Commentationes Mathematicae Universitatis Carolinae

Charles Curtis Lindner

Construction of quasigroups having a large number of orthogonal mates

Commentationes Mathematicae Universitatis Carolinae, Vol. 12 (1971), No. 3, 611--617

Persistent URL: http://dml.cz/dmlcz/105368

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 1971

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

Commentationes Mathematicae Universitatis Carolinae

12,3 (1971)

CONSTRUCTION OF QUASIGROUPS HAVING A LARGE NUMBER OF ORTHOGONAL MATES

Charles C. LINDNER, Auburn

1. Introduction. The object of this paper is to give a construction which produces a quasigroup having a large number of orthogonal mates, any two of which differ by more than a permutation. By a pair of quasigroups differing by more than a permutation we mean that neither of the associated latin squares can be obtained from the other by a renaming of the symbols on which they are based. In particular we prove the following theorem.

Theorem. If there are s mutually orthogonal quasigroups of order v, t mutually orthogonal quasigroups of order q containing t mutually orthogonal subquasigroups of order p, and r mutually orthogonal quasigroups of order $q-p$, then there is a quasigroup of order $v(q-p)+p$ having at least $(s-2)(t-1)^{v}(r-1)^{v^2-v}$ orthogonal mates any two of which differ by more than a permutation. If $p=0$ we obtain a quasigroup of order vq having at least $(s-2)(t-1)^{v^2}$ orthogonal mates.

The proof of this theorem is based on a generalization of A. Sade's singular direct product. In particu-

---

AMS, Primary 05B15
Secondary 20N05

Ref.Ž. 8.812,2,
2.722.9

lar, a combination of the generalized singular direct products defined by the author in [1] and [2].

2. Definitions. Let $(V, \odot)$ be an idempotent quasigroup and Q a set. For each v in V let $\sigma(v)$ be a binary operation on Q so that $(Q, \sigma(v))$ is a quasigroup. Further suppose that $P \subseteq Q$ is such that all of the operations agree on P and such that $(P, \sigma(v))$ is a subquasigroup of $(Q, \sigma(v))$. For each (v, w) $v \neq w$ in V, let $\otimes(v, w)$ be a binary operation on $P' = Q \setminus P$ so that $(P', \otimes(v, w))$ is a quasigroup. We remark here that the $|V|^2 - |V|$ operations $\otimes(v, w)$ are not necessarily related to each other; the $|V|$ operations $\sigma(v)$ are not necessarily related to each other; and finally that none of the $|V|^2 - |V|$ operations $\otimes(v, w)$ are necessarily related to any of the $|V|$ operations $\sigma(v)$. We now define a generalized singular direct product denoted by $V_{\odot} \times Q(\sigma(v),$ $P, P' \otimes(v, w))$, to be the quasigroup $\oplus$ defined on the set $P \cup (P' \times V)$ as follows:

(1) $p_1 \oplus p_2 = p_1 \sigma(v) p_2 = p_1 \sigma(w) p_2$ if $p_1, p_2 \in P$;

(2) $p \oplus (p', v) = (p \sigma(v) p', v)$ if $p \in P$, $p' \in P'$, $v \in V$;

(3) $(p', v) \oplus p = (p' \sigma(v) p, v)$ if $p \in P$, $p' \in P'$, $v \in V$;

(4) $(p'_1, v) \oplus (p'_2, v) = p'_1 \sigma(v) p'_2$ if $p'_1 \sigma(v) p'_2 \in P$
$= (p'_1 \sigma(v) p'_2, v)$ if $p'_1 \sigma(v) p'_2 \in P'$;

(5) $(p'_1, v) \oplus (p'_2, w) = (p'_1 \otimes(v, w) p'_2, v \odot w)$ if $v \neq w$.

We remark that if we take $\sigma(v) = \sigma(w)$ for all v, w in V we have the generalized singular direct product defined in [1], whereas if we take $\otimes(v,w) = \otimes(v',w')$ for all (v,w), (v',w') we have the generalized singular direct product defined in [2]. If we take both of these restrictions we have A. Sade's singular direct product [3]. Finally if we take $P = \emptyset$ and $\sigma(v) = \sigma(w) = \otimes(v,w)$ for all v, w in V we have the ordinary direct product.

If in the generalized singular direct product $V_{\odot} \times Q(\sigma(v), P, P' \otimes (v,w))$ all of the operations $\sigma(v) = \sigma$ we will replace $\sigma(v)$ by σ. Similarly if all $\otimes(v,w) = \otimes$ we will replace $\otimes(v,w)$ by $\otimes$.

3. Proof of the theorem. Let $(V, \odot_1)$, $(V, \odot_2)$, ..., $(V, \odot_{s-1})$ be $s-1$ mutually orthogonal idempotent quasigroups, and (Q, σ_1), (Q, σ_2), ..., (Q, σ_t) t mutually orthogonal quasigroups containing t subquasigroups (p, σ_1), (P, σ_2), ..., (P, σ_t) so that $\sigma_1 = \sigma_2 =, ..., = \sigma_t$ on P. Let $P' = Q \setminus P$ and $(P', \otimes_1)$, $(P', \otimes_2)$, ..., $(P', \otimes_k)$ be k mutually orthogonal quasigroups. Let $M = V_{\odot_1} \times Q(\sigma_1, P, P' \otimes_1)$ be the singular direct product formed from $(V, \odot_1)$, (Q, σ_1) and $(P', \otimes_1)$. M of course has order $v(q-p) + p$. Now let $\mathcal{M}$ denote the set of all generalized singular direct products of the form $V_{\odot_i} \times Q(\sigma(v), P, P' \otimes (v,w))$ where $\odot_i \in \{\odot_2, \odot_3, ..., \odot_{s-1}\}$, $\sigma(v) \in \{\sigma_2, \sigma_3, ..., \sigma_t\}$

and $\otimes(v, w) \in \{\otimes_2, \otimes_3, \dots, \otimes_k\}$. Clearly $\mathcal{M}$ contains $(s-2)(t-1)^v(k-1)^{v^2-v}$ distinct quasigroups. The proof will be complete if we can show that (i) each member of $\mathcal{M}$ is orthogonal to M, and (ii) no member of $\mathcal{M}$ can be obtained from any other member of $\mathcal{M}$ by a permutation.

(i) Let $A \in \mathcal{M}$. Without loss in generality we can take $A = V_{\otimes_2} \times (\sigma(v), P, P' \otimes (v, w))$. Now if $\sigma(v)$ is the same operation for all v in V and $\otimes(v, w)$ is the same operation for all $v \neq w$ in V we have the ordinary singular direct product which A. Sade has shown is orthogonal to M, [3]. Suppose we take $A' = V_{\otimes_2} \times Q(\sigma_2, P, P' \otimes_2)$. Now for each v in V the copy of (Q, σ_1) in M and the copy of (Q, σ_2) in A' are both based on $P \cup (P' \times \{v\})$. Since (Q, σ_1) and (Q, σ_2) are orthogonal so are their copies in M and A'. Hence, if we superimpose the latin squares associated with their copies in M and A' we obtain $\{P \cup (P' \times \{v\})\} \times \{P \cup (P' \times \{v\})\}$. Now if for any v in V we replace (Q, σ_2) by $(Q, \sigma(v))$, $\sigma(v) \in \{\sigma_2, \sigma_3, \dots, \sigma_t\}$, in the construction of A' the copy of $(Q, \sigma(v))$ is still based on $P \cup (P' \times \{v\})$. Since (Q, σ_1) and $(Q, \sigma(v))$ are orthogonal, superimposing the latin squares associated with their copies still gives $\{P \cup (P' \times \{v\})\} \times \{P \cup (P' \times \{v\})\}$. Since all copies of the $(Q, \sigma(v))$ agree on P we can replace σ_2 by $\sigma(v)$ in the construction of A' with the result that the singular direct product

$A'' = V_{\odot_2} \times Q(\sigma(v), P, P' \otimes_2)$ is still orthogonal to $\mathcal{M}$.

Now let $v \neq w \in V$. The latin squares associated with $(P', \otimes_1)$ in $\mathcal{M}$ is based on $P' \times \{v \odot_1 w\}$ and the latin square associated with $(P', \otimes_2)$ in A'' is based on $P' \times \{v \odot_2 w\}$. Since $(P', \otimes_1)$ and $(P', \otimes_2)$ are orthogonal if we superimpose their associated latin squares in $\mathcal{M}$ and A'' we obtain $\{P' \times \{v \odot_1 w\} \times \{P' \times \{v \odot_2 w\}\}$. As above if in the construction of A'' we replace $(P', \otimes_2)$ by $(P', \otimes(v, w))$, $\otimes(v,w) \in \{\otimes_2, \otimes_3, \ldots, \otimes_k\}$,

the latin square associated with $(P', \otimes(v, w))$ is still based on $P' \times \{v \odot_2 w\}$. Since $(P', \otimes(v, w))$ is orthogonal to $(P', \otimes_1)$ if we superimpose their associated latin squares in $\mathcal{M}$ and A'' we still obtain $\{P' \times \{v \odot_1 w\}\} \times \{P' \times \{v \odot_2 w\}\}$. It follows that we can replace $\otimes_2$ by $\otimes(v, w)$ in the construction of A'' and the resulting quasigroups $A = V_{\odot_2} \times Q(\sigma(v), P, P' \otimes(v, w))$ are still orthogonal to $\mathcal{M}$.

(ii) Now let $M_i = V_{\odot_i} \times Q(\sigma(v), P, P' \otimes(v, w))$ and $M_j = V_{\odot_j} \times Q(\sigma(v), P, P' \otimes(v, w))$ belong to $\mathcal{M}$. One of two things is true: either $\sigma(v)$ is the same in the construction of both M_i and M_j for each v in V or the centrary. If $\sigma(v)$ is the same for all $v \in V$, since each of $(V, \odot_i)$ and $(V, \odot_j)$ is idempotent the latin squares associated with the $(Q, \sigma(v))$, $v \in V$, in M_i and M_j are identical and in the same relative position. Hence, any permutation, other than the identity, applied to one of M_i, M_j cannot give the other. On the other hand if $\sigma(v)$ is different for some $v \in V$, then the subquasigroup of M_i based on $P \cup (P' \times \{v\})$ is orthogonal to the subquasigroup of M_j based on $P \cup (P' \times \{v\})$. Again it follows that no permutation will transform one of M_i, M_j into the other.

This completes the proof of the theorem.

4. <u>Examples</u>. (i) Since $17 = 4(5-1) + 1$ and there are 3 mutually orthogonal quasigroups of order 4 and 4 mutually orthogonal quasigroups of order 5 containing 4 mutually orthogonal quasigroups of order 1, there is a quasigroups of order 17 having at least 331, 776 orthogonal mates, any two differing by more than a permutation. (ii) Since $22 = 7(4-1) + 1$, similar remarks produce a quasigroup of order 22 having at least 512 orthogonal mates, no one of which can be obtained from the other by a permutation.

References

[1] C.C. LINDNER: The generalized singular direct product for quasigroups, Can.Math.Bull. 14(1971),61-63.

[2] C.C. LINDNER: Construction of quasigroups using the singular direct product, Proc.Amer.Math. Soc.(to appear).

[3] A. SADE: Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens, Ann.Ac.Sci. Bruxelles, Sér.I.,74(1960),91-99.

Auburn University
Auburn, Alabama
U.S.A.

(Oblatum 30.3.1971)