Available online at www.sciencedirect.com

ScienceDirect

European Journal of Combinatorics 29 (2008) 507–513

European Journal of Combinatorics

www.elsevier.com/locate/ejc

On irreducible n-ary quasigroups with reducible retracts

Denis Krotov

Sobolev Institute of Mathematics, pr-t Ak. Koptyuga, 4, Novosibirsk, 630090, Russia

Received 26 October 2006; accepted 22 January 2007
Available online 1 March 2007

Abstract

An n-ary operation $Q : \Sigma^n \to \Sigma$ is called an n-ary quasigroup of order $|\Sigma|$ if in $x_0 = Q(x_1, \dots, x_n)$ knowledge of any n elements of $x_0, \dots, x_n$ uniquely specifies the remaining one. An n-ary quasigroup Q is permutably reducible if $Q(x_1, \dots, x_n) = P\left(R(x_{\sigma(1)}, \dots, x_{\sigma(k)}), x_{\sigma(k+1)}, \dots, x_{\sigma(n)}\right)$ where P and R are $(n-k+1)$-ary and k-ary quasigroups, σ is a permutation, and $1 < k < n$. For even n we construct a permutably irreducible n-ary quasigroup of order $4r$ such that all its retracts obtained by fixing one variable are permutably reducible. We use a partial Boolean function that satisfies similar properties. For odd n the existence of permutably irreducible n-ary quasigroups with permutably reducible $(n-1)$-ary retracts is an open question; however, there are nonexistence results for 5-ary and 7-ary quasigroups of order 4.
© 2007 Elsevier Ltd. All rights reserved.

1. Introduction

An n-ary operation $Q : \Sigma^n \to \Sigma$, where Σ is a nonempty set, is called an *n-ary quasigroup* or *n-quasigroup* (*of order* $|\Sigma|$) if in the equality $z_0 = Q(z_1, \dots, z_n)$ knowledge of any n elements of $z_0, z_1, \dots, z_n$ uniquely specifies the remaining one [1]. The definition is symmetric with respect to the variables $z_0, z_1, \dots, z_n$, and sometimes it is convenient to use a symmetric form for the equation $z_0 = Q(z_1, \dots, z_n)$. For this reason, we will write

$$Q\langle z_0, z_1, \dots, z_n\rangle \overset{\text{def}}{\iff} z_0 = Q(z_1, \dots, z_n). \tag{1}$$

If we assign some fixed values to $l \le n$ variables in the predicate $Q\langle z_0, \dots, z_n\rangle$ then the $(n-l+1)$-ary predicate obtained corresponds to an $(n-l)$-quasigroup. Such a quasigroup is called a *retract* of Q. We say that an n-quasigroup Q is *A-reducible* if

$$Q\langle z_0, \dots, z_n\rangle \iff Q'(z_{a_1}, \dots, z_{a_k}) = Q''(z_{b_1}, \dots, z_{b_{n-k+1}}) \tag{2}$$

E-mail address: krotov@math.nsc.ru.

0195-6698/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2007.01.005

where $A = \{a_1, \dots, a_k\} = \{0, \dots, n\} \setminus \{b_1, \dots, b_{n-k+1}\}$ and Q' and Q'' are k- and $(n-k+1)$-quasigroups. An n-quasigroup is *permutably reducible* if it is A-reducible for some $A \subset \{0, \dots, n\}$, $1 < |A| < n$. In what follows we omit the word "permutably" because we consider only that type of reducibility (often, "reducibility" of n-quasigroups denotes the so-called (i, j)-reducibility; see Remark 1). In other words, an n-quasigroup is reducible if it can be represented as a repetition-free superposition of quasigroups with smaller arities. An n-quasigroup is *irreducible* if it is not reducible.

In [2,3], it was shown that if the maximum arity m of an irreducible retract of an n-quasigroup Q belongs to $\{3, \dots, n-3\}$ then Q is reducible. Nevertheless, this interval does not contain 2 and $n-2$, and thus cannot guarantee the nonexistence of an irreducible n-quasigroup all of whose $(n-1)$-ary retracts are reducible. In this paper we show that, in the case of order $4r$, such an n-quasigroup exists for even $n \geq 4$. In the case of odd n, as well as in the case of orders that are not divisible by 4, the question remains open; however, as the result of an exhaustive computer search, we can state the following:

- There is no irreducible 5- or 7-quasigroup of order 4 such that all its $(n-1)$-ary retracts are reducible.

For given order, constructing irreducible n-quasigroups with reducible $(n-1)$-ary retracts is a more difficult task than simply constructing irreducible n-quasigroups. In the last case we can break the reducibility of an n-quasigroup by changing it locally [4]. For our aims local modifications do not work properly because they also break the reducibility of retracts.

In Section 2 we use a variant of the product of n-quasigroups of order 2 to construct n-quasigroups of order 4 from partial Boolean functions defined on the even (or odd) vertices of the Boolean $(n+1)$-cube. The class constructed plays an important role for the n-quasigroups of order 4; up to equivalence, it gives almost all n-quasigroups of order 4; see [5]. It turns out that the reducibility of such an n-quasigroup is equivalent to a similar property, separability, of the corresponding partial Boolean function. So, for this class the main question is reduced to the same question for partial Boolean functions. In Section 3 we construct a partial Boolean function with the required properties. In Section 4 we consider the graph interpretation of the result.

2. n-Quasigroups of order 4 and partial Boolean functions

In this section we consider n-quasigroups over the set $\Sigma = Z_2^2 = \{[0,0], [0,1], [1,0], [1,1]\}$ and partial Boolean functions defined on the following subsets of the Boolean hypercube $E^{n+1} \stackrel{\mathrm{def}}{=} \{0,1\}^{n+1}$:

$$E_\alpha^{n+1} \stackrel{\mathrm{def}}{=} \{(x_0, \dots, x_n) \in E^{n+1} \mid x_0 + \cdots + x_n = \alpha\}, \quad \alpha \in \{0, 1\}.$$

All calculations with elements of $\{0, 1\}$ are made modulo 2, while all calculations with indices are modulo $n+1$; for example, x_{-1} means the same as x_n. Note that, since any coordinate (say, the 0th) in E_0^{n+1} is the sum of the others, partial Boolean functions defined on E_0^{n+1} (as well as on E_1^{n+1}) can be considered as Boolean functions on E^n; however, the form that is symmetrical with respect to all $n+1$ coordinates helps to improve the presentation, as in the case of n-quasigroups.

We will use the following notation: if $j \geq i$ then

- $\overline{i, j}$ means $i, i+1, \dots, j$;
- x_i^j means $x_i, x_{i+1}, \dots, x_j$;

- $|x_i^j|$ means the sum $x_i + x_{i+1} + \cdots + x_j$;
- $[x, y]_i^j$ means $[x_i, y_i], [x_{i+1}, y_{i+1}], \ldots, [x_j, y_j]$;
- 0^k means k zeros.

Given $\alpha \in \{0, 1\}$ and $\lambda : E_\alpha^{n+1} \to \{0, 1\}$, define the n-quasigroup $Q_{\alpha,\lambda}$ as

$$Q_{\alpha,\lambda}\langle [x, y]_0^n \rangle \overset{\text{def}}{\iff} \begin{cases} |x_0^n| = \alpha, \\ |y_0^n| = \lambda(x_0^n) \end{cases} \tag{3}$$

or, equivalently,

$$Q_{\alpha,\lambda}([x, y]_1^n) \overset{\text{def}}{=} \left[|x_1^n| + \alpha, |y_1^n| + \dot{\lambda}(x_1^n) \right] \tag{4}$$

where $\dot{\lambda}(x_1^n) \overset{\text{def}}{=} \lambda(|x_1^n| + \alpha, x_1^n)$ is a representation of λ as a Boolean function $E^n \to \{0, 1\}$. Note that we will use α only in the proof of Theorem 1((b), (c)), and it is not needed for formulating the main result. In Lemma 1 below, we will see that the reducibility property of $Q_{\alpha,\lambda}$ corresponds to a similar property of the function λ.

We say that a partial Boolean function $\lambda : E_\alpha^{n+1} \to \{0, 1\}$ is *A-separable* if

$$\lambda(x_0^n) \equiv \lambda'(x_{a_1}, \ldots, x_{a_k}) + \lambda''(x_{b_1}, \ldots, x_{b_m}) \tag{5}$$

where $A = \{a_1^k\} = \{\overline{0, n}\} \setminus \{b_1^m\}$ and $\lambda' : E^k \to \{0, 1\}$, $\lambda'' : E^m \to \{0, 1\}$ are Boolean functions. (Here and elsewhere $\equiv$ means that the two expressions are identical on the region of the left one.) λ is *separable* if it is A-separable for some $A \subset \{\overline{0, n}\}$, $2 \le |A| \le n - 1$.

Lemma 1. *Let $A \subset \{\overline{0, n}\}$. The n-quasigroup $Q_{\alpha,\lambda}$ is A-reducible if and only if the partial Boolean function $\lambda : E_\alpha^{n+1} \to \{0, 1\}$ is A-separable.*

In the proof, we will use the following simple fact [2,3]:

Lemma 2. *Assume two n-quasigroups Q_1 and Q_2 are $\{\overline{0, k-1}\}$-reducible. If $Q_1\langle z_0^{k-1}, z_k, 0^{n-k}\rangle \iff Q_2\langle z_0^{k-1}, z_k, 0^{n-k}\rangle$ and $Q_1\langle z_0, 0^{k-1}, z_k^n\rangle \iff Q_2\langle z_0, 0^{k-1}, z_k^n\rangle$ then Q_1 and Q_2 are identical.*

Proof of Lemma 1. Clearly, (5) implies (2) with $Q = Q_{\alpha,\lambda}$ (see (3)), and $Q' = Q_{\alpha,\mu}$, $Q'' = Q_{0,\nu}$ where $\dot{\mu} = \lambda'$, $\dot{\nu} = \lambda''$ (see (4)).

Let us prove the converse. Suppose $Q_{\alpha,\lambda}$ is A-reducible. Without loss of generality assume $\alpha = 0$ and $A = \{\overline{0, k-1}\}$. Using Lemma 2, we can verify that $Q_{0,\lambda}\langle [x, y]_0^n\rangle$ defined by (3) is equivalent to

$$\begin{cases} |x_0^n| = 0, \\ |y_0^n| = \lambda(x_0^{k-1}, |x_0^{k-1}|, 0^{n-k}) + \lambda(|x_0^{k-1}|, 0^{k-1}, |x_0^{k-1}|, 0^{n-k}) + \lambda(|x_k^n|, 0^{k-1}, x_k^n). \end{cases}$$

Comparing with (3), we find that $\lambda(x_0^n) \equiv \lambda'(x_0^{k-1}) + \lambda''(x_k^n)$ where

$$\lambda'(x_0^{k-1}) \overset{\text{def}}{=} \lambda(x_0^{k-1}, |x_0^{k-1}|, 0^{n-k}) + \lambda(|x_0^{k-1}|, 0^{k-1}, |x_0^{k-1}|, 0^{n-k}),$$

$$\lambda''(x_k^n) \overset{\text{def}}{=} \lambda(|x_k^n|, 0^{k-1}, x_k^n).$$

Therefore λ is $\{\overline{0, k-1}\}$-separable. $\square$

The following main theorem results from Lemma 1 and Theorem 2 from the next section. Although the proof depends on Theorem 2, it is straightforward, and placing it first hardly leads to a mishmash.

Theorem 1. *Let $n \geq 4$ be even and $f(x_0^n) \overset{\text{def}}{=} \sum_{i=0}^{n} \sum_{i=1}^{\lfloor n/4 \rfloor} x_i x_{i+j}$ for all $x_0^n \in E_0^{n+1}$. Then:*

(a) *The n-quasigroup $Q_{0,f}$ is irreducible.*
(b) *Every $(n-1)$-ary retract $Q^i_{[\alpha,\gamma]}$ obtained from $Q_{0,f}$ by fixing the ith variable $[x_i, y_i] := [\alpha, \gamma]$ is reducible.*
(c) *$Q_{0,f}$ has an irreducible $(n-2)$-ary retract.*

Proof. The theorem is a corollary of the properties of the function f discussed in the next section.

(a) By Lemma 1, the claim follows directly from Theorem 2(a).
(b) It is straightforward that $Q^i_{[\alpha,\gamma]} = Q_{\alpha, f^i_\alpha + \gamma}$ where f^i_α is obtained from f by fixing the ith variable $x_i := \alpha$. So, by Lemma 1, the reducibility of $Q^i_{[\alpha,\gamma]}$ is a corollary of the separability of f^i_α (Theorem 2(b)).

Similarly, (c) follows from the fact that fixing two variables we can get a non-separable subfunction of f (Theorem 2(c)). □

Remark 1. An n-quasigroup is called (i, j)-*reducible* if it is $\{i, \dots, i + j - 1\}$-reducible for some $i \in \{1, \dots, n\}$ and $j \in \{2, \dots, n - 1\}$ meeting $i + j - 1 \leq n$. Clearly, the property of (i, j)-reducibility is stronger than the permutable reducibility and is not invariant under changing the argument order; this property was considered e.g. in [1]. Using an appropriate argument permutation (more precisely, replacing f by $f'(x_0, x_1, \dots, x_n) \overset{\text{def}}{=} f(x_0, x_2, \dots, x_{2n \bmod (n+1)})$), we can strengthen the statement of Theorem 1(b) getting the (i, j)-reducible $(n-1)$-ary retracts.

Remark 2. Using $Q_{0,f}$ (or $Q_{0,f'}$, see Remark 1), it is not difficult to construct an irreducible n-quasigroup of order $4r$ with reducible ((i, j)-reducible) $(n-1)$-ary retracts for any $r > 0$: if $(G, *)$ is a commutative group of order $|G| = r \leq \infty$ then the n-quasigroup $Q_f^{(G,*)}$ (and, similarly, its retracts) defined as

$$Q_f^{(G,*)}([w, z]_1^n) \overset{\text{def}}{=} [w_1 * \cdots * w_n, Q_{0,f}(z_1^n)], \quad w_i \in G,\ z_i \in Z_2^2 \tag{6}$$

inherits all the reducibility properties of $Q_{0,f}$ (and its retracts). Indeed, if $Q_{0,f}$ is A-reducible then, obviously, $Q_f^{(G,*)}$ is A-reducible too. Conversely, let $Q_f^{(G,*)}$ be A-reducible. Since the group $(G, *)$ is commutative, we can assume without loss of generality that $A = \{\overline{0, k-1}\}$. Using Lemma 2, we can check that

$$Q_f^{(G,*)}([w, z]_1^n) \equiv [w_1 * \cdots * w_n, Q_{0,f}(z_1^{k-1}, q^{-1}(Q_{0,f}(0^{k-1}, z_k^n)), 0^{n-k})]$$

with $q(z) \overset{\text{def}}{=} Q_{0,f}(0^{k-1}, z, 0^{n-k})$. Comparing with (6) gives a reduction of $Q_{0,f}$.

3. Properties of the partial Boolean function f

In this section we prove the key theorem of the paper:

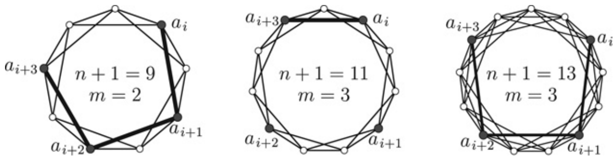

Fig. 1. It is natural to represent a square-free (i.e., without monomials of type x_i^2) quadratic form over Z_2 by the graph whose ith and jth vertices are connected if and only if the form contains the monomial $x_i x_j$. The figure presents the graph corresponding to the form (7) with $n = 8$, $n = 10$, and $n = 12$.

Theorem 2. *Let $n \geq 4$ be even and the partial Boolean function $f : E_0^{n+1} \to \{0, 1\}$ be represented by the following polynomial:*

$$f(x_0^n) \stackrel{\text{def}}{=} \sum_{i=0}^{n} \sum_{j=1}^{\lfloor n/4 \rfloor} x_i x_{i+j} \tag{7}$$

(see Fig. 1). Put $m \stackrel{\text{def}}{=} \lfloor (n+2)/4 \rfloor$. Then:

(a) *The partial Boolean function f is not separable.*
(b) *For all $i \in \{\overline{0, n}\}$ and $\alpha \in \{0, 1\}$ the subfunction $f_\alpha^i : E_\alpha^n \to \{0, 1\}$ obtained from $f(x_0^n)$ by fixing $x_i := \alpha$ is $\{i + m, i - m\}$-separable (here and in what follows, for subfunctions we leave the same numeration of variables as for the original function).*
(c) *For all $i \in \{\overline{0, n}\}$ and $\alpha, \beta \in \{0, 1\}$ the subfunction $g_{\alpha,\beta}^i : E_{\alpha+\beta}^{n-1} \to \{0, 1\}$ obtained from $f(x_0^n)$ by fixing $x_i := \alpha$, $x_{i+m} := \beta$ is not separable.*

Proof. (a) Let A be an arbitrary subset of $\{\overline{0, n}\}$ such that $2 \leq |A| \leq n-1$, and let $B \stackrel{\text{def}}{=} \{\overline{0, n}\} \setminus A$. We will show that f is not A-separable, using the following two simple facts:

Lemma 3. *Assume a partial Boolean function $f : E_0^{n+1} \to \{0, 1\}$ is A-separable. Then each (partial) subfunction f' obtained from $f(x_0^n)$ by fixing some variables $x_{v_1}, \ldots, x_{v_k}$ is A'-separable with $A' \stackrel{\text{def}}{=} A \setminus \{v_1^k\}$.*

Lemma 4. *Let $\gamma_{01}, \gamma_{02}, \gamma_{03}, \gamma_{12}, \gamma_{13}, \gamma_{23} \in \{0, 1\}$. A partial Boolean function*

$$h(x_0, x_1, x_2, x_3) \stackrel{\text{def}}{=} \gamma_{01}x_0x_1 + \gamma_{02}x_0x_2 + \gamma_{03}x_0x_3 + \gamma_{12}x_1x_2 + \gamma_{13}x_1x_3 + \gamma_{23}x_2x_3 :$$

$E_0^4 \to \{0, 1\}$ *is $\{0, 1\}$-separable only if $\gamma_{02} + \gamma_{03} + \gamma_{12} + \gamma_{13} = 0$.*

(Lemma 3 is straightforward from the definition. Proof of Lemma 4: From the $\{0, 1\}$-separability of h we derive $h(0, 0, 0, 0) + h(1, 1, 1, 1) = h(1, 1, 0, 0) + h(0, 0, 1, 1)$. Substituting the definition of h, we get $\gamma_{02} + \gamma_{03} + \gamma_{12} + \gamma_{13} = 0$.)

Consider the cyclic sequence $a_i = i \cdot m \bmod (n + 1)$, $i = 0, \ldots, n$. Since $n + 1 = 4m \pm 1$, we see that m and $n + 1$ are relatively prime, and $\{a_0^n\} = \{\overline{0, n}\}$. At least one of the following holds (recall that indices are calculated modulo $n + 1$):

(1) $a_i, a_{i+1} \in A$, $a_{i+2}, a_{i+3} \in B$ or $a_i, a_{i+1} \in B$, $a_{i+2}, a_{i+3} \in A$ for some i. Assigning zeros to all variables of $f(x_0^n)$ except $x_{a_i}, x_{a_{i+1}}, x_{a_{i+2}}, x_{a_{i+3}}$ we get the partial Boolean function

$$f'(x_{a_i}, x_{a_{i+1}}, x_{a_{i+2}}, x_{a_{i+3}}) \equiv \begin{cases} x_{a_i}x_{a_{i+1}} + x_{a_{i+1}}x_{a_{i+2}} + x_{a_{i+2}}x_{a_{i+3}}, & \text{if } n \equiv 0 \bmod 4, \\ x_{a_i}x_{a_{i+3}}, & \text{if } n \equiv 2 \bmod 4 \end{cases}$$

(see Fig. 1, the dark nodes), which is not $\{a_i, a_{i+1}\}$-separable, by Lemma 4. Therefore f is not A-separable, by Lemma 3.
(2) $a_i, a_{i+2} \in A$, $a_{i+1} \in B$ or $a_i, a_{i+2} \in B$, $a_{i+1} \in A$ for some i. Without loss of generality assume $0 \in A$, $m \in B$, $2m \in A$. Note that the polynomial (7) contains exactly one of the monomials $x_0 x_b$, $x_{2m} x_b$ for each $b \neq 0, m, 2m$. Take $b \in B \setminus \{m\}$. Assigning zeros to all variables of $f(x_0^n)$ except x_0, x_m, x_{2m}, x_b we get the partial Boolean function

$$f''(x_0, x_{2m}, x_m, x_b) \equiv \begin{cases} x_0 x_m + x_m x_{2m} + \alpha x_0 x_b + \beta x_m x_b + \bar{\alpha} x_{2m} x_b, & \text{if } n \equiv 0 \bmod 4, \\ \alpha x_0 x_b + \beta x_m x_b + \bar{\alpha} x_{2m} x_b, & \text{if } n \equiv 2 \bmod 4 \end{cases}$$

with $\alpha, \beta \in \{0, 1\}$, $\bar{\alpha} \stackrel{\text{def}}{=} 1 - \alpha$. In any case, $f''(x_0, x_m, x_{2m}, x_b)$ is not $\{0, 2m\}$-separable, by Lemma 4. It follows that f is not A-separable, by Lemma 3.
(b) Without loss of generality we assume $i = 0$. Put

$$\tilde{x}_k \stackrel{\text{def}}{=} |x_{k-\lfloor n/4 \rfloor}^{k-1}| + |x_{k+1}^{k+\lfloor n/4 \rfloor}| = |x_{k-\lfloor n/4 \rfloor}^{k+\lfloor n/4 \rfloor}| + x_k.$$

Note that $m + \lfloor n/4 \rfloor = n/2$, and $m - \lfloor n/4 \rfloor$ is 0 or 1; in both cases,

$$|x_0^n| \equiv (\tilde{x}_m + x_m + \tilde{x}_{-m} + x_{-m} + x_0).$$

Since $|x_0^n|$ equals zero everywhere on E_0^{n+1}, we can represent f as follows:

$$\begin{aligned} f(x_0^n) &\equiv \sum_{i=0}^{n} \sum_{j=1}^{\lfloor n/4 \rfloor} x_i x_{i+j} + (\tilde{x}_m + x_m + \tilde{x}_{-m} + x_{-m} + x_0)(\tilde{x}_m + x_{-m}) \\ &\equiv \sum_{i=0}^{n} \sum_{j=1}^{\lfloor n/4 \rfloor} x_i x_{i+j} + x_m \tilde{x}_m + x_{-m} \tilde{x}_{-m} + (x_m + x_{-m} + x_0) x_{-m} + S \end{aligned}$$

where S does not depend on x_m and x_{-m}. It is easy to see that this representation does not contain any monomial $x_k x_{k'}$ with $k \in \{-m, m\}$, $k' \notin \{0, -m, m\}$. This means that after fixing x_0 we obtain a $\{-m, m\}$-separable partial Boolean function.
(c) Without loss of generality assume $i = 0$. Let A be an arbitrary subset of $\{\overline{1, m-1}, \overline{m+1, n}\}$ such that $2 \leq |A| \leq n - 2$; let $B \stackrel{\text{def}}{=} \{\overline{1, m-1}, \overline{m+1, n}\} \setminus A$. If the sequence a_i, $i = \overline{0, n}$ is defined as in (a) then either (1) or (2) holds or
(3) $A = \{a_2, a_n\} = \{2m, -m\}$ or $B = \{2m, -m\}$ (recall that the numbers $a_0 = 0$ and $a_1 = m$ correspond to the fixed variables). As in the cases (1) and (2), assigning zeros to all variables of $g_{\alpha,\beta}^0(x_1^{m-1}, x_{m+1}^n) = f(\alpha, x_1^{m-1}, \beta, x_{m+1}^n)$ except x_{2m}, x_{-m}, x_1, x_n, we find that $g_{\alpha,\beta}^0$ is not A-separable by Lemmas 3 and 4. $\square$

In the proof of the part (b) we exploit the fact that after removing a vertex, say 0, in the corresponding graph (see Fig. 1) the remaining vertex set will be the disjoint union of the two vertices m and $-m$ and their neighborhoods. This partly explains why our construction does not work in the case of even $n+1$. In the following remark we compare our results with the situation with (total) Boolean functions.

Remark 3. Say that a Boolean function $\mu(x_1, \ldots, x_n) : E^n \to \{0, 1\}$ is *separable* if it is A-separable for some $A \subset \{\overline{1, n}\}$ where $1 \leq |A| \leq n - 1$ and A-separability means the same as for partial Boolean functions. Then (*) every non-separable n-ary Boolean function μ has a non-separable $(n-1)$-ary subfunction obtained from μ by fixing some variable. (Assume the contrary; consider a maximal non-separable k-ary subfunction μ'; and prove that $\mu = \mu' + \mu''$

for some $(n-k)$-ary μ'' where the free variables in μ' and μ'' do not intersect). Our investigation shows that the situation with the partial Boolean functions on E_0^{n+1} is more complex; a statement like (*) fails for even n and holds for $n = 5$ and $n = 7$. Question: does it hold for every odd n?

4. Remark. Switching separability of graphs

As noted in the comments on Fig. 1, each square-free quadratic form $p(x_0^n)$ over Z_2 can be represented by the graph with $n+1$ vertices $\{0,\ldots,n\}$ such that vertices i and j are adjacent if and only if $p(x_0^n)$ contains the monomial $x_i x_j$. In this section we define the concept of graph switching separability that corresponds to the separability of the corresponding quadratic polynomial considered as a partial Boolean function $E_0^{n+1} \to \{0,1\}$.

We first define a graph transformation, which is known as a *graph switching* or *Seidel switching*. The result of *switching* a set $U \subseteq V$ in a graph $G = (V, E)$ is defined as the graph with the same vertex set V and the edge set $E \triangle E_{U,V\setminus U}$ where $E_{U,V\setminus U} \stackrel{\text{def}}{=} \{\{u,v\} \mid u \in U, v \in V\setminus U\}$. We say that the graph $G = (V, E)$ is *switching-separable* if $V = V_1 \cup V_2$ where $|V_1| \geq 2$, $|V_2| \geq 2$, $V_1 \cap V_2 = \emptyset$, and for some $U \subseteq V$ switching U in G gives a graph with no edges between V_1 and V_2. Clearly, if a graph is switching-separable then all its switchings are switching-separable. The class of all switchings of a graph is known as a *switchings class* and is equivalent to a *two-graph*; see e.g. [6]. From Theorem 2 and the computer search reported in the introduction, we can derive the following:

Corollary 1. *For every odd $|V| \geq 5$ there exists a non-switching-separable graph $G = (V, E)$ such that every subgraph generated by $|V| - 1$ vertices is switching-separable. If $|V| = 6$ or $|V| = 8$ then such graphs do not exist.*

References

[1] V.D. Belousov, n-Ary Quasigroups, Shtiintsa, Kishinev, 1972 (in Russian).
[2] D.S. Krotov, On decomposability of distance 2 MDS codes, in: Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT'2004, Kranevo, Bulgaria, 2004, pp. 247–253.
[3] D.S. Krotov, On reducibility of n-quasigroups, Discrete Math. (2006) (submitted for publication). eprint math.CO/0607284, arXiv.org, Available at: http://arxiv.org/abs/math/0607284.
[4] D.S. Krotov, V.N. Potapov, On reconstructing reducible n-ary quasigroups and switching subquasigroups (2006) (in preparation). eprint math.CO/0608269, arXiv.org, Available at: http://arxiv.org/abs/math/0608269.
[5] V.N. Potapov, D.S. Krotov, Asymptotics for the number of n-quasigroups of order 4, Siberian Math. J. 47 (4) (2006) 720–731, doi:10.1007/s11202-006-0083-9. Translated from Sibirsk. Mat. Zh. 47(4) (2006) 873–887.
[6] E. Spence, Two-graphs, in: C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 686–694.