \min\{p_1^{u_1}, \dots, p_s^{u_s}\} \geqslant 4$. Then there exists a quasigroup power set containing $m - 2$ quasigroups of order n.*

Proof. Let

$$p_1^{u_1} \leqslant p_2^{u_2} \leqslant \cdots \leqslant p_s^{u_s}, \quad \text{where } p_i^{u_i} \neq 2, 3,$$

$$\text{and} \quad Q_i(\Sigma_i) = \left\{F, E, A_i, A_i^2, \dots, A_i^{p_i^{u_i}-2}\right\}$$

be a complete cyclic S-system of order $p_i^{u_i} = |Q_i|,\ i = 1, 2, \dots, s$. By Corollary 1 of [3] such an S-system is an S-system over a field of order $p_i^{u_i}$ and its binary operations have the form (1). Using the direct product of QPSs, we deduce that $(Q_1 \times Q_2 \times \cdots \times Q_s)(\Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_s)$ is a QPS of size $p_1^{u_1} - 2$ containing quasigroups of order n. □

Note that, under different representations of a number n by powers of prime numbers, the quasigroup power sets obtained by Theorem 2 are different. For example, if $n = 7 \cdot 5^2$ we can construct a QPS of 5 quasigroups, whereas for $n = 5 \cdot 5 \cdot 7$ we obtain a QPS of 3 quasigroups of order n.

As has been noted, numbers of the form $6k+2$ present definite difficulties for the construction of latin power sets (or QPSs). As an application of Theorem 2 let us consider numbers of this form when k is odd, i.e.

$$n = 6(2t+1) + 2 = 12t + 8 = 2^2(3t+2), \quad t \geqslant 1$$

$$(n = 20, 32, 44, 56, \dots, 92, 104, \dots, 140, 152, \dots).$$

Corollary 2. *Let $n = 12t + 8,\ t \geqslant 1$. Then there exists a QPS containing at least two quasigroups of order n. If $t = 4k,\ k \geqslant 1$ then there exists a QPS containing at least three quasigroups. Moreover, if $k = 1$, then there exists a QPS of five quasigroups. For $2 \leqslant k \leqslant 9$ there exists a QPS of six quasigroups.*

Proof. The number $n = 2^2(3t+2)$ is not divisible by three. This implies that, in the factorization of n into prime powers, all $p_i^{\alpha_i} \geqslant 4$ and so, according to Theorem 2, there exists a QPS consisting of at least two quasigroups of order n.

Let $t = 4k$, $k \geqslant 1$, then $n = 2^3(6k+1)$ where $6k+1$ is an odd number $\geqslant 7$ that is not divisible by 2 and 3. Thus, the number 5 is the least possible divisor of $6k+1$ and by Theorem 2, there exists a QPS of three quasigroups of order n.

By Theorem 2 there exist QPSs of at least five quasigroups of order $n = 56$ ($t = 4$, $k = 1$). If $t = 4k$, $2 \leqslant k \leqslant 8$, then $6k+1 = 13, 19, 25, 31, 37, 43, 49\ldots$ and there exist QPSs of at least six quasigroups of order $n = 104 = (2^3 \cdot 13), 152 = (2^3 \cdot 19), 200, 248, \ldots, 392 = (2^3 \cdot 7^2)$. □

4. Quasigroup power sets and BIB$(\mathbf{v}; \mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_s})$

To obtain a further construction of QPSs, we use a generalization of the concept of a balanced incomplete block design called by R.C. Bose and S.S. Shrikhande a *pairwise balanced block design of index unity and type* $(v; k_1, k_2, \ldots, k_s)$ (for brevity, we shall write $BIB(v; k_1^s)$) (see [6], page 400; [12], page 271). Such a design comprises a set of v elements arranged in $b = \sum_{i=1}^{s} b_i$ blocks such that there are b_1 blocks each of which contains k_1 elements; b_2 blocks each of which contains k_2 elements, ... b_s blocks each of which contains k_s elements ($k_i \leqslant v$ for $i = 1, 2, \ldots, s$), and in which each pair of the v distinct elements occurs together in exactly one of the b blocks.

The latter condition implies that

$$v(v-1) = \sum_{i=1}^{s} b_i k_i (k_i - 1).$$

If $k_1 = k_2 = \cdots = k_s = k$, then we obtain the (pairwise) balanced incomplete block design ($BIB(v, b, r, k, 1)$).

By Theorem 11.2.2 [6] if a pairwise balanced block design of index unity and type $(v; k_1^s)$ exists and for each k_i there exists a set of $q_i - 1$ mutually orthogonal latin squares of that order then it is possible to construct a set of $q-2$ mutually orthogonal latin squares of order v, where $q = \min\{q_1, q_2, \ldots, q_s\}$.

We prove that an analogous statement is true for latin power sets (that is for QPSs) using a constructing of idempotent quasigroups by means of

$BIB(v;k_1^s)$ given in [4] (see also [10]). First, we describe briefly the construction of such quasigroups from [4].

Let $Q_1, Q_2, \ldots, Q_b$ be blocks of $BIB(v;k_1^s)$, given on a set Q, and $Q_1(A_1), Q_2(A_2), \ldots, Q_b(A_b)$ be idempotent quasigroups. Note that, in contrast to [4], we assume for the sake of simplicity that these quasigroups are given on the blocks of the BIB.

Define the operation $(\cdot)$ on the set Q in the following way:

$$x \cdot y = \begin{cases} A_i(x,y), & \text{if } \ x,y \in Q_i,\ x \neq y; \\ x, & \text{if } \ x = y. \end{cases} \tag{2}$$

The groupoid $Q(\cdot)$ is an idempotent quasigroup and the operation $(\cdot)$ will be denoted by

$$(\cdot) = A = [A_i]_{i=1}^b(v;k_1^s). \tag{3}$$

The quasigroup $Q(\cdot)$ consists of quasigroups defined on the blocks of the $BIB(v;k_1^s)$.

Now we prove the following

Proposition 2. *In* (3)*, let* A_i *be an idempotent quasigroup for any* $i = 1, 2, \ldots, b$*. Then*

$$A^k = [A_i^k]_{i=1}^b(v;k_1^s) \tag{4}$$

for any natural number k*.*

Proof. First notice that $x, A(x,y) \in Q_i$ where $x \neq y$, iff $x, y \in Q_i$. Granted this and the idempotency of A and A_i for any $i = 1, 2, \ldots, b$, by (2) we have

$$\begin{aligned} A^2(x,y) &= A(x, A(x,y)) = \\ &= \begin{cases} A_i(x, A(x,y)), & \text{if } \ x, A(x,y) \in Q_i,\ A(x,y) \neq x; \\ x, & \text{if } \ A(x,y) = x; \end{cases} \\ &= \begin{cases} A_i(x, A_i(x,y)), & \text{if } \ x,y \in Q_i,\ x \neq y; \\ x, & \text{if } \ x = y; \end{cases} \\ &= \begin{cases} A_i^2(x,y), & \text{if } \ x,y \in Q_i,\ x \neq y; \\ x, & \text{if } \ x = y. \end{cases} \end{aligned}$$

Thus,

$$A^2 = [A_i^2]_{i=1}^b(v;k_1^s). \tag{5}$$

Further, since A, A_i, A_i^2 are idempotent quasigroups for all $i = 1, 2, \ldots, b$, then using (2) and (5) we have

$$A^3(x,y) = A^2(x, A(x,y)) =$$

$$= \begin{cases} A_i^2(x, A(x,y)), & \text{if} \quad x, A(x,y) \in Q_i,\ A(x,y) \neq x; \\ x, & \text{if} \quad A(x,y) = x; \end{cases}$$

$$= \begin{cases} A_i^2(x, A_i(x,y)), & \text{if} \quad x, y \in Q_i,\ \ x \neq y; \\ x, & \text{if} \quad x = y; \end{cases}$$

$$= \begin{cases} A_i^3(x,y), & \text{if} \quad x, y \in Q_i,\ \ x \neq y; \\ x, & \text{if} \quad x = y. \end{cases}$$

Hence,

$$A^3 = [A_i^3]_{i=1}^b(v; k_1^s).$$

Extending this argument (that is, using induction on the index l) and taking into account that A_i^l, $i = 1, 2, \ldots, b$, $l = 1, 2, \ldots, k-1$, and A^l, $l = 1, 2, \ldots, k-1$, are all idempotent quasigroups we obtain equality (4). □

Now it is easy to prove the following

Theorem 3. *Suppose that there exists a BIB of index unity and type* $(v; k_1, k_2, \ldots, k_s)$ *and that, for every* k_i, $i = 1, 2, \ldots, s$, *there exists a QPS of a size* m *with idempotent quasigroups of order* k_i. *Then there exists a QPS of* m *quasigroups of order* v.

Proof. Let a $BIB(v; k_1^s)$ be given on a set Q and have the blocks $, Q_1, Q_2, \ldots, Q_b$, $|Q_i| \in \{k_1, k_2, \ldots, k_s\}$. Let the following quasigroup power sets of size m on these blocks be given:

$$\begin{array}{lll} Q_1(\Sigma_1) & : & \Sigma_1 = \{A_1, A_1^2, \ldots, A_1^m\}, \\ Q_2(\Sigma_2) & : & \Sigma_2 = \{A_2, A_2^2, \ldots, A_2^m\}, \\ \ldots\ldots & & \ldots\ldots\ldots\ldots\ldots\ldots \\ Q_b(\Sigma_b) & : & \Sigma_b = \{A_b, A_b^2, \ldots, A_b^m\}, \end{array}$$

where $Q_1(A_1), Q_2(A_2), \ldots, Q_b(A_b)$ are idempotent quasigroups (then all their powers in the power sets are also idempotent).

Consider the following quasigroups on the set Q:

$$C_1 = [A_i]_{i=1}^b(v; k_1^s), \quad C_2 = [A_i^2]_{i=1}^b(v; k_1^s), \quad \ldots, \quad C_m = [A_i^m]_{i=1}^b(v; k_1^s).$$

Using (4) we obtain that $C_2 = C_1^2$, $C_3 = C_1^3$, $\ldots$, $C_m = C_1^m$. Hence, $Q(\Sigma) : \Sigma = \{C_1, C_1^2, \ldots, C_1^m\}$ is a QPS of size m containing quasigroups of order v. □

Corollary 3. *If there exists a* $BIB(v; k_1^s)$ *where* k_i, $i = 1, 2, \ldots, s$ *are powers of primes and* $t = \min\{k_1, k_2, \ldots, k_s\} \geqslant 4$, *then there exists a QPS containing* $t - 2$ *quasigroups of order* v.

Proof. As k_i, $i = 1, 2, \ldots, s$, are prime powers then, by Corollary 1 of [3], for every k_i there exists a complete cyclic S-system (over a field of order k_i). This S-system contains $k_i - 2$ (idempotent) quasigroups. Now, applying Theorem 3 completes the proof. □

Corollary 4. *Let $k, k+1, m, x$ be prime powers, $4 \leqslant k \leqslant m$, $4 \leqslant x \leqslant m$, $t = \min\{k, x\}$. Then there exists a QPS which contains $t-2$ quasigroups of order $v = km + x$.*

Proof. Let $N(m)$ denote the largest possible number of mutually orthogonal latin squares of order m which can exist in a single mutually orthogonal set and $k \leqslant N(m) + 1 \leqslant m$, $x \leqslant m$. Then (see [6], p. 412–413) there exists a $BIB(km + x; k, k+1, x, m)$ of index unity.

Since m is a prime power then there exists a complete set of mutually orthogonal latin squares (i.e. $N(m) = m - 1$) of order m. In this case the equalities $k \leqslant m$ and $k \leqslant N(m) + 1$ are equivalent. Finally use Corollary 3 taking into account that under our conditions $\min\{k, k+1, x, m\} = \min\{k, x\}$. □

Next we apply Theorem 3, Corollary 3 and Corollary 4 to construct a number of QPSs using some known BIBs $(v; b, r, k, 1)$ and BIBs $(v; k_1^s)$.

Let a $BIB(v, b, r, k, 1)$ be given on a set Q, $|Q| = v$. By removing one element from this BIB, we can obtain a $BIB(v-1; k-1, k)$, that contains r blocks of $k-1$ elements and $b-r$ blocks of k elements. In the table presented below we give initial BIBs $(v, b, r, k, 1)$ (with the numbers assigned to them in the Table of Appendix I of [12]), the corresponding $BIB(v-1; k-1, k)$, the size of QPS obtained by Corollary 3 and also that obtained by Theorem 2 (for comparison) for the same values of v.

BIB No. from [12]	BIB $(v; b, r, k, 1)$	BIB $(v-1; k-1, k)$	Size QPS by Cor. 3	Size QPS by Th. 2
7	$(21, 21, 5, 5, 1)$	$(20; 4, 5)$	2	2
11	$(25, 30, 6, 5, 1)$	$(24; 4, 5)$	2	–
25	$(57, 57, 8, 8, 1)$	$(56; 7, 8)$	5	5
36	$(64, 72, 9, 8, 1)$	$(63; 7, 8)$	5	5
37	$(73, 73, 9, 9, 1)$	$(72; 8, 9)$	6	6
42	$(41, 82, 10, 5, 1)$	$(40; 4, 5)$	2	3
45	$(81, 90, 10, 9, 1)$	$(80; 8, 9)$	6	3
51	$(45, 99, 11, 5, 1)$	$(44; 4, 5)$	2	2
108	$(61, 183, 15, 5, 1)$	$(60; 4, 5)$	2	–
[6], p.403		$(22; 4, 7)$	2	–

Now we use Corollary 4 to obtain new QPSs with quasigroups of order $v = km + x$, where the numbers k, m, x satisfy the conditions of the corollary. In the table given below, we present some $BIB(km+x; k, k+1, x, m)$ with such values of k, m, x and also the sizes of the QPSs (with quasigroups of order $v = km + x$) constructed by Corollary 4 and Theorem 2 corresponding to them.

BIB $(km + x; k, k + 1, x, m)$	$v = km + x$	Size of QPS by Cor. 4	Size of QPS by Th. 2
$(60; 7, 8, 4, 8)$	$60 = 2^2 \cdot 3 \cdot 5$	2	–
$(63; 7, 8, 7, 8)$	$63 = 3^2 \cdot 7$	5	5
$(69; 8, 9, 5, 8)$	$69 = 3 \cdot 23$	3	–
$(76; 8, 9, 4, 9)$	$76 = 2^2 \cdot 19$	2	2
$(80; 8, 9, 8, 9)$	$80 = 2^4 \cdot 5$	6	3
$(92; 8, 9, 4, 11)$	$92 = 2^2 \cdot 23$	2	2
$(93; 8, 9, 5, 11)$	$93 = 3 \cdot 31$	3	–
$(95; 8, 9, 7, 11)$	$95 = 5 \cdot 19$	5	3
$(96; 8, 9, 8, 11)$	$96 = 2^5 \cdot 3$	6	–
$(99; 8, 9, 11, 11)$	$99 = 3^2 \cdot 11$	6	7
$(108; 8, 9, 4, 13)$	$108 = 2^2 \cdot 3^3$	2	2
$(111; 8, 9, 7, 13)$	$111 = 3 \cdot 37$	5	–
$(112; 8, 9, 8, 13)$	$112 = 2^4 \cdot 7$	6	5
$(115; 8, 9, 11, 13)$	$115 = 5 \cdot 23$	6	3
$(132; 8, 9, 4, 16)$	$132 = 2^2 \cdot 3 \cdot 11$	2	–
$(133; 8, 9, 5, 16)$	$133 = 7 \cdot 19$	3	5
$(135; 8, 9, 7, 16)$	$135 = 3^3 \cdot 5$	5	3
$(136; 8, 9, 8, 16)$	$136 = 2^3 \cdot 17$	6	6
$(140; 8, 9, 4, 17)$	$140 = 2^2 \cdot 5 \cdot 7$	2	2
$(141; 8, 9, 5, 17)$	$141 = 3 \cdot 47$	3	–
$(141; 8, 9, 13, 16)$	$141 = 3 \cdot 47$	6	–
$(143; 8, 9, 7, 17)$	$143 = 11 \cdot 13$	5	9
$(144; 8, 9, 8, 17)$	$144 = 2^4 \cdot 3^2$	6	7
$(145; 8, 9, 9, 17)$	$145 = 5 \cdot 29$	6	3
$(147; 8, 9, 11, 17)$	$147 = 3 \cdot 7^2$	6	–
$(152; 8, 9, 16, 17)$	$152 = 2^3 \cdot 19$	6	6
$(153; 8, 9, 17, 17)$	$153 = 3^2 \cdot 17$	6	7

The parameters of the following BIBs $(km+x; k, k+1, x, m)$:

$$(20;4,5,4,4),\ (24;4,5,4,5),\ (25;4,5,5,5),\ (32;4,5,4,7),$$
$$(33;4,5,5,7),\ (35;4,5,7,7),\ (36;4,5,4,8),\ (37;4,5,5,8),$$
$$(39;4,5,7,8),\ (40;4,5,8,8),\ (40;4,5,4,9),\ (41;4,5,5,9),$$
$$(43;4,5,7,9),\ (44;4,5,8,9),(45;4,5,9,9)$$

also satisfy the conditions of Corollary 4. Using these BIBs one can construct QPSs containing at least two quasigroups of order v.

Appendix

Now we give an illustrative example using the construction of QPSs from Section 2.

Let $H(\oplus, \cdot)$, where $H = \{0,1,2,3,4,\}$, be the finite field formed by the residues modulo 5. The element 2 is a generating element of the (cyclic) multiplicative group of this field, so we take the quasigroup $A(x,y) = (1-2)x + 2y = 4x + 2y$ as the defining quasigroup for a complete (cyclic) $S-$system $H(\tilde{\Sigma})$, $\tilde{\Sigma} = \{F, E, A, A^2, A^3\}$. The Cayley table of the quasigroup A is as follows:

A	0	1	2	3	4
0	0	2	4	1	3
1	4	1	3	0	2
2	3	0	2	4	1
3	2	4	1	3	0
4	1	3	0	2	4

As a block design we use the following

$$BIB(v,b,r,k,1) = BIB(21,21,5,5,1) = S(5,5)$$

on the set $Q = \{1,2,3,4,5,6,7,8,9,a,b,c,d,e,f,g,h,k,m,n,p\}$ of 21 elements and 21 blocks:

B_1 : $1,2,3,4,5$, B_8 : $3,7,a,h,n$, B_{15} : $5,8,b,h,k$,
B_2 : $2,6,a,e,k$, B_9 : $4,7,d,g,k$, B_{16} : $1,k,m,n,p$,
B_3 : $3,6,b,g,p$, B_{10} : $5,7,c,e,p$, B_{17} : $2,9,d,h,p$,
B_4 : $4,6,c,h,m$, B_{11} : $1,e,f,g,h$, B_{18} : $3,9,c,f,k$,
B_5 : $5,6,d,f,n$, B_{12} : $2,8,c,g,n$, B_{19} : $4,9,b,e,n$,
B_6 : $1,a,b,c,d$, B_{13} : $3,8,d,e,m$, B_{20} : $5,9,a,g,m$,
B_7 : $2,7,b,f,m$, B_{14} : $4,8,a,f,p$, B_{21} : $1,6,7,8,9$.

This block design is isomorphic to the finite projective plane of order 4 and corresponds to a complete set of orthogonal latin squares of order 4.

According to the results of Section 2 it is sufficient to construct the quasigroup $Q(B)$:

$$B(x,y)=\begin{cases} A^{\alpha_i}, & \text{if } x,y\in Q_i,\ x\neq y,\\ x, & \text{if } x=y.\end{cases}$$

Then $Q(\Sigma)$, $\Sigma=\{B,B^2,B^3\}$ is a QPS. The Cayley table for the quasigroup $Q(B)$ we fill out by subquasigroups given on the blocks of the BIB. These subquasigroups are isomorphic to the quasigroup $H(A)$:

$B(x,y)=\alpha_i^{-1}A(\alpha_i x,\alpha_i y),\ x,y\in Q_i$ or $B(\beta_i x,\beta_i y)=\beta_i A(x,y),\ x,y\in H,$

$\beta_i=\alpha_i^{-1},\ \ i=1,2,...,21,\ \ \alpha_i:Q_i\to H,\ \ \alpha_i=\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4\\ 0 & 1 & 2 & 3 & 4\end{pmatrix},$

if $Q_i=\{a_0,a_1,a_2,a_3,a_4\}$ (in the order of listing). For example

$$\alpha_1=\begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 0 & 1 & 2 & 3 & 4\end{pmatrix},\quad \alpha_{15}=\begin{pmatrix} 5 & 8 & b & h & k\\ 0 & 1 & 2 & 3 & 4\end{pmatrix}.$$

The quasigroup $Q(B)$ is defined by the following table.

B	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	k	m	n	p
1	1	3	5	2	4	7	9	6	8	b	d	a	c	f	h	e	g	m	p	k	n
2	5	2	4	1	3	a	b	c	d	k	m	n	p	6	7	8	9	e	f	g	h
3	4	1	3	5	2	b	a	d	c	n	p	k	m	8	9	6	7	f	e	h	g
4	3	5	2	4	1	c	d	a	b	p	n	m	k	9	8	7	6	g	h	e	f
5	2	4	1	3	5	d	c	b	a	m	k	p	n	7	6	9	8	h	g	f	e
6	9	k	p	m	n	6	8	1	7	e	g	h	f	2	5	3	4	a	c	d	b
7	8	m	n	k	p	1	7	9	6	h	f	e	g	5	2	4	3	d	b	a	c
8	7	n	m	p	k	9	6	8	1	f	h	g	e	3	4	2	5	b	d	c	a
9	6	p	k	n	m	8	1	7	9	g	e	f	h	4	3	5	2	c	a	b	d
a	d	e	h	f	g	2	3	4	5	a	c	1	b	k	p	m	n	6	9	7	8
b	c	f	g	e	h	3	2	5	4	1	b	d	a	n	m	p	k	8	7	9	6
c	b	g	f	h	e	4	5	2	3	d	a	c	1	p	k	n	m	9	6	8	7
d	a	h	e	g	f	5	4	3	2	c	1	b	d	m	n	k	p	7	8	6	9
e	h	a	d	b	c	k	p	m	n	6	9	7	8	e	g	1	f	2	3	4	5
f	g	b	c	a	d	n	m	p	k	8	7	9	6	1	f	h	e	3	2	5	4
g	f	c	b	d	a	p	k	n	m	9	6	8	7	h	e	g	1	4	5	2	3
h	e	d	a	c	b	m	n	k	p	7	8	6	9	g	1	f	h	5	4	3	2
k	p	6	9	7	8	e	g	h	f	2	5	3	4	a	c	d	b	k	n	1	m
m	n	7	8	6	9	h	f	e	g	5	2	4	3	d	b	a	c	1	m	p	k
n	m	8	7	9	6	f	h	g	e	3	4	2	5	b	d	c	a	p	k	n	1
p	k	9	6	8	7	g	e	f	h	4	3	5	2	c	a	b	d	n	1	m	p

The subquasigroup on the block B_{15} has the following Cayley table:

	5	8	b	h	k
5	5	b	k	8	h
8	k	8	h	5	b
b	h	5	b	k	8
h	b	k	8	h	5
k	8	h	5	b	k

The subquasigroup on B_1 is in the left top corner of the Cayley table of the quasigroup $Q(B)$.

From the quasigroup $Q(B)$ it is easy to obtain the quasigroups B^2 and B^3. Thus we obtain a QPS $\{B, B^2, B^3\}$.

References

[1] **V. D. Belousov**: *Systems of quasigroups with generalized identities*, (Russian), Uspehi mat. nauk **20(121)** (1965), 75 – 146.

[2] **G. B. Belyavskaya and A. M. Cheban**: *S-systems of an arbitrary index, I*, (Russian), Mat. issled. **7** (1972)), 27 – 49.

[3] **G. B. Belyavskaya and A. M. Cheban**: *S−systems of an arbitrary index, II*, (Russian), Mat. issled. **7** (1972), 3 – 13.

[4] **G. B. Belyavskaya**: *Interlacing of quasigroups by means of block designs*, (Russian), Combin. analiz **3** (1974), 49 – 53.

[5] **J. Dénes**: *When is there a latin power set* ?, Amer. Math. Monthly **104** (1997), 563 – 565.

[6] **J. Dénes and A. D. Keedwell**: *Latin squares and their applications*, Akadémiai Kiadó, Budapest 1974.

[7] **J. Dénes, G. L. Mullen and S. J. Suchower**: *A note on power sets of latin squares*, J. Combin. Math. Combin. Computing **16** (1994), 27 – 31.

[8] **J. Dénes and P. J. Owens**: *Some new latin power sets not based on groups*, J. Comb. Theory, Ser. A **85** (1999), 69 – 82.

[9] **J. Dénes and P. Petroczki**: *A Digital encrypting communication system*, Hungarian Patent No. 201437A, 1990.

[10] **R. Guérin**: *Existence et propriétés des carrés latin orthogonaux, II*, Publ. Inst. Statist. Univ. Paris, **15** (1966), 215 – 293.

[11] **M. Hall**: *Group Theory*, (Russian), Moscow 1962.

[12] **M. Hall**: *Combinatorial theory*, (Russian), Moscow 1970.

[13] **A. D. Keedwell**: *On R-sequenceability and R_h-sequenceability of groups*, Combinatorics '81 (Rome 1981), North-Holland Math. Stud. **78**, North-Holland, Amsterdam–New York 1983, 535 – 548.

[14] **H. B. Mann**: *On orthogonal latin squares*, Bull. Amer. Math. Soc. **50** (1944), 249 – 257.

[15] **H. B. Mann**: *The construction of orthogonal latin squares*, Ann. Math. Statist. **13** (1942), 418 – 423.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5
MD-2028 Chishinau
Moldova

Received November 15, 2001
Revised April 12, 2002