Characterization of $c$-circulant digraphs of degree two which are circulant

J.M. Brunat*, M. Maureso, M. Mora

Dept. de Matemática Aplicada II, Universitat Politècnica de Catalunya, c/Pau Gargallo 5, 08028 Barcelona, Spain

Abstract

A $c$-circulant digraph $G_N(c, \Delta)$ has $\mathbb{Z}_N$ as its vertex set and adjacency rules given by $x \rightarrow cx + a$ with $a \in \Delta \subset \mathbb{Z}_N$. The $c$-circulant digraphs of degree two which are isomorphic to some circulant digraph are characterized, and the corresponding isomorphism is given. Moreover, a sufficient condition is obtained for a $c$-circulant digraph to be a Cayley digraph.

1. Introduction

Given a positive integer $N$, a subset $\Delta$ of $\mathbb{Z}_N$ and $c \in \mathbb{Z}_N$, $c \neq 0$, the $c$-circulant digraph $G_N(c, \Delta)$ has $\mathbb{Z}_N$ as set of vertices and adjacency rules given by $x \rightarrow cx + a$ with $a \in \Delta$. A 1-circulant digraph is called a circulant digraph. A $c$-circulant digraph can have loops but not parallel arcs.

The adjacency matrix of a $c$-circulant digraph is a $c$-circulant matrix, i.e., a matrix such that each row except the first is obtained from the preceding row by shifting the elements cyclically $c$ columns to the right. A 1-circulant matrix is called a circulant matrix. Circulant and $c$-circulant matrices have been studied in [1, 5].

Some families of digraphs proposed in the literature with good diameter, routings or connectivity are $c$-circulant digraphs. For instance, the generalized De Bruijn digraphs $G_N(d, \{0, 1, \ldots, d-1\})$ and the generalized Kautz digraphs $G_N(-d, \{1, 2, \ldots, d\})$ are $c$-circulant digraphs; see [6]. In particular, so are the De Bruijn digraphs $B(d, D)$ and the Kautz digraphs $K(d, D)$ defined by

$$B(d, D) = G_{d^r}(d, \{0, 1, \ldots, d-1\}), \quad K(d, D) = G_{d^r+d^{r-1}}(-d, \{1, 2, \ldots, d\}).$$

---

1 Work supported in part by the Spanish Research Council (Comisión Interministerial de Ciencia y Tecnología, CICYT) under project TIC 94-0592.

* Corresponding author. E-mail: brunat@ma2.upc.es.
Cayley digraphs have been proposed as a model for designing, analyzing and improving symmetric interconnection networks [2, 4, 7]. Let us remember that given a group \( \Gamma \) and a generating set \( A = \{a_1, \ldots, a_d\} \) of \( \Gamma \), the Cayley digraph \( \text{Cay}(\Gamma, A) \) has \( \Gamma \) as set of vertices and every vertex \( x \) is adjacent to the \( d \) vertices \( xa_i, 1 \leq i \leq d \). For instance, if \( A \) is a generating set of \( \mathbb{Z}_N \), then the circulant digraph \( G_N(1, A) \) is the Cayley digraph \( \text{Cay}(\mathbb{Z}_N, A) \). Finite Cayley digraphs are strongly connected and vertex transitive. They have been characterized by Sabidussi [10] (for undirected graphs, however the proof is similar in the directed case): A strongly connected digraph is a Cayley digraph if and only if its automorphism group has a subgroup which acts regularly on the set of vertices.

In this context, the general question of deciding which \( c \)-circulant digraphs are Cayley digraphs is raised. In [3], for instance, Kautz digraphs which are Cayley digraphs are characterized. In this paper we give necessary and sufficient conditions for a \( c \)-circulant digraph of degree two \( G_N(c, \{a_1, a_2\}) \) to be isomorphic to some circulant digraph \( G_N(1, \{b_1, b_2\}) \). In this case, explicit formulas for \( b_1 \) and \( b_2 \) and for the isomorphism are obtained.

In Section 2 we summarize some known results about \( c \)-circulant digraphs. In Section 3 we give sufficient conditions for \( G_N(c, A) \) to be a Cayley digraph. The rest of the paper is devoted to the main result about \( c \)-circulant digraphs of degree two.

2. Previous results

Throughout this paper the greatest common divisor of \( k \) integers \( x_1, \ldots, x_k \) is denoted by \( (x_1, \ldots, x_k) \). Let \( G_N(c, A) \) be a \( c \)-circulant digraph with \( A = \{a_1, \ldots, a_d\} \). We define the following parameters:

\[
g = (N, c),
\]

\[
m = (N, a_1 - a_2, a_1 - a_3, \ldots, a_1 - a_d),
\]

\[
r = N/m
\]

\[
s_0 = 0, \quad s_i = 1 + c + c^2 + \cdots + c^{i-1} \pmod{N}, \quad i \in \mathbb{Z}, i \geq 1.
\]

Let us recall some results about \( c \)-circulant digraphs drawn from [8, 9, 11]. If \( x \) is a vertex of a Cayley digraph \( \text{Cay}(\Gamma, A) \), the indegree and outdegree of \( x \) is \( d = |A| \). So, if a \( c \)-circulant digraph is a Cayley digraph, it must be regular. Regular \( c \)-circulant digraphs of degree \( d \) are characterized as follows:

**Proposition 2.1.** Let \( G_N(c, A) \) be a \( c \)-circulant digraph and, for \( k = 0, \ldots, g - 1 \), let \( A_k = \{a \in A: a \equiv k \pmod{g}\} \). Then \( G_N(c, A) \) is regular of degree \( d \) if and only if \( g \) divides \( d \) and \( |A_k| = d/g \) for \( k = 0, \ldots, g - 1 \).
The strongly connected c-circulant digraphs have been characterized in the following arithmetical way.

**Proposition 2.2.** Let \( G_N(c, \Delta) \) be a c-circulant digraph, \( N^* \) the greatest divisor of \( N \) such that \( (N^*, c) = 1 \) and \( m^* = (N^*, a_1 - a_2, \ldots, a_1 - a_d) \). The digraph \( G_N(c, \Delta) \) is strongly connected if and only if

(i) \( \Delta \) contains all congruence classes modulo \( g \);

(ii) \( (N^*, a_1, \ldots, a_d) = 1 \);

(iii) \( \{s_i \pmod{m^*} : 1 \leq i \leq m^*\} = \mathbb{Z}_{m^*} \).

Let \( m^* = 2^{x_1} p_1^{y_1} \cdots p_k^{y_k} \) be the prime decomposition of \( m^* \) and define

\[ m_0^* = 2^{\min\{2, x_1\}} p_1 \cdots p_k. \]

Then the condition (iii) in Proposition 2.2 can be replaced by the condition

(iii') \( c \equiv 1 \pmod{m_0^*} \),

see [8].

Note that if \( g = (N, c) = 1 \), then condition (i) is automatically satisfied, \( N^* = N \) and \( m^* = m \).

If \( |\Delta| = 2 \) and \( G_N(c, \Delta) \) is strongly connected then it is 2-regular. Indeed, from condition (i), it must be either \( g = 1 \) or \( g = 2 \). If \( g = 1 \), the condition of Proposition 2.1 is obviously satisfied. If \( g = 2 \), then one of the elements of \( \Delta \) is even and the other is odd, so \( 1 = |\Delta_0| = |\Delta_1| = d/g \). Then, Proposition 2.1 can also be applied.

All c-circulant digraphs considered in the rest of the paper are regular and strongly connected.

Note that if \( G_N(c, \Delta) \) is vertex transitive, the number of loops is 0 or \( N \). The number of loops in a c-circulant digraph is given by the following proposition.

**Proposition 2.3.** Let \( G_N(c, \Delta) \) be a c-circulant digraph and define \( g_1 = (N, c - 1) \) and \( \Delta = \{a \in \Delta : a \equiv 0 \pmod{g_1}\} \). Then the number of loops of \( G_N(c, \Delta) \) is \( g_1 | \Delta | \).

Let \( k \) be an integer with \( k \geq 2 \). A digraph \( G = (V, E) \) is a \( k \)-generalized cycle if there exist subsets \( V_0, \ldots, V_{k-1} \) of \( V \) such that if \((u, v) \in E\), then \( u \in V_i \) and \( v \in V_{i+1} \) for some \( i = 0, \ldots, k - 1 \), where the subscripts are taken modulo \( k \). The sets \( V_i \) are called stable sets.

**Proposition 2.4.** A c-circulant digraph \( G_N(c, \Delta) \) is a \( k \)-generalized cycle if and only if \( k \) divides \( m \). In particular, \( G_N(c, \Delta) \) is an \( m \)-generalized cycle if and only if \( m > 1 \).

Given a c-circulant digraph \( G_N(c, \Delta) \) with \( m > 1 \), we define \( A_i = \{x \in \mathbb{Z}_N : x \equiv i \pmod{m}\} \) for \( i = 0, \ldots, m - 1 \). It has been shown in [11] that the stable sets of \( G_N(c, \Delta) \) are \( B_i = A_{\sigma(i)} \), where \( \sigma \) is an appropriate permutation of \( \{0, \ldots, m - 1\} \). In the following proposition we give a more precise description of the sets \( B_i \), which will be useful later. Take the subscripts in such a way that \( 0 \in B_0 = A_0 \). Note that \( B_0 \) is the subgroup of \( \mathbb{Z}_N \) generated by \( a_1 - a_2, \ldots, a_1 - a_d \). We have:
Proposition 2.5. Let $G_N(c, \Delta)$ be a c-circulant digraph with $m > 1$. Then the stable sets of $G_N(c, \Delta)$ are

$$B_i = s_i a_1 + B_0, \quad 0 \leq i \leq m - 1.$$  
Moreover, if $a$ is a generator of $B_0$ in $\mathbb{Z}_N$, then every $x \in \mathbb{Z}_N$ admits a unique expression of the form

$$x = s_i a_1 + xa, \quad 0 \leq i \leq m - 1, \quad 0 \leq a \leq r - 1.$$  

Proof. Since $N = mr$ and $m = (N, a_1 - a_2, \ldots, a_1 - a_d)$, the sets $A_i$ are the cosets of $B_0$ in $\mathbb{Z}_N$. Now, $s_i a_1$ is adjacent to the vertex

$$c s_i a_1 + a_1 = (1 + c s_i) a_1 = (1 + c(1 + c + \cdots + c^{i-1}))a_1 = s_{i+1} a_1$$

so the vertices $0 = s_0 a_1, a_1 = s_1 a_1, s_2 a_1, \ldots, s_{m-1} a_1$ belong to the consecutive stable sets. Then $B_i = s_i a_1 + B_0$ are the stable sets.

If $x \in \mathbb{Z}_N$, there exists a unique $i, 0 \leq i \leq m - 1$ such that $x \in B_i = s_i a_1 + B_0$. Since each element in $B_0$ admits a unique expression $xa$ with $0 \leq a \leq r - 1$, the result is obtained. □

Note that $s_m a_1$ belongs to $B_0$. If we consider the digraph $G_N(c, \{1, 1 + m\})$, which has the same first stable set $B_0$ as $G_N(c, \Delta)$, we obtain $s_m \in B_0$, i.e. $s_m \equiv 0$ (mod $m$).

3. Cayley c-circulant digraphs

It has been shown in [11] that if $c^m = 1$, then the c-circulant digraph $G_N(c, \Delta)$ is vertex transitive. The proof can be modified in order to show that it is, in fact, a Cayley digraph.

Proposition 3.1. If $c^m = 1$, then the digraph $G_N(c, \Delta)$ is a Cayley digraph.

Proof. If $m = 1$ then $c = 1$ and $G_N(c, \Delta) = G_N(1, \Delta) = \text{Cay}(\mathbb{Z}_N, \Delta)$.

If $m > 1$, then $G_N(c, \Delta)$ is an $m$-generalized cycle. Let $B_0, \ldots, B_{m-1}$ be the stable sets with $0 \in B_0$. The condition $c^m = 1$ implies that the map defined by $i \mapsto c^i$ is a group homomorphism from $\mathbb{Z}_m$ to the multiplicative group $\mathbb{Z}_N^\times$ of the units of $\mathbb{Z}_N$.

Let $e(x) = i$ if $x \in B_i$. For $h \in \mathbb{Z}_N$, we define

$$\phi_h(x) = x + c^{e(x)} h.$$  
It has been shown in [11] that $\phi_h$ is an automorphism of $G_N(c, \Delta)$. Note that

$$\phi_h(B_0) = B_{e(h)} \quad \text{and} \quad \phi_h(B_{e(x)}) = B_{e(h) + e(x)}.$$  

Now,

$$\phi_{h_1} \circ \phi_{h_2}(x) = \phi_{h_1}(x + c^{e(x)} h_2) = x + c^{e(x)} h_2 + c^{e(x)} + e(h_2) h_1$$

$$= x + c^{e(x)} (h_2 + c^{e(h_2)} h_1) = \phi_{h_1 + c^{e(h_2)}}(x).$$
Therefore, the set \( \Gamma = \{ \phi_h : h \in \mathbb{Z}_N \} \) is closed under composition. Hence, it is a subgroup of \( \text{Aut} \, G_N(c, \Delta) \).

Since \( \phi_h(0) = h \), it follows that the group \( \Gamma \) acts transitively. If \( \phi_h(0) = 0 \), we have \( h = c\phi_0(0) = 0 \), so \( \phi_h = \phi_0 \) is the identity map. Thus, the group \( \Gamma \) acts regularly on the vertex set of \( G_N(c, \Delta) \). Then Sabidussi's theorem implies that \( G_N(c, \Delta) \) is the Cayley digraph \( \text{Cay}(\Gamma, \{ \phi_a : a \in \Delta \}) \). \( \square \)

The converse of the Proposition 3.1 is not true. For instance, take \( N = 12 \), \( c = 10 \) and \( \Delta = \{4, 1\} \). The digraph \( G_{12}(10, \{4, 1\}) \) is strongly connected of degree 2. We have \( m = (12, 3) = 3 > 1 \), the stable sets being \( B_0 = \{0, 3, 6, 9\} \), \( B_1 = \{1, 4, 7, 10\} \), \( B_2 = \{2, 5, 8, 11\} \). The permutations of \( \mathbb{Z}_N \),

\[
\begin{align*}
\phi_1 &= (0 1 2)(3 10 5)(4 11 9)(6 7 8), \\
\phi_2 &= (0 4 8)(1 5 9)(2 6 10)(3 7 11),
\end{align*}
\]

are automorphisms of \( G_N(c, \Delta) \). The group \( \Gamma \) generated by \( \phi_1 \) and \( \phi_2 \) acts regularly on \( \mathbb{Z}_N \), so \( G_N(c, \Delta) \simeq \text{Cay}(\Gamma, \{ \phi_1, \phi_2 \}) \). Nevertheless, \( c^m = 10^3 \neq 1 \) (mod \( N \)) because \( c = 10 \) is not a unit of \( \mathbb{Z}_{12} \).

A \( c \)-circulant digraph can be circulant with the same labeling of vertices. The following is a necessary and sufficient condition for this.

**Proposition 3.2.** The identity map of \( \mathbb{Z}_N \) is an isomorphism from \( G_N(c, \Delta) \) to \( G_N(1, \Delta) \) if and only if \( \Delta = \overline{\Delta} \) and \( \Delta + 1 = \Delta + c \).

**Proof.** Let the identity be an isomorphism from \( G_N(c, \Delta) \) to \( G_N(1, \overline{\Delta}) \). By equating the sets of vertices adjacent from 0 in the two digraphs, we obtain \( \Delta = \overline{\Delta} \). By equating the sets of vertices adjacent from 1, we have \( \Delta + c = \overline{\Delta} + 1 = \Delta + 1 \).

Conversely, suppose that \( \overline{\Delta} = \Delta \) and \( \Delta + 1 = \Delta + c \). We must prove that

\[
x + \Delta = cx + \Delta \tag{1}
\]

for all \( x \in \mathbb{Z}_N \). For \( x = 0 \) and \( x = 1 \), the condition (1) is satisfied by hypothesis. If \( x \geq 2 \) and it is satisfied by \( x - 1 \), then

\[
x + \Delta = x - 1 + \Delta + 1 = c(x - 1) + \Delta + 1 = c(x - 1) + \Delta + c = cx + \Delta. \quad \square
\]

4. \( c \)-circulant digraphs of degree two which are circulant

We begin with an arithmetic lemma which will be useful later. If \( a \) and \( b \) are integers and \( \delta = (a, b) \), it is known that there exist integers \( t \) and \( z \) such that \( at + bz = \delta \) (Bezout identity). The integers \( t, z \) are not unique: If \( t_0, z_0 \) satisfy \( at_0 + bz_0 = \delta \), then for every integer \( \xi \) the numbers

\[
t = t_0 + \frac{b}{\delta} \xi, \quad z = z_0 - \frac{a}{\delta} \xi,
\]


Lemma 4.1. If $a, b$ are integers and $\delta = (a, b)$, then there exist integers $t, z$ such that $(t, b) = 1$ and $at + bz = \delta$.

Proof. If $\delta = 1$ and $at_0 + bz_0 = 1$, then $(t_0, b) = 1$. Suppose then that $\delta > 1$. Let $t_0, z_0$ be integers such that $at_0 + bz_0 = \delta$. For every prime divisor $p$ of $b$ which does not divide $b/\delta$, the equation

$$t_0 + (b/\delta)z = 1 \pmod{p}$$

has a unique solution modulo $p$. By the Chinese Remainder Theorem, there is a unique solution $\xi_0$ of the system of congruences

$$t_0 + (b/\delta)z = 1 \pmod{p}, \quad p \text{ prime, } p \mid b, \quad p \not| (b/\delta)$$

modulo the product of these primes.

Consider the solution $(t_1, z_1)$ of $at + bz = \delta$ defined by

$$t_1 = t_0 + (b/\delta)\xi_0, \quad z_1 = t_0 - (a/\delta)\xi_0$$

and let $p$ be a prime dividing both $t_1$ and $b$.

If $p$ divides $b/\delta$, then $p$ divides $t_1 - (b/\delta)\xi_0 = t_0$. Hence, $p$ divides $(a/\delta)t_0 + (b/\delta)\xi_0 = 1$ which is a contradiction.

If $p$ does not divide $b/\delta$, the condition $t_1 = t_0 + (b/\delta)\xi_0 = 1 \pmod{p}$ implies $(p, t_1) = 1$, which contradicts $p \mid t_1$. Therefore $(t_1, b) = 1$. \qed

In what follows, we only consider $c$-circulant digraphs $G_N(c, \Delta)$ with $\Delta = \{a_1, a_2\}$. $a_1 \neq a_2$. The case $N = 2$ is trivial, so we can also assume $N \geq 3$.

First we give a necessary condition for a $c$-circulant digraph $G_N(c, \Delta)$ to be a circulant digraph.

Lemma 4.2. Let $G_N(c, \Delta)$ be a $c$-circulant digraph which is a circulant digraph. Then one of the following conditions holds:

(A) $c(a_1 - a_2) = 0$;
(B) $(c - 1)(a_1 - a_2) = 0$;
(C) $(c + 1)(a_1 - a_2) = 0$.

Proof. Let $f$ be an isomorphism from $G_N(c, \Delta)$ to $G_N(1, \overline{\Delta})$, $\overline{\Delta} = \{b_1, b_2\}$. Because $G_N(1, \overline{\Delta})$ is vertex transitive, we may assume, without loss of generality, that $f(0) = 0$. This implies that $f(\Delta) = \overline{\Delta}$. Let $b_1 = f(a_1)$ and $b_2 = f(a_2)$. The vertices $b_1$ and $b_2$ are adjacent to $b_1 + b_2$ in $G_N(1, \overline{\Delta})$, so one of the two vertices $ca_1 + a_i$ adjacent from $a_i$
equals one of the two vertices \(ca_2 + a_i\) adjacent from \(a_2\). Then we have the following four possibilities:

1. \(ca_1 + a_1 = ca_2 + a_1\), which is equivalent to (A);
2. \(ca_1 + a_1 = ca_2 + a_2\), which is equivalent to (C);
3. \(ca_1 + a_2 = ca_2 + a_1\), which is equivalent to (B);
4. \(ca_1 + a_2 = ca_2 + a_2\), which is equivalent to (A).

For instance, we have seen in Section 2 that the digraph \(G_{12}(10, \{4, 1\})\) is a Cayley digraph. Nevertheless, it is not a circulant digraph because, modulo 12, \(c(a_1 - a_2) = 30 = 6 \neq 0\), \((c - 1)(a_1 - a_2) = 27 = 3 \neq 0\) and \((c + 1)(a_1 - a_2) = 33 = 9 \neq 0\).

**Corollary 4.3.** Let \(G_N(c, \Lambda)\) be a \(c\)-circulant digraph with \(m = 1\). Then \(G_N(c, \Lambda)\) is a circulant digraph if and only if \(c = 1\).

**Proof.** If \(c = 1\) then, by definition, \(G_N(c, \Lambda)\) is circulant.

Conversely, if \(m = (N, a_1 - a_2) = 1\) then \(a_1 - a_2\) is a unit of \(Z_N\). By applying Lemma 4.2, we have either \(c = 0\), \(c = -1\) or \(c = 1\).

By definition of a \(c\)-circulant digraph, \(c \neq 0\).

Now suppose that \(c = 1\) then \(N = 1\). As in Proposition 2.3, take \(g_1 = (N, c - 1) = (N, N - 2)\) and \(\Lambda = \{a \in \Lambda\, : a \equiv 0 \mod g_1\}\). We have \(g_1 \leq 2\).

If \(g_1 = 1\), then \(|\Lambda| = 2\) and \(G_N(c, \Lambda)\) has exactly \(g_1|\Lambda| = 2\) loops, hence it is not vertex transitive.

If \(g_1 = 2\), then \(N\) is even. Since \(a_1 - a_2\) is a unit, it is odd, so, in \(\Lambda = \{a_1, a_2\}\), there is one even number and one odd number. Thus, \(|\Lambda| = 1\) and \(G_N(c, \Lambda)\) has exactly \(g_1|\Lambda| = 2\) loops. Therefore, it is not vertex transitive.

Since \(c \neq 0, -1\), it follows that \(c = 1\).

**Proposition 4.4.** Let \(G_N(c, \Lambda)\) be a \(c\)-circulant digraph with \(m > 1\). If \(r = 2\), then \(G_N(c, \Lambda)\) is circulant. If \(g = 2\), then \(G_N(c, \Lambda)\) is circulant if and only if \(r = 2\).

**Proof.** It is easy to check that all the \(m\)-generalized cycles with stable sets of cardinality \(r = 2\) and regular of degree 2 are isomorphic to the circulant digraph \(G_N(1, \{1 + N/2, 1\})\).

Now, suppose that \(g = 2\) and that \(f\) is an isomorphism from \(G_N(c, \Lambda)\) to the circulant digraph \(G_N(1, \Lambda)\), \(\Lambda = \{b_1, b_2\}\). We can suppose \(f(0) = 0, f(a_1) = b_1\) and \(f(a_2) = b_2\).

In \(G_N(c, \Lambda)\), the vertex 0 is adjacent to \(a_1\) and \(a_2\). The vertex \(N/2\) is also adjacent to \(c(N/2) + a_1 = a_2\) and \(c(N/2) + a_2 = a_1\). The two vertices adjacent to \(b_1\) in \(G_N(1, \Lambda)\) are 0 and \(b_1 - b_2\), hence \(f(N/2) = b_1 - b_2\). Therefore, \(b_1 - b_2 = f(N/2)\) is adjacent to \(b_2 = f(a_2)\). Thus, \((b_1 - b_2) + b_1 = b_2, 2(b_1 - b_2) = 0\) and the order of \(b_1 - b_2\) is 2. We see that in \(G_N(1, \Lambda)\), the stable sets have cardinality \(r = 2\), so it is the same in \(G_N(c, \Lambda)\).
The previous results give a complete answer when \( m = 1 \) or \( r = 2 \) or \( g = 2 \). Therefore, we can restrict ourselves to the cases \( m > 1 \), \( r > 2 \) and \( g = 1 \).

If \( g = 1 \), then \( c \) is a unit of \( \mathbb{Z}_N \) and condition (A) in Proposition 4.2 implies \( a_1 - a_2 = 0 \), which is a contradiction. Therefore, if \( G_N(c, \Lambda) \) is circulant with \( g = 1 \), it satisfies either (B) or (C).

Let \( G_N(c, \Lambda) \) and \( G_N(1, \Lambda) \) be \( m \)-generalized cycles with \( \Lambda = \{a_1, a_2\} \), \( \tilde{\Lambda} = \{b_1, b_2\} \) and \( m = (N, a_1 - a_2) = (N, b_1 - b_2) > 1 \). As in Proposition 2.5, let

\[
B_i = s_i a_1 + \langle a_1 - a_2 \rangle \quad \text{for } 0 \leq i \leq m - 1.
\]

A \( \text{p(seudo)-isomorphism} \) from \( G_N(c, \Lambda) \) to \( G_N(1, \tilde{\Lambda}) \) is a bijection \( f: \mathbb{Z}_N \to \mathbb{Z}_N \) such that \( f(0) = 0 \), \( f(a_i) = b_1 \), \( f(a_2) = b_2 \) and \( f(cx + \Lambda) = f(x) + \tilde{\Lambda} \) for all \( x \in \mathbb{Z}_N \setminus B_{m-1} \). Thus, \( f \) has the property of an isomorphism except (perhaps) for the adjacencies from \( B_{m-1} \) to \( B_0 \).

A closed alternating path is a sequence of different vertices \( x_0, y_0, x_1, y_1, x_2, \ldots, x_{r-1}, y_{r-1}, x_0 \) such that \( x_i \) is adjacent to \( y_i \) and to \( y_{i-1} \) (where the subscripts are taken modulo \( r \)).

**Lemma 4.5.** If there is a \( \text{p-isomorphism} \) from \( G_N(c, \Lambda) \) to \( G_N(1, \tilde{\Lambda}) \), then it is unique.

**Proof.** Let \( f \) be a \( \text{p-isomorphism} \). From every vertex \( x \) there are exactly two closed alternating paths beginning at the vertex \( x \). The map \( f \) applies the closed alternating path

\[
0a_1 x_1 y_1 \cdots x_{r-1} a_2 0
\]

on the unique closed alternating path beginning with the vertices \( 0 = f(0) \) and \( b_1 = f(a_1) \), say

\[
0b_1 x'_1 y'_1 \cdots x'_{r-1} b_2 0.
\]

As \( r > 2 \), we have \( x'_i = f(x_i) \) and \( y'_i = f(y_i) \). Therefore, \( f \) is unique on \( B_0 \) and \( B_1 \). If \( f \) is unique on \( B_j \) for \( j \leq i \), the alternating closed path

\[
x_0 y_0 x_1 y_1 x_2 \cdots x_{r-1} y_{r-1} x_0, \quad x_k \in B_i, \quad y_k \in B_{i+1}
\]

is applied on the closed alternating path

\[
f(x_0) y'_0 f(x_1) y'_1 \cdots f(x_{r-1}) y'_{r-1} f(x_0),
\]

hence \( y'_i = f(y_i) \) for \( i = 0, \ldots, r - 1 \). Thus, \( f \) is unique on \( B_{i+1} \). \( \Box \)

**Proposition 4.6.** Let \( G_N(c, \{a_1, a_2\}) \) be a \( c \)-circulant digraph with \( r > 2 \), \( g \leq 1 \) and \( (c - 1)(a_1 - a_2) = 0 \) and let \( G_N(1, \{b_1, b_2\}) \) be a circulant digraph. Suppose that \( m = (N, a_1 - a_2) = (N, b_1 - b_2) > 1 \). Then the map \( f \) defined by

\[
f: s_i a_1 + \alpha(a_1 - a_2) \mapsto i b_1 + \alpha(b_1 - b_2), \quad 0 \leq i \leq m - 1, \quad 0 \leq \alpha \leq r - 1,
\]

is a \( \text{p-isomorphism} \). In particular, if \( \gamma_0 \) is such that \( s_m a_1 = \gamma_0(a_1 - a_2) \), \( 0 \leq \gamma_0 \leq r - 1 \), then \( f \) is an isomorphism if and only if \( m b_1 = \gamma_0(b_1 - b_2) \).
Proof. Because of Proposition 2.5 the map \( f \) is well-defined. The vertex 
\( x = s_i a_1 + x (a_1 - a_2), 0 \leq i \leq m - 2, \) is adjacent to the vertices 
\[
x' = cs_i a_1 + cx (a_1 - a_2) + a_1 = (cs_i + 1) a_1 + x (a_1 - a_2) = s_{i+1} a_1 + x (a_1 - a_2),
\]
\[
x'' = cs_i a_1 + cx (a_1 - a_2) + a_2 + (a_1 - a_1) = s_{i+1} a_1 + (x - 1) (a_1 - a_2).
\]
We have 
\[
f(x') = (i + 1) b_1 + x (b_1 - b_2) = ib_1 + x (b_1 - b_2) + b_1 = f(x) + b_1,
\]
\[
f(x'') = (i + 1) b_1 + (x - 1) (b_1 - b_2) = ib_1 + x (b_1 - b_2) + b_2 = f(x) + b_2.
\]
so \( f \) is a \( p \)-isomorphism.

Now, let \( 0 \leq \gamma_0, \gamma_1 \leq r - 1 \) be such that \( s_m a_1 = \gamma_0 (a_1 - a_2) \) and \( m b_1 = \gamma_1 (b_1 - b_2). \) A vertex \( x = s_{m-1} a_1 + x (a_1 - a_2) \) is adjacent to the vertices 
\[
x' = s_m a_1 + x (a_1 - a_2) = (\gamma_0 + x) (a_1 - a_2),
\]
\[
x'' = s_m a_1 + (x - 1) (a_1 - a_2) = (\gamma_0 + x - 1) (a_1 - a_2).
\]
On the other hand, \( f(x) = (m - 1) b_1 + x (b_1 - b_2) \) is adjacent to the vertices 
\[
y' = (\gamma_1 + x) (b_1 - b_2),
\]
\[
y'' = (\gamma_1 + x - 1) (b_1 - b_2).
\]
If \( \gamma_0 = \gamma_1, \) then \( y' = f(x') \) and \( y'' = f(x''), \) hence \( f \) is an isomorphism.

Conversely, if \( f \) is an isomorphism, \( f\{x', x''\} = \{y', y''\}. \) If \( f(x') = y'' \) and \( f(x'') = y', \) we have \( \gamma_0 + x = \gamma_1 + x - 1 \) and \( \gamma_0 + x + 1 = \gamma_1 + x \) (modulo \( r \)). This implies \( \gamma_1 + 1 = \gamma_0 = \gamma_1 - 1, \) so \( r = 2, \) a contradiction. Therefore, it must be \( f(x') = y' \) and 
\( f(x'') = y''. \) Hence \( \gamma_1 = \gamma_0. \)

When \( G_N(c, A) \) is circulant, the set \( \{b_1, b_2\} \) can sometimes be taken the same as \( \{a_1, a_2\}. \)

Corollary 4.7. Let \( G_N(c, A) \) be a c-circulant digraph with \( r > 2, \) \( q = 1, \) \( m > 1 \) and 
\( (c - 1)(a_1 - a_2) = 0. \) If \( (s_m - m) a_1 = 0, \) then the map \( f \) defined by 
\[f: \ s_i a_1 + x (a_1 - a_2) \mapsto i a_1 + x (a_1 - a_2),\]
is an isomorphism from \( G_N(c, A) \) to \( G_N(1, A). \) In particular, if \( m \) is odd, then \( f \) is an isomorphism.

Proof. By taking \( b_1 = a_1 \) and \( b_2 = a_2 \) in Proposition 4.6, we have 
\( m b_1 = m a_1 = s_m a_1 = \gamma_0 (a_1 - a_2) = \gamma_0 (b_1 - b_2). \) Hence \( f \) is an isomorphism.

Now suppose that \( m \) is odd. From \( (c - 1)(a_1 - a_2) = 0 \) (mod \( N \)) it follows that 
\( c - 1 = 0 \) (mod \( r \)). Since the digraph is strongly connected and \( s_m = 0 \) (mod \( m \)), we have 
\[
s_1 + s_2 + \cdots + s_{m-1} \equiv 1 + 2 + \cdots + (m - 1) = \frac{m - 1}{2} \cdot m \equiv 0 \) (mod \( m \)).
Thereby,
\[ s_m - m = 1 + c + c^2 + \cdots + c^{m-1} - m = (c - 1) + (c^2 - 1) + \cdots + (c^{m-1} - 1) \]
\[ = (c - 1)(s_1 + s_2 + \cdots + s_{m-1}) = 0 \pmod{N}, \]
and the condition \((s_m - m)a_1 = 0\) is satisfied. \(\Box\)

For instance, take \(N = 108, c = 37, a_1 = 43, a_2 = 1\). It can easily be checked that \(G_{108}(37, \{43, 1\})\) is strongly connected, \(g = (108, 37) = 1, m = (108, 42) = 6, \)
\(r = 108/6 = 18\) and \((c - 1)(a_1 - a_2) = 36\cdot 42 = 0 \pmod{108}\). Now, \(s_m = s_6 = \sum_{i=0}^{5} 37^i = 6 = m \pmod{108}\), so \(s_m - m = 0\) and \((s_m - m)a_1 = 0\). Therefore, \(G_{108}(37, \{43, 1\}) \cong G_{108}(1, \{43, 1\})\).

An example which satisfies the hypothesis of the Corollary 4.7 with \(m\) odd is the \(c\)-circulant digraph \(G_{539}(78, \{1, 8\})\). We have \(m = 7\) and then \(G_{539}(78, \{1, 8\}) = G_{539}(1, \{1, 8\})\).

**Proposition 4.8.** Let \(G_N(c, A)\) be a \(c\)-circulant digraph with \(r > 2, g = 1, m > 1\) and \((c - 1)(a_1 - a_2) = 0\), and let \(\gamma_0\) be such that \(s_m a_1 = \gamma_0(a_1 - a_2), 0 < \gamma_0 < r - 1\). Then \(G_N(c, A)\) is a circulant digraph if and only if \((\gamma_0, r, m) = 1\).

**Proof.** Let \(G_N(c, A)\) be circulant and let \(f\) be an isomorphism from \(G_N(c, A)\) to \(G_N(1, A)\) with \(f(0) = 0, f(a_1) = b_1, f(a_2) = b_2\). We have \(mb_1 = \gamma_0(b_1 - b_2) \pmod{N}\). Let \(t\) be such that \(b_1 - b_2 = mt\). Then \(mb_1 = \gamma_0mt + zN = \gamma_0mt + zm\) for some integer \(z\), hence \(b_1 = \gamma_0t + rz\). Let \(\delta\) be a divisor of \((\gamma_0, r, m)\). Then \(\delta\) divides \(b_1\) and \(m\). Since the digraphs are strongly connected, we have \((N, b_1, b_2) = 1\). Then \(\delta\) divides \((m, b_1) = (N, b_1 - b_2, b_1) = (N, b_1, b_2) = 1, so \(\delta = 1\) and \((\gamma_0, r, m) = 1\).

Conversely, suppose that \((\gamma_0, r, m) = 1\). From Lemma 4.1, by taking \(b_1 = (\gamma_0, r)\) there are \(t, z\) such that \(b_1 = \gamma_0t + rz \pmod{N}\) with \((t, r) = 1\). Now, we take \(b_2 = b_1 - mt \pmod{N}\). Then \((N, b_1, b_2) = (mr, b_1, b_1 - mt) = (mr, mt, b_1) = (m, \gamma_0, r) = 1\) and \((N, b_1 - b_2) = (mr, mt) = m\). Thus, \(G_N(1, \{b_1, b_2\})\) is a strongly connected circulant digraph with \(m = (N, a_1 - a_2) = (N, b_1 - b_2)\). Moreover \(mb_1 = m(\gamma_0t + rz) = \gamma_0mt = \gamma_0(b_1 - b_2) \pmod{N}\). From Proposition 4.6, the map defined by \(s_1a_1 + \alpha(a_1 - a_2) \mapsto ib_1 + \alpha(b_1 - b_2)\) is an isomorphism. \(\Box\)

For instance, take \(N = 960, c = 241, a_1 = 11, and a_2 = 7\). The digraph \(G_N(c, A)\) is strongly connected with \(a_1 - a_2 = 4, g = (960, 241) = 1, m = (960, 4) = 4\) and \(r = N/r = 240\). We have \(s_m a_1 = 484\cdot 11 = 524 = 131\cdot 4\), so \(\gamma_0 = 131\). From \((\gamma_0, r, m) = (131, 240, 4) = 1\), it follows that \(G_{960}(241, \{11, 7\})\) is a circulant digraph.

The first generator \(b_1\) is given by \(b_1 = (\gamma_0, r) = (131, 240) = 1\). We have \(1 = 11\cdot 131 - 6\cdot 240\), so \(t = 11\). The second generator is \(b_2 = b_1 - mt = -43 = 917\) and \(G_{960}(241, \{11, 7\})\) is isomorphic to the circulant digraph \(G_{960}(1, \{1, 917\})\).

Next we consider the case when \((c + 1)(a_1 - a_2) = 0\).
Proposition 4.9. Let $G_N(c, \{a_1, a_2\})$ be a $c$-circulant digraph with $r > 2$, $g = 1$ and $(c + 1)(a_1 - a_2) = 0$. Let $G_N(1, \{b_1, b_2\})$ be a circulant digraph with $m = (N, a_1 - a_2) = (N, b_1 - b_2) > 1$. Then the map $f$ defined by

$$f: s_i a_1 + \alpha(a_1 - a_2) \mapsto ib_1 + ((-1)^{i+1}z - \left\lfloor \frac{i}{2} \right\rfloor)(b_1 - b_2),$$

$$0 \leq i \leq m - 1, \quad 0 \leq \alpha \leq r - 1,$$

is a $p$-isomorphism from $G_N(c, \{a_1, a_2\})$ to $G_N(1, \{b_1, b_2\})$. Moreover, if $\gamma_0$ is such that $s_m a_1 = \gamma_0(a_1 - a_2), 0 \leq \gamma_0 \leq r - 1$, then $f$ is an isomorphism if and only if $m$ is even and $mb_1 = (-\gamma_0 + m/2)(b_1 - b_2)$.

Proof. From Proposition 2.5 the map $f$ is well defined. The vertex $x = s_i a_1 + \alpha(a_1 - a_2), 0 \leq i \leq m - 2$, is adjacent to the vertices

$$x' = cs_i a_1 + c\alpha(a_1 - a_2) + a_1 = s_{i+1} a_1 - \alpha(a_1 - a_2),$$

$$x'' = cs_i a_1 + c\alpha(a_1 - a_2) + a_2 = s_{i+1} a_1 - (\alpha + 1)(a_1 - a_2).$$

We have

\begin{align*}
\quad f(x') &= (i + 1)b_1 + \left((-1)^{i+1}z - \left\lfloor \frac{i}{2} \right\rfloor\right)(b_1 - b_2) \\
&= ib_1 + \left((-1)^{i+1}z - \left\lfloor \frac{i}{2} \right\rfloor\right)(b_1 - b_2) + b_1 \\
&= \begin{cases} 
ib_1 + ((-1)^{i+1}z - [i/2])(b_1 - b_2) + b_1 = f(x) + b_1 & \text{if } i \text{ is even} \\
ib_1 + ((-1)^{i+1}z - [i/2] - 1)(b_1 - b_2) + b_1 = f(x) + b_2 & \text{if } i \text{ is odd}
\end{cases}
\end{align*}

and

\begin{align*}
\quad f(x'') &= (i + 1)b_1 + \left((-1)^{i+1}z - (\alpha + 1)\right)\left\lfloor \frac{i}{2} \right\rfloor(b_1 - b_2) \\
&= ib_1 + \left((-1)^{i+1}z - \left\lfloor \frac{i}{2} \right\rfloor\right) + ((-1)^{i+1})(b_1 - b_2) + b_1 \\
&= \begin{cases} 
ib_1 + ((-1)^{i+1}z - [i/2])(b_1 - b_2) - (b_1 - b_2) + b_1 = f(x) + b_2 & \text{if } i \text{ is even} \\
ib_1 + ((-1)^{i+1}z - [i/2] - 1 + ((-1)^{i+1})(b_1 - b_2) + b_1 = f(x) + b_1 & \text{if } i \text{ is odd}
\end{cases}
\end{align*}

so $f$ is a $p$-isomorphism.

Suppose that $f$ is an isomorphism. In $G_N(c, d)$, the vertex $x = s_{m-1}a_1 + \alpha(a_1 - a_2)$ is adjacent to the vertices

$$x' = s_m a_1 - \alpha(a_1 - a_2) = (\gamma_0 - \alpha)(a_1 - a_2),$$

$$x'' = s_m a_1 - (\alpha + 1)(a_1 - a_2) = (\gamma_0 - \alpha - 1)(a_1 - a_2).$$
Let $\gamma_1$ be such that $mb_1 = \gamma_1(b_1 - b_2)$. In $G_N(1, A)$, the vertex $f(x)$ is adjacent to the vertices

$$y' = mb_1 + \left( (-1)^m x - \left\lfloor \frac{m-1}{2} \right\rfloor \right)(b_1 - b_2) = \left( \gamma_1 + (-1)^m x - \left\lfloor \frac{m-1}{2} \right\rfloor \right)(b_1 - b_2),$$

and

$$y'' = mb_1 + \left( (-1)^m x - \left\lfloor \frac{m-1}{2} \right\rfloor - 1 \right)(b_1 - b_2)$$

$$= \left( \gamma_1 + (-1)^m x - \left\lfloor \frac{m-1}{2} \right\rfloor - 1 \right)(b_1 - b_2).$$

Since $f$ is an isomorphism, we have $f \{x', x''\} = \{y', y''\}$.

Suppose that $m$ is odd. If $f(x') = y'$ and $f(x'') = y''$, we have

$$m-1 \quad y_1 - a - 1 = - \left( y_0 - a \right),$$

$$(\text{modulo } r),$$

hence $r = 2$, a contradiction. Analogously, if $f(x') = y''$ and $f(x'') = y'$, then we have

$$y_1 - a - \left\lfloor \frac{m-1}{2} \right\rfloor - 1 = - (y_0 - a - 1)$$

Then,

$$2x = y_0 + \gamma_1 - \left\lfloor \frac{m-1}{2} \right\rfloor + 1$$

for all $x$. Hence, $r = 2$ which is a contradiction. Thus, $m$ must be even. In this case, $f(x') = y'$ and $f(x'') = y''$ implies $r = 2$ as before. Therefore, $f(x') = y''$ and $f(x'') = y'$, which imply $\gamma_1 = - \gamma_0 + m/2$.

Conversely, if $m$ is even and $mb_1 = \left( \gamma_0 + m/2)(b_1 - b_2\right)$, it is routine to check that $f(x') = y''$ and $f(x'') = y'$, hence $f$ is an isomorphism. 

In the same way as Proposition 4.7 and Corollary 4.8, the following results can be shown.

**Corollary 4.10.** Let $G_N(c, A)$ be a c-circulant digraph with $r > 2$, $g = 1$, $m > 1$ even and $(c + 1)(a_1 - a_2) = 0$. If $(s_m + m) a_1 = (m/2)(a_1 - a_2)$, then the map $f$ defined by

$$f: sa_1 + x(a_1 - a_2) \mapsto ia_1 + ((-1)^{i+1} x - \left\lfloor i/2 \right\rfloor)(a_1 - a_2),$$

is an isomorphism from $G_N(c, A)$ to $G_N(1, A)$.
Proposition 4.11. Let $G_N(c, A)$ be a $c$-circulant digraph with $r > 2$, $g = 1$, $m > 1$ and $(c + 1)(a_1 - a_2) = 0$. Then $G_N(c, A)$ is a circulant digraph if and only if $m$ is even and $(-\gamma_0 + m/2, m, r) = 1$.

For instance, let us consider the strongly connected $c$-circulant digraph $G_{30}(11, \{1, 11\})$. We have $g = (30, 11) = 1$, $m = (30, 10) = 10$, $r = 3$, $(c + 1)(a_1 - a_2) = -120 = 0 \pmod{30}$, $s_m = s_{10} = 0$. Then $10 = (s_m + m)a_1 = (m/2)(a_1 - a_2) = 5\cdot(-10) = -20 = 10 \pmod{30}$, hence $G_{30}(11, \{1, 11\}) \cong G_{30}(1, \{1, 11\})$.

As an example of an application of Proposition 4.11, take the digraph $G_{154}(43, \{1, 29\})$. It is strongly connected, $(c + 1)(a_1 - a_2) = 44 \cdot(-28) = 0 \pmod{154}$ and has parameters $q = 1$, $m = 14$, $r = 11$. Moreover, $s_{14} = 0$, so $\gamma_0 = 0$. Since $(-\gamma_0 + m/2, m, r) = 1$, the digraph is circulant. Take $b_1 = (-\gamma_0 + m/2, r) = (7, 11) = 1$. From $7(-3) + 11 \cdot 2 = 1$ and $(-3, 11) = 1$ it follows $b_2 = 1 - 14(-3) = 43 \pmod{154}$. Therefore, $G_{154}(43, \{1, 29\}) \cong G_{154}(1, \{1, 43\})$.

Finally, we give the following characterization which follows from the previous results.

Proposition 4.12. Let $G_N(c, A)$ be a $c$-circulant digraph with $c > 1$. Then $G_N(c, A)$ is a circulant digraph if and only if one of the following conditions is satisfied:

(i) $m > 1$ and $r = 2$;
(ii) $m > 1$, $r > 2$, $g = 1$, $(c - 1)(a_1 - a_2) = 0$ and $(\gamma_0, r, m) = 1$;
(iii) $m > 1$, $r > 2$, $g = 1$, $(c + 1)(a_1 - a_2) = 0$, $m$ is even and $(-\gamma_0 + m/2, r, m) = 1$.

References