ISSN 0032-9460, Problems of Information Transmission, 2010, Vol. 46, No. 3, pp. 219–224. © Pleiades Publishing, Inc., 2010.
Original Russian Text © D.S. Krotov, V.N. Potapov, 2010, published in Problemy Peredachi Informatsii, 2010, Vol. 46, No. 3, pp. 22–28.

CODING THEORY

On Switching Equivalence of n-ary Quasigroups of Order 4 and Perfect Binary Codes[1]

D. S. Krotov and V. N. Potapov

Sobolev Institute of Mathematics,
Siberian Branch, Russian Academy of Sciences, Novosibirsk
Novosibirsk State University
krotov@math.nsc.ru vpotapov@math.nsc.ru

Received November 6, 2009; in final form, May 14, 2010

Abstract—We prove that arbitrary n-ary quasigroups of order 4 can be transformed into each other by successive switchings of $\{a, b\}$-components. We prove that perfect (closely packed) binary codes with distance 3 whose rank (dimension of the linear span) is greater by 1 or 2 than the rank of a linear perfect code can be taken to each other by successive switchings of i-components.

DOI: 10.1134/S0032946010030026

1. INTRODUCTION

A powerful tool for investigation in the theory of single-error-correcting binary codes is the i-component switching method, which consists in successively replacing subsets of a code and preserving the code parameters at each step. Constructions of perfect codes with various nontrivial properties have been obtained by this method (see surveys [1, 2]; see also recent paper [3] and bibliography therein). Presently, very little is known about switching classes of perfect binary codes, i.e., equivalence classes in which codes can be obtained from one another by several successive switchings of i-components. In [4] a perfect code of length 15 was found that does not belong to the switching class of the Hamming code. In recent paper [5], using computer-aided complete classification of perfect binary codes of length 15, the number of switching classes of such codes was found; this number is 9. At the same time it was found that all perfect binary codes of length 15 with rank (dimension of the linear span) from 11 to 13 belong to one switching class, and up to now this has been only empirically justified. In the present paper we prove (Section 3) a similar statement for perfect binary codes of arbitrary length and of rank greater than the minimum by at most 2.

As is shown in [6], all such codes (perfect binary codes of rank at most +2) can be described using a concatenated construction [7] in terms of n-ary quasigroups of order 4. Using a characterization [8] of such quasigroups, we deduce in Section 4 that they all belong to one switching class under an appropriate definition of a switching for quasigroups. This fact is a key point in the proof of a similar statement for perfect codes of small rank.

2. BASIC DEFINITIONS

Denote by E^n the set of ordered binary n-tuples (vertices). The *Hamming distance* $d(\overline{x}, \overline{y})$ between vertices $\overline{x} = (x_1, x_2, \ldots, x_n)$ and $\overline{y} = (y_1, y_2, \ldots, y_n)$ is the number of positions in which

[1] Supported in part by the Federal Target Program "Research and Educational Personnel of Innovation Russia" for 2009–2013, government contract no. 02.740.11.0429, and Russian Foundation for Basic Research, project nos. 10-01-00424 and 10-01-00616.

$\overline{x}$ and $\overline{y}$ differ. The set of vertices that are at distance at most one from $\overline{x}$ is said to be a *ball* of radius 1 centered at $\overline{x}$ and is denoted by $\mathcal{B}(\overline{x})$.

A set $C \subset E^n$ is said to be a *perfect binary code with distance* 3 of length n (in what follows, we call it a *perfect code*) if $|\mathcal{B}(\overline{x}) \cap C| = 1$ for every vertex $\overline{x} \in E^n$. It is known that perfect binary codes of length n exist only if $n = 2^t - 1$, where t is a positive integer. The *rank* of a code is the dimension of its linear span. A linear (i.e., coinciding with its linear span) perfect code (with distance 3) is called a *Hamming code*; such a code is unique up to a permutation of coordinates. A perfect code is said to be of rank $+r$ if its rank is greater by r than the rank (dimension) of the Hamming code of the same length.

Let Σ be an arbitrary nonempty set of a finite cardinality k. A function $f\colon \Sigma^n \to \Sigma$ is called an *n-ary quasigroup of order k* if $f(\overline{x}) \neq f(\overline{y})$ for any two elements $\overline{x}, \overline{y} \in \Sigma^n$ that differ in exactly one position.[2]

In what follows, we assume that $\Sigma = \{0, 1, 2, 3\}$ and consider n-ary quasigroups of order 4 only. By $\oplus$ we denote a binary operation on Σ defined by the table

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

(the set Σ with the operation $\oplus$ is a group isomorphic to the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$). Note that the n-ary quasigroup $g(x_1, \ldots, x_n) \equiv x_1 \oplus \ldots \oplus x_n$ plays a key role in the characterization [8] of quasigroups of order 4.

For n-ary quasigroups and perfect codes, we define the notions of switching components and switching equivalence, which play the main role in our analysis.

By an *$\{a, b\}$-component* of an n-ary quasigroup f we call a nonempty subset $S \subset \Sigma^n$ such that $f(S) = \{a, b\}$ and for any $\overline{x}$ in S and any i in $\{1, \ldots, n\}$ there exists exactly one $\overline{y}$ in S that differs from $\overline{x}$ in the ith coordinate only. A trivial example of an $\{a, b\}$-component is the whole preimage $f^{-1}(\{a, b\})$, which is denoted by $S_{a,b}(f)$; sometimes, it can be split into smaller $\{a, b\}$-components.

We say that a function g is obtained from an n-ary quasigroup f by *switching* of an $\{a, b\}$-component S if

$$g(\overline{x}) = \begin{cases} f(\overline{x}) & \text{for } x \notin S, \\ a & \text{for } x \in S,\ f(\overline{x}) = b, \\ b & \text{for } x \in S,\ f(\overline{x}) = a. \end{cases}$$

The definition of an $\{a, b\}$-component immediately implies that g is an n-ary quasigroup. We say that n-ary quasigroups f and g are *switching equivalent* if one can be obtained from another by finitely many successive switchings of $\{a, b\}$-components, where pairs of elements $a, b \in \Sigma$ can be different for different switchings.

An *i-component* of a perfect code $C \subset E^n$ is a subset $K \subset C$ such that the set D obtained from C by inverting the ith coordinate in all binary tuples from K is a perfect code. In this case it is said that D is obtained from C by *switching* of the i-component K. We say that perfect codes A and B are *switching equivalent* if one can be obtained from another by finitely many successive switchings of i-components, where the numbers i, $i \in \{1, \ldots, n\}$, can be different for different switchings.

[2] This definition does not apply to infinite-order quasigroups.

3. SWITCHING EQUIVALENCE OF PERFECT CODES OF RANK AT MOST +2

The construction proposed in [7] relates n-ary quasigroups and perfect codes. Consider a particular case of this construction. Fix a linear perfect code (Hamming code) $R \subset E^n$. Assume that for each $\overline{r} \in R$ we have an n-ary quasigroup $f_{\overline{r}}\colon \Sigma^n \to \Sigma$. Denote

$$C_0^0 = \{0000, 1111\}, \quad C_1^0 = \{1001, 0110\}, \quad C_2^0 = \{0101, 1010\}, \quad C_3^0 = \{0011, 1100\},$$
$$C_0^1 = \{0001, 1110\}, \quad C_1^1 = \{1000, 0111\}, \quad C_2^1 = \{0100, 1011\}, \quad C_3^1 = \{0010, 1101\},$$
$$C_0 = \{000, 111\}, \quad C_1 = \{100, 011\}, \quad C_2 = \{010, 101\}, \quad C_3 = \{001, 110\}.$$

Define a subset $C \subset E^{4n+3}$ by

$$C = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in \Sigma^n} Q_{\overline{r},\overline{a},f_{\overline{r}}(\overline{a})}, \quad Q_{\overline{r},\overline{a},a_0} = C_{a_0} \times C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \ldots \times C_{a_n}^{r_n}. \tag{1}$$

The obtained code C is perfect. Indeed, as one can easily check, for any word $\overline{x}$ in E^{4n+3} there is a unique way to obtain a codeword by changing at most one symbol in $\overline{x}$. To each such $\overline{x}$ there correspond unique $\overline{r}'$, $\overline{a}'$, and b such that $\overline{x} \in Q_{\overline{r}',\overline{a}',b}$. If $\overline{r}' \notin R$, then there exists a unique word $\overline{r} \in R$ that differs from $\overline{r}'$ in a single position i. Then, by changing $\overline{x}$ in four coordinates corresponding to i, we obtain a codeword $\overline{c}$; moreover, as follows from the definition of an n-ary quasigroup, a particular coordinate among these four is uniquely determined by the condition $b = f_{\overline{r}}(\overline{a})$, $\overline{c} \in Q_{\overline{r},\overline{a},b}$. If $\overline{r}' \in R$, then from a similar condition we find which of the first three coordinates should be changed (or nothing should be changed; then $\overline{x} \in C$).

It is easily seen that codes defined by (1) are of rank at most +2. It was shown in [6] that the converse is also true.

Lemma 1. *Any perfect code of rank at most +2 can be represented, up to a permutation of coordinates, using construction* (1).

The following statement is directly implied by definitions.

Proposition 1. *Let a perfect code $C \subset E^{4n+3}$ satisfy equality* (1). *Assume that an n-ary quasigroup $f_{\overline{r}}$, $\overline{r} \in R$, has an $\{a, b\}$-component S. Then the set*

$$K = \bigcup_{\overline{a} \in S} Q_{\overline{r},\overline{a},f_{\overline{r}}(\overline{a})}$$

is an i-component of a perfect code C, where $i = a \oplus b \in \{1, 2, 3\}$. Moreover, switching of the $\{a, b\}$-component S in the quasigroup $f_{\overline{r}}$ is equivalent to switching of the i-component in the code C.

Proof. The sets C_a and C_b are defined in such a way that they are obtained from each other by inversion in the ith coordinate, where $i = a \oplus b$. Therefore, interchanging the values $a \leftrightarrow b$ in the quasigroup $f_{\overline{r}}$ results in the inversion of the ith coordinate in the corresponding set of words. $\triangle$

A key role in the proof of Theorem 1 below is played by Theorem 2, proved in Section 4, which states that *any two n-ary quasigroups of order 4 can be transformed into each other by successive switchings of $\{0, 1\}$-, $\{0, 2\}$-, and $\{2, 3\}$-components.*

Theorem 1. *Any perfect code C of rank at most +2 is switching equivalent to some linear perfect Hamming code. Morover, to obtain the Hamming code from C, it suffices to use switchings of i-components by at most two coordinates i.*

Proof. Lemma 1 in fact reduces the proof of the theorem to analysis of codes of the form (1). It follows from Theorem 2 that any code of the form (1) can be taken to any other code of the form (1) (including a linear code) by successive switchings of $\{0, 1\}$-, $\{0, 2\}$-, and $\{2, 3\}$-components in n-ary quasigroups $f_{\overline{r}}$, $\overline{r} \in R$. By Proposition 1, any such transformation is switching of an i-component of a resulting perfect code, $i \in \{0 \oplus 1, 0 \oplus 2, 2 \oplus 3\} = \{1, 2\}$. $\triangle$

Corollary. *All perfect codes of a fixed length and of rank at most $+2$ are switching equivalent.*

Proof. Taking into account Theorem 1, it remains to prove the following well-known folklore fact: *two Hamming codes, C and D, of the same length are switching equivalent.* It suffices to consider the case where D is obtained from C by a permutation (transposition) of two coordinates, say j and k, since an arbitrary permutation can be obtained by successively applying transpositions. Denote by $\overline{e}_{jk}$ the word of the considered code length with ones in positions j and k and zeros in the other positions. By $\overline{c}_{jk}$ we denote the codeword of C that is at distance at most 1 from $\overline{e}_{jk}$. Such a codeword exists by the definition of a perfect code, and since a linear code C contains the all-zero codeword, $\overline{c}_{jk}$ has precisely three nonzero coordinates: j, k, and some i. Let $C' = C \setminus D$. This set consists of exactly all codewords of C that contain one zero and one one in positions j and k; i.e., the action of the transposition in question on C is equivalent to the translation of the subset C' by the vector $\overline{e}_{jk}$. Obviously, $C' = C' + \overline{c}_{jk}$, whence we deduce

$$D = (C \setminus C') \cup (C' + \overline{e}_{jk}) = (C \setminus C') \cup (C' + (\overline{c}_{jk} + \overline{e}_{jk})).$$

Thus, D is obtained from C by switching of the i-component C', as required. $\triangle$

Note that in the proof of the switching equivalence of Hamming codes we essentially used linearity of the codes. For nonlinear perfect codes, the question of existence of two perfect codes that are equivalent in the sense of permutation of coordinates but not switching equivalent remains open. However, such codes become switching equivalent if we allow switchings with inversion of two coordinates simultaneously. Combinatorial properties of such switchings are not much different from switchings of i-components, since the latter also correspond to two-coordinate switchings in an extended perfect code obtained from the original one by adding the overall parity check.

4. SWITCHING EQUIVALENCE OF n-ARY QUASIGROUPS OF ORDER 4

We say that an n-ary quasigroup f is *semilinear* if there exist $a, b \in \Sigma$ such that the characteristic function of the set $S_{a,b}(f) = f^{-1}(\{a, b\})$ can be represented as a sum modulo 2 of one-variable functions:

$$\chi_{S_{a,b}(f)}(x_1, \ldots, x_n) \equiv \chi_{S_1}(x_1) + \ldots + \chi_{S_n}(x_n) \mod 2, \tag{2}$$

where S_i, $i \in \{1, \ldots, n\}$, are subsets of Σ (of cardinality 2, as follows from the definition of an n-ary quasigroup).

We say that an n-ary quasigroup g is *linear* if

$$g(x_1, \ldots, x_n) \equiv \pi_1(x_1) \oplus \ldots \oplus \pi_n(x_n) \tag{3}$$

for some permutations $\pi_1, \ldots, \pi_n$ of the set Σ.

Proposition 2 [9, Section 4]. *If g is a linear n-ary quasigroup, then for any distinct a and b from Σ the set $S_{a,b}(g)$ can be represented in the form* (2)*. Conversely, if g is an n-ary quasigroup and for some pairwise distinct a, b, and c from Σ the sets $S_{a,b}(g)$ and $S_{a,c}(g)$ can be represented in the form* (2)*, then g is a linear quasigroup.*

The following statement is directly implied by definitions.

Proposition 3. *Let ℓ be a linear n-ary quasigroup, and let q be a semilinear m-ary quasigroup, $2 \le m$. Then their composition $\ell(\overline{x}, q(\overline{y}))$ is a semilinear quasigroup.*

Proposition 4. *Let q be an m-ary quasigroup, and let h and ℓ be switching equivalent n-ary quasigroups. Then the quasigroups $h(\overline{x}, q(\overline{y}))$ and $\ell(\overline{x}, q(\overline{y}))$ are switching equivalent.*

Proof. Let ℓ be obtained from h by switching of an $\{a,b\}$-component S. It is easily seen that $S=\{\overline{x}\in\Sigma^n \mid h(\overline{x})\neq\ell(\overline{x})\}$. Then the set

$$S'=\{(\overline{x},\overline{y})\in\Sigma^{n+m-1} \mid h(\overline{x},q(\overline{y}))\neq\ell(\overline{x},q(\overline{y}))\}$$

is an $\{a,b\}$-component of the quasigroup $h(\overline{x},q(\overline{y}))$, and the quasigroup $\ell(\overline{x},q(\overline{y}))$ is obtained from $h(\overline{x},q(\overline{y}))$ by switching of S'. The definition of switching equivalence implies the desired result. $\triangle$

Proposition 5. *For any $n\in\mathbb{N}$, all linear n-ary quasigroups are switching equivalent.*

Proof. We show that if an n-ary quasigroup g can be represented in the form (3), then the quasigroup f obtained by replacing any permutation π_i with the identical permutation is switching equivalent to g. Since the operation $\oplus$ is commutative and associative, without loss of generality we may assume that $i=1$. We have $g(x_1,\overline{y})=\ell_{\pi_1}(x_1,q(\overline{y}))$ and $f(x_1,\overline{y})=\ell(x_1,q(\overline{y}))$, where $\ell(x,z)=x\oplus z$, $\ell_{\pi_1}(x,z)=\pi_1(x)\oplus z$, and $q(x_2,\dots,x_n)\equiv\pi_2(x_2)\oplus\ldots\oplus\pi_n(x_n)$. Since the binary quasigroups ℓ and ℓ_{π_1} are switching equivalent (which can be verified directly for any permutation π_1), Proposition 4 implies switching equivalence of g and f.

Thus, remaining within a switching equivalence class, we can start with any linear n-ary quasigroup of the form (3) and then replace one by one all the permutations π_i, $i=1,\dots,n$, by identical permutations. $\triangle$

Proposition 6. *For any $n\in\mathbb{N}$, every semilinear n-ary quasigroup is switching equivalent to some linear quasigroup.*

Proof. First consider two n-ary quasigroups, f and g, such that the sets $S_{a,b}(f)$ and $S_{a,b}(g)$ coincide. We show that f and g can be obtained from one another by switchings of $\{a,b\}$- and $\{c,d\}$-components, where $\{c,d\}=\Sigma\setminus\{a,b\}$.

Consider a function $h\colon\Sigma^n\to\Sigma$ coinciding with f on $S_{a,b}(f)$ and with g on $S_{c,d}(f)$. Clearly, h is a quasigroup. The set

$$D_{c,d}=\{\overline{x}\in\Sigma \mid f(\overline{x})\neq h(\overline{x})\}$$

must be a $\{c,d\}$-component, which implies switching equivalence of f and h. Similarly, g is obtained from h by switching of an $\{a,b\}$-component. Thus, switching equivalence of f and g is proved.

It remains to note that for any set $S_{a,b}(f)$ satisfying (2) we can choose permutations $\pi_1,\dots,\pi_n$ such that the linear quasigroup g defined by (3) satisfies the equality $S_{a,b}(g)=S_{a,b}(f)$. This means that every semilinear quasigroup is switching equivalent to some linear quasigroup. $\triangle$

An n-ary quasigroup f is said to be *separable* if there exists an integer m, $2\le m<n$, an $(n-m+1)$-ary quasigroup h, an m-ary quasigroup q, and a permutation $\sigma\colon\{1,\dots,n\}\to\{1,\dots,n\}$ such that

$$f(x_1,\dots,x_n)\equiv h(q(x_{\sigma(1)},\dots,x_{\sigma(m)}),x_{\sigma(m+1)},\dots,x_{\sigma(n)}).$$

Without loss of generality, we may always assume that q is not separable.

In [8], a description of n-ary quasigroups of order 4 in the above terms is obtained; namely, the following statement is proved.

Lemma 2. *Every n-ary quasigroup of order 4 is separable or semilinear.*

Using auxiliary statements proved above, we derive a consequence of this lemma.

Theorem 2. *For any $n\in\mathbb{N}$, all n-ary quasigroups of order 4 are switching equivalent. Moreover, any two n-ary quasigroups of order 4 can be taken to one another by successive switchings of $\{0,1\}$-, $\{0,2\}$-, and $\{2,3\}$-components.*

Proof. Using induction on n, we prove that any n-ary quasigroup is switching equivalent to some linear quasigroup. For $n=1,2$ this is verified directly. Assume that the claim is proved

for n-ary quasigroups for all $n < r$; let us prove it for $n = r$. Consider an arbitrary n-ary quasigroup f. It follows from Lemma 2 that f is either semilinear, and then by Proposition 6 is switching equivalent to a linear quasigroup, or separable, and then can be represented in the form

$$f(x_1, \ldots, x_n) \equiv h(q(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}),$$

where the quasigroup q is not separable and hence is semilinear. By the induction hypothesis, h is switching equivalent to some linear quasigroup ℓ. Then by Proposition 4 the quasigroup f is switching equivalent to g, where

$$g(x_1, \ldots, x_n) \equiv \ell(q(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}).$$

By Proposition 3, g is semilinear, and by Proposition 6 it is switching equivalent to a linear quasigroup. This completes the induction step.

Now switching equivalence of all n-ary quasigroups of order 4 follows from Proposition 5.

To prove the second part of the theorem, it remains to explain why it suffices to use switchings of components of the specified types only. The point is that, for instance, switching of some $\{1, 2\}$-component S of the quasigroup f can be replaced by switching of $S_{0,1}(f)$, then switching of the $\{0, 2\}$-component that S becomes after the first switching, and then again switching of the $\{0, 1\}$-component $S_{0,1}$ but now of the new quasigroup. The result is the same as after the single switching of the $\{1, 2\}$-component S. In this way we can completely eliminate switchings of $\{0, 3\}$-, $\{1, 2\}$-, and $\{1, 3\}$-components from a chain of transformations. $\triangle$

The author is grateful to a reviewer for interest to the paper and for valuable remarks on improving the presentation.

REFERENCES

1. Romanov, A.M., Survey of the Methods for Constructing Nonlinear Perfect Binary Codes, *Diskretn. Anal. Issled. Oper., Ser. 1*, 2006, vol. 13, no. 4, pp. 60–88 [*J. Appl. Ind. Math.* (Engl. Transl.), 2008, vol. 2, no. 2, pp. 252–269].

2. Solov'eva, F.I., On Perfect Binary Codes, *Discrete Appl. Math.*, 2008, vol. 156, no. 9, pp. 1488–1498.

3. Avgustinovich, S.V. and Krotov, D.S., Embedding in a Perfect Code, *J. Combin. Des.*, 2009, vol. 17, no. 5, pp. 419–423.

4. Phelps, K.T. and LeVan, M., Switching Equivalence Classes of Perfect Codes, *Des. Codes Cryptogr.*, 1999, vol. 16, no. 2, pp. 179–184.

5. Östergård, P.R.J., Pottonen, O., and Phelps, K.T., The Perfect Binary One-Error-Correcting Codes of Length 15: Part II—Properties, *IEEE Trans. Inform. Theory*, 2010, vol. 56, no. 6, pp. 2571–2582.

6. Avgustinovich, S.V., Heden, O., and Solov'eva, F.I., The Classification of Some Perfect Codes, *Des. Codes Cryptogr.*, 2004, vol. 31, no. 3, pp. 313–318.

7. Phelps, K.T., A General Product Construction for Error Correcting Codes, *SIAM J. Algebr. Discrete Methods*, 1984, vol. 5, no. 2, pp. 224–228.

8. Krotov, D.S. and Potapov, V.N., n-Ary Quasigroups of Order 4, *SIAM J. Discrete Math.*, 2009, vol. 23, no. 2, pp. 561–570.

9. Potapov, V.N. and Krotov, D.S., Asymptotics for the Number of n-Quasigroups of Order 4, *Sibirsk. Mat. Zh.*, 2006, vol. 47, no. 4, pp. 873–887 [*Siberian Math. J.* (Engl. Transl.), 2006, vol. 47, no. 4, pp. 720–731].