Discrete Mathematics 77 (1989) 285–297
North-Holland

SYMMETRIC QUASIGROUPS OF ODD ORDER

Shmuel SCHREIBER
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat Gan 52100, Israel

Presented to Professor Haim Hanani on his 75th birthday,
with sincere good wishes.

Quasigroups of yet another type turn out to be related to Steiner Triple Systems, though the connection is rather loose and not as precise as in the various coordinatizing bijections described in [3]. However, families of *pairs* formed by abelian groups of odd order and quasigroups defined on the same set of elements have repeatedly been used in the literature to construct Large Sets [8] of Steiner Triple Systems. In Section 1, these quasigroups and their association with abelian groups are described, while Section 2 is devoted to applications to STSs.

1. Definitions and basic properties

1.1. *Quasigroups and squodds*

A quasigroup on a set X is a mapping $(\cdot)$ from $X \cdot X$ onto X such that of three elements of X satisfying $a \cdot b = c$, any two determine the third uniquely; that is, for any $x \in X$, the mapping $y \rightarrow x \cdot y$ of X into X is one-to-one onto, a permutation. The operation (and the quasigroup) is said to be *totally symmetric* if $a \cdot b = c$ implies $b \cdot a = c$ and $c \cdot a = b$. We shall often write x^2 for $x \cdot x$, although this is only customary in the associative case, and call it the *square* of x. An element x of a quasigroup is called *idempotent* if it equals its own square, $x = x \cdot x$.

Suppose the totally symmetric quasigroup $Q(\cdot)$ on the set X contains an idempotent ω, and no other x for which $x \cdot x = \omega$, which also excludes $\omega \cdot x = x$. Then the multiplication by ω permutes the elements of $X \backslash \omega$ in pairs, since $\omega \cdot x = \omega$ for $x \neq \omega$ would imply $\omega \cdot \omega = x$, contrary to the assumption $\omega \cdot \omega = \omega$. Thus the order v of X, if finite, must be odd. If in addition, one requires ω to be the *only* idempotent, this order has to be prime to 3, as can be seen by counting the v^2 entries in the standard multiplication table of Q; indeed, an equality such as $a \cdot b = c$, with all threes values distinct, requires six entries, one for each ordered pair of factors, while one of the form $a \cdot a = b$ requires 3 entries. Adding one for $\omega \cdot \omega = \omega$, we find $v^2 \equiv 1 (\mathrm{mod}\, 3)$. Write X^* for $X \backslash \omega$. The quasigroups to be discussed will satisfy some more restrictions.

Definition 1.1.1. A SQUODD (short for Symmetric Quasigroups of Odd Order)

$Q(\cdot)$ on a set X of order v is

(i) a totally symmetric quasigroup with a unique idempotent $\omega \in X$, for which
(ii) the mapping $x \rightarrow x \cdot x$ is a *permutation* π of the set $X^* = X \backslash \omega$ and
(iii) every cycle of π is of even length.

Example 1.1.2.

	ω	a	b	c	d
ω	ω	c	d	a	b
a	c	b	a	ω	d
b	d	a	c	b	ω
c	a	ω	b	d	c
d	b	d	ω	c	a

$\leftrightarrow (\omega\omega\omega), (\omega ac), (\omega bd), (aab), (bbc), (ccd), (dda).$

It is often convenient to list the squodd by enumerating its $(v+1)(v+2)/6$ triples, instead of the full multiplication table.

Remark 1.1.3. No cycle in the permutation π can be of length less than 4, since a cycle of length 2, $x \cdot x = y$, $y \cdot y = x$ would require $x \cdot y = x$ and $x \cdot y = y$ at the same time.

1.2. Graph notation and direct sums

Given a squodd $Q(\cdot)$ on a set of order v, form a graph of v vertices, labelled by the (unordered) pairs (x, x^2), $x \in X$, two vertices being connected by an edge if their labels have an entry in common; then the graph will consist of a single *loop* on the vertex (ω, ω) and of one or more cycles of even order. It is well known that a graph containing no cycles of odd order is *bipartite,* that is, its vertices may be partitioned (eventually in more than one way) into two classes, with no edge connecting two vertices of the same class. The whole graph so obtained, which will be termed the *diagonal graph* of the squodd $Q(\cdot)$, will thus consist of one *odd* component, the loop on (ω, ω), and a bipartite graph with vertices labelled by certain pairs of elements of X^*, which we will call the *main part* of the diagonal graph.

Definition 1.2.1. Given two graphs, G_1 with vertex set X_1 and G_2 with vertex set X_2, the *direct sum* $G_1 \oplus G_2$ will be a graph whose vertices are the *ordered* pairs (x_1, x_2), $x_i \in X_i$, in which $((x_1, x_2), (y_1, y_2))$ form an edge if and only if (x_1, y_1) is an edge of G_1 *and* (x_2, y_2) one of G_2.

The following lemma will also find application later on:

Lemma 1.2.2. *The direct sum of two graphs is bipartite if and only if at least one of the summands is bipartite.*

Proof. Since the only graphs that are not bipartite are the ones containing cycles of odd order, it is sufficient to verify the easily checked claim that a cycle of order a in the sum can only be generated by a cycle of order b in one summand, and one of order c in the other, where a is the least common multiple of b and c. □

Definition 1.2.3. Let $Q_1(\llcorner)$ be a squodd on the set X_1, with idempotent ω_1, and $Q_2(\neg)$ a squodd on the set X_2, with idempotent ω_2; then the *direct sum* of Q_1 and Q_2, denoted by $Q_1 \oplus Q_2$, is a quasigroup $Q(*)$ on $X_1 \times X_2$, with $(x_1, x_2) * (y_1, y_2) = (z_1, z_2)$ if and only if $x_1 \llcorner y_1 = z_1$ *and* $x_2 \neg y_2 = z_2$, $(x_i, y_i, z_i \in X_i)$.

Proposition 1.2.4. *The direct sum of two squodds is a squodd. Moreover, if the direct sum of two quasigroups satisfying conditions* (i) *and* (ii) *of Definition* 1.1.1 *satisfies condition* (iii) *as well, so does each summand.*

Proof. It is obviously enough to verify the second statement.

The diagonal graph of the sum consists of 4 parts:

(1) the loop with single vertex (ω_1, ω_2),

(2) the part derived from elements of the form (x_1, ω_2), with $x_1 \in X_1^*$, which is isomorphic to the *main part* of the diagonal graph of $Q_1(\llcorner)$,

(3) the part derived from elements of the form (ω_1, x_2) with $x_2 \in X_2^*$, isomorphic to the *main part* of the diagonal graph of $Q_2(\neg)$,

(4) the part derived from elements of the form (x_1, x_2) with $x_1 \in X_1^*$ and $x_2 \in X_2^*$ isomorphic to the *direct sum* (in the sense of Definition 1.2.1) of the main parts of the diagonal graphs of the summands, and thus to the direct sum of parts (2) and (3).

By Lemma 1.2.2, the graph consisting of parts (2), (3) and (4) – which is the main part of the diagonal graph of $Q(*)$ – will be bipartite if, and only if, parts (2) and (3) are bipartite, too. □

1.3. Squodds and abelian groups; The main example

For some of the constructions in the sequel, the multiplicative order of -2 modulo an odd prime p is relevant.

Lemma 1.3.1.

(α) *If* $p \equiv 3 \pmod 8$, *the multiplicative order of* -2 *is an odd integer*;

(β) *If* $p \equiv 5 \pmod 8$, *the multiplicative order of* -2 *is a multiple of* 4;

(γ) *If* $p \equiv 7 \pmod 8$, *the multiplicative order of* -2 *is twice an odd number*;

(δ) *If* $p \equiv 1 \pmod 8$, *the multiplicative order of* -2 *may be either odd, or a multiple of* 4, *or twice an odd number.*

(In fact, a heuristic consideration, which can be made precise by a zeta-function argument, will show that for $6N$ primes selected at random from the sequence $8k+1$, with N large, about N will satisfy condition (α), another N condition (γ), and $4N$ condition (β).)

Proof. All four statements follow from the fact (see any elementary text on the Theory of Numbers) that $\underline{-2}$ is a quadratic residue for primes $\equiv 1$ or $3 \pmod 8$ and a non-residue for primes $\equiv 5$ or $7 \pmod 8$. □

Definition 1.3.1.1 An odd prime p will be designated as an α-prime, a β-prime, or a γ-prime, according to the condition in Lemma 1.3.1 satisfied by the multiplicative order of $-2 \pmod p$.

Definition 1.3.1.2 Let A be an abelian group, written additively, on a set X of order v, $(v, 6) = 1$, let $h \in A$ and $Q(\cdot)$ a Totally Symmetric quasigroup on X. Then the quasigroup $Q(*)$, defined by

$$(x+h)*(y+h) = (x \cdot y) + h$$

(which is obviously isomorphic to $Q(\cdot)$) will be called an h-shift of $Q(\cdot)$ with respect to A.

Definition 1.3.1.3 Let A be an abelian group, written additively, on a set X of order v, $(v, 6) = 1$, and $h \in A$. Then we shall designate the quasigroup $Q(*)$, defined by

$$x*y = z \Leftrightarrow x+y+z = 3h \text{ in } A$$

as $\mathrm{Der}_h A$, and we shall write $\mathrm{Der}(A)$ for $\mathrm{Der}_0(A)$.

Proposition 1.3.2. *For A and h as above,* $\mathrm{Der}_h(A)$ *will be a squodd if, and only if, no α-prime divides the order v of A.*

Proof. The quasigroup will obviously be totally symmetric, with the *unique* idempotent h; for, with $k \neq h$ and $3k = 3h$ we have $3(k-h) = 0$ and thus, by the hypothesis on v, $k = h$, a contradiction. Similarly, no diagonal element is repeated, for $a_1 + a_1 + b = a_2 + a_2 + b = 3h$ implies $2a_2 = 2a_1$, thus again $a_2 = a_1$, v being odd. It only remains to check whether all cycles in the diagonal permutation of $A\backslash(h)$ are of even length, and for this we may obviously assume $h = 0$.

Given any $a \neq 0$ in A, its order will be some w, dividing v. The diagonal cycle generated by a in $\mathrm{Der}_0(A)$ will then be

$$\langle a, (-2)^1 a, (-2)^2 a, \ldots, (-2)^{k-1} a\rangle, \quad \text{with } (-2)^k \equiv 1 \pmod w.$$

For w a β-prime or a γ-prime, k will be even, by Lemma 1.3.1. If w is some power p^r of a β-prime or a γ-prime p, k will be the exponent of -2 for p, multiplied by some power $\leqslant r$ of p, thus again even. If w is a product of such prime powers, k will again be even, being the l.c.m. of the exponents for the single prime powers. Recall finally that if v is divisible by any α-prime p, A will necessarily contain some element b of order p, which, again by Lemma 1.3.1, will generate a cycle of odd length. □

As an example we may translate Example 1.1.2 above into $\mathrm{Der}_2(C_5)$, setting $\omega = 2$, $a = 0$, $b = 1$, $c = 4$, $d = 3$; or consider $\mathrm{Der}_4(C_7)$, which gives the triples:

(005), (014), (023), (066), (113), (122), (156), (246), (255), (336), (345), (444).

However, if we attempt the same operation on C_{11} with, say, 0 as idempotent, we shall find the two *odd* diagonal cycles $\langle 1, 9, 4, 3, 5\rangle$ and $\langle 2, 7, 8, 6, 10\rangle$. We shall, however, see in a later section that squodds exist of any finite order, prime to 6.

Whether or not the order v of A, $(v, 6) = 1$, satisfies the restriction of Proposition 1.3.2, we have:

Proposition 1.3.2.1 *For $h, k \in A$, $k \neq h$,* $\mathrm{Der}_k(A)$ *and* $\mathrm{Der}_h(A)$ *have no triple in common.*

Proof. If $x + y + z = 3h = 3k$, then $3(k - h) = 0$. Thus $k - h = 0$ by the hypothesis on v. □

This is equivalent to saying that no two triples in $\mathrm{Der}_k(A)$ are *shifts* of each other, or belong to the same additive A-orbit. It is easy to check that there are $(v + 1)(v + 2)/6$ such orbits of triples: one for triples with three equal entries, $v - 1$ for triples with one entry repeated and $(v - 1)(v - 2)/6$ for triples with 3 distinct entries.

Definition 1.3.2.2 Given an abelian group A, and a squodd $Q(\cdot)$, on a set X of order v, $(v, 6) = 1$, the pair (A, Q) will be called an I-pair if all triples of $Q(\cdot)$ belong to different A-orbits (or: if no two triples of $Q(\cdot)$ are A-*congruent*).

If we consider the diagonal entries of $Q(\cdot)$, $(x, x \cdot x)$ as (unordered) *pairs* rather than as triples with one entry repeated, we certainly *cannot* require all $v - 1$ of these to fall into different A-orbits, since there are only $(v - 1)/2$ such orbits. We may, however, require:

Definition 1.3.3. Given an abelian group A, and a squodd $Q(\cdot)$ on a set X of order v, $(v, 6) = 1$; if no two triples of $Q(\cdot)$ with 3 distinct entries are A-congruent, and if, in addition, the main part of the diagonal graph of $Q(\cdot)$ remains bipartite when one connects by an edge any two vertices representing pairs of elements in the same A-orbit, we shall call the pair (A, Q) a D-pair.

This condition, incidentally, ensures the appearance of exactly two pairs from each A-orbit, covering the $v-1$ diagonal entries (x, x^2) with $x^2 \neq x$; for if three congruent pairs were to appear, the added edges would form a triangle.

Example 1.3.3.1 $\mathrm{Der}(C_5)$ does *not* form a D-pair with C_5: the diagonal sequence is $(1,3)$, $(3,4)$, $(4,2)$, $(2,1)$, the vertices of a quadrangle. But since $4-2=3-1$ and $2-1=4-3$, the two additional edges turn this into the Complete Graph on 4 vertices, K_4, which is certainly not bipartite.

Example 1.3.3.2 $\mathrm{Der}_4(C_7)$, considered above, forms a D-pair with C_7. The vertices $(0,5)$, $(5,2)$, $(2,1)$, $(1,3)$, $(3,6)$, $(6,0)$ form a hexagon, in which the additional edges $((0,5),(1,3))$, $((5,2),(3,6))$ and $((2,1),(6,0))$ close *even* cycles. We shall see that this is due to 7 being a γ-prime.

Examples 1.3.3.3 and 1.3.3.4. The reader is invited to check in detail that the following two squodds form D-pairs with C_{11}:

(α) [1]: (0 0 0), (0 1 6), (0 2 3), (0 4 8), (0 5 7), (0 9 10), (1 4 5), (1 7 9), (1 8 10), (2 6 7), (2 8 9), (2 4 10), (3 4 7), (3 5 10), (3 6 9), (5 6 8); (1 1 2), (2 2 5), (5 5 9), (9 9 4), (4 4 6), (6 6 10), (10 10 7), (7 7 8), (8 8 3), (3 3 1).

(β) [4]: (0 0 0), (0 1 10), (0 2 6), (0 3 5), (0 4 7), (0 8 9), (1 3 4), (1 5 6), (1 7 9), (2 4 9), (2 5 10), (2 7 8), (3 6 7), (3 9 10), (4 5 8), (6 8 10); (1 1 2), (2 3 3), (3 3 8), (8 8 1), (4 4 6), (6 6 9), (9 9 5), (5 5 7), (7 7 10), (10 10 4).

Note that these two squodds do *not* form I-pairs with C_{11}: thus in the first (7 7 8) and (1 1 2) are C_{11}-congruent, and so are (6 6 10) and (5 5 9), (8 8 3) and (9 9 4); while in the second, we find (2 2 3) and (1 1 2), (10 10 4) and (3 3 8), (5 5 7) and (4 4 6), (6 6 9) and (7 7 10).

Proposition 1.3.3.5 *Let A be an abelian group of order v, $(v, 6)=1$, $h \in A$, and let $\mathrm{Der}_h(A)$ be a squodd. Then $(A, \mathrm{Der}_h(A))$ form a D-pair if, and only if, all the prime factors of v are γ-primes.*

Proof. Note that two pairs of elements of A, (a_1, a_2) and (b_1, b_2), are congruent if $b_2-b_1=\pm(a_2-a_1)$, and that the differences between successive elements in the diagonal cycle generated by $x \neq h$,

$$\langle x, 3h-2x, -3h+4x, 9h-8x, -15h+16x, \ldots, h+(-2)^i(x-h), \ldots\rangle$$

equal $3(h-x)$ multiplied by successive powers of -2 modulo w, if w is the order of $x-h$ in A. Since $\mathrm{Der}_h(A)$ is a squodd, the multiplicative order of -2 in C_w, by Proposition 1.3.2, will be even, say $2k$. If w happens to be a β-prime or a γ-prime p, then $(-2)^k$ will equal -1 modulo p, and after k steps along the cycle we shall encounter a pair whose difference is $-3(h-x)$, congruent to the first, and from then onwards, pairs k steps apart will remain congruent to the end of the cycle. If p is a β-prime, k is even and (compare Example 1.3.3.1) the added edges will close odd cycles, while if p is a γ-prime, k is odd (compare Example 1.3.3.2) and the added edges will close even cycles, and thus the bipartite character of the main part of the diagonal graph will be preserved.

The rest of the proof follows exactly the same lines as that of Proposition 1.3.2. □

The D-pairs so obtained are automatically I-pairs, by Proposition 1.3.2.1 and Definition 1.3.2.2.

Following this, and in view of several applications further on, we may introduce

Definition 1.3.4. The pairs (A, Q) will be called an I-D-pair if it is both an I-pair and a D-pair.

By Proposition 1.3.3.5, $(C_{13}, \mathrm{Der}_h(C_{13}))$ cannot form an I-D-pair. However, not all such pairs are formed by derivation. The reader is invited to examine the following example of a squodd forming an I-D-pair with C_{13}:

Example 1.3.4.1 [2]. (0 0 0), (0 1 9), (0 2 7), (0 3 11), (0 4 6), (0 5 8), (0 10 12), (1 2 3), (1 4 5), (1 7 12), (1 8 11), (2 4 12), (2 6 11), (2 9 10), (3 4 8), (3 5 9), (3 7 10), (4 7 11), (5 6 12), (5 10 11), (6 7 9), (6 8 10), (8 9 12); (1 1 6), (6 6 3), (3 3 12), (12 12 11), (11 11 9), (9 9 4), (4 4 10), (10 10 1), (2 2 5), (5 5 7), (7 7 8), (8 8 2).

1.3.5. *Pairs and direct sum operations*

As both abelian groups and squodds are closed under direct sum operations, we may look at what happens to pairs in this context.

Proposition 1.3.5.1. *I-pairs are closed under Direct Sum operations. If both (A_1, Q_1) and (A_2, Q_2) are I-pairs, so is $(A_1 \oplus A_2, Q_1 \oplus Q_2)$.*

Proof omitted.

A similar statement for D-pairs does *not* hold. In fact:

Proposition 1.3.5.2. *I-D-pairs are closed under Direct Sum operations. Moreover, if A_i, Q_i are defined on a set X_i, $i = 1, 2$, and if $(A_1 \oplus A_2, Q_1 \oplus Q_2)$ is a D-pair, then each of (A_i, Q_i) is already an I-D-pair, and so is the sum.*

Proof. Since Lemma 1.2.2 ensures that the bipartite character of the main part of the diagonal graph containing the added edges in each summand will not be violated by the Direct Sum operation, it is enough to prove the second statement.

Let 0_i be the zero of A_i, and ω_i the idempotent of Q_i; then $Q_1 \oplus Q_2$ will contain elements of the form (ω_1, a_2) forming a squodd isomorphic to Q_2, whose pairs and triples are acted on by the shift-operations of the subgroup $\langle (0_1, h_2) \rangle$ of $A_1 \oplus A_2$, so (A_2, Q_2) should be at least a D-pair; and similarly for (A_1, Q_1).

Suppose one summand, say (A_2, Q_2), is *not* an I-D-pair; then its diagonal (compare Examples 1.3.3.3, 1.3.3.4) contains A_2-congruent triples, (a_2, a_2, b_2) and $(a_2+h_2, a_2+h_2, b_2+h_2)$. If $x_1 \cdot y_1 = z_1$ in Q_1, and all 3 entries of (x_1, y_1, z_1) are distinct, $Q_1 \oplus Q_2$ contains the two triples $((x_1, a_2), (y_1, a_2), (z_1, b_2))$ and $((x_1, a_2+h_2), (y_1, a_2+h_2), (z_1, b_2+h_2))$, the second being a shift of the first by $(0_1, h_2) \in A_1 \oplus A_2$, contrary to the first condition in Definition 1.3.3, and so $(A_1 \oplus A_2, Q_1 \oplus Q_2)$ cannot be a D-pair. □

We conclude the first section with the following statement, whose proof will be omitted.

Proposition 1.3.5.3. *I-pairs, D-pairs and I-D-pairs are closed under shifting. If (A, Q) is an I-pair (D-pair, I-D-pair) and, for some $h \in A$, Q^* is an h-shift of Q* (cf. Definition 1.3.1.2) *then (A, Q^*) is again an I-pair (D-pair, I-D-pair).*

2. Applications

2.1. *Squodds, coloured graphs and Steiner Triple Systems*

Since this account is intended to appear in the present Volume, Steiner Triple Systems are bound to crop up. We shall indeed find that squodds lead to STSs, and vice versa, although in nowhere the precise manner is which Ganter and Werner use the various algebras in their paper [3] to coordinate these combinatorial structures. We shall therefore not present the reader with any of those bijections between definitions, by which these authors illustrate their elegant results – in the present case, it would smack of pretence. Anyway. . .

Proposition 2.1.1. (1) *Given a squodd $Q(\cdot)$ on a set X of order v, there is at least one way to derive from it a Steiner Triple System B on the $v+2$ marks $\langle X \cup \langle \infty_1, \infty_2 \rangle \rangle$, where $\infty_1, \infty_2 \notin X$ are two additional marks.*

(2) *Given a Steiner Triple System (B) on a set Y, and a Flag – that is, a triple $(b_0; b_1, b_2) \in B$ in which b_0 is marked – there is at least one way to obtain from it a squodd $Q(\cdot)$ on $Y \backslash (b_1, b_2)$, whose idempotent is b_0.*

Proof. (α) Use the elements $(\omega, x, y, \ldots)$ of X to label, firstly, the vertices of the complete graph $G \sim K_v$ of order v, and secondly a Store of v colours. For each $y, z \in X$, $y \neq z$, we now colour the edge (y, z) of G with the colour x if $y \cdot z = x$ in Q, *and* if x is different from both y and z. Note that no two edges of the same colour can have a vertex in common, since if both (p, q) and (q, r) were to be coloured s, this would mean $q \cdot s = p$ and $q \cdot s = r$. This leaves uncoloured only the edges (x, x^2), $x \neq \omega$, and constitutes the first coloration, or F-coloration, of the edges of G. It is readily seen that the uncoloured edges form a two-factor of $G \backslash \omega$; that is, every vertex of $G \backslash \omega$ is the endpoint of 2 such edges. This two-factor, forming the main part of the diagonal graph of $Q(\cdot)$ – except that this time its vertices are labelled by single elements of X^* instead of *pairs* as in 1.2 – is made up of one or more cycles – closed simple polygons – each of some *even* order, by condition (iii) in Definition 1.1.1.

(β) The edges of even cycles being 2-colourable, that is, one may colour them in 2 different colours without edges of a given colour having a vertex in common, we now take two more colours, ∞_1 and ∞_2, and colour the edges in each cycle alternately ∞_1 and ∞_2. In doing this, it should be noted, we have one arbitrary choice when two-colouring the edges of each cycle. Call this the second coloration, or S-coloration, of the edges of G. Now we adjoin two vertices, ∞_1 and ∞_2. If (x, y) has been coloured ∞_i, we then connect x to the vertex ∞_i by an edge coloured y, and y by one coloured x. Finally, we connect ω and ∞_1 by an edge coloured ∞_2, and to ∞_2 by an edge coloured ∞_1, and ∞_1 and ∞_2 by an edge coloured ω. Thus we have obtained a partition of the edges of the complete graph on $X \cup \langle \infty_1, \infty_2 \rangle$ into triangles, each edge being coloured with the label of the opposite vertex, which partition is obviously a Steiner Triple System on $X \cup \langle \infty_1, \infty_2 \rangle$, and this concludes the proof of (1).

(γ) Conversely, if B is a Steiner Triple System on a set Y of order w, we label the vertices of a graph $H \simeq K_w$ by the elements of Y, and for each $(x, y, z) \in B$ we colour each edge of the triangle (x, y, z) by a colour bearing the label of the opposite vertex. If $b_1, b_2 \in Y$, let $(b_0, b_1, b_2) \in B$, that is, let b_0 be the third vertex of the corresponding triangle. Removing vertices b_1, b_2 and deleting all the edges through them from H, we are left with a complete graph $G \sim K_{w-2}$, in which the edges coloured b_1 form a 1-factor of $G \backslash b_0$, and so do the edges coloured b_2. This is an S-coloration of the edges of G. We note that these two 1-factors (which we might as well uncolour, obtaining an F-coloration of G) form together a two-factor of $G \backslash b_0$, consisting of one or more cycles of even length.

(δ) We now construct a squodd $Q(\cdot)$ on $Y - \langle b_1, b_2 \rangle$. If $(x, y, z) \in B \backslash (b_0, b_1, b_2)$, set $x \cdot y = z$; set $b_0 \cdot b_0 = b_0$. Next, *orient* each cycle in the two-factor in one of the two possible ways, and note that this again gives us one arbitrary choice per cycle. If an edge in this orientation has been directed from x to y, set $x \cdot x = y$. Now the totally symmetric mapping from $(Y - \langle b_1, b_2 \rangle) \times (Y - \langle b_1, b_2 \rangle)$ onto $Y - \langle b_1, b_2 \rangle$ has been defined for the whole domain, and we have a squodd. □

Remark 2.1.2. Apart from the fact that the resulting G-graph depends on the choice Flag in B – or pair of elements b_1, b_2 in Y – the arbitrary choices in (β) and (δ) above are enough indication that there cannot be much connection between the structures of STSs and those of squodds obtained from them as described.

There are, up to isomorphism, two STSs of order 13; one, the cyclical one, has a larger group of automorphisms, of order 39. The other one has only a group of order 6, isomorphic to S_3. Its 78 possible flags give rise to no less than 17 classes of s-coloured G-graphs, and thus to a larger number of non-isomorphic squodds (from some of which one may obtain the first, cyclical STS of order 13). It is reasonable to assume that as the order increases, squodds proliferate still more quickly than STSs, which gives us some excuse not to go further into the question of their structure. So far, the only claim to the title of Variety in the algebraic sense that squodds have, is closure under Direct Sum operations (Proposition 1.2.4), but they certainly form a "variety" in the colloquial sense.

Corollary 2.1.3. *Squodds exist of any finite order prime to* 6.

Remark 2.1.4. The converse contribution of directly constructed squodds, say from Proposition 1.3.2 (Derivation) and 1.2.4 (Direct Sum) is rather modest, because of the absence of a direct construction for prime orders $p \equiv 3 (\bmod 8)$.

2.2. *D-pairs and packings* (*or*: *Denniston Large Systems*)

For $(v, 6) = 1$, let us imagine $v + 2$ points in space, no 4 in the same plane, forming $v(v+1)(v+2)/6$ triangles, v through each edge. If we can use v colours to colour all these triangles so that no two triangles of the same colour have an edge in common, then on labelling the $v + 2$ points, or vertices with different marks, each pair of marks will appear just once as an edge of a triangle of a given colour, and the triads of vertices of this family of triangles will form an STS. Thus such a colouring achieves a partition of all the triads of marks into v disjoint STSs, or a Large Triple System on the $v + 2$ marks.

In particular, the set of labels may consist of the v elements of an abelian group A and of two more marks, $\infty_1, \infty_2 \notin A$. If, in this case, the set of triangles of a given colour is derived from any other such set by adding a fixed $h \in A^*$ to each vertex label other than ∞_1 or ∞_2, we speak of a Denniston Large System, or a Packing (with the aid of A) or an A-Packing.

Proposition 2.2.1. *Given an abelian group A on a set X of order v, $(v, 6) = 1$, and an A-Packing $B_0, B_1, \ldots, B_{v-1}$ on $Y =: X \cup \langle \infty_1, \infty_2 \rangle$, the squodd Q_i derived from the flag $(h_i, \infty_1, \infty_2) \in B_i$ as described in Proposition* 2.1.1 *above forms a D-pair (A, Q_i) with A. Conversely, the* STS*s on $X \cup \langle \infty_1, \infty_2 \rangle$ constructed from the squodd Q_i in a D-pair (A, Q_i) as described in Proposition* 2.1.1, *and from all A-shifts of Q_i, form an A-Packing on $X \cup \langle \infty_1, \infty_2 \rangle$.*

Proof. The first condition of Definition 1.3.3, on triples with 3 distinct entries, is satisfied by hypothesis. Also by hypothesis, no pair (x, y) with $(\infty_1, x, y) \in B_i$ can be A-congruent to another pair (x', y') with $(\infty_1, x', y') \in B_i$, and similarly for ∞_2. Thus, after the "orienting" step of stage δ) in the proof of 2.1.1, we may relabel each vertex in the diagonal graph, this time by a pair of marks, the original mark and the following one, and be assured that if (x, y) is congruent in A to (z, u) then $(\infty_1, x, y) \in B_i$ implies $(\infty_2, z, u) \in B_i$; thus adding an edge between (x, y) and (z, u) will not contravene the bipartite character of this graph.

This completes the proof of the direct claim. The proof of the converse is easy and will be omitted. □

The first Large Steiner System, found in 1850 by Kirkman and rediscovered by Cayley, is actually of this type, derived from the (unique) STS on 9 marks by fixing two entries and permuting the other 7 cyclically, one step at a time. The subject began to develop around 1973, with Teirlinck [10] showing how to derive a Large System of order $3w$ from one of order w, by a simple construction ("Triplicating"). Rosa [7], using Latin Squares with no subsquare of order 2, derived Large Systems of order $2w+1$ from given ones of order w ("Duplicating"). Denniston [1], concentrating on prime orders, constructed D-pairs with the cyclical group C_p for $p = 11$, 13, 17, 19, 23, 29, 31, 41, 47, 59, 67, exploiting for the larger values of p either the full multiplicative groups of $\mathbb{Z}_p^*$ or large subgroups M, in the sense that if $\lambda \in M$ and $x \cdot y = z$ in $Q(\cdot)$, $(\lambda x) \cdot (\lambda y) = \lambda z$ as well. Except for $p = 11$, 13 and 29, all of these actually form I-D-pairs. Therefore, with the hindsight of Proposition 1.3.5.2, we now know that just as there exists a Packing of order $31+2$ and one of order $67+2$ there exists one of order $31 \cdot 67 + 2 = 2079$ as well. (A Large System of this order may be obtained in yet another way: start with Kirkman's result of order 9, and proceed as indicated:

$$9 \xrightarrow{D} 19 \xrightarrow{T} 57 \xrightarrow{D} 115 \xrightarrow{D} 231 \xrightarrow{T} 693 \xrightarrow{T} 2079,$$

where D denotes Rosa's "duplication", and T, Teirlinck's "triplication".) The I-D-pair of Example 1.3.4.1, used in [2] to form a sequence of 13 *resolvable* STSs thus obtaining a Packing of order 15, may of course serve in such Direct Sum operations too. Around the same time, Wilson [11] and others became aware of the results of Proposition 1.3.3.5 above and derived Denniston Large Systems from the I-D-pairs so obtained. Denniston had been unaware of this, and his constructions for C_{23}, C_{31} and C_{47} show again that Derivation is not the unique source of I-D-pairs. The excellent summary of the state of the art up to around 1980 in [8] already mentions the general belief prevailing at the time that Large Systems exist for every feasible order >7; and in a series of papers in 1984, Lu [5, 6] covered nearly all the ground, so at the time of his premature death only six values were left in doubt (which, I am told, have also been settled since then).

2.3. *I-D-pairs and Teirlinck's Second Construction*

Since a computer search has shown that the only two D-pairs with C_{11} are those of Examples 1.3.3.3 and 1.3.3.4, we know from Proposition 1.3.5.2 that the Direct Sum of one of those with an I-D-pair of order v will *not* lead even to a D-pair of order $11v$; thus a Large System of order $11v+2$ cannot be obtained in this way. However, we owe to Teirlinck [10] the following remarkable result taken from [8], which seems a fitting note on which to close this account:

Theorem 2.3.1 (Teirlinck). *Given any Large System of order $u+2$, and an I-D-pair $(A, Q_0(\cdot))$ of order v, there exists a Large System of order $u \cdot v + 2$.*

Proof. Not matter what its structure, we may rename the entries in the triples of the given Large System to be the elements of $Z_u \cup \langle \infty_1, \infty_2 \rangle$ numbering the respective STSs $B_1, B_2, \ldots, B_u$. For simplicity, let $0 \in A$ be the idempotent of $Q_0(\cdot)$, and a_i that of its ith A-shift. Also, let F_1, F_2 be a bi-partition of the diagonal pairs of $Q_0(\cdot)$. We now construct $u \cdot v$ STSs C_{ij} on $V =: (A \times Z_u) \cup \langle \infty_1, \infty_2 \rangle$ as follows:

For each $a_i \in A$ and $j \in Z_u$, $C_{ij} = C_{ij}^{(1)} \cup C_{ij}^{(2)} \cup C_{ij}^{(3)}$, consisting of the following triples on V:

$$\begin{aligned} C_{ij}^{(1)} = {} & \langle \infty_1, \infty_2, (a_i, z_j) \rangle \mid ((\infty_1, \infty_2, z_j) \in B_j) \cup \langle (\infty_k, (a_i, x), (a_i, y)) \rangle \\ & \mid ((\infty_k, x, y) \in B_j) \cup \langle ((a_i, x), (a_i, y), (a_i, z)) \rangle \mid ((x, y, z) \in B_j), \quad k = 1, 2; \\ C_{ij}^{(2)} = {} & \langle \infty_k, (a_i + b, x), (a_i + b \cdot b, x) \rangle \mid (b \in A^*, x \in Z_u, (b, b \cdot b) \in F_k, \quad k = 1, 2)) \\ & \cup \langle ((a_i + b, x), (a_i + b, y), (a_i + b \cdot b, (x+y)/2 + j)) \rangle \\ & \mid (b \in A^*, \quad x, y \in Z_u, \quad y \neq x); \\ C_{ij}^{(3)} = {} & \langle (a_i + b, x), (a_i + c, y), (a_i + b \cdot c, (x + y + j)) \rangle \\ & \mid (x, y \in Z_u, \quad b \neq c \neq b \cdot c \neq b \in A^*), \end{aligned}$$

where in $C_{ij}^{(3)}$, each triple of $Q_0(\cdot)$ is taken on *one* fixed order with every pair x, y of Z_u. Notation might perhaps have been shorter if in $C_{ij}^{(2)}$ and $C_{ij}^{(3)}$ we had omitted a_i and taken the dot operation in $Q(\cdot)$ to be read as taking place in Q_i, the ith A-shift of $Q_0(\cdot)$, but with the present one it seems easier to verify that any triple of V actually appears in some C_{ij}. □

It should also be noted that, apart from Proposition 1.3.5.2, this is, so to say, the first instance of I-D-pairs finding "full employment". With I-pairs alone, we could not have the first term in $C_{ij}^{(2)}$, since the partition into two one-factors F_k would not work and $(\infty_k, (a_i + b, x), (a_i + b \cdot b, x))$ would reappear as some $(\infty_k, (c \cdot c, x), (c, x))$; while with D-pairs alone, for a given x and y, we should be meeting again triples from the second term of $C_{ij}^{(2)}$ as (c, x), (c, y), $(c \cdot c, (x+y)/2 + j)$. The reader might wish to verify this with the I-pair $(C_5, \mathrm{Der}(C_5))$, and with the two D-pairs of Examples 1.3.3.3 and 1.3.3.4.

References

[1] R.H.F. Denniston, Some packings with Steiner triple systems, Discrete Math. 9 (1974) 213–227.

[2] R.H.F. Denniston, Sylvester's problem of the 15 schoolgirls, Discrete Math. 9 (1974) 229–233.

[3] B. Ganter and H. Werner, Co-ordinating Steiner Systems, Ann. Discrete Math. 7 (1980) (Topics on Steiner Systems, C.C. Lindner and A. Rosa, eds.) 3–24.

[4] E.S. Kramer and D.M. Mesner, The possible (impossible) systems of 11 disjoint $S(2, 3, 13)$'s ($S(3, 4, 14)$'s) with automorphism of order 11, Utilitas Math. 7 (1975) 55–58.

[5] Jia-Xi Lu, On large sets of disjoint Steiner triple systems, I, II, III, J. Combin. Theory (A) 34 (1983) 140–146, 147–155, 156–182.

[6] Jia-Xi Lu, On large sets of disjoint Steiner triple systems, IV, V, VI, J. Combin. Theory (A) 37 (1984) 136–163, 164–188, 189–192.

[7] A. Rosa, A theorem on the maximum number of disjoint Steiner systems, J. Combin. Theory (1) 18 (1975) 305–312.

[8] A. Rosa, Intersection properties of Steiner systems, Ann. Discrete Math. 7 (1980) 115–128.

[9] L. Teirlinck, On the maximum number of disjoint Steiner Triple Systems, Discrete Math. 6 (1973) 299–300.

[10] L. Teirlinck, Combinatorial Structures, Thesis, Vrije Universiteit Brussel, Dept. voor Wiskunde, 1976.

[11] R.M. Wilson, Some partition of all triples into Steiner triple systems, Hypergraph Seminar, Ohio State Univ. 1972, Lecture Notes in Math. 411 (Springer, Berlin, 1974) 267–277.