# Orthogonality and transversals

**Quasigroups induced by a coordinatization of an affine plane.** A finite affine plane may be obtained from $(Q,+,\cdot,0,1)$, where $(Q,+,0)$ is a group, $(Q^*,\cdot,1)$ a loop, if $0a = a0 = 0$ for all $a \in Q$ and the equation $ax + c = bx$ has a unique solution whenever $a, b \in Q$ and $a \neq b$. This is what will be assumed further on. In infinite case the existence of the affine plane also needs the condition that the equation $xa + c = xb$ has a unique solution whenever $a, b \in Q$ and $a \neq b$.

For each $c \in Q^*$ define a binary operation $*_c$ on $Q$, $c \in Q^*$, by

$$a *_c b = a + cb \text{ for every } a, b \in Q.$$

If $x *_c b = a$, then $x + cb = a$ and $x = a - cb$. If $a *_c y = b$, then $a + cy = b$, $cy = -a + b$ and $y = c\backslash(-a + b)$ ($c\backslash 0$ is defined as 0). This shows that $(Q, *_c)$ is a quasigroup for all $c \in Q^*$.

Suppose now that $c, d \in Q^*$ and $c \neq d$. Let us consider $u, v \in Q$ and ask for which $(x, y) \in Q^2$

$$x *_c y = u \text{ and } x *_d y = v.$$

Any such $(x, y)$ fulfils $x = u - cy$ and $x = v - dy$. Thus $cy - u = -x = dy - v$. Therefore $cy = dy - v + u$. Since $c \neq d$ there exists only one $y \in Q$ that fulfils the latter equality, and $(u - cy, y)$ is the only solution to the equations above.

The latter fact may be expressed also by saying that the quasigroups $(Q, *_c)$ and $(Q, *_d)$ are orthogonal, in the sense described below.

**Orthogonality.** Quasigroups $(Q,\cdot)$ and $(Q,*)$ are said to be *orthogonal* if for all $u, v \in Q$ there exists exactly one pair $(x, y) \in Q \times Q$ such that $xy = u$ and $x * y = v$. Two latin squares of the same order (and the same set of symbols) are said to be *orthogonal* if they may be interpreted as multiplication tables of orthogonal quasigroups.

A set of quasigroups $(Q, *_1)$, $\dots$, $(Q, *_k)$ is said to be *mutually orthogonal* if $(Q, *_i)$ and $(Q, *_j)$ are orthogonal whenever $1 \leq i < j \leq k$. Similarly define *mutually orthogonal latin squares.* The latter is often abbreviated as MOLS.

If $(Q,+,\cdot,0,1)$ coordinatizes an affine plane and $|Q| = n$, then $(Q, *_c)$, $c \in Q^*$ is a set of $n - 1$ mutually orthogonal quasigroups. The affine plane induced by $(Q,+,\cdot,0,1)$ thus yields $n - 1$ mutually orthogonal latin squares of order $n$.

For each $n \geq 2$ denote by $N(n)$ the maximum size of MOLS of order $n$. We shall explain why $N(n) \leq n - 1$ and why a set of $n - 1$ MOLS describes an affine plane of order $n$ or, and thus also a a projective plane of order $n$. (The order of an affine plane is the number of points upon a line. The order of an projective plane is the number of points upon a line diminished by one.)

**Transversal designs from orthogonal quasigroups.** Suppose that $(Q, *_i)$, $1 \leq i \leq k$, is a set of mutually orthogonal quasigroups, $k \geq 2$. Put $\Omega = Q \times \{\infty, 0, 1, \dots, k\}$. Construct a block design upon $\Omega$ with groups $Q \times \{\infty\}$, $Q \times \{0\}$, $Q \times \{1\}$, $\dots$, $Q \times \{k\}$ in such a way that $\{(a_\infty, \infty), (a_0, 0), (a_1, 1), \dots, (a_k, k)\}$ is a block if and only if there exist $x, y \in Q$ such that $(a_\infty, a_0, a_1, \dots, a_k) = (x, y, x *_1 y, \dots, x *_k y)$.

A block is thus fully determined by $x = a_\infty$ and $y = a_0$. If $1 \leq i \leq k$, then it is also fully determined by $x = a_\infty$ and $x *_i y = a_i$, or by $y = a_0$ and $x *_i y = a_i$. If $1 \leq i < j \leq k$ then for any $a_i$ and $a_j$ there exist unique $x, y \in Q$ such that $x *_i y = a_i$ and $x *_j y = a_j$. This means that there exists a unique block that passes through $(a_i, i)$ and $(a_j, j)$. We have verified that the design is a transversal $(k + 2)$-design of order $n = |Q|$.

**Orthogonal quasigroups from transversal designs.** Let us have a transversal $(k+2)$-design, $k \geq 2$. Denote the groups by $G_\infty$, $G_0$ and $G_i$, $1 \leq i \leq k$. The groups are of the same size. Let $Q$ be a set for which there exist bijections $\gamma_j \colon Q \to G_j$, $j \in \{\infty, 0, 1, \dots, k\}$. Bijections $\gamma_\infty$, $\gamma_0$ and $\gamma_i$, $1 \leq i \leq k$, provide a quasigroup $(Q, *_i)$ in which $x *_i y = z$ whenever there exists a block of the design that passes through $\gamma_\infty(x)$, $\gamma_0(y)$ and $\gamma_i(z)$.

Suppose that $1 \leq i < j \leq k$ and consider $u, v \in Q$. There exists exactly one block $B$ of the design that passes through $\gamma_i(u)$ and $\gamma_j(v)$. Let $x, y \in Q$ be such that $\gamma_\infty(x) \in B$ and $\gamma_0(y) \in B$. Then $x *_i y = u$ and $x *_j y = v$. The block $B$ is determined uniquely by $(i, j, u, v)$. There thus exists a unique pair $(x, y) \in Q \times Q$ such that $x *_i y = u$ and $x *_j y = v$. This means that quasigroups $(Q, *_1)$, …, $(Q, *_k)$ are mutually orthogonal.

**Maximum number of orthogonal latin squares.** A transversal $(k+2)$-design of order $n$ satisfies $k+2 \leq n+1$, and the equality holds if and only if the design is a dual of an affine plane.

Therefore $k \leq N(n) \leq n-1$, and $N(n) = n-1$ if and only if there exists a projective plane of order $n$. If $n$ is a power of a prime, then $N(n) = n-1$. It is widely believed that there are no other $n > 1$ with $N(n) = n-1$. Lower estimates of $N(n)$ are a popular topic. For the upper estimates the following seem to be the only results available:

- $N(6) = 1$ (a classical result belonging to Euler);
- $N(10) \leq 8$ (one of the first big achievements of computer based combinatorics);
- $N(n) \leq n-2$ if $n \equiv 1, 2 \bmod 4$ and $n$ cannot be expressed as a sum of two integer squares. (This is known as Bruck-Ryser Theorem.)

There are many constructions of two orthogonal latin squares. The construction is more difficult if $n = 4k+2$. A pair of orthogonal latin squares exists for each $n > 2$, $n \neq 6$. Thus $N(n) \geq 2$ if $n > 2$ and $n \neq 6$.

**Definition of a transversal.** Let $L$ be a latin square. A set $T$ of cells of $L$ is called a *transversal* if

(1) in each row there occurs exactly one cell of $T$;
(2) in each column there occurs exactly one cell of $T$; and
(3) every symbol occurs in exactly one cell of $T$.

It is easy to observe that isotopic transformations map a transerval upon a transversal, and that a transformation of a latin square upon its parastrophe maps transversals upon transversals. The number of transversals hence is an invariant of the main class of a given latin square.

**Transversals in order 5.** Let $L$ be a latin square. To find a transversal one may start from a cell in the uppermost row, look for a cell in the next row which is not in a conflict with the chosen cell (i.e., contains a different symbol and is in a different row) and continue in the similar manner further on. This can lead to a stalemate—at some row there is no way how to continue. Two examples of partial transversals that cannot be completed are the two cases upon the left below. The latin square in question is a representative of the (only) isotopy class of latin squares of order 5 that are not isotopic to a latin square induced by addition modulo 5. This square possesses exactly three transversals, all of them pass through the cell in the leftmost column that carries the symbol 2. One of them is upon the right.

| | | | | |
|---|---|---|---|---|
| $\boxed{1}$ | 2 | 3 | 4 | 5 |
| 2 | 1 | $\boxed{4}$ | 5 | 3 |
| 3 | 4 | 5 | 1 | $\boxed{2}$ |
| 4 | 5 | 2 | $\boxed{3}$ | 1 |
| 5 | 3 | 1 | 2 | 4 |

| | | | | |
|---|---|---|---|---|
| 1 | 2 | $\boxed{3}$ | 4 | 5 |
| 2 | 1 | 4 | $\boxed{5}$ | 3 |
| 3 | $\boxed{4}$ | 5 | 1 | 2 |
| 4 | 5 | 2 | 3 | $\boxed{1}$ |
| 5 | 3 | 1 | 2 | 4 |

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | $\boxed{4}$ | 5 |
| $\boxed{2}$ | 1 | 4 | 5 | 3 |
| 3 | 4 | $\boxed{5}$ | 1 | 2 |
| 4 | 5 | 2 | 3 | $\boxed{1}$ |
| 5 | $\boxed{3}$ | 1 | 2 | 4 |

**Transversals in order 4.** The latin square upon the left is given by addition modulo 4. As will proved later, this square possesses no transversal. Next to it there is an isotopic square which was obtained by switching middle two rows and columns. By flipping the intercalate in the bottom right corner there arises a latin square that yields the multiplication table of a Klein group. The indicated two transversals comprise all transversals that pass through the cell in the left top corner. This latin square possesses eight transversals.

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 0 |
| 2 | 3 | 0 | 1 |
| 3 | 0 | 1 | 2 |

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 2 | 0 | 3 | 1 |
| 1 | 3 | 2 | 0 |
| 3 | 1 | 0 | 2 |

| | | | |
|---|---|---|---|
| $\boxed{0}$ | 1 | 2 | 3 |
| 2 | 0 | $\boxed{3}$ | 1 |
| 1 | 3 | 0 | $\boxed{2}$ |
| 3 | $\boxed{1}$ | 2 | 0 |

| | | | |
|---|---|---|---|
| $\boxed{0}$ | 1 | 2 | 3 |
| 2 | 0 | 3 | $\boxed{1}$ |
| 1 | $\boxed{3}$ | 0 | 2 |
| 3 | 1 | $\boxed{2}$ | 0 |

**Transversals and complete mappings.** Let $Q$ be a quasigroup. A mapping $\varphi\colon Q \to Q$ is said to be *complete* if

- $\varphi$ is a permutation of $Q$; and
- the mapping $x \mapsto x\varphi(x)$ is also a permutation of $Q$.

If $\varphi$ is a complete mapping of $Q$, then the cells $(x, \varphi(x))$ form a transversal in the multiplication table of $Q$. On the other hand, for each transversal $T$ of the multiplication table there exists a permutation $\varphi$ such that $(x, \varphi(x))$ are the cells of $T$. This is because cells of $T$ cover all rows and all columns. The fact that each symbol occurs exactly once in a cell of $T$ means that $x \mapsto x\varphi(x)$ permutes $Q$. Transversals and complete mappings thus describe the same phenomenon.

**Transversals and orthogonal squares.** Let $(Q, \cdot)$ be a quasigroup. Let $(Q, *)$ be a quasigroup orthogonal to $(Q, \cdot)$. Choose $a \in Q$. For each $x \in Q$ there is only one solution $y$ to $x * y = a$. Denote this solution by $\varphi_a(x)$ (thus $\varphi_a(x)$ gives the result of division of $a$ by $x$ in $(Q, *)$). Since $y$ is determined uniquely, $\varphi_a$ is a permutation of $Q$. For each $b \in Q$ there exists exactly one pair $(x, y)$ such that $xy = b$ and $x * y = a$. Since $y$ is equal to $\varphi_a(x)$, by the definition of $\varphi_a$, the existence and uniqueness of $(x, y)$ may be rephrased by saying that for each $b$ there exists exactly one $x \in Q$ such that $x\varphi_a(x) = b$. In others words, $x \mapsto x\varphi_a(x)$ is a permutation of $Q$. The mapping $\varphi_a$ is complete for each $a \in Q$.

If $a \neq b$, then $\varphi_a(x) \neq \varphi_b(x)$ for each $x \in Q$. This means that the transversals $T_a = \{(x, \varphi_a(x)); x \in Q\}$ form a decomposition of the multiplication table of $(Q, \cdot)$.

The process described above may be reversed in the sense that if $L$ is a latin square of order $n$ that is partitioned by transversals $T_1, \ldots, T_n$, then this partition yields an orthogonal latin square. To define such a square consider a bijection $\gamma$ of $\{1, \ldots, n\}$ upon the set of symbols, and put $\gamma(k)$ into cell $(i, j)$ if $(i, j)$ belongs to $T_k$.

**No transversals modulo $2^n$.** Consider the addition modulo $2^n$, $n \geq 1$. First note that if $\alpha$ permutes $\mathbb{Z}_{2^n}$, then

$$\sum_{i \in \mathbb{Z}_{2^n}} \alpha(i) \equiv \sum_{i=0}^{2^n-1} i \equiv 2^{n-1} \bmod 2^n$$

This is because $i + (2^n - i) \equiv 0 \bmod 2^n$ whenever $0 \leq i < 2^{n-1}$.

Suppose now that $\varphi$ is a complete mapping of $(\mathbb{Z}_{2^n}, +)$. Since $\varphi$ permutes $\mathbb{Z}_{2^n}$, there has to be $\sum \varphi(x) = 2^{n-1}$. Since $\psi\colon x \to x + \varphi(x)$ also permutes $\mathbb{Z}_{2^n}$, there has to be $\sum \psi(x) = 2^{n-1}$. However

$$\sum \psi(x) = \sum (x + \varphi(x)) = \sum x + \sum \varphi(x) = 2^{n-1} + 2^{n-1} = 0,$$

a contradiction. Thus **the addition table modulo $2^n$ possesses no transversal**.

**Groups of odd order.** If $G$ is a group of odd order then the main diagonal is a transversal of the multiplication table of $G$. In other words $x \mapsto x^2$ permutes $G$.

To verify this it suffices to show that $x^2 = y^2$ implies $x = y$, for any $x, y \in Q$. Choose $m = 2k + 1$ such that the orders of both $x$ and $y$ divide $m$. Thus $x^m = 1 = y^m$, and

$$x = x^{m+1} = x^{2(k+1)} = (x^2)^{k+1} = (y^2)^{k+1} = y^{m+1} = y.$$

**Complete mappings and groups.** If $\varphi$ is a complete mapping of a group $G$, then $R_a\varphi$ is also a complete mapping of $G$, for any $a \in G$. Indeed $x \mapsto x\varphi(x)$ is a permutation of $G$ if and only $x \mapsto x\varphi(x)a$ is a permutation of $G$.

Note that the latter observation may not be generalized to loops since the associativity of groups is involved. The observation has an important consequence: Each complete mapping of a group induces a set of complete mappings all of which together partition the multiplication table into transversals. A transversal of a group multiplication table thus induces a latin square that is orthogonal to the table.

**Orthomorphisms.** An *orthomorphism* of a group $G$ is a permutation $\psi$ of $G$ such that $x \mapsto x^{-1}\psi(x)$ is a permutation of $G$.

If $\psi$ is an orthomorphism, then $\varphi\colon x \mapsto x^{-1}\psi(x)$ is a complete mapping since $\psi(x) = x\varphi(x)$. If $\varphi$ is a complete mapping of $G$, then $x \mapsto x\varphi(x)$ is an orthomorphism. There is thus a 1–1 connection between orthomorphisms and complete mappings.

Note that what is here called a complete mapping or an orthomorphism, might be precised by calling it a left complete mapping or a left orthomorphism (the right complete mapping would refer to $\varphi(x)x$ and the right orthomorphism to $\varphi(x)x^{-1}$). Note also that the notion of orthomorphism may be generalized to quasigroups, by writing $x\backslash\psi(x)$ in place of $x^{-1}\psi(x)$.

**Orthomorphisms and automorphisms.** An automorphism $\alpha$ of a group $G$ is said to be *fixed point free* if $\alpha(x) = x$ implies $x = 1$, for all $x \in G$. **An automorphism of a finite group is an orthomorphism if and only if it is fixed point free.** Indeed, $x^{-1}\varphi(x) = y^{-1}\varphi(y) \Leftrightarrow yx^{-1} = \varphi(yx^{-1})$.

There are many groups which offer a plenty of fixed point free automorphisms. If $V$ is a vector space then an invertible linear mapping $\varphi \in GL(V)$ is fixed point free if and only if 1 is not its eigenvalue. If $V$ is an elementary abelian $p$ group, then $V$ may be equipped with the structure of a finite field, say $F$. In such a case the mapping $x \mapsto \lambda x$ is a fixed point free automorphism of $(F, +)$ whenever $\lambda \in F^*$, $\lambda \neq 1$. In fact, a complete set of mutually orthogonal latin squares may be constructed in this way.

**Orthomorphisms and normal subgroups.** Let $N$ be a normal subgroup of a finite group $G$, and let $\nu$ be an orthomorphism of $N$. Suppose that $G/N$ is of order $k$ and that $t_1, \dots, t_k$ are representatives of cosets modulo $N$. Suppose also that $\tilde{\psi}$ is an orthomorphism of $G/N$. Set $\psi(nt_i) = \nu(n)t_j$ whenever $\tilde{\psi}(t_iN) = t_jN$, $n \in N$ and $1 \le i \le k$. The claim is that $\psi$ is an orthomorphism of $G$.

*Proof.* The fact that $\psi$ permutes $G$ follows immediately from the definition. Suppose that $x^{-1}\psi(x) = y^{-1}\psi(y)$. Assume that $x = nt_i$ and $y = mt_j$. Then $(t_iN)^{-1}\tilde{\psi}(t_iN) = (t_jN)^{-1}\tilde{\psi}(t_jN)$, which results in $t_iN = t_jN$ and $i = j$. Assume that $t_kN = \tilde{\psi}(t_iN)$, and put $t = t_i = t_j$ and $s = t_k$.

The assumption is that $(nt)^{-1} \cdot \nu(n)s = (mt)^{-1} \cdot \nu(m)s$. Cancelling $t^{-1}$ on the left and $s$ on the right yields $n^{-1}\nu(n) = m^{-1}\nu(m)$ and $n = m$. Hence $x = y$. □

**The existence of a complete mapping in a finite group.** As shown above, the existence of a complete mapping in a group may be proved via factorization. Normal subgroups of solvable groups are more easily accessible. Hence it is no wonder that they were the first for which it was proved that

> a group of even order possesses a complete mapping if and only if
> its Sylow 2-group is **not** cyclic.

The complete proof of this fact depends upon the Classification of Finite Simple Groups (CFSG).

**Ryser's conjecture** states that in each latin square of odd order there exists a transversal. The least order for which it is not known whether the conjecture holds is equal to eleven.

In fact, Ryser originally conjectured that the order of a latin square has the same parity as the number of transversals it possesses. This is true for even orders, as proved by Balasubramanian. On the other hand, there exist latin squares of odd order with even number of transversals.

**Filling a latin square row by row.** A *latin rectangle* is a $k \times n$ table such that each of the $k$ rows contains each of the $n$-element symbols, and no symbol appears twice in the same column. Latin squares thus are the $n \times n$ latin rectangles.

Using a result that is known as Hall's matching theorem it is not difficult to show that each latin rectangle may be completed to a latin square.

**Smetaniuk** proved that an $n \times n$ array that is filled in at most $n - 1$ cells may be completed to a latin squares if there are no two cells in the same row or column that would be filled by the same symbol.

**Exercise.** Let $G$ be a group. Describe all subsquares of the multiplication table of $G$.