ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Switching of covering codes

Patric R.J. Östergård [a], William D. Weakley [b,*]

[a] Department of Communications and Networking, Aalto University, School of Electrical Engineering, P.O. Box 13000, 00076 Aalto, Finland

[b] Department of Mathematical Sciences, Indiana University–Purdue University Fort Wayne, Fort Wayne, IN 46805, United States

ARTICLE INFO

Article history:
Received 29 September 2016
Received in revised form 18 October 2017
Accepted 19 October 2017
Available online xxxx

Keywords:
Automorphism group
Covering code
Dominating set
Error-correcting code
Hypercube
Switching

ABSTRACT

Switching is a local transformation of a combinatorial structure that does not alter the main parameters. Switching of binary covering codes is studied here. In particular, the well-known transformation of error-correcting codes by adding a parity-check bit and deleting one coordinate is applied to covering codes. Such a transformation is termed a semiflip, and finite products of semiflips are semiautomorphisms. It is shown that for each code length $n \geq 3$, the semiautomorphisms are exactly the bijections that preserve the set of r-balls for each radius r. Switching of optimal codes of size at most 7 and of codes attaining $K(8,1) = 32$ is further investigated, and semiautomorphism classes of these codes are found. The paper ends with an application of semiautomorphisms to the theory of normality of covering codes.

1. Introduction

Transformations of combinatorial structures that do not alter the basic parameters have been studied since the early days of combinatorics. In [12], the first author unifies much of the theory of such transformations under the concept of switching. For binary codes, the following definition is given in [12].

Definition 1. A *switch* of a binary code is a transformation that concerns exactly one coordinate and keeps the studied parameter of the code unchanged.

For binary (error-correcting) codes with a prescribed minimum distance d, all possible transformations that fulfill Definition 1 can be obtained easily and quickly [12]. A transformation that first extends the code with a parity-check bit and then punctures it in one coordinate can be seen as fulfilling Definition 1, by letting the extended coordinate replace the punctured one. This transformation is called a semiflip. The technique of extending a code with a parity-check bit is well known, especially as a means of showing that $A(n+1, d+1) = A(n, d)$ for d odd, where $A(n, d)$ denotes the maximum size of a binary code of length n and minimum distance d.

Semiflips constitute switches also for covering codes, that is, the covering radius of the code is not altered by the transformation, as shown in [3, Example 3.1.4], originally due to Struik [14, Lemma 3.7]. This paper is devoted to an in-depth study of the semiflip and its application to binary covering codes in particular.

We need a formal definition of codes and related notations. Let $\mathbb{Z}$ denote the set of integers, and let $\mathbb{Z}_2 = \{0, 1\}$ be the group of integers modulo 2. For each positive integer n, let $\mathbb{Z}_2^n$ denote the set of binary words of length n. A *(binary) code* of length n is a nonempty subset of $\mathbb{Z}_2^n$, and its elements are called *codewords*.

* Corresponding author.
E-mail addresses: patric.ostergard@aalto.fi (P.R.J. Östergård), weakley@ipfw.edu (W.D. Weakley).

https://doi.org/10.1016/j.disc.2017.10.020
0012-365X/© 2017 Elsevier B.V. All rights reserved.

We write $\mathbf{0}$ for the all-zero word. For each i, $1 \le i \le n$, $\mathbf{e}_i$ is the word that has 1 only in coordinate i. The value in the ith coordinate of a word $\mathbf{c}$ is denoted by c_i. We write $\bar{\mathbf{c}}$ for the word obtained by complementing each coordinate of $\mathbf{c}$, and say the words $\mathbf{c}$ and $\bar{\mathbf{c}}$ are *complementary*. For $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$, the *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is the number of coordinates in which they differ; d_H is a metric on $\mathbb{Z}_2^n$. For each integer r, $0 \le r \le n$, the *(closed) r-ball* centered at $\mathbf{x}$ is $\{\mathbf{y} \in \mathbb{Z}_2^n : d_H(\mathbf{x}, \mathbf{y}) \le r\}$, denoted by $B_r(\mathbf{x})$.

A code is *d-error-correcting* if the d-balls centered at the codewords are pairwise disjoint. A code of length n is a *covering code of covering radius r* if $\mathbb{Z}_2^n$ is the union of the r-balls centered at the codewords. A code is *perfect* if for some nonnegative integer r it is both r-error-correcting and r-covering; that is, the r-balls centered at codewords tile $\mathbb{Z}_2^n$.

The paper is organized as follows. The concept of switching is considered in more detail in Section 2, where the semiflip is formally introduced. Semiautomorphisms, the symmetries induced by semiflips, are studied in Section 3, and in Section 4 it is shown that semiautomorphisms preserve code properties. In Section 5 the metric naturally associated with semiautomorphisms is introduced, and a short proof is given of a theorem of Perkel and Miller on automorphism groups of cube powers. Switching classes of small covering codes are studied in Section 6. In Section 7 a characterization of normal covering codes is given.

2. Switching of codes

In [12], it is shown how all possible switches of a binary t-error-correcting code C (so $d = 2t + 1$) can be found via a particular bipartite graph $G = (V, E)$. Let m be the coordinate where the switch is to take place. Then $V = V_0 \cup V_1$ with one vertex in V_j for each codeword $\mathbf{c} \in C$ with $c_m = j$. Moreover, there is an edge between the vertices corresponding to two codewords $\mathbf{c}, \mathbf{c}' \in C$ exactly when $d_H(\mathbf{c}, \mathbf{c}') = 2t + 1$ and $c'_m = \overline{c_m}$. There is now a one-to-one correspondence between the switches and the sets of connected components of G; a set of connected components gives the codewords whose value in coordinate m is to be altered.

Fix the coordinate where a switch of a binary code is to be made, and let C' be the set of codewords that are altered according to Definition 1. Such a switch is called *minimal* if for each proper subset $C'' \subset C'$, an alteration of the codewords in C'' (in the same coordinate) does not constitute a switch. For error-correcting codes, a minimal switch clearly corresponds to one connected component of the graph G defined above. It is not clear if minimal switches of covering codes can be characterized in a compact way; for error-correcting codes, one pays attention to non-codewords only indirectly (that is, in considering distance between codewords) but this does not suffice for covering codes.

Switching of covering codes was not considered in [12] through an exhaustive characterization but through the specific (well-founded) transformation that we now describe. Given a code C with covering radius r, we wish to make a switch in place m that produces a code with the same covering radius. If a particular codeword is changed, it is likely that some nearby codewords will need to be changed to keep the covering radius from increasing, and these changes will require further changes. For this reason, we iteratively build the set H of codewords to be changed as follows: a singleton *starting set* H_1, containing the first word to be changed, is given, along with what we will call a *propagation rule*: a function $P : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \{\text{true}, \text{false}\}$. For each $i \ge 1$, once H_i is determined, we set $H_{i+1} = \{\mathbf{y} \in C : P(\mathbf{x}, \mathbf{y}) \text{ for some } \mathbf{x} \in H_i$ and $\mathbf{y} \notin \cup_{j=1}^{i} H_j\}$. Since $\mathbb{Z}_2^n$ is finite, $H_k = \emptyset$ for some k, and we set $H = \cup_{i=1}^{k-1} H_i$.

The propagation rule studied in [12] is

$$d_H(\mathbf{x}, \mathbf{y}) \le 2r + 1,\ d_H(\mathbf{x}, \mathbf{y}) \text{ odd, and } y_m = \overline{x_m}. \tag{1}$$

When this rule is used with any starting set H_1, we will call the result a *standard covering switch*. In [12, Theorem 1] it is shown that this type of switch produces a code with the same covering radius as the original code.

Note that if $d_H(\mathbf{c}, \mathbf{c}') = 1$ in a covering code, then a standard covering switch of one of these codewords will propagate to the other, which just leads to a transposition of the labeling of these two codewords. So the definition of standard switches of covering codes may be modified by ignoring such pairs of codewords. (This *might* have an impact on a larger set of codewords, as a propagation of changes through these codewords is stopped.)

Suppose that a standard covering switch has starting set $H_1 = \{\mathbf{x}\}$. If the codeword $\mathbf{y}$ is also altered by the switch (that is, $y \in H$), parity and (1) imply:

$$\text{Either } d_H(\mathbf{x}, \mathbf{y}) \text{ is even and } y_m = x_m, \text{ or } d_H(\mathbf{x}, \mathbf{y}) \text{ is odd and } y_m = \overline{x_m}. \tag{2}$$

This implies that there will usually be nontrivial standard covering switches—ones where not all codewords will have coordinate m altered.

We now turn to the semiflip, which was informally defined in the Introduction. We will show (see the last claim of Proposition 3) that a semiflip is a switch with (2) as propagation rule, which means all the changes are made at the first step.

For any nonempty set S, we let $\mathrm{Sym}(S)$ denote the group of permutations of S and further abbreviate $\mathcal{S}_n := \mathrm{Sym}(\{1, \ldots, n\})$. The identity mapping on S is denoted by ι_S; we will often omit the subscript if it is clear from the context. We further define $\pi : \mathbb{Z} \to \mathbb{Z}_2$ by $\pi(n) =$ parity of n, and we use the same name for a mapping $\pi : \mathbb{Z}_2^n \to \mathbb{Z}_2$ where $\pi(\mathbf{x})$ is the parity of the weight of $\mathbf{x}$.