Bull. Korean Math. Soc. **57** (2020), No. 2, pp. 295–309
https://doi.org/10.4134/BKMS.b190204
pISSN: 1015-8634 / eISSN: 2234-3016

LINEAR AND NON-LINEAR LOOP-TRANSVERSAL CODES IN ERROR-CORRECTION AND GRAPH DOMINATION

Mehmet Dağli, Bokhee Im, and Jonathan D. H. Smith

Abstract. Loop transversal codes take an alternative approach to the theory of error-correcting codes, placing emphasis on the set of errors that are to be corrected. Hitherto, the loop transversal code method has been restricted to linear codes. The goal of the current paper is to extend the conceptual framework of loop transversal codes to admit nonlinear codes. We present a natural example of this nonlinearity among perfect single-error correcting codes that exhibit efficient domination in a circulant graph, and contrast it with linear codes in a similar context.

1. Introduction

Loop transversal codes embody an alternative approach to the theory of error-correcting and error-detecting codes, as described in a number of earlier papers [2–4, 6, 9] and elsewhere [1, 5], [10, §I.4.4]. Instead of directly addressing the construction of the code, the approach places initial emphasis on the set of errors that are to be corrected. Algebraic structure is created on this set of errors, for example using a greedy algorithm, or by other means. A combination of the algebraic structure on the error set with the inherent structure of the channel then yields the code itself through a process known as *local duality.* In particular, the perfect binary and ternary Golay codes are constructed greedily in this fashion [4, Tables 3, 4]. Loop transversal codes handle white noise and non-white noise error patterns, such as burst errors, with equal facility [3]. For the binary case, loop transversal codes have been related to Gröbner basis methods [7, Rem. 2.54].

Until now, the study of loop transversal codes has been limited to the linear case, where the algebraic structure on the set of errors is that of an abelian group. (Nevertheless, Aydinyan did use linear loop transversal codes over $\mathbb{Z}/_4$

Received February 21, 2019; Accepted August 14, 2019.

2010 *Mathematics Subject Classification.* 94B60, 20N05, 05C69.

Key words and phrases. Loop transversal code, nonlinear code, quasigroup, loop, circulant graph, efficient domination.

The second author was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF-2017R1D1A3B05029924).

to produce nonlinear Gray codes over $\mathbb{Z}/_2$ [1].) The goal of the current paper is to extend the conceptual framework of loop transversal codes in channels with abelian group structure so that they may also include nonlinear codes. We then discuss a natural example of the occurrence of this nonlinearity, in the context of perfect single-error correcting codes for efficient domination of a circulant graph.

The extended treatment of loop transversal codes is presented in Section 2. The full general setting (2.1) is an abelian group channel where addition from the product of a code subset and an error ball subset yields a bijection with the channel. In other terms, an arbitrary channel word is decomposed uniquely as the sum of a codeword and an error in the decoding process.

Under reasonable assumptions, decoding the sum of errors yields algebraic structure on the error ball, as discussed in §2.2. The code is linear, i.e., a subgroup of the channel, only if this error ball structure is an abelian group (Corollary 2.14). Note that the error ball need not form a subgroup of the channel group. Thus in our loop transversal interpretation of the Division Algorithm for division by a positive divisor d (Example 2.2), the channel forms the free abelian group of integers, while the error ball, the set of possible remainders, forms the finite group of residues modulo d.

Moving beyond the previous context for loop transversal codes, we now define a code to be *quasilinear* if the algebraic structure on the error ball forms a (necessarily commutative) quasigroup. Theorem 2.11 shows that this is the case, for example, if the error ball is finite, or invariant under negation of channel words. The question then arises as to whether there are any quasilinear codes which are not actually linear. Example 2.15 provides a positive answer to this key question.

In the more general nonlinear setting, §2.3 examines the process by which the code may be recovered from the error ball structure. In the linear case, this was achieved by the Principle of Local Duality as summarized in Corollary 2.18. Here, in combination with the inherent abelian group structure of the channel, the binary addition operation on the error ball suffices to recover the code. In the new, more general setting, the duality survives, but may lose its local character. In the linear case it suffices to know the errors assigned to the sum of pairs of errors under the decoding process, but the nonlinear case may require the errors assigned to sums of large numbers of errors, as described by the Principle of Duality formulated in Theorem 2.16.

While the key Example 2.15 of a genuinely nonlinear loop transversal code was initially presented in the abstract, it actually arises naturally in the context of perfect single-error correcting codes given by efficient dominating sets in circulant graphs. To set the stage for the example, Section 3 examines the role of linear codes as efficient dominating sets in circulants. Theorem 3.1 provides the relevant necessary and sufficient number-theoretical conditions for their occurrence, while Theorem 3.2 gives a sufficient condition for the error balls centered at any vertex to carry isomorphic abelian group structure. By a result of Obradović *et al.* [8], it follows that no efficient dominating set in a circulant of degree less than 5 can yield a nonlinear code.

Section 4.1 then frames Example 2.15 as a nonlinear error ball for an efficient dominating set in the circulant $C_{12}(1,5,6)$, the wreath product of C_6 with K_2, which has degree 5. Serving as a nonlinear analogue of Theorem 3.2 for this example, Theorem 4.3 shows that all the nonlinear error ball structures in $C_{12}(1,5,6)$ are isomorphic.

The paper generally follows the conventions of [10] for notation and concepts that are not otherwise explained. In particular, in order to avoid a plethora of brackets in discussions of non-associative structures, algebraic notation (with arguments preceding functions) is employed as the default option.

2. Loop transversal codes

2.1. Nonlinear codes

Let $(A,+,0)$ be an abelian group. Suppose that there are subsets K and B of A such that the restricted addition

$$\nabla\colon K\times B\to A;(k,b)\mapsto k+b \tag{2.1}$$

is an isomorphism of sets. In particular, disjoint union decompositions

$$A=\coprod_{k\in K}(k+B)\quad\text{and}\quad A=\coprod_{b\in B}(K+b) \tag{2.2}$$

are consequences of the isomorphism property for (2.1).

Lemma 2.1. *Given the isomorphism* (2.1)*, the equality*

$$(K-K)\cap(B-B)=\{0\}$$

holds.

Proof. Suppose that $k_1-k_2=b_1-b_2$ for $k_1,k_2\in K$ and $b_1,b_2\in B$. Then $k_1+b_2=k_2+b_1$. Since (2.1) is injective, it follows that $k_1=k_2$ and $b_1=b_2$, so that $k_1-k_2=b_1-b_2=0$. □

Using the terminology of coding theory, the group A is called the *channel*, while the set K is called the *code*. Elements of A may be described as *words*, while elements of K are said to be *codewords*. The code K is described as *linear* if it forms a subgroup of A, while the term *nonlinear* applies to general codes. The set B is called the *error set* or *ball*. Its elements are *errors*. The ball B is defined as *symmetric* if $-B=B$. For example, in a *binary channel* of length l, where $A\cong(\mathbb{Z}/_2,+,0)^l$ has exponent 2, the ball will always be symmetric.

Suppose that

$$\Delta\colon A\to K\times B;x\mapsto(x^\delta,x^\varepsilon)$$

is the inverse of the set isomorphism (2.1). In other words,

$$x=x^\delta+x^\varepsilon \tag{2.3}$$

for all x in A, while

$$(k+b)^\delta = k \quad \text{and} \quad (k+b)^\varepsilon = b \tag{2.4}$$

for codewords k and errors b. The relation (2.3) is read as *decoding* a word x to a codeword x^δ, with the implication that error x^ε occurred during transmission through the channel A. Thus the map $\delta\colon A \to K$ is described as *decoding*, while $\varepsilon\colon A \to B$ is described as *error-detection*. The structure (A, Δ), which implicitly includes K as the codomain of δ and B as the codomain of ε, is described as a *coding scheme*.

Example 2.2. Consider the channel $A = (\mathbb{Z}, +, 0)$ of integers under addition, with linear code $K = d\mathbb{Z}$ for a positive divisor $d \in \mathbb{Z}$, and asymmetric ball $B = \mathbb{Z}/_d = \{0, 1, \dots, d-1\}$. The Division Algorithm, yielding a unique quotient $q \in \mathbb{Z}$ and remainder $r \in B$ for each dividend $x = dq + r$, gives a coding scheme (A, Δ) with $\Delta\colon x \mapsto (dq, r)$.

Remark 2.3. Note that the general axioms for a coding scheme are completely symmetric in K and B. Nevertheless, linguistically, the interpretive vocabulary breaks the symmetry. In general, relationships between K and B, and results (such as Theorem 2.16 below) that determine features of one of K or B from the other, are said to embody *duality*.

Definition 2.4. A coding scheme (A, Δ) is said to be *coherent* if:

- $\forall\, k \in K\,,\ k^\delta = k$; and
- $|\delta(B)| = 1$.

Example 2.5. The coding scheme of Example 2.2 is coherent.

By abuse of language, one often says simply that a code K is coherent, as in the following example. This example will be examined repeatedly throughout the paper, and studied in full detail in Section 4.

Example 2.6. Consider $A = (\mathbb{Z}/_{12}, +, 0)$, with a coherent, nonlinear code $K = \{3, 6\}$ and symmetric ball $B = \{6, -5, -1, 0, 1, 5\}$. Then the respective decoding and error-detection maps are given by the following table:

$x \in A$	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
$x^\delta \in K$	6	3	3	3	6	6	6	3	3	3	6	6
$x^\varepsilon \in B$	1	5	6	-5	5	6	-5	-1	0	1	-1	0

Lemma 2.7. *Suppose that (A, Δ) is a coherent coding scheme with code K and symmetric ball B.*

(a) *The ball B contains* 0.
(b) $K \cap B = \{0^\delta\}$.
(c) *The error-detection map restricts to a well-defined bijection*

$$\varepsilon\colon B \to B; b^\varepsilon = b - 0^\delta \tag{2.5}$$

on the ball.

Proof. (a) Consider a codeword k. Since $k = k^\delta + k^\varepsilon = k + k^\varepsilon$, one has $0 = k^\varepsilon \in B$.

(b) Since $0 = 0^\delta + 0^\varepsilon$ and the ball is symmetric, $0^\delta = -0^\varepsilon \in -B = B$, so $K \cap B \supseteq \{0^\delta\}$. Conversely, if $k \in K \cap B$, then $k = k^\delta \in \delta(B) = \{0^\delta\}$.

(c) For each element b of B, one has $b = b^\delta + b^\varepsilon = 0^\delta + b^\varepsilon$, so $b^\varepsilon = b - 0^\delta$. Thus the map $\varepsilon \colon B \to B$ has

$$B \to B; b \mapsto b + 0^\delta \tag{2.6}$$

as a two-sided inverse. □

Remark 2.8. Under the assumptions of Lemma 2.7, the formula (2.5) for ε only applies to elements of the ball. In Example 2.6, for instance, one has $4^\varepsilon = 1 \neq -2 = 4 - 6 = 4 - 0^\delta$.

2.2. Algebra on the ball

Let (A, Δ) be a coding scheme. For each natural number m, define an m-ary operation

$$\mu^m \colon B^m \to B; (b_1, \dots, b_m) \mapsto \prod_{i=1}^m b_i$$

with

$$\prod_{i=1}^m b_i = (b_1 + \cdots + b_m)^\varepsilon \tag{2.7}$$

for $b_1, \dots, b_m$ in B. In compound expressions involving elements of the ball, the operations $\prod_{i=1}^m b_i$ will bind more strongly than the abelian group operations from $(A, +, 0)$.

Example 2.9. The initial instances of (2.7) are as follows.

$m = 0$: The nullary operation μ^0 selects the constant element 0^ε of B.

$m = 1$: The unary operation $\mu^1 \colon B \to B$ is just the restriction to B of the error map $\varepsilon \colon A \to B$.

$m = 2$: A commutative binary operation $*$ called *multiplication* is defined on the ball B by

$$b_1 * b_2 = (b_1 + b_2)^\varepsilon \tag{2.8}$$

for $b_1, b_2 \in B$. In other words,

$$b_1 + b_2 \in K + (b_1 * b_2) \tag{2.9}$$

within the second disjoint union decomposition of (2.2).

Remark 2.10. The definition of the operation $*$ on the ball B only involves the decomposition of the subset $B + B$ of A in (2.2). In this sense, one may consider the binary algebra $(B, *)$ as a *local* structure within the channel A.

A magma $(M, \circ)$, i.e., a set M with a binary operation $\circ$, is a *quasigroup* if knowledge of any two of the elements x, y, z of M within the equation $x \circ y = z$ serves to specify the third element uniquely. The coding scheme (A, Δ), and more informally the code K itself, are then described as *quasilinear* if $(B, *)$ is a quasigroup.

Theorem 2.11. *Consider the ball B, with operation* (2.8)*.*

(a) *For each element b of B, the left multiplication*

$$L_*(b)\colon B \to B; x \mapsto b * x \tag{2.10}$$

is injective.

(b) *If B is finite, then K is quasilinear.*

(c) *If B is symmetric, then K is quasilinear.*

Proof. (a) Suppose that there are elements b_1, b_2, b_3 of B such that $b_1 * b_2 = b_1 * b_3$. By (2.9), one has

$$b_1 + b_2 = k_2 + b_1 * b_2 \quad \text{and} \quad b_1 + b_3 = k_3 + b_1 * b_3$$

for elements k_2, k_3 of K. Thus

$$b_2 - b_3 = k_2 - k_3 \in (K - K) \cap (B - B) = \{0\}$$

by Lemma 2.1, so that $b_2 = b_3$.

(b) When B is finite, the injective left multiplications (2.10) become bijective. Thus the commutative structure $(B, *)$ is a quasigroup.

(c) Suppose that $B = -B$. For any given $b_1, b_2 \in B$, it will be shown that there is an element b of B with $b_1 * b = b_2$, so that $L(b_1)$ becomes surjective. Combined with the injectivity from (a), this will show that the left multiplications (2.10) become bijective, making the commutative structure $(B, *)$ a quasigroup.

Consider the element $b_1 - b_2$ of A. By the second decomposition in (2.2), there are elements k of K and b' of B such that $b_1 - b_2 = k + b'$. Thus for $b = -b' \in B$, one has $b_1 - b_2 = k - b$ or

$$K + (b_1 * b) \ni b_1 + b = k + b_2 \in K + b_2$$

by (2.9). Thus $b_1 * b = b_2$, as required. □

A simple application of (2.5) yields the following.

Lemma 2.12. *Let (A, Δ) be a coherent coding scheme with code K and symmetric ball B. Suppose $b_1, b_2 \in B$. Then*

$$b_1 * b_2 = (b_1 + b_2)^\varepsilon = b_1 - 0^\delta + b_2$$

if $b_1 + b_2 \in B$.

Proposition 2.13. *Let (A, Δ) be a coherent coding scheme with code K and symmetric ball B. Then the multiplication $*$ on B has 0^δ as a two-sided identity element.*

Proof. For $b \in B$, one has $b + 0^\delta \in B$ by (2.6). Then $b * 0^\delta = b$ by Lemma 2.12, so 0^δ is a two-sided identity element for the commutative binary operation $*$ on B. □

Recall that a *loop* is a quasigroup $(M, \circ)$ with an *identity element* e, so that $e \circ x = x = x \circ e$ for all x in M.

Corollary 2.14. *Let* (A, Δ) *be a coherent coding scheme with code* K *and symmetric ball* B*.*

(a) *The structure* $(B, *, 0^\delta)$ *is a commutative loop.*
(b) *If the code* K *is linear, then* $0^\delta = 0$*, and* $(B, *, 0)$ *is an abelian group.*

Proof. (a) Since B is symmetric, Theorem 2.11(c) shows that $(B, *)$ is a quasigroup.

(b) If K is linear, then $0 \in K$, so the coherence implies $0^\delta = 0$. The second disjoint union decomposition of (2.2) shows that B is a transversal to the (normal) subgroup K of the abelian group A. Within an abelian group, each such transversal is a normalized loop transversal, and there is an isomorphism

$$(B, *, 0) \to (A/K, +, K); b \mapsto K + b \tag{2.11}$$

(compare [10, Example I.4.3.4]). □

Example 2.15. In the context of Example 2.6, the multiplication $*$ on the ball is given by the following commutative loop table, with $6 = 0^\delta$ as the identity element:

$*$	6	-5	-1	0	1	5
6	6	-5	-1	0	1	5
-5	-5	-1	0	1	5	6
-1	-1	0	-5	5	6	1
0	0	1	5	6	-5	-1
1	1	5	6	-5	-1	0
5	5	6	1	-1	0	-5

Note that

$$(1 * 1) * (1 * 1) = -1 * -1 = -5\,,$$

while

$$((1 * 1) * 1) * 1 = ((-1) * 1) * 1 = 6 * 1 = 1\,.$$

Thus the multiplication $*$ on B is not associative, or even power-associative.

2.3. The ball determines the code

Let (A, Δ) be a coding scheme. The operation (2.7) on the ball, together with (2.3), yields

$$\begin{aligned} b_1 + \cdots + b_m &= (b_1 + \cdots + b_m)^\delta + (b_1 + \cdots + b_m)^\varepsilon \\ &= (b_1 + \cdots + b_m)^\delta + \prod_{i=1}^{m} b_i \end{aligned}$$

and thus

$$(b_1 + \cdots + b_m)^\delta = \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i \tag{2.12}$$

for $b_1, \dots, b_m$ in the ball.

Theorem 2.16 (Principle of Duality). *Consider a coding scheme (A, Δ). Suppose that the ball B generates the monoid $(A, +, 0)$. Then the set*

$$\Big\{ \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i \;\Big|\; m \in \mathbb{N}\,,\ b_1, \dots, b_m \in B \Big\} \tag{2.13}$$

constitutes the code K.

Proof. Certainly, the relation (2.12) shows that each element of (2.13) is a codeword. Conversely, let k be a codeword. By (2.2), one has $a = k + b$ for some word a and error b, where $k = a^\delta$ and $b = a^\varepsilon$. Since B generates the monoid $(A, +, 0)$, there is a natural number m with a collection $b_1, \dots, b_m$ of elements of B such that $a = \sum_{i=1}^{m} b_i$. The relation (2.12) then yields $k = \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i$. □

Example 2.17. In the context of Examples 2.6 and 2.15, the codeword $6 = 0 - 0^\varepsilon$ is given by taking $m = 0$ in (2.13). The other codeword is $3 = (1 + 1) - (-1) = (1 + 1) - (1 * 1)$, taking $m = 2$ and $b_1 = b_2 = 1$.

Corollary 2.18 (Principle of Local Duality, [3, §2], [6, (1.5)], [9, (1.4)], [10, Prop. I.4.4.3]). *Suppose that B generates the monoid $(A, +, 0)$. Then if the code K is linear, it is determined entirely by the group structures $(A, +)$ and $(B, *)$.*

Proof. When $(B, *)$ is an abelian group, one has $\prod_{i=1}^{m} b_i = b_1 * \cdots * b_m$ for natural numbers m and elements $b_1, \dots, b_m$ of the ball. □

3. Linear codes in circulants

For a positive integer n, consider the additive group $(\mathbb{Z}/_n, +, 0)$ of integers modulo n. Let J be a subset of $\{1, 2, \dots, \lfloor n/2 \rfloor\}$. The *circulant graph* $\mathcal{C}_n(J)$ is then defined as the (simple, regular) graph on the vertex set $\mathbb{Z}/_n$ whose edge set is $E = \{\{x, x+d\} \mid x \in \mathbb{Z}/_n, d \in J\}$. In this context, J is known as the *jump set.* For $J = \{s_1, \dots, s_r\}$, the circulant $\mathcal{C}_n(J)$ is also written as $\mathcal{C}_n(s_1, \dots, s_r)$.

3.1. Perfect linear single-error correcting codes

In the guise of efficient domination, perfect single-error correcting codes in connected circulant graphs of degree 3 or 4 were studied in [8]. Within a general circulant $\mathcal{C}_n(J)$, the following provides a loop-transversal analysis of perfect, single-error correcting codes, linear in the cyclic channel $\mathbb{Z}/_n$.

Theorem 3.1. *Consider a circulant $\mathcal{C}_n(J)$ of degree d. Let $b = 1 + d$. Then $\mathcal{C}_n(J)$ admits a perfect, single-error correcting code, being linear in the channel $(\mathbb{Z}/_n, +, 0)$ if and only if b divides n and $\pm J$ comprises a full set of non-zero residues modulo b.*

Proof. When $\mathcal{C}_n(J)$ admits a perfect, single-error correcting linear code, the d-element set of single errors is $\pm J$ modulo n, so the cardinality of the full error set B (including the trivial error 0) is b. The perfect code partitions the n-element channel into disjoint balls of radius 1, each of size b, centered at the codewords. In particular, b divides n. Since the code is linear in the channel $(\mathbb{Z}/_n, +, 0)$, it is the subgroup $b\mathbb{Z}/_n$ of $\mathbb{Z}/_n$. Consider an integer e with $0 \leq e < b$. Suppose that the residue e modulo n decodes to $e^\delta = bq$ modulo n, for some integer q. Then the error incurred is $e - e^\delta = e - bq$ modulo n. Thus the error set includes each residue e modulo b.

Conversely, suppose that b divides n and $\pm J$ comprises a full set of non-zero residues modulo b. Define $B = \{0\} \cup (\pm J)$ modulo n. Then $|B| = b$. Addition modulo b defines a group structure $(B, *)$ on the set of trivial and single errors. Corollary 2.18 then yields a perfect, single-error correcting loop-transversal code $b\mathbb{Z}/_n$ in the channel $(\mathbb{Z}/_n, +, 0)$ equipped with the metric structure of $\mathcal{C}_n(J)$. □

3.2. Isomorphism of linear error-ball groups

Theorem 3.2. *Consider a circulant graph $C_n(J)$. Assume that the vertices in the efficient dominating set are equally spaced, i.e., form a coset of a subgroup K_0 of order n/k in $\mathbb{Z}/_n$. Then the error ball centered at any vertex is isomorphic to $\mathbb{Z}/_k$.*

Proof. Since K_0 as a code is linear, the error ball B_0 centered at the vertex 0 has the structure of the abelian group $\mathbb{Z}/_k$ provided by the isomorphism (2.11). Now consider the code $K_l = l + K_0$, and the ball B_l centered at an arbitrary vertex $l + kt$. Define a mapping

$$\varphi : B_0 \to B_l; b \mapsto b + l + kt\,.$$

Let $b_1, b_2 \in B_0$. There exists an integer s such that

$$b_1 *_{B_0} b_2 = (b_1 + b_2)^{\varepsilon_{B_0}} = (\underbrace{ks}_{\in K_0} + \underbrace{b_1 + b_2 - ks}_{\in B_0})^{\varepsilon_{B_0}} = b_1 + b_2 - ks.$$

Then it follows that

$$\begin{aligned}\varphi(b_1 *_{B_0} b_2) &= \varphi(b_1 + b_2 - ks) \\ &= b_1 + b_2 - ks + l + kt \\ &= (\underbrace{l + kt + ks}_{\in K_l} + \underbrace{b_1 + b_2 - ks + l + kt}_{\in B_l})^{\varepsilon_{B_l}} \\ &= (b_1 + l + kt + b_2 + l + kt)^{\varepsilon_{B_l}} \\ &= (\varphi(b_1) + \varphi(b_2))^{\varepsilon_{B_l}} \\ &= \varphi(b_1) *_{B_l} \varphi(b_2)\,.\end{aligned}$$

Hence B_0 and B_l are isomorphic. □

By [8], the vertices in an efficient dominating set are necessarily equally spaced for circulant graphs of degree two, three and four. Thus, we obtain the following result.

Corollary 3.3. *In a code yielding an efficient dominating set for a circulant, any error ball of order* 3, 4 *or* 5 *forms an abelian group.*

4. Nonlinear codes in the circulant $C_{12}(1,5,6)$

Corollary 3.3 shows that efficient dominating sets in circulants of degree less than 5 have error balls with abelian group structure. The aim of this section is to interpret the nonlinear error ball structure exhibited successively in Examples 2.6, 2.15 and 2.17 within the context of efficient dominating sets for circulants.

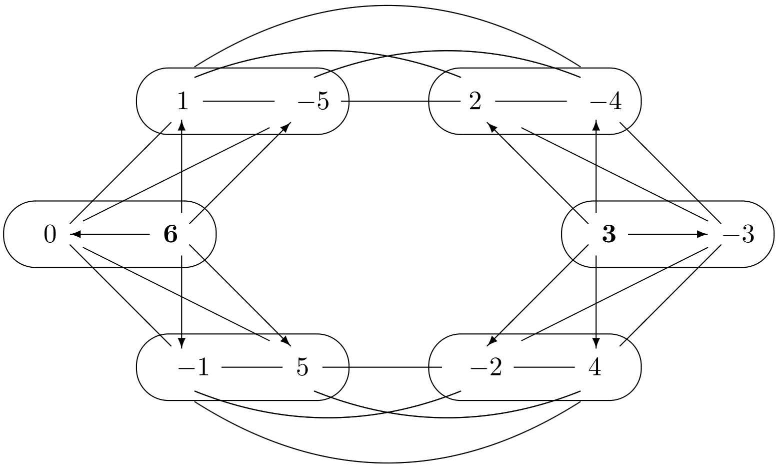

FIGURE 1. The perfect dominating set $\{3, 6\}$ in $C_{12}(1, 5, 6)$

4.1. Perfect nonlinear single-error correcting codes

Consider the code $K = \{3, 6\}$ of Example 2.6, with symmetric error ball $B = \{6, -5, -1, 0, 1, 5\}$. As displayed in Figure 1, this code represents a perfect dominating set or single-error correcting code in the circulant $C_{12}(1, 5, 6)$, the wreath product graph $C_6 \operatorname{wr} K_2$.

4.2. Isomorphism of non-linear error-ball loops

Consider the circulant graph $C_{12}(1, 5, 6)$, namely $C_6 \operatorname{wr} K_2$, as presented in §4.1. For a given k in $\mathbb{Z}/_{12}$, there are two different error-ball loops centered at the vertex k, namely B_k^+ and B_k^-. They correspond respectively to the codes $K_k^+ = \{k, k+3\}$ and $K_k^- = \{k, k-3\}$. Thus Example 2.6 presents the code K_6^- and error-ball B_6^-. In this section, we show that all of the 24 error-ball loops corresponding to perfect dominating sets in the circulant $C_{12}(1, 5, 6)$ are isomorphic.

Proposition 4.1. *For a residue $k \in \mathbb{Z}/_{12}$, there is a loop isomorphism f_k or $f\colon (B_k^+, *) \to (B_k^-, *); x \mapsto 2k - x$.*

Proof. Note that f is bijective. Let $b_1, b_2 \in B_k^+$. Since 3 is not in the jump set, either $b_1 + b_2 - k \in B_k^+$ or $b_1 + b_2 - (k+3) \in B_k^+$. We consider each case separately.

Case I. Let $b_1 + b_2 - k \in B_k^+$. Then

$$\begin{aligned} b_1 *_{B_k^+} b_2 &= (b_1 + b_2)^{\varepsilon_{B_k^+}} \\ &= (\underbrace{k}_{\in K_k^+} + \underbrace{b_1 + b_2 - k}_{\in B_k^+})^{\varepsilon_{B_k^+}} \\ &= b_1 + b_2 - k. \end{aligned}$$

It follows that

$$f(b_1 *_{B_k^+} b_2) = f(b_1 + b_2 - k) = 3k - b_1 - b_2.$$

Note that $3k - b_1 - b_2 \in B_k^-$. Since 3 is not in the jump set, we have $3k - b_1 - b_2 + 3 \notin B_k^-$. Now, $4k - b_1 - b_2 \in \mathbb{Z}/_{12}$ can be written as

$$\underbrace{k}_{\in K_k^-} + \underbrace{3k - b_1 - b_2}_{\in B_k^-} \qquad \text{or} \qquad \underbrace{k-3}_{\in K_k^-} + \underbrace{3k - b_1 - b_2 + 3}_{\notin B_k^-}.$$

Then we have

$$\begin{aligned} f(b_1) *_{B_k^-} f(b_2) &= (2k - b_1) *_{B_k^-} (2k - b_2) \\ &= (4k - b_1 - b_2)^{\varepsilon_{B_k^-}} \\ &= (k + 3k - b_1 - b_2)^{\varepsilon_{B_k^-}} \\ &= 3k - b_1 - b_2 \\ &= f(b_1 *_{B_k^+} b_2). \end{aligned}$$

Case II. Let $b_1 + b_2 - (k+3) \in B_k^+$. Then

$$\begin{aligned} b_1 *_{B_k^+} b_2 &= (b_1 + b_2)^{\varepsilon_{B_k^+}} \\ &= (\underbrace{k+3}_{\in K_k^+} + \underbrace{b_1 + b_2 - (k+3)}_{\in B_k^+})^{\varepsilon_{B_k^+}} \\ &= b_1 + b_2 - (k+3). \end{aligned}$$

It follows that

$$f(b_1 *_{B_k^+} b_2) = f(b_1 + b_2 - (k+3)) = 3k - b_1 - b_2 + 3.$$

Since $3k - b_1 - b_2 + 3 \in B_k^-$, we have $3k - b_1 - b_2 \notin B_k^-$. Note that $4k - b_1 - b_2$ can be written as

$$\underbrace{k}_{\in K_k^-} + \underbrace{3k - b_1 - b_2}_{\notin B_k^-} \qquad \text{or} \qquad \underbrace{k-3}_{\in K_k^-} + \underbrace{3k - b_1 - b_2 + 3}_{\in B_k^-}.$$

Then it follows that

$$\begin{aligned} f(b_1) *_{B_k^-} f(b_2) &= (2k - b_1) *_{B_k^-} (2k - b_2) \\ &= (4k - b_1 - b_2)^{\varepsilon_{B_k^-}} \\ &= (k - 3 + 3k - b_1 - b_2 + 3)^{\varepsilon_{B_k^-}} \\ &= 3k - b_1 - b_2 + 3 \\ &= f(b_1 *_{B_k^+} b_2). \end{aligned}$$

In conclusion, $f(b_1 *_{B_k^+} b_2) = f(b_1) *_{B_k^-} f(b_2)$ in either case, so that f is an isomorphism. □

Proposition 4.2. *For residues $k, l \in \mathbb{Z}/_{12}$, the map $\phi_l^k \colon x \mapsto l - k + x$ gives loop isomorphisms $(B_k^+, *) \to (B_l^+, *)$ and $(B_k^-, *) \to (B_l^-, *)$.*

Proof. We give the proof by considering two cases as above.

Case I. If $b_1 + b_2 - k \in B_k^+$, then $b_1 *_{B_k^+} b_2 = b_1 + b_2 - k$, and

$$\phi_l^k(b_1 *_{B_k^+} b_2) = \phi_l^k(b_1 + b_2 - k) = l - 2k + b_1 + b_2.$$

Since $l - 2k + b_1 + b_2 \in B_l^+$, we have $l - 2k + b_1 + b_2 - 3 \notin B_l^+$. The residue $2l - 2k + b_1 + b_2 \in \mathbb{Z}/_{12}$ can be written as

$$\underbrace{l}_{\in K_l^+} + \underbrace{l - 2k + b_1 + b_2}_{\in B_l^+} \qquad \text{or} \qquad \underbrace{l+3}_{\in K_l^+} + \underbrace{l - 2k + b_1 + b_2 - 3}_{\notin B_l^+}.$$

It follows that

$$\begin{aligned}\phi_l^k(b_1) *_{B_l^+} \phi_l^k(b_2) &= (l-k+b_1) *_{B_l^+} (l-k+b_2)\\ &= (2l-2k+b_1+b_2)^{\varepsilon_{B_l^+}}\\ &= (l+l-2k+b_1+b_2)^{\varepsilon_{B_l^+}}\\ &= l-2k+b_1+b_2\\ &= \phi_l^k(b_1 *_{B_k^+} b_2)\,.\end{aligned}$$

Case II. If $b_1+b_2-(k+3) \in B_k^+$, then $b_1 *_{B_k^+} b_2 = b_1+b_2-(k+3)$, and

$$\begin{aligned}\phi_l^k(b_1 *_{B_k^+} b_2) &= \phi_l^k(b_1+b_2-(k+3))\\ &= l-2k+b_1+b_2-3.\end{aligned}$$

Note that $l-2k+b_1+b_2-3 \in B_l^+$ and $l-2k-b_1-b_2 \notin B_l^+$. The residue $2l-2k+b_1+b_2 \in \mathbb{Z}/_{12}$ can be written as

$$\underbrace{l}_{\in K_l^+} + \underbrace{l-2k+b_1+b_2}_{\notin B_l^+} \qquad \text{or} \qquad \underbrace{l+3}_{\in K_l^+} + \underbrace{l-2k+b_1+b_2-3}_{\in B_l^+}\,.$$

It follows that

$$\begin{aligned}\phi_l^k(b_1) *_{B_l^+} \phi_l^k(b_2) &= (l-k+b_1) *_{B_l^+} (l-k+b_2)\\ &= (2l-2k+b_1+b_2)^{\varepsilon_{B_l^+}}\\ &= (l+3+l-2k+b_1+b_2-3)^{\varepsilon_{B_l^+}}\\ &= l-2k+b_1+b_2-3\\ &= \phi_l^k(b_1 *_{B_k^+} b_2)\,.\end{aligned}$$

Hence $\phi_l^k : B_k^+ \to B_l^+$ is an isomorphism.

The proof of $\phi_l^k : B_k^- \to B_l^-$ is similar, considering the two cases where $b_1+b_2-k \in B_k^-$ or $b_1+b_2-(k-3) \in B_k^-$. □

Propositions 4.1 and 4.2 contribute to the following.

Theorem 4.3. *All* 24 *error-ball loops corresponding to perfect dominating sets in the circulant* $C_{12}(1,5,6)$ *are isomorphic. Thus for residues* $k, l \in \mathbb{Z}/_{12}$*, there is a commutative diagram*

(4.1)
$$\begin{tikzcd}(B_k^+, *) \arrow[r, "f_k"] \arrow[d, "\phi_l^k"'] & (B_k^-, *) \arrow[d, "\phi_l^k"] \\ (B_l^+, *) \arrow[r, "f_l"'] & (B_l^-, *)\end{tikzcd}$$

of isomorphisms between the loops $(B_k^+,*),(B_k^-,*),(B_l^+,*)$ *and* $(B_l^-,*)$.

Proof. It remains to confirm the commutativity of (4.1). The diagram chase

$$\begin{tikzcd}
x \arrow[rr, mapsto, "f_k"] \arrow[dd, mapsto, "\phi_l^k"'] & & 2k-x \arrow[d, mapsto, "\phi_l^k"] \\
& & l-k+(2k-x) \arrow[dl, equal] \\
l-k+x \arrow[r, mapsto, "f_l"'] & 2l-(l-k+x) &
\end{tikzcd}$$

performs that task. □

References

[1] R. Aydinyan, *Loop Transversal Codes over Finite Rings*, ProQuest LLC, Ann Arbor, MI, 2005.

[2] R. Aydinyan and J. D. H. Smith, *Loop transversal codes for error detection*, J. Combin. Math. Combin. Comput. **58** (2006), 153–159.

[3] D.-H. Choi and J. D. H. Smith, *Greedy loop transversal codes for correcting error bursts*, Discrete Math. **264** (2003), no. 1-3, 37–43. https://doi.org/10.1016/S0012-365X(02)00548-4

[4] F.-L. Hsu, F. A. Hummer, and J. D. H. Smith, *Logarithms, syndrome functions, and the information rates of greedy loop transversal codes*, J. Combin. Math. Combin. Comput. **22** (1996), 33–49.

[5] F. A. Hummer, *Loop Transversal Codes*, ProQuest LLC, Ann Arbor, MI, 1992.

[6] F. A. Hummer and J. D. H. Smith, *Greedy loop transversal codes, matrices, and lexicodes*, J. Combin. Math. Combin. Comput. **22** (1996), 143–155.

[7] I. Márquez-Corbella, *A combinatorial commutative algebra approach to complete decoding*, Ph.D. Thesis, Universidad de Valladolid, 2013.

[8] N. Obradović, J. Peters, and G. Ružić, *Efficient domination in circulant graphs with two chord lengths*, Inform. Process. Lett. **102** (2007), no. 6, 253–258. https://doi.org/10.1016/j.ipl.2007.02.004

[9] J. D. H. Smith, *Loop transversals to linear codes*, J. Combin. Inform. System Sci. **17** (1992), no. 1-2, 1–8.

[10] J. D. H. Smith and A. B. Romanowska, *Post-Modern Algebra*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1999. https://doi.org/10.1002/9781118032589

Mehmet Dağli
Department of Mathematics
Amasya University
Amasya, 05000, Turkey
Email address: mehmet.dagli@amasya.edu.tr

Bokhee Im
Department of Mathematics
Chonnam National University
Gwangju 61186, Korea
Email address: bim@jnu.ac.kr

Jonathan D. H. Smith
Department of Mathematics
Iowa State University
Ames, Iowa 50011-2104, USA
Email address: jdhsmith@iastate.edu