General properties of c-circulant digraphs

Article *in* Ars Combinatoria -Waterloo then Winnipeg- · January 1988

3 authors, including:

Miquel Angel Fiol
Universitat Politècnica de Catalunya

GENERAL PROPERTIES OF C-CIRCULANT DIGRAPHS

M. Mora, O. Serra & M.A. Fiol

Polytechnic University of Catalonia

ABSTRACT

A digraph is said to be c-circulant if its adjacency matrix is c-circulant. This paper deals with general properties of this family of digraphs, as isomorphisms, regularity, strong connectivity, diameter and the relation between c-circulant digraphs and the line digraph technique.

1. INTRODUCTION

Given two positive integers c and N, and $\Delta=\{a_1,\ldots,a_d\}$ a subset of $\mathbb{Z}_N$, the c-circulant digraph (cCD) $G_N(c,\Delta)$ has set of vertices $\mathbb{Z}_N$ and adjacency rules given by $i \longrightarrow ci+a_s$, $a_s\in\Delta$ for every i in $\mathbb{Z}_N$. The adjacency matrix of $G_N(c,\Delta)$ is the c-circulant matrix $A=c\text{-circ}(\alpha_1,\ldots,\alpha_N)$, where $\alpha_i=1$ iff $i\in\Delta$, and each row is a "forward shift of c places" of the preceding one. Conversely, a (0,1) c-circulant matrix $A=c\text{-circ}(\alpha_1,\ldots,\alpha_N)$ is the adjacency matrix of $G_N(c,\Delta)$ where $\Delta=\{i\in\mathbb{Z}_N : \alpha_i=1\}$. From our definition, a cCD can have loops but not parallel arcs.

Some families of digraphs proposed in the literature with good diameter, routing or connectivity properties, are cCD's. For instance, the generalized de Bruijn digraphs, $G_N(d,\{0,\ldots,d-1\})$, see [8,10], and the Imase&Itoh digraphs, also known as generalized Kautz digraphs, $D_N(-d,\{1,\ldots,d\})$, see [9]. De Bruijn and Kautz digraphs can be viewed themselves as cCD's. When c=1, $D_N(1,\Delta)$ is the Cayley diagram of $\mathbb{Z}_N$ with respect to the set Δ.

In this paper we study some general properties of these digraphs . In Section 2, we characterize some families of subsets Δ that give rise to isomorphic digraphs. For instance, for N prime, there exists a unique cCD of degree 2 for every c≠1 (up to isomorphism). The out-degree of all vertices is the order of Δ, and we give in Section 3 their in-degrees. This leads to the characterization of the cCD's

This work has been supported by the "Comision Asesora para la Investigacion Cientifica y Tecnica",(CAICYT), under project n. 1180-84.

that are regular. In Section 4, necessary and sufficient conditions over c and Δ for a cCD to be strongly connected are given. In Section 5, we determine when a cCD is the line digraph of some digraph G', and when G' is in turn a cCD. Finally, in Section 6 we discuss some questions about the diameter of a cCD.

Through the paper, $\Gamma^+(x)$ denotes the set of vertices adjacent from a vertex x, and $d^+(x)=|\Gamma^+(x)|$ its cardinality. Similarly, $\Gamma^-(x)$ denotes the set of vertices adjacent to x, and $d^-(x)=|\Gamma^-(x)|$ its cardinality. The elements of the set Δ are denoted by a_i, $\Delta=\{a_1,\dots,a_d\}$, and g denotes the greatest common divisor of N and c.

2. ISOMORPHISMS

For a given value of c, different choices of the subset Δ may produce isomorphic cCD's. A family of subsets that give raise to isomorphic digraphs is characterized below. All equations in this section must be understood in the ring $\mathbb{Z}_N$.

2.1. Proposition: Let c be a given element in $\mathbb{Z}_N\setminus\{0,1\}$, and $g_1=\gcd(N,c-1)$. Then, $G_N(c,\Delta)$ is isomorphic to $G_N(c,\Delta+kg_1)$, for any k in $\mathbb{Z}_N$.

Proof: Let p be any solution of $(c-1)x=-kg_1$. The bijection

$$f_p:\mathbb{Z}_N \longrightarrow \mathbb{Z}_N$$
$$x \longrightarrow x+p$$

is an isomorphism between $G_N(c,\Delta)$ and $G_N(c,\Delta+kg_1)$ since, for every a in Δ,

$$f_p(cx+a) = cx+a+p = c(x+p)+(a+kg_1) = cf_p(x)+(a+kg_1).\square$$

Notice that, when c=1, the maps f_p defined above are automorphisms of the Cayley diagram $G_N(1,\Delta)$.

2.2. Proposition: Let r be in $\mathbb{Z}_N^*$. Then, $G_N(c,\Delta)$ is isomorphic to $G_N(c,r\Delta)$.

Proof: The bijection $h_r:\mathbb{Z}_N\longrightarrow\mathbb{Z}_N$ given by $h_r(x)=rx$ is an isomorphism between the two digraphs since, for every a in Δ,

$$h_r(cx+a)=(cx+a)r=crx+ar=ch_r(x)+ar.\square$$

From Propositions 2.1 and 2.2, we have in general $G_N(c,\Delta) \cong G_N(c, r\Delta+kg_1)$ when $c>1$. This fact considerably reduces the variety of cCD's for each c. For instance, when N is a prime, $G_N(c,\Delta) \cong G_N(c,(a_2-a_1)^{-1}(\Delta-a_1))$. So we can consider that $a_1=0$ and $a_2=1$. In particular, there is only one cCD of degree 2 for N a prime and each $c\neq1$, namely $G_N(c,\{0,1\})$.

3. REGULARITY OF $G_N(c,\Delta)$

Clearly, the out-degree of any vertex in $G_N(c,\Delta)$ is the order of Δ, since $cx+a_i \equiv cx+a_j \pmod N$ iff $i=j$. So, cCD's are d-out-regular. In order to compute the in-degree of a vertex x let us define the subsets $\Delta_k=\{a\in\Delta : a\equiv k \pmod g\}$ for $k=0,\dots,g-1$, $g=\gcd(c,N)$. The set $\Gamma^-(x)$ can be written as $\bigcup_{a\in\Delta}\{y: cy+a\equiv x \pmod N\}$. So, if $x\equiv a \pmod g$, g divides x-a and the congruence $cy+a\equiv x \pmod N$ has g solutions for y, hence, $|\{y: cy+a\equiv x \pmod N\}|=g$. On the other hand, if $x\not\equiv a \pmod g$, the above equation has no solution and $|\{y: cy+a\equiv x \pmod N\}|=0$. From that, we obtain

$$d^-(x)=|\Delta_k|\cdot g \quad \text{if } x\equiv k \pmod g. \qquad (1)$$

Now, it is easy to see that the number of vertices in $G_N(c,\Delta)$ with a given in-degree hg is $n_h(N/g)$, where n_h is the number of Δ_k's such that $|\Delta_k|=h$. In particular, we obtain

3.1. Proposition: $G_N(c,\Delta)$ is d-regular iff $|\Delta_k|=d/g$ for all k.

4. STRONG CONNECTIVITY

In this section we want to determine when a cCD is strongly connected, that is, when it is possible to find directed paths from any vertex to any other one in the digraph. We first consider the case when c and N are relatively prime, and then the result is generalized.

a) Case $\gcd(N,c)=1$.

4.1. Lemma: $G_N(c,\Delta)$ is strongly connected iff there exists a path from vertex 0 to any vertex.

Proof: The direct sense of the statement is clear. For the converse, we first prove that for any arc $[x, cx+a_i]$ there exists a directed path from $cx+a_i$ to x. Since we assume that $g=1$, the maps $\gamma_i: \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$ given by $\gamma_i(x)=cx+a_i$ are permutations in $\mathbb{Z}_N$; hence, for every i, there exists a positive integer k such that $\gamma_i^k=Id$, and $\gamma_i^{k-1}=\gamma_i^{-1}$, while γ_i^{k-1} corresponds to a path in the digraph. So, for every path from vertex 0 to a vertex y, we can find a path from y to 0, and hence from y to any other vertex in the digraph.□

4.2. Lemma: The set of integers $\{1, 1+c, \ldots, 1+c+\ldots+c^k; k\in \mathbb{N}\}$ contains all the congruence classes modulo m, $m>1$, iff so does the set $\{1, 1+c, \ldots, 1+c+\ldots+c^{m-1}\}$.

Proof: Suppose that $\{1+c+\ldots+c^k \pmod m \,; k\in \mathbb{N}\} = \mathbb{Z}_m$. If $\gcd(c,m)=h$, then $1+c+\ldots+c^k \equiv \lambda h+1 \pmod m$, $\lambda\in \mathbb{Z}$, hence we must have $h=1$.

Denote by α the $\min\{k\in \mathbb{N}: 1+c+\ldots+c^{k-1}\equiv 0 \pmod m\}$. Since $c^{\alpha}-1=(c-1)(1+c+\ldots+c^{\alpha-1})\equiv 0 \pmod m$, we have $c^{\alpha}\equiv 1 \pmod m$ and $c^{\lambda\alpha+r}\equiv c^r \pmod m$ for all λ in $\mathbb{N}$ and $0\le r<\alpha$, from which we obtain

$\{1+c+\ldots+c^s \pmod m; s=0,\ldots,\alpha-1\}=\{1+c+\ldots+c^k \pmod m; k\in \mathbb{N}\}=\mathbb{Z}_m$.

Since all the elements of the form $1+c+\ldots+c^s \pmod m$, $s=0,\ldots,\alpha-1$, are different, we must have $\alpha=m$ as stated in the lemma. The converse is obvious.□

4.3. Proposition: Let m be the $\gcd(N, \alpha_2, \ldots, \alpha_d)$, where $\alpha_i=a_i-a_1$, $i=2,\ldots,d$. The digraph $G_N(c,\Delta)$ is strongly connected iff

i) $\gcd(N, a_1, \ldots, a_d)=1$

ii) $\{1+c+\ldots+c^s \pmod m \;;\; s=0,\ldots,m-1\}=\mathbb{Z}_m$

Proof: Let us first suppose that the digraph is strongly connected. If $\gcd(N, a_1, \ldots, a_d)=r$, from vertex 0 we reach the vertices $c^{k-1}a_{i_1}+\ldots+ca_{i_{k-1}}+a_{i_k} \pmod N$, $k\in \mathbb{N}$, $a_{i_j}\in\Delta$, that are all multiple of r. Hence we must have $r=1$. On the other hand, the set of vertices attainable from vertex 0 can be written as

$$\{ (\sum_{j=0}^{k-1} c^j)a_1 + \sum_{j=0}^{k-1} c^j \alpha_{i_{k-j}} \pmod N ; k \in \mathbb{N} \} \qquad (2)$$

where $\alpha_{i_j} = a_{i_j} - a_1$, $1 \le i_j \le d$. Now, since $\sum_{j=0}^{k-1} c^j \alpha_{i_{k-j}} \equiv 0 \pmod m$, and all vertices are reachable from vertex zero, we must have

$$\{(c^{k-1}+..+c+1)a_1 \pmod m \; ; k \in \mathbb{N}\} = \mathbb{Z}_m . \qquad (3)$$

From $\gcd(N,\alpha_2,\ldots,\alpha_d)=m$ and (i), we obtain $\gcd(m,a_1)=1$, hence, (3) is equivalent to $\{(c^{k-1}+..+c+1) \pmod m \; ; k \in \mathbb{N}\} = \mathbb{Z}_m$. By Lemma 4.2, this last equation holds iff $\{1+c+\ldots+c^s \pmod m \; ; s=0,\ldots,m-1\} = \mathbb{Z}_m$.

Reciprocally, suppose that i) and ii) are satisfied. Let j be any element in $\mathbb{Z}_N$. Since $(m,a_1)=1$, there exist integers r,s such that $j=mr+a_1 s$. From ii) we know that there exists a positive integer t such that $s \equiv 1+c+..+c^t \pmod m$, hence, $j=mr'+a_1(1+c+..+c^t)$, and, by Lemma 4.2, t can be chosen such that $t>Ndm$. On the other hand, by i) there exist integers $\gamma_1,\ldots,\gamma_d$ such that $mr'=\gamma_1 N+\gamma_2\alpha_2+..+\gamma_d\alpha_d$, and we can write $j \equiv \varepsilon_2\alpha_2+..+\varepsilon_d\alpha_d+a_1(1+c+..+c^t) \pmod N$, where $0 \le \varepsilon_i < N$ and $\varepsilon_i \equiv \gamma_i \pmod N$. Now, since $c^m \equiv 1 \pmod N$, each ε_i can be written as a sum of ones as $\varepsilon_i \equiv c^{mq_i}+c^{m(q_i+1)}+..+c^{m(q_i+\varepsilon_i-1)} \pmod N$, where $q_i=\varepsilon_2+..+\varepsilon_{i-1}$ and $q_2=0$. Since we have taken $t>Ndm>(\varepsilon_2+\ldots+\varepsilon_d)m$, j can be expressed by

$$j \equiv \sum_{i=0}^{t} b_i c^i + (\sum_{i=0}^{t} c^i)a_1 \pmod N; \quad b_i = \begin{cases} \alpha_k \text{ when } i \equiv 0 \pmod m \text{ and } mq_k \le i < m(q_k+\varepsilon_k) \\ \alpha_1 = 0 \text{ otherwise} \end{cases}$$

Compared with (2), this expression shows that vertex j can be reached from vertex 0 in t steps, and, by Lemma 4.1, the digraph is strongly connected.□

b) Case $\gcd(N,c)=g>1$.

4.4 Proposition: $G_N(c,\Delta)$ is strongly connected iff

i) Δ contains all congruence classes modulo g, and

ii) $G_{N/g}(c,\Delta)$ is strongly connected.

Proof: First assume that $G_N(c,\Delta)$ is strongly connected. Then, all its vertices must have a nonzero in-degree. As it was shown in Section 2, this implies i). Now, for every couple i,j of vertices in $G_N(c,\Delta)$ there exist a_{i_j}'s in Δ such that $j\equiv c^k i+c^{k-1}a_{i_1}+..+a_{i_k}$ (mod N), and this congruence is also satisfied in $Z_{N/g}$, so $G_{N/g}(c,\Delta)$ is strongly connected.

Now suppose that (i) and (ii) hold. Let i,j be any two elements in Z_N and a an element in Δ such that $j\equiv a$ (mod g). So, there exist integers λ,r and s such that $j-a=\lambda g=\lambda(rc+sN)$, hence

$$j-a\equiv\lambda rc \pmod N. \tag{4}$$

Since $G_{N/g}(c,\Delta)$ is strongly connected, there exist a_{i_j}'s in Δ such that $\lambda r\equiv c^k i+c^{k-1}a_{i_1}+..+a_{i_k}$ (mod N/g), from which we obtain $\lambda rc\equiv c^{k+1}i+c^k a_{i_1}+..+ca_{i_k}$ (mod N). Using (4), we can write

$$j\equiv c^{k+1}i+c^k a_{i_1}+..+ca_{i_k}+a \pmod N$$

and the proposition follows.□

This last proposition can be recursively applied until we obtain a divisor N' of N such that gcd(N',c)=1. More precisely, let N' be the greatest divisor of N such that gcd(N',c)=1, and $m=\gcd(N',a_2-a_1,\ldots,a_d-a_1)$. Then we have

4.5. Corollary: The digraph $G_N(c,\Delta)$ is strongly connected iff

i) Δ contains all congruence classes modulo g

ii) $\gcd(N',a_1,\ldots,a_d)=1$

iii) $\{1+c+..+c^s \pmod m)\ ;s=0,\ldots,m-1\}=Z_m$

Proof: By ii) and iii), $G_{N'}(c,\Delta)$ is strongly connected, and by i) and Proposition 4.4, $G_N(c,\Delta)$ is strongly connected. The converse is similarly proved.□

Condition iii) in this last Corollary can be written in an easier way as $c\equiv1$ (mod m') , where m' is obtained from m as follows. If $m=2^\alpha p_1^{\beta_1}..p_k^{\beta_k}$ is the prime decomposition of m, then $m' = 2^{\min(2,\alpha)}p_1 \cdots p_k$. The somewhat cumbersome proof of this equivalence is not included here.

5. THE LINE DIGRAPH OF A cCD

Given a digraph G, its line digraph L(G) has the arcs of G as vertices, and the vertex [x,y] is adjacent to the vertex [x',y'] in L(G) iff the arc [x,y] is incident to the arc [x',y'] in G, see [5].

In this section we establish when the digraph $G_N(c,\Delta)$ is the line digraph of some other digraph G. When $G_N(c,\Delta)$ has no vertices with in-degree zero, we also determine when G is again a cCD.

For $k=0,1,\dots,g-1$, we denote by Δ_k the set $\Delta_k=\{a\in\Delta: a\equiv k \pmod g\}$, and by n_k its order.

5.1. Proposition: There exists a digraph G such that $G_N(c,\Delta)\cong L(G)$ iff

i) there exists a divisor p of N such that $n_k=N/p$ or zero for each k, and

ii) if $n_k\neq 0$, then $\Delta_k=\{b_k+\lambda m;\ \lambda=0,1,\dots,(N/p)-1\}$ for some b_k in Δ.

Proof: We use the fact that any digraph G is a line-digraph iff $\forall x,y\in V(G)$, either $\Gamma^+(x)\cap\Gamma^+(y)=\emptyset$ or $\Gamma^+(x)=\Gamma^+(y)$, see [6]. First we assume that $G_N(c,\Delta)\cong L(G)$ for some digraph G. If n_k is 0 or 1 for each k, conditions i) and ii) hold for p=N. Now, suppose that $n_k=r>1$ for some k. Let us write $\Delta_k=\{a_0,\dots,a_{r-1}\}, 0\le a_0<\dots<a_{r-1}<N$, and let p be the $\min\{\beta_i, i=0,\dots,r-1\}$, where $\beta_i=a_i-a_{i-1}, i=1,\dots,r-1$, and $\beta_0=N+a_0-a_{r-1}$. We take the subindices mod r. Suppose that $p=\beta_j$, and let x_0 be a solution of $cx\equiv a_{j+1}-a_j \pmod N$. (such a solution exists since $a_{j+1}\equiv a_j \pmod g$). Then, $cx_0+a_j\equiv a_{j+1} \pmod N$ implies $\Gamma^+(x_0)\cap\Gamma^+(0)\neq\emptyset$, hence $\Gamma^+(x_0)=\Gamma^+(0)$. So, there exists a_l in Δ_k such that $cx_0+a_{j+1}\equiv a_l \pmod N$. Now, $cx_0+a_{j+1}\equiv cx_0+a_j+m\equiv a_{j+1}+m\equiv a_l \pmod N$, hence we must have $a_l=a_{j+2}$ and $\beta_{j+1}=\beta_j=p$. By repeating this reasoning over $j+2,\dots,j+r$, we obtain $pr=N$ and $\Delta_k=\{a_1+\lambda p;\lambda=0,\dots,(N/p)-1\}$ as stated in ii). Finally, suppose that $n_{k'}$ is also different

from zero, and that $\Delta_{k'}=\{a'_1+\lambda p';\lambda=0,\ldots,(N/p')-1\}$. As we have seen before, $cx_o+a'_1\in\Gamma^+(x_o)=\Gamma^+(0)$, hence, there exists some a'_l in $\Delta_{k'}$ such that $cx_o+a'_1\equiv a'_l \pmod N$, where $a'_1\not\equiv a'_l \pmod N$ $(x_o\not\equiv 0)$, so $n_{k'}\geq 2$. Now, $a'_l-a'_1\equiv cx_o\equiv p \pmod N$, hence $p'|p$. By symmetry we also obtain $p|p'$, and so $p=p'$.

Conversely, if condition i) and ii) hold, suppose that $\Gamma^+(x)\cap\Gamma^+(y)\neq\emptyset$, that is, $cx+a\equiv cy+b \pmod N$ for some $a,b\in\Delta$. Since $c(x-y)\equiv b-a \pmod N$ we must have $a\equiv b \pmod g$, or $a,b\in\Delta_k$ for some k. Now, $c(x-y)\equiv\lambda p \pmod N$ leads to $cx\equiv cy+\lambda p \pmod N$ and $cx+\Delta_k\equiv cy+\Delta_k+\lambda p\equiv cy+\Delta_k \pmod N$ for each $s=0,\ldots,g-1$, hence $\Gamma^+(x)=\Gamma^+(y)$. So $G_N(c,\Delta)$ is a line digraph of some digraph. □

From Proposition 5.1, if $G_N(c,\Delta)$ is a line digraph, we must have $n_k=0$ or N/p. If $n_k\neq 0$, all elements in Δ_k are congruent modulo p, from which we deduce that $g|p$. On the other hand, as it has been shown in Section 3, the indegree of every vertex in the digraph must be 0 or $(N/p)g$. When all vertices have a nonzero indegree, the digraph is d-regular, and we have $(N/p)g=d$ and $N=d(p/g)$. In this case, the digraph G such that $L(G)\cong G_N(c,\Delta)$ can be determined by the following proposition.

5.2 Proposition: Assume that $G_N(c,\Delta)$ is a line digraph, that it is d-regular, and that no two elements in Δ are congruent modulo N/d. Then, $G_N(c,\Delta)\cong L(G_{N/d}(c,\Delta))$.

Proof: As we have seen in the proof of Proposition 5.1, if $c(x-y)\equiv 0 \pmod p$, we have $\Gamma^+(x)=\Gamma^+(y)$. From $g|p$ and $p|N$, the last congruence is equivalent to $\frac{c}{g}(x-y)\equiv 0 \pmod{\frac{p}{g}}$, which leads to $x\equiv y \pmod{\frac{p}{g}}$ (since $\gcd(\frac{p}{g},\frac{c}{g})=1$). Hence, as $\frac{N}{d}=\frac{p}{g}$, $x\equiv y \pmod{\frac{N}{d}}$ implies $\Gamma^+(x)=\Gamma^+(y)$. Since for each x there are other d-1 elements in $\mathbf{Z}_N$ which satisfy the last congruence (and the digraph is d-regular) we conclude that $\Gamma^+(x)=\Gamma^+(y)$ iff $x\equiv y \pmod{\frac{N}{d}}$. So, the family of subsets $\Gamma^+(i)$, $i=0,\ldots,(N/d)-1$ is a partition of $V(G_N(c,\Delta))=\mathbf{Z}_N$. From this fact, we can deduce that the map

$$f:\bigcup_{i=0}^{(N/d)-1}\Gamma^+(i)\longrightarrow V(L(D))$$

given by $f(ci+a_k)=[i,ci+a_k]$, where the integers in the right side are taken modulo N/d, is well defined and injective, hence, it is a bijection between the set of vertices of the two digraphs. On the other hand, if $ci+a_k \equiv j \pmod{(N/d)}$, $f(ci+a_k)=[i,j]$, and $f(c(ci+a_k)+a_s)=[j,cj+a_s]$ for each a_s in Δ, so f is also an isomorphism between the two digraphs.□

This last proposition can be also stated when Δ contains congruent elements modulo N/d. In this case, G is a "c-circulant" digraph with parallel arcs corresponding to repeated elements in Δ. The proof for this general case is basically the same as that of Proposition 5.2.

As a particular case of Proposition 5.2, we have the following result

5.3. Corollary: If $\gcd(c,Nd)=d$, $N\geq d$, and Δ contains all congruence classes modulo d, then $L(G_N(c,\Delta))\cong G_{Nd}(c,\Delta)$.

From this last corollary, we obtain the known fact that the line digraph of a generalized Kautz digraph of N vertices is the generalized Kautz digraph of Nd vertices, see [7]. This fact is also true for the generalized de Bruijn digraphs, and for the de Bruijn and Kautz digraphs themselves, see [5].

6. SOME QUESTIONS ABOUT THE DIAMETER

As it is well known, the diameter D of a digraph with N vertices and maximum out-degree d is low bounded by $D(d,N)=\lceil \log_d(N(d-1)+1)\rceil-1$, see [1]; c-circulant digraphs supply good families of digraphs whose diameter attains this minimum value. The generalized de Bruijn digraphs, $D_N(d,(0,\ldots,d-1))$, have diameter $D(d,N)$ when $(d^D-1)/(d-1)<N\leq d^D$, and diameter $D(d,N)+1$ when $d^D<N\leq(d^{D+1}-1)/(d-1)$, see [8,10]. So, there are known families of cCD's with minimum diameter for $N\leq d^D$. On the other hand, it is shown in [9] that the generalized Kautz digraphs $D_N(-d,(1,\ldots,d))$ have diameter $D(d,N)$ when $N=d^D+d^{D-b}$ for b odd, $1\leq b\leq D$. In what follows, we deal with the problem of

finding cCD's with minimum diameter and order greater than d^D.

A digraph is said to be a generalized m-cycle, $m>1$, if there exists a partition $\{A_1 \ldots A_m\}$ of its set of vertices such that the vertices of A_i are adjacent to those in A_{i+1}, see [4].

6.1. Lemma: Let $G_N(c,\Delta)$ be strongly connected, and let m denote the $\gcd(N,\alpha_2,\ldots,\alpha_d)$, where $\alpha_i = a_i - a_1$. If $m>1$, $G_N(c,\Delta)$ is a generalized m-cycle.

Proof: Let $A_i = \{x \in \mathbb{Z}_N : x \equiv i \pmod m\}$, $i=0,\ldots,m-1$, and consider the digraph G such that $V(G)=\{0,\ldots,m-1\}$ and there exists an arc from i to j iff there exists an arc in $G_N(c,\Delta)$ from a vertex in A_i to a vertex in A_j. If two vertices x, y in $G_N(c,\Delta)$ belong to the same set A_i, we have $c(x-y)+(a_s-a_t)= =c(x-y)+\alpha_s-\alpha_t \equiv 0 \pmod m$ for any a_s, a_t in Δ. So, all the vertices adjacent from x and y belong to the same set A_j for some j. Then, G is a 1-out-regular digraph, and the map $f:\mathbb{Z}_N \longrightarrow V(G)$ defined as $f(x)= x \pmod m$ is a graph homomorphism between $G_N(c,\Delta)$ and G. Since $G_N(c,\Delta)$ is strongly connected, so must be G, hence it is a cycle, and $G_N(c,\Delta)$ is a generalized m-cycle.□

It can be easily seen that an generalized m-cycle can not have diameter $D(d,N)$ for $N>d^D$.

On the other hand, when c=1 it is shown in [3] that if a digraph $G_N(1,\{a_1,\ldots,a_d\})$ has diameter D we must have $N<\binom{d+D}{d}$. So $N<d^D$ if $d>3$, $D>1$, and these digraphs are not suitable for our problem. For d=3 and $D>2$, or d=2 and $D>3$, we have $N<d^D$ again, so we only consider the case $c>1$.

We have some more restrictions to obtain cCD's with diameter D and order greater than d^D.

6.2. Lemma: Suppose that $c>1$. Let g_1 denote the $\gcd(N,c-1)$, and $A=\{a\in\Delta : a\equiv 0 \pmod{g_1}\}$. Then, the number of loops in $G_N(c,\Delta)$ is $|A|g_1$.

Proof: The digraph $G_N(c,\Delta)$ has a loop in vertrex x_o iff it is a solution of the congruence $(c-1)x\equiv -a \pmod N$. This equation has g_1 solutions for each $a\in A$, and it has no solutions for $a\in\Delta\setminus A$. Moreover, these solutions are different for each element in A, hence $G_N(c,\Delta)$ has $|A|g_1$ loops.□

From Lemma 6.2, if $g_1=1$, the digraph contain loops, and it can not have minimum diameter for $N>d^D$. If $g_1=2$, either the digraph has loops or $m\geq 2$, and the diameter is not minimum again. Finally, if $g=\gcd(c,N)>d$, we know from Proposition 4.4 that $G_N(c,\Delta)$ is not strongly connected. So our search can be restricted to the following values of the parameters:

$$m=\gcd(N,\alpha_2,\ldots,\alpha_d)=1$$

$$g=\gcd(N,c)\leq d$$

$$g_1=\gcd(N,c-1)>2 \quad (\text{and } A=\{a\in\Delta: a\equiv 0 \pmod{g_1}\}=\emptyset)$$

From our study and computer exploration, we conjecture that when $d>2$ the only solutions of our problem are the generalized Kautz digraphs for $N=d^D+d^{D-b}$, b odd. Unfortunately we have not found the proof of this conjecture yet. The case d=2 could be a little easier. In this case, from $m=\gcd(N,a_2-a_1)=1$ and Proposition 2.2, we can consider $\Delta=\{a,a+1\}$. Now, if g=2, we know from Proposition 5.2 that $G_N(c,\Delta)=L(G_{N/2}(c,\Delta))$. It can be seen that a d-regular digraph G has minimum diameter iff so does L(G), see [5]. So we can restrict ourselves to the case g=1. In this case, the Cayley diagram $G_5(1,\{1,2\})$ and its iterate line digraphs $G_N(c,\{1,2\})$ with $N=2^k+2^{k-2}$, $c\equiv 1 \pmod 5$ and $\gcd(N,c)=2$, have minimum diameter. Except for this new family, and for the generalized Kautz digraphs, we conjecture again that there is no solution to our problem in the case d=2.

REFERENCES

[1] I. Alegre, J.L.A. Yebra, M.A. Fiol, M. Valero and T. Lang, "An algorithm to minimize the diameter of directed graphs", Coms. SEIR '2, Santiago de Compostela, Spain (1982).

[2] D.Z. Du and F.K. Hwang, "Generalized de Bruijn digraphs", (1986), to appear.

[3] M. A. Fiol, "Aplicaciones de la Teoría de Grafos al diseño de redes de interconexión", Ph.D. Thesis, Polytechnic University of Catalonia (1982).

[4] M. A. Fiol, I. Alegre, J.L.A. Yebra and J. Fabrega, "Digraphs with walks of equal lenght between vertices", Graph Theory and its Applications to Algorithms and Computer Science, John Wiley & Sons, New York (1985), pp.313-322.

[5] M.A. Fiol, J.L.A. Yebra and I. Alegre, "Line digraph iterations and the (d,k) problem", IEEE Trans. Comp. C-33 (1984), pp. 400-403.

[6] C. Heuchenne, "Sur une certaine correspondance entre graphes", Bull. Soc. Roy. Sc. Liège, 33, pp. 743-753 (1964).

[7] N. Homobono, "Résistance aux pannes de grands réseaux d'interconnexion", Thése 3ème. Cycle, Université Paris-Sud, Centre d'Orsay, France (1987).

[8] M. Imase and M. Itoh, "Design to minimize diameter on building-block networks", IEEE Trans. Comp. C-30, pp.439-442 (1983).

[9] M. Imase and M. Itoh, "A design for directed graphs with minimum diameter", IEEE Trans. Comp. C-32, pp.782-784 (1983).

[10] S.M. Reddy, D.K. Pradham and J.G. Kuhl, "Directed graphs with minimum diameter and maximal connectivity", School of Engineering Oakland Univ., Tech. Rep. (1980).