SIAM J. DISCRETE MATH
Vol. 6, No. 4, pp. 655-676, November 1993

010

REPRESENTATIONS OF BOREL CAYLEY GRAPHS*

K. WENDY TANG† AND BRUCE W. ARDEN‡

Abstract. There is a continuing search for dense (δ, D) interconnection graphs, that is, regular, undirected, degree δ graphs with diameter D and having a large number of nodes. Cayley graphs formed by Borel subgroups currently contribute to some of the densest known ($\delta = 4, D$) graphs for a range of D [1]. However, the group theoretic representation of these graphs makes the development of efficient routing algorithms difficult. In an earlier report, it was shown that all Cayley graphs have generalized chordal ring (GCR) representations [2]. In this paper, it is shown that all degree-4 Borel Cayley graphs can also be represented by the more restrictive chordal rings (CR) through a constructive proof. A step-by-step algorithm to transform any degree-4 Borel Cayley graph into a CR graph is provided. Examples are used to illustrate this concept.

Key words. interconnection network, massively parallel computer, Cayley graph, Borel Cayley graph, generalized chordal ring, chordal ring

AMS subject classifications. 68R10, 68M07, 68RXX

1. Introduction.

Multiprocessors and *multicomputers* are two major categories of parallel computers [3]. In the former, processors communicate via shared memory, whereas in the latter, each processor has its own local memory (hence a computer), and communication is via message passing. Whether it is a shared-memory multiprocessor or a message-passing multicomputer, an efficient *interconnection network* to interconnect the communicating elements is critical to the performance of the parallel computer [4]. In the design of an interconnection network, there are two major issues, the interconnection *topology* and *routing algorithms*.

An interconnection topology can be modeled as a graph. To model a multicomputer system, we consider *regular*, *undirected* graphs with no *multiple edges* between any pair of nodes. A graph is regular when it has the same number of incident edges, or *degree*, at every node [5]. Nodes of the graph correspond to processors with local memory, and the edges represent connections between these elements. Due to the limited number of connections that can be made to real chips, we are interested primarily in regular graphs of small degree. For a given small degree, we are interested in *dense graphs* [6]. A *dense graph* is one with a large number of nodes for a given *diameter*. The diameter is the maximum *distance* between all node pairs. Here *distance* between two nodes refers to the smallest number of hops between the two nodes. A dense graph allows the interconnection of a large number of processing elements with a potentially small communication delay. Furthermore, a *symmetric graph* is also desirable, because then an identical routing algorithm can be used at every node [3].

A variety of network topologies and routing algorithms have been proposed as interconnection models [7]–[12]. However, graphs originally generated from these topologies have not been the densest for their interconnection degree. The search for (δ,D) graphs that connect the maximum number of nodes with a degree δ and diameter D continues [6]. Among these (δ,D) graphs, the degree-4 graphs (i.e., $\delta = 4$) receive special attention because of the realizability of degree-4 interconnections. The TRANSPUTER™ chips are examples of such connectability [13].

Amid the many interconnection models, a special class of symmetric graphs, Cayley graphs, is an attractive candidate [1], [14], [15]. Besides their symmetric property, Cayley

*Received by the editors August 1, 1992; accepted for publication November 19, 1992.
†Department of Electrical Engineering, State University of New York at Stony Brook, Stony Brook, New York 11794-2350.
‡Department of Electrical Engineering, University of Rochester, Rochester, New York 14627.

graphs from the Borel subgroup, *Borel Cayley graphs* for short, are the densest known degree-4 graphs for a range of diameters ($D = 7, \ldots, 13$) [1]. In other words, these degree-4 graphs interconnect the largest number of nodes for this degree and range of diameter ($D = 7, \ldots, 13$), thus potentially minimizing communication delay in a parallel computer. However, practical implementation of these graphs as an interconnection model in a multicomputer system is hampered by the lack of a systematic *representation* or *structure* of Borel Cayley graphs. Originally, Borel Cayley graphs are defined over a group of matrices, which has no simple ordering and hence no regular graph structure. This representation problem of Borel Cayley graphs makes the development of routing algorithms difficult.

Generalized chordal rings (GCR) [12] and the more specialized *chordal rings* (CR) [10], on the other hand, are two existing topologies that are defined in the integer domain and have a systematic and regular structure. The definitions and properties of GCR and CR graphs are reviewed in the next section. In an earlier report, we proved that *any* Cayley graph can be represented as GCRs and provided a sufficient condition for Cayley graphs to have CR representations [2]. This paper concentrates on degree-4 *Borel Cayley graphs*. We present another interesting result concerning the representations of these graphs. Namely, *all* degree-4 Borel Cayley graphs have the more restrictive CR representations, in addition to other GCR representations. A CR is a special case of a GCR. It includes a Hamiltonian cycle formed by edges connecting adjacent integers in the modulo n labels, thus permitting a *distance-reduction* routing algorithm, called *CR routing*. Given a degree-4 Borel Cayley graph with $n = pk$ nodes, where p is a prime number and $k < p$, is a factor of $p - 1$, this distance-reduction algorithm requires a small table of $O(k)$. However, the algorithm is *suboptimal* in the sense that a shortest path is not guaranteed. Simulation shows that a more dynamic approach produces pathlength closer to optimal. The details of CR routing, its simulation, and other routing algorithms are discussed in other papers [16]–[18].

This paper is organized as follows. In §2 we review the definitions of GCRs, CRs, Cayley graphs, and Borel Cayley graphs. The proposition that all Cayley graphs have GCR representations and the sufficient condition for a Cayley graph to have a CR representation are also restated. In §3 we prove that all degree-4 Borel Cayley graphs have CR representations. Section 4 includes three examples to illustrate the transformation of degree-4 Borel Cayley graphs to CRs. Finally, in §5 we present a summary and conclusions.

2. Review. In this section, we review the definitions of GCRs, CRs, Cayley graphs in general, and Borel Cayley graphs in particular. We begin with the definition of GCR.

DEFINITION 1. A graph $\mathbf{R}$ is a GCR if nodes of $\mathbf{R}$ can be labeled with integers mod n (the number of nodes) and if there is a divisor q of n such that node i is connected to node j if and only if node $i + q \pmod{n}$ is connected to node $j + q \pmod{n}$.

According to this definition, vertices of a GCR are classified into q classes, each class with n/q elements. The classification is based on modulo q arithmetic. Two vertices having the same residue (mod q) are considered to be in the same class. That is, class i consists of the following nodes: $i,\ i + q,\ i + 2q,\ \ldots,\ i + (m - 1)q \pmod{n}$, where $m = n/q$ and node i is the *representing element* of class i. Since i connects to j implies that $i + q$ connects to $j + q \pmod{n}$, nodes in the same class have the same connection rules defined by the *connection constants* or *GCR constants*. When the GCR constants for the different classes are known, connections of the entire graph are defined.

For example, Fig. 1 shows a degree-4 GCR with ten nodes and $q = 2$ classes. The connection rules for these classes can be defined as follows: Let $\mathbf{V} = \{0, 1, \ldots, 9\}$. For

any $i \in \mathbf{V}$, if

$$\begin{aligned} i \bmod 2 =: \text{“0”} &: i \text{ is connected to } i+2, i+3, i-1, i-2 \pmod{10}; \\ =: \text{“1”} &: i \text{ is connected to } i+1, i+4, i-4, i-3 \pmod{10}. \end{aligned}$$

In this case, the vertices of the graph are numbered from 0 to 9 and are divided into even and odd classes. For the even vertices, the connection constants are $+2$, $+3$, -1, and -2, and, for the odd vertices, the connection constants are $+1$, $+4$, -4, and -3. The addition of these connection constants to the node label is done in modulo n arithmetic.

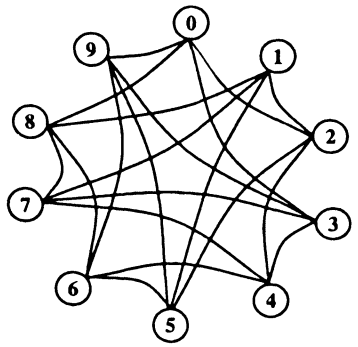

FIG. 1. *A degree-4* GCR ($n = 10$, $q = 2$).

This class-structure of a GCR provides a *regular structure* and a *concise* and *simple* way of describing connectivity in the integer domain, therefore making GCR an attractive representation.

A CR is a special case of GCR, in which every node has $+1$ and -1 modulo n connections. In other words, a CR satisfies the connection condition in Definition 1, and, in addition, all the nodes on the peripheral of the ring are connected to form a Hamiltonian cycle.

Figure 2 shows a degree-4 CR with ten nodes and $q = 2$ classes. The connection rules for these classes can be defined as follows: Let $\mathbf{V} = \{0, 1, \ldots, 9\}$. For any $i \in \mathbf{V}$, if

$$\begin{aligned} i \bmod 2 =: \text{“0”} &: i \text{ is connected to } i+1, i-1, i+2, i-2 \pmod{10}; \\ =: \text{“1”} &: i \text{ is connected to } i+1, i-1, i+4, i-4 \pmod{10}. \end{aligned}$$

Note that every class has $+1$ and -1 as GCR constants and that nodes on the peripheral of the ring are connected.

The construction of Cayley graphs is described by finite (algebraic) group theory. Recall that a group (**V**, *) consists of a set **V**, which is closed under inversion, and a single law of composition *, also known as group multiplication. There also exists an identity element $I \in \mathbf{V}$. A group is finite if there is a finite number of elements in **V**.

DEFINITION 2. A graph $\mathbf{C} = (\mathbf{V}, \mathbf{G})$ is a Cayley graph with vertex set **V** if two nodes $v_1, v_2 \in \mathbf{V}$ are adjacent $\Leftrightarrow v_1 = v_2 * g$ for some $g \in \mathbf{G}$, where (**V**, *) is a finite group and $\mathbf{G} \subset \mathbf{V} \backslash \{I\}$. **G** is called the generator set of the graph and I is the identity element of the finite group (**V**, *).

The definition of a Cayley graph requires nodes to be elements in a group but does not specify a particular group. A class of Cayley graphs that contributes to the densest

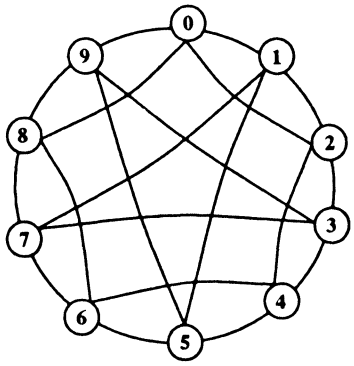

FIG. 2. *A degree-4* CR ($n = 10, q = 2$).

degree-4 graphs arises from a subgroup, the Borel subgroup $\mathbf{BL}_2(\mathbf{Z}_p)$, of the general linear 2×2 matrices $\mathbf{GL}_2(\mathbf{Z}_p)$. The definition of the Borel subgroup is as follows.

DEFINITION 3. If $\mathbf{V}$ is a Borel subgroup, $\mathbf{BL}_2(\mathbf{Z}_p)$, of $\mathbf{GL}_2(\mathbf{Z}_p)$, then

$$\mathbf{V} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x = a^t \pmod p,\ y \in \mathbf{Z}_p,\ t \in \mathbf{Z}_k \right\},$$

where a is a fixed parameter $\in \mathbf{Z}_p \backslash \{0, 1\}$, p is prime, and k is the order of a. That is, $a^k = 1 \pmod p$, and k is a factor of $p - 1$.

Thus, the nodes of Borel Cayley graphs are 2×2 matrices that satisfy the definition of a Borel subgroup, and modular matrix multiplication is chosen as the group operation *. Note that the variables of a Borel matrix are $t \in \mathbf{Z}_k$ and $y \in \mathbf{Z}_p$. In other words, there are $n = \mid \mathbf{V} \mid = p \times k$ nodes. By choosing specific generators, Chudnovsky, Chudnovsky, and Denneau [1] constructed the densest, nonrandom ($\delta = 4, D$) graphs known for $D = 7, \ldots, 13$ from Borel Cayley graphs (Table 1). In a separate research effort, Dinneen [20] and Campbell et al. [21] have constructed small diameter symmetric networks from Cayley graphs formed by linear groups. Interestingly, for the cases of $\delta = 4, D = 7, \ldots, 13$, these graphs have the same number of nodes as the Borel Cayley graphs in Table 1. Our investigation [22] showed that the Borel group can be formulated as a special case of the linear group described in [20].

TABLE 1
Comparisons of degree-4 graphs.

Diameter	Borel Cayley graphs	Moore bound	Known graphs (1987)
7	1,081	4,371	856
8	2,943	13,119	1,872
9	7,439	39,363	4,352
10	15,657	118,095	13,056
11	41,831	354,291	–
12	82,901	1,062,879	–
13	140,607	3,118,643	–

The *Moore bound* shown in Table 1 is an upper bound for the number of nodes in a degree-4 graph with diameter D. By arranging the nodes of a graph as a tree, the Moore bound shows that

$$n \leq 1 + \delta + \delta(\delta - 1) + \cdots + \delta(\delta - 1)^{D-1} = \frac{\delta(\delta - 1)^D - 2}{\delta - 2}.$$

Graphs attaining this Moore bound are called *Moore graphs* and are the densest possible for that degree and diameter. However, Moore graphs have been proved to be nonexistent except for some trivial cases. Specfically, these include complete graphs ($D = 1$) and rings ($\delta = 2$). Otherwise, it has been shown that Moore graphs exist only for diameter equals 2, degree equals 3, the Peterson graph, or diameter equals 2, degree equals 7, the Hoffman–Singleton graph, and possibly for diameter equals 2, degree 57 [12]. Given this general impossibility of constructing Moore graphs, there has been a long-standing search to find the densest regular graphs of a given degree and diameter. It is also worth noting that the Borel Cayley graph discovered by Chudnovsky, Chudnovsky, and Denneau [1] with $D = 11$, $\delta = 4$ has $n = 38,764$. In our research, we have discovered yet another denser Borel Cayley graph with $n = 41,831$ for $D = 11$, $\delta = 4$.

However, useful representations of Borel Cayley graphs are a challenge. These graphs are defined over a group of matrices, which lack a simple ordering that is very helpful in the development of efficient routing schemes. Furthermore, in this original matrix definition, there is no concise description of connections. Adjacent nodes can be identified only through modular matrix multiplications. The problem of finding an optimal path between nonadjacent nodes is not trivial. In an earlier report, we proved that all Cayley graphs can be represented by GCR [2]. This GCR representation is useful for routing because nodes are defined in the integer domain and there is a systematic description of connections. Different time and space efficient routing algorithms are devised for Borel Cayley graphs as a result of their GCR representations [16]–[18].

We restate this proposition as follows.

PROPOSITION 1. *For any finite Cayley graph* $\mathbf{C}$ *with vertex set* $\mathbf{V}$ *and any* $T \in \mathbf{V}$ *such that* $T^m = I$, *there exists a GCR representation of* $\mathbf{C}$ *with divisor* $q = n/m$, *where* $n = |\ \mathbf{V}\ |$.

The proof of this proposition is included in [2] and not repeated here. In the course of proving this proposition, we have constructed a step-by-step algorithm to transform any Cayley graph into a GCR. This algorithm is summarized in Table 2. The element T is referred to as the transform element, and it can be any element in the vertex set. In other words, this transformation is not unique. In the next section, we show that, by choosing a specific transform element $\mathbf{T}$ and class representing elements a_i (Table 2), all degree-4 Borel Cayley graphs have CR representations.

TABLE 2
An algorithm to generate a GCR representation.

To generate a GCR with divisor q,
choose an element T in $\mathbf{V}$ where $T^m = I$ and $m = n/q$.
For any element a in $\mathbf{V}$, define $\mathbf{N}(a)$ as
$\mathbf{N}(a) = \{x \in \mathbf{V}\colon x = T^s a\} \quad s = 0, 1, \ldots, (m-1)$

1. Construct $\mathbf{N}(a_i)$, $i = 0, \ldots, (q-1)$ by picking arbitrary $a_i \in V \setminus \mathbf{N}(a_0) \setminus \ldots \setminus \mathbf{N}(a_{i-1})$; $a_0, a_1, \ldots, a_{q-1}$ are the representative elements in partitions $\mathbf{N}(a_0), \mathbf{N}(a_1), \ldots, \mathbf{N}(a_{q-1})$.
2. Associate $a_i \rightarrow i, \quad i = 0, 1, \ldots, (q-1)$ and $T^s a_i \rightarrow i + sq$, $s = 0, \ldots, (m-1)$. This forms the q classes of the GCR.
3. Obtain the connecting constant for each class:
   For each class i of the GCR, find the neighboring nodes of the representing element, a_i.
   e.g., if a_i is adjacent to a node, $b = T^s a_j$,
   then any node w in class i is connected to $w + j + sq - i$.

In [2] we also provided a sufficient condition for a Cayley graph to have a CR representation. For convenience, we restate this proposition as follows.

PROPOSITION 2. *Let A, B be two distinct generators of a finite Cayley graph* **C**. *Assume that* $A \neq B^{-1}$, $A^q = I$, *and* $m = n/q$. *If* $(AB)^m = I$ *or* $(A^{-1}B)^m = I$, *then CR representations with divisor q exist. The transform element* $T = AB$ *or* $A^{-1}B$ *and the representing element of class* 0 *is I and of class i is* A^i, $i = 1, \ldots, q-1$.

3. CR representations. In this section, we show that all connected degree-4 Borel Cayley graphs have CR representations. During our studies of Borel Cayley graphs, we discovered some useful properties of the subgroup. These properties and their proofs are presented here. Throughout this section, we assume a *connected* degree-4 Borel Cayley graph with n nodes and parameters a, p, and k, as defined in Definition 3, and generators $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}^{-1}$, and $\mathbf{B}^{-1}$, where

$$\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}.$$

Furthermore, the order of $\mathbf{A}$ and $\mathbf{B}$ are k_1 and k_2, where $k_1, k_2 \in \mathbf{Z}_k$.

PROPOSITION 3. *Let*

$$\mathbf{X} = \begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix} \in \mathbf{BL}_2(\mathbf{Z}_p)$$

and $\mathbf{X} \neq \mathbf{I}$ *be a Borel matrix, as defined in Definition* 3. *If q is the order of* $\mathbf{X}$, *i.e., q is the smallest positive integer such that* $\mathbf{X}^q = \mathbf{I}$, *then*

$$q = \begin{cases} \dfrac{\mathrm{LCM}(t,k)}{t} & \text{if } t \neq 0, \\ p & \text{if } t = 0, \end{cases}$$

where LCM(*t,k*) *denotes the least common multiple of t and k.*

Proof. We have

$$\mathbf{X}^q = \begin{pmatrix} a^{qt} & (a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0)y \\ 0 & 1 \end{pmatrix},$$

$$\mathbf{X}^q = \mathbf{I} \Rightarrow \begin{cases} qt = 0 \pmod k \text{ and } (a^{(q-1)t} + a^{(q-2)t} + \ldots + a^0) = 0 \pmod p \\ \text{or} \\ qt = 0 \pmod k \text{ and } y = 0. \end{cases}$$

Case 1. $t \neq 0$. In this case,

$$(a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0) = 0 \pmod p \Rightarrow qt = 0 \pmod k$$

because

$$\begin{aligned} & (a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0) = 0 && \pmod p \\ \Rightarrow\ & (a^t - 1)(a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0) = 0 && \pmod p \\ \Rightarrow\ & a^{qt} - 1 = 0 && \pmod p \\ \Rightarrow\ & qt = 0 && \pmod k. \end{aligned}$$

Hence

$$\begin{aligned} \mathbf{X}^q = \mathbf{I} &\Rightarrow qt = 0 \pmod k \\ &\Rightarrow q = \frac{\mathrm{LCM}\,(t,k)}{t}. \end{aligned}$$

Case 2. $t = 0$. In this case, $y \neq 0$; otherwise $\mathbf{X} = \mathbf{I}$. Hence

$$\mathbf{X}^q = \mathbf{I} \Rightarrow \begin{cases} qt = 0 & (\text{mod } k) \quad \text{and} \\ (a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0) = 0 & (\text{mod } p), \end{cases}$$

$$\begin{aligned} & (a^{(q-1)t} + a^{(q-2)t} + \cdots + a^0) = 0 \quad (\text{mod } p) \\ \Rightarrow \quad & q = 0 \quad (\text{mod } p) \\ \Rightarrow \quad & q = p. \qquad \square \end{aligned}$$

PROPOSITION 4. *We have*

$$\mathbf{B} \neq \mathbf{A}^m \quad \textit{for any integer } m \in \mathbf{Z}_k.$$

Proof. If $\mathbf{B} = \mathbf{A}^m$, the generators of the graph are $\mathbf{A}, \mathbf{A}^m, \mathbf{A}^{k_1-1}, \mathbf{A}^{k_1-m}$, which implies that all nodes in the graph can be written as multiples of $\mathbf{A}$. This means that some nodes in the graph are not connected because there are at most $k_1 < n$ different multiples of $\mathbf{A}$. $\square$

PROPOSITION 5. *We have*

$$(1) \qquad (1 - a^{t_2})y_1 = (1 - a^{t_1})y_2 \quad (\text{mod } p) \Leftrightarrow \mathbf{AB} = \mathbf{BA}.$$

The proof of this proposition is a straightforward substitution and is omitted.

PROPOSITION 6. *If* $\mathbf{AB} = \mathbf{BA}$, *then, for any path* $\mathbf{X}$ *with* m_1 *as the net number of generator* $\mathbf{A}$ *and with* m_2 *as the net number of generator* $\mathbf{B}$,

$$\mathbf{X} = \mathbf{A}^{m_1}\,\mathbf{B}^{m_2},$$

where

$$\begin{aligned} m_1 &= \textit{number of } \mathbf{A} - \textit{number of } \mathbf{A}^{-1} \quad (\text{mod } k_1), \\ m_2 &= \textit{number of } \mathbf{B} - \textit{number of } \mathbf{B}^{-1} \quad (\text{mod } k_2). \end{aligned}$$

Proof. Since $\mathbf{A}^{-1} = \mathbf{A}^{k_1-1}$ and $\mathbf{B}^{-1} = \mathbf{B}^{k_2-1}$, it suffices to consider paths composed of generators $\mathbf{A}$ and $\mathbf{B}$ only. We use mathematical induction to prove this proposition.

If $m_1 = m_2 = 1$, $\mathbf{AB} = \mathbf{BA}$. Obviously, the proposition also holds for $m_1 = 1, m_2 = 0$ and $m_1 = 0, m_2 = 1$. Hence the proposition is true for $m_1 \leq 1$ and $m_2 \leq 1$.

Assume the proposition holds for $m_1 \leq m_1'$ and $m_2 \leq m_2'$ for some integers $m_1' \in \mathbf{Z}_{k_1}$ and $m_2' \in \mathbf{Z}_{k_2}$.

Consider $m_1 = m_1' + 1$ and $m_2 = m_2'$. There exists an integer $l = 0, \ldots, m_2'$ such that

$$\begin{aligned} \mathbf{X} &= \underbrace{\cdots\cdots}_{m_1'A,\ (m_2'-l)B}\ \mathbf{AB}^l \\ &= \mathbf{A}^{m_1'}\mathbf{B}^{m_2'-l}\mathbf{AB}^l \qquad \text{(by assumption)}. \end{aligned}$$

Furthermore, $\mathbf{B}^{m_2'-l}\mathbf{A} = \mathbf{AB}^{m_2'-l}$ by assumption. Hence

$$\mathbf{X} = \mathbf{A}^{m_1'+1}\,\mathbf{B}^{m_2'}.$$

Similarly, the proposition is true for $m_1 = m_1' + 1$ and $m_2 = m_2' + 1$. By the principle of mathematical induction, the proposition is true for all $m_1 \in \mathbf{Z}_{k_1}$ and $m_2 \in \mathbf{Z}_{k_2}$. □

Based on Propositions 5 and 6, we have three useful corollaries.

COROLLARY 1. *If* $\mathbf{AB} = \mathbf{BA}$, *then the graph is disconnected.*

Proof. If $\mathbf{AB} = \mathbf{BA}$, from Proposition 6, an element $\mathbf{X}$ in the graph is represented as

$$\mathbf{X} = \mathbf{I} \quad \text{or} \quad \mathbf{A}^{m_1} \quad \text{or} \quad \mathbf{B}^{m_2} \quad \text{or} \quad \mathbf{A}^{m_1}\mathbf{B}^{m_2},$$

where $m_1 = 1, \ldots, k_1 - 1$, $m_2 = 1, \ldots, k_2 - 1$. In other words, there are at most

$$1 + (k_1 - 1) + (k_2 - 1) + (k_1 - 1)(k_2 - 1) \leq 1 + 2(k - 1) + (k - 1)^2 = k^2$$

different $\mathbf{X}$. Since k is a factor of $p - 1$ (Definition 3),

$$n = p \times k > k^2,$$

which implies that some nodes of the graph cannot be generated by $\mathbf{A}$, $\mathbf{B}$, and hence the graph is disconnected. □

COROLLARY 2. *The values of* t_1 *and* t_2 *cannot be both zero.*

Proof. We have

$$\begin{aligned} & t_1 = t_2 = 0 \\ \Rightarrow \quad & (1 - a^{t_2})y_1 = (1 - a^{t_1})y_2 \\ \Leftrightarrow \quad & \mathbf{AB} = \mathbf{BA} \qquad \text{(by (1))}, \end{aligned}$$

which implies the graph is disconnected by Corollary 1. □

COROLLARY 3. *The values of* y_1 *and* y_2 *cannot be both zero.*

Proof. We have

$$\begin{aligned} & y_1 = y_2 = 0 \\ \Rightarrow \quad & (1 - a^{t_2})y_1 = (1 - a^{t_1})y_2 \\ \Leftrightarrow \quad & \mathbf{AB} = \mathbf{BA} \qquad \text{(by (1))}, \end{aligned}$$

which implies that the graph is disconnected by Corollary 1. □

PROPOSITION 7. *For any path* $\mathbf{X}$ *composed of generators* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}^{-1}$, *and* $\mathbf{B}^{-1}$,

$$\begin{aligned} \mathbf{X} &= \begin{pmatrix} a^{\langle it_1 + jt_2 \rangle_k} & \langle gy_1 + hy_2 \rangle_p \\ 0 & 1 \end{pmatrix} \\ \Rightarrow \quad & (1 - a^{t_1})g + (1 - a^{t_2})h = 1 - a^{it_1 + jt_2} \qquad (\text{mod } p), \end{aligned}$$

where $\langle x \rangle_k$ *denotes* x mod k.

Proof. We prove this proposition by induction on the length of the path. For the single step path $\mathbf{X} = \mathbf{A}$,

$$\begin{aligned} & i = 1, \qquad j = 0, \\ & g = 1, \qquad h = 0, \\ & (1 - a^{t_1})g = 1 - a^{t_1}. \end{aligned}$$

Therefore, the proposition holds. Similarly, the proposition holds for $\mathbf{X} = \mathbf{B}, \mathbf{A}^{-1}, \mathbf{B}^{-1}$.

Assume the proposition holds for some path $\mathbf{X}'$. That is,

$$\mathbf{X}' = \begin{pmatrix} a^{\langle i't_1 + j't_2\rangle_k} & \langle g'y_1 + h'y_2\rangle_p \\ 0 & 1 \end{pmatrix}$$

and

$$(1 - a^{t_1})g' + (1 - a^{t_2})h' = 1 - a^{i't_1 + j't_2} \qquad (\bmod p).$$

Consider the path

$$\mathbf{X}'\mathbf{A} = \begin{pmatrix} a^{\langle (i'+1)t_1 + j't_2\rangle_k} & \langle (g' + a^{i't_1 + j't_2})y_1 + h'y_2\rangle_p \\ 0 & 1 \end{pmatrix};$$

$$\begin{aligned} &(1 - a^{t_1})(g' + a^{i't_1 + j't_2}) + (1 - a^{t_2})h' \qquad (\bmod p) \\ &= (1 - a^{t_1})g' + (1 - a^{t_2})h' + (1 - a^{t_1})a^{i't_1 + j't_2} \qquad (\bmod p) \\ &= 1 - a^{i't_1 + j't_2} + (1 - a^{t_1})a^{i't_1 + j't_2} \qquad (\bmod p) \quad \text{(by assumption)} \\ &= 1 - a^{(i'+1)t_1 + j't_2} \qquad (\bmod p). \end{aligned}$$

That is, the proposition holds for $\mathbf{X}'\mathbf{A}$. Similarly, the proposition is true for $\mathbf{X}'\mathbf{A}^{-1}$, $\mathbf{X}'\mathbf{B}, \mathbf{X}'\mathbf{B}^{-1}$. By the principle of mathematical induction, the proposition is true for any path $\mathbf{X}$. □

PROPOSITION 8. *For any paths* $\mathbf{X}$, $\mathbf{Y}$, *composed of generators* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}^{-1}$, *and* $\mathbf{B}^{-1}$, *let*

$$\mathbf{X} = \begin{pmatrix} a^{\langle it_1 + jt_2\rangle_k} & \langle gy_1 + hy_2\rangle_p \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad \mathbf{Y} = \begin{pmatrix} a^{\langle i't_1 + j't_2\rangle_k} & \langle g'y_1 + h'y_2\rangle_p \\ 0 & 1 \end{pmatrix},$$

where $\langle x\rangle_p$ *denotes* $x \pmod p$. *Then*

$$\begin{aligned} &\mathbf{X} = \mathbf{Y} \\ \Leftrightarrow\ &it_1 + jt_2 = i't_1 + j't_2 \qquad (\bmod k) \end{aligned}$$

and

$$\begin{cases} g = g' \textit{and } h = h' \qquad (\bmod p) \quad \textit{or} \\ (1 - a^{t_2})y_1 = (1 - a^{t_1})y_2 \qquad (\bmod p). \end{cases}$$

Proof. Since

$$\begin{aligned} \mathbf{X} &= \begin{pmatrix} a^{\langle it_1 + jt_2\rangle_k} & \langle gy_1 + hy_2\rangle_p \\ 0 & 1 \end{pmatrix}, \\ \mathbf{Y} &= \begin{pmatrix} a^{\langle i't_1 + j't_2\rangle_k} & \langle g'y_1 + h'y_2\rangle_p \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

from Proposition 7,

$$\begin{aligned} (1 - a^{t_1})g + (1 - a^{t_2})h &= 1 - a^{it_1 + jt_2} \qquad (\bmod p), \\ (1 - a^{t_1})g' + (1 - a^{t_2})h' &= 1 - a^{i't_1 + j't_2} \qquad (\bmod p) \end{aligned} \tag{2}$$

($\Rightarrow$)

$$\begin{aligned} & \mathbf{X} = \mathbf{Y} \\ \Rightarrow \quad & it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \\ \Rightarrow \quad & (1-a^{t_1})g + (1-a^{t_2})h = (1-a^{t_1})g' + (1-a^{t_2})h' \pmod{p} \quad \text{from (2)} \\ \Rightarrow \quad & (1-a^{t_1})(g-g') = (1-a^{t_2})(h'-h) \pmod{p} \end{aligned} \tag{3}$$

Also,

$$\begin{aligned} & \mathbf{X} = \mathbf{Y} \\ \Rightarrow \quad & gy_1 + hy_2 = g'y_1 + h'y_2 \pmod{p} \\ \Rightarrow \quad & (g-g')y_1 = (h'-h)y_2 \pmod{p}. \end{aligned} \tag{4}$$

From (3) and (4), we have

$$\begin{aligned} & (1-a^{t_2})y_1 = (1-a^{t_1})y_2 \pmod{p} \quad \text{or} \\ & g = g' \quad \text{and} \quad h = h' \pmod{p}. \end{aligned}$$

($\Leftarrow$) Obviously,

$$\left.\begin{aligned} & it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \\ & g = g' \quad \text{and} \quad h = h' \pmod{p} \end{aligned}\right\} \Rightarrow \mathbf{X} = \mathbf{Y}.$$

On the other hand, from (2),

$$\begin{aligned} & it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \\ \Rightarrow \quad & (1-a^{t_1})g + (1-a^{t_2})h = (1-a^{t_1})g' + (1-a^{t_2})h' \pmod{p}. \end{aligned}$$

Since $(1-a^{t_2})y_1 = (1-a^{t_1})y_2 \pmod{p}$ and from Corollaries 2 and 3, t_1, t_2 and y_1, y_2 are not both zero, we have

$$\begin{aligned} & (1-a^{t_2})y_1(1-a^{t_1})g + (1-a^{t_1})y_2(1-a^{t_2})h \\ = \quad & (1-a^{t_2})y_1(1-a^{t_1})g' + (1-a^{t_1})y_2(1-a^{t_2})h' \pmod{p} \\ \Rightarrow \quad & gy_1 + hy_2 = g'y_1 + h'y_2 \pmod{p} \\ \Rightarrow \quad & \mathbf{X} = \mathbf{Y}. \quad \square \end{aligned}$$

COROLLARY 4. *Let* $\mathbf{X}$, $\mathbf{Y}$ *be defined as in Proposition* 8. *For a connected degree-*4 *Borel Cayley graph*,

$$\mathbf{X} = \mathbf{Y} \Leftrightarrow \begin{cases} it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \quad \textit{and} \\ g = g' \textit{ and } h = h' \pmod{p}. \end{cases}$$

Proof. From Proposition 8,

$$\begin{aligned} & \mathbf{X} = \mathbf{Y} \\ \Leftrightarrow \quad & it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \end{aligned}$$

and

$$\begin{aligned} & g = g' \text{ and } h = h' \pmod{p} \quad \text{or} \\ & (1-a^{t_2})y_1 = (1-a^{t_1})y_2 \pmod{p}. \end{aligned}$$

However, from Proposition 5 and Corollary 1,

$$(1 - a^{t_2})y_1 = (1 - a^{t_1})y_2 \pmod{p} \Leftrightarrow \mathbf{AB} = \mathbf{BA} \Rightarrow \text{the graph is disconnected.}$$

Hence, for a connected degree-4 Borel Cayley graph,

$$\mathbf{X} = \mathbf{Y} \Leftrightarrow \begin{cases} it_1 + jt_2 = i't_1 + j't_2 \pmod{k} \text{ and} \\ g = g' \text{ and } h = h' \pmod{p}. \end{cases} \quad \square$$

With the above propositions and corollaries, we are now ready to state the main result of this paper.

PROPOSITION 9. *All connected degree-4 Borel Cayley graphs have CR representations.*

Proof. We consider three cases. In the first two cases, the idea of the proof is to construct a specific GCR with $q = k$ classes. We choose the transform element

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}, \qquad y' \neq 0,$$

and the representing element of class j to be

$$a_j = \begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix},$$

where $i,\ j = 0, \ldots, k-1$, $\bar{y}_j \in \mathbf{Z}_p$ and no two classes have the same value for i. These choices ensure that any Borel matrix element

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}$$

can be classified by the value t. Furthermore, if we can choose the class representing elements such that

$$a_0 \sim a_1 \sim \cdots \sim a_{k-1} \sim \mathbf{T} * a_0$$

(the symbol $\sim$ denotes adjacency), we have a CR representation.

For the third case, we prove that the sufficient condition in Proposition 2 is satisfied and hence a CR representation.

Case 1. $t_1, t_2 \neq 0$ and either $(t_1, k) = 1$ or $(t_2, k) = 1$. Without loss of generality, we assume that $(t_1, k) = 1$, (t_1 and k are relatively prime). In other words, multiples of $t_1 \pmod{k}$ span the set $\{1, \ldots, (k-1)\}$. Since $t_2 \in \{1, \ldots, (k-1)\}$, we have

$$m\, t_1 = t_2 \pmod{k} \qquad \text{for some } m = 1, \ldots, (k-1).$$

We consider a GCR with

$$\mathbf{T} = \mathbf{B}\mathbf{A}^{k-1-m}\mathbf{B}(\mathbf{A}^{-1})^{m-1}. \tag{5}$$

Claim. It holds that

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$$

for some $y' \in \mathbf{Z}_p$ and $y' \neq 0$.

Proof. Note that the superscript t of the first element of any matrix

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}$$

can be found by counting the net number of generators **A** and **B** that composed the matrix. As an example, for matrix $\mathbf{X} = \mathbf{AB}$, its t value is $t_1 + t_2 \pmod{k}$. Counting the net number of generators **A** and **B** in (5),

$$t_2 + (k - 1 - m)t_1 + t_2 + (m - 1)(k - t_1) = 0 \qquad (\text{mod } k).$$

Hence the first element of **T** is 1. We proceed to prove that $\mathbf{T} \neq \mathbf{I}$. Since $mt_1 = t_2 \pmod{k}$, we let $\mathbf{B} = \mathbf{HA}^m$, where $\mathbf{H} = \left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ for some $z \in Z_p$ and $z \neq 0$ because $\mathbf{B} \neq \mathbf{A}^m$ as stated in Proposition 4,

$$\begin{aligned}
\mathbf{T} = \mathbf{I} \Rightarrow \quad & \mathbf{BA}^{k-1-m}\mathbf{B} = \mathbf{A}^{m-1} \\
\Rightarrow \quad & \mathbf{HA}^m\mathbf{A}^{k-1-m}\mathbf{HA}^m = \mathbf{A}^{m-1} \\
\Rightarrow \quad & \mathbf{HA}^{-1}\mathbf{H} = \mathbf{A}^{-1} \\
\Rightarrow \quad & \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix}, \qquad z' = \langle -a^{-t_1}y_1 \rangle_p \\
\Rightarrow \quad & \begin{pmatrix} a^{k-t_1} & (a^{k-t_1}+1)z + z' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix} \\
\Rightarrow \quad & (a^{k-t_1} + 1)z = 0 \qquad (\text{mod } p) \\
\Rightarrow \quad & a^{k-t_1} = -1 \qquad (\text{mod } p) \\
\Rightarrow \quad & 2(k - t_1) = 0 \qquad (\text{mod } k) \\
\Rightarrow \quad & (t_1, k) \neq 1 \qquad (\text{a contradiction}).
\end{aligned}$$

Hence $\mathbf{T} \neq \mathbf{I}$. According to Proposition 3,

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix} \Rightarrow \mathbf{T}^p = \mathbf{I}.$$

We can construct a GCR with divisor $q = k$ and choose the representing elements according to (5). That is, the representing element of class j, a_j is the composition of the first j elements in (5). Specifically,

$$\begin{aligned}
a_0 &= \mathbf{I}; \\
a_1 &= \mathbf{B}; \\
a_2 &= \mathbf{BA}; \\
&\vdots \\
a_{q-m} &= \mathbf{B}\,\mathbf{A}^{k-1-m}; \\
a_{q-m+1} &= \mathbf{B}\,\mathbf{A}^{k-1-m}\,\mathbf{B}; \\
a_{q-m+2} &= \mathbf{B}\,\mathbf{A}^{k-1-m}\,\mathbf{B}\,\mathbf{A}^{-1}; \\
&\vdots \\
a_{q-1} &= \mathbf{B}\,\mathbf{A}^{k-1-m}\,\mathbf{B}\,(\mathbf{A}^{-1})^{m-2}.
\end{aligned}$$

Note that

$$\begin{aligned} a_0 &\sim a_1 = a_o * \mathbf{B};\\ a_1 &\sim a_2 = a_1 * \mathbf{A};\\ &\vdots\\ a_{q-2} &\sim a_{q-1} = a_{q-2} * \mathbf{A}^{-1};\\ a_{q-1} &\sim \mathbf{T} * a_0 = \mathbf{T} = a_{q-1} * \mathbf{A}^{-1}, \end{aligned}$$

where the symbol $\sim$ denotes adjacency. Furthermore, given

$$a_j = \begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix},$$

the i values for representing elements $a_0, \ldots, a_{q-1}$ are

$$0, m\,t_1,\ (m+1)\,t_1,\ \ldots,\ (k-1)\,t_1,\ (m-1)\,t_1,\ (m-2)\,t_1,\ \ldots,\ t_1,$$

where $t_2 = mt_1 \pmod{k}$. Since $(t_1, k) = 1$, these values of i span the entire set of $\{0, \ldots, k-1\}$. In other words, we have a CR representation.

An alternate way to construct a CR representation is to choose

$$\mathbf{T} = \mathbf{B}^{-1}(\mathbf{A}^{-1})^{k-1-m}\mathbf{B}^{-1}\mathbf{A}^{m-1}.$$

In this case,

$$\begin{aligned} a_0 &= \mathbf{I};\\ a_1 &= \mathbf{B}^{-1};\\ a_2 &= \mathbf{B}^{-1}\,\mathbf{A}^{-1};\\ &\vdots\\ a_{q-m} &= \mathbf{B}^{-1}\,(\mathbf{A}^{-1})^{k-1-m};\\ a_{q-m+1} &= \mathbf{B}^{-1}\,(\mathbf{A}^{-1})^{k-1-m}\,\mathbf{B}^{-1};\\ a_{q-m+2} &= \mathbf{B}^{-1}\,(\mathbf{A}^{-1})^{k-1-m}\,\mathbf{B}^{-1}\,\mathbf{A};\\ &\vdots\\ a_{q-1} &= \mathbf{B}^{-1}\,(\mathbf{A}^{-1})^{k-1-m}\,\mathbf{B}^{-1}\,\mathbf{A}^{m-2}. \end{aligned}$$

The proof of this construction is similar to the one shown above and is not repeated.

Case 2. $t_1, t_2 \neq 0$ and $(t_1, k) \neq 1$ and $(t_2, k) \neq 1$.

In this case, $(t_1, t_2) = 1$ (t_1 and t_2 are relatively prime) because otherwise the graph is disconnected. Furthermore, $t_1 k_1 = t_2 k_2 = k$. Since t_1 and t_2 are relatively prime, we can divide the set $\{0, \ldots, k-1\}$ into t_1 distinct subsets each with k_1 elements as follows:

$$\begin{gathered} \{0, t_1, \ldots, (k_1-1)t_1\},\\ \{t_2, t_2+t_1, \ldots, t_2+(k_1-1)t_1\},\\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots\\ \{(t_1-1)t_2, (t_1-1)t_2+t_1, \ldots, (t_1-1)t_2+(k_1-1)t_1\}. \end{gathered}$$

If each number in the above subsets represents the superscript i of a class representing element

$$a_j = \begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix},$$

where y_j is an integer in z_p, the corresponding class representing element within one subset (on the same row) can be cyclically connected by generator $\mathbf{A}$, and those on the same column can be connected, but not cyclically, by generator $\mathbf{B}$. As discussed at the outset of this proof, the idea is to construct a specific GCR by choosing the transform element

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}, \qquad y' \neq 0,$$

and the representing element of class j,

$$a_j = \begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix}$$

such that the superscript i spans the set $\{0, 1, \ldots, k-1\}$ and $a_0 \sim a_1 \sim \cdots \sim a_{k-1} \sim \mathbf{T} * a_0$, where the symbol $\sim$ denotes adjacency.

In this case, the problem of finding such choices for $\mathbf{T}$ and class representing elements $a_0, \ldots, a_{q-1}$ is the same as finding a Hamiltonian cycle to "march through" the k numbers in the subsets, starting from 0. There are two ways of constructing this Hamiltonian cycle, depending on whether t_1 is odd or even. Figures 3 and 4 show a Hamiltonian cycle for $t_1 = 2, 3$. In these cases, $\mathbf{T} = \mathbf{B}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-1}$ and $\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}\mathbf{A}$. The mathematical formulations of these two subcases are as follows.

Subcase 1. t_1 is odd. We define the integer $d = (t_1 - 1)/2$. In this case, we consider a GCR with

$$\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d\mathbf{A}. \tag{6}$$

Claim. It holds that

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$$

for some $y' \in \mathbf{Z}_p$ and $y' \neq 0$.

Proof. By counting the net numbers of $\mathbf{A}$ and $\mathbf{B}$ in (6),

$$(t_1 - 1)t_2 - t_1 + \frac{t_1 - 1}{2}(-t_2 + 2t_1 - t_2 - 2t_1) + t_1 = 0 \pmod{k},$$

the first element of $\mathbf{T}$ is 1. We proceed to prove that $\mathbf{T} \neq \mathbf{I}$. Let

$$\mathbf{T} = \mathbf{I},$$

$$\Rightarrow \begin{pmatrix} 1 & gy_1 + hy_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0y_1 + 0y_2 \\ 0 & 1 \end{pmatrix}, \tag{7}$$

where

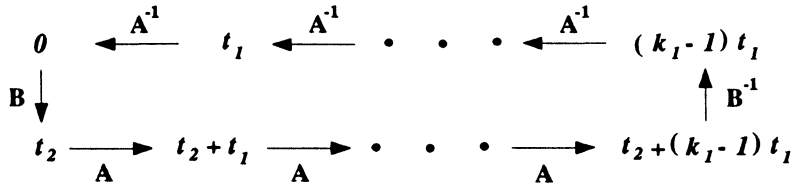

FIG. 3. *A Hamiltonian cycle for* $t_1 = 2$.

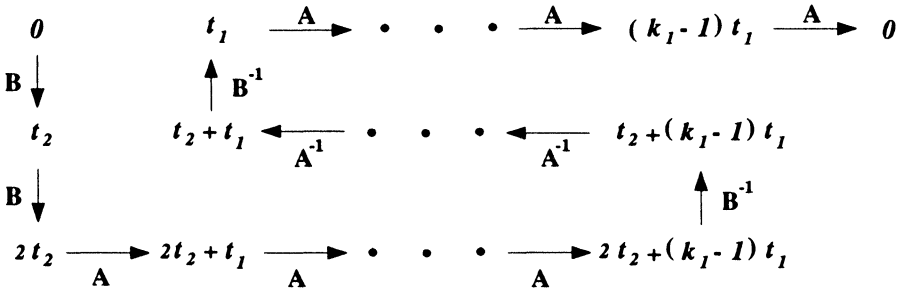

FIG. 4. *A Hamiltonian cycle for* $t_1 = 3$.

$$g = -a^{2dt_2-t_1} + \sum_{i=1}^{d}\{a^{(2i-1)t_2-t_1} + a^{(2i-1)t_2} - a^{2(i-1)t_2} - a^{2(i-1)t_2-t_1}\} + a^{-t_1} \pmod p, \tag{8}$$

$$h = \sum_{i=0}^{2d-1} a^{it_2} - \sum_{i=1}^{d}\{a^{(2i-1)t_2-t_1} + a^{2(i-1)t_2+t_1}\} \pmod p. \tag{9}$$

Equations (8) and (9) are obtained by observing that, from (6),

$$\begin{aligned}\mathbf{T} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d\mathbf{A} \\ &= \mathbf{B}^{2d}\mathbf{A}^{-1}\{\mathbf{B}^{-1}\mathbf{A}^2\mathbf{B}^{-1}\mathbf{A}^{-2}\}^d\mathbf{A},\end{aligned}$$

and, for any Borel matrix,

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{A} = \begin{pmatrix} a^{t+t_1} & \langle y + a^t y_1\rangle_p \\ 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{A}^{-1} = \begin{pmatrix} a^{t-t_1} & \langle y - a^{t-t_1} y_1\rangle_p \\ 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{B} = \begin{pmatrix} a^{t+t_2} & \langle y + a^t y_2\rangle_p \\ 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{B}^{-1} = \begin{pmatrix} a^{t-t_2} & \langle y - a^{t-t_2} y_2\rangle_p \\ 0 & 1 \end{pmatrix}.$$

Hence

$$\mathbf{B}^{2d} = \begin{pmatrix} a^{2dt_2} & \sum_{i=0}^{2d-1} a^{it_2} y_2 \\ 0 & 1 \end{pmatrix},$$

$$\mathbf{B}^{2d}\mathbf{A}^{-1} = \begin{pmatrix} a^{2dt_2-t_1} & \sum_{i=0}^{2d-1} a^{it_2} y_2 - a^{2dt_2-t_1} y_1 \\ 0 & 1 \end{pmatrix},$$

$$\mathbf{B}^{2d}\mathbf{A}^{-1}\mathbf{B}^{-1} = \begin{pmatrix} a^{(2d-1)t_2-t_1} & \left(\sum_{i=0}^{2d-1} a^{it_2} - a^{(2d-1)t_2-t_1}\right) y_2 - a^{2dt_2-t_1} y_1 \\ 0 & 1 \end{pmatrix},$$

$$\vdots$$

$$\mathbf{B}^{2d}\mathbf{A}^{-1}\{\mathbf{B}^{-1}\mathbf{A}^{2}\mathbf{B}^{-1}\mathbf{A}^{-2}\}^{d}\mathbf{A} = \begin{pmatrix} 1 & gy_1 + hy_2 \\ 0 & 1 \end{pmatrix},$$

where g and h are described by (8) and (9).

From (7) and Corollary 4, $g = h = 0 (\text{mod } p)$. That is,

$$\begin{aligned} & g = 0 \pmod p \\ \Rightarrow\ & a^{2dt_2-t_1} - a^{-t_1} = \sum_{i=1}^{d} \left\{ a^{(2i-1)t_2-t_1} - a^{2(i-1)t_2-t_1} \right\} \\ & \qquad + \sum_{i=1}^{d} \left\{ a^{(2i-1)t_2} - a^{2(i-1)t_2} \right\} \pmod p \qquad (10) \\ & \qquad = (a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2-t_1} + (a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p \\ & \qquad = (a^{-t_1}+1)(a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p. \end{aligned}$$

Similarly,

$$\begin{aligned} h = 0 \pmod p \Rightarrow \sum_{i=0}^{2d-1} a^{it_2} &= (a^{t_2-t_1} + a^{t_1}) \sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p \\ \Rightarrow \sum_{i=1}^{d} a^{2(i-1)t_2} &= (a^{t_2-t_1} + a^{t_1})^{-1} \sum_{i=0}^{2d-1} a^{it_2} \pmod p. \end{aligned} \qquad (11)$$

Using (10) and (11), we have

$$(a^{t_2-t_1}+a^{t_1})\,(a^{2dt_2-t_1}-a^{-t_1}) = (a^{-t_1}+1)\,(a^{t_2}-1)\sum_{i=0}^{2d-1} a^{it_2} \qquad (\mathrm{mod}\ p)$$

$$\Rightarrow\quad a^{(2d+1)t_2-2t_1}-a^{t_2-2t_1}+a^{2dt_2}-1 = (a^{t_2-t_1}-a^{-t_1}+a^{t_2}-1)\sum_{i=0}^{2d-1} a^{it_2}$$

$$= \sum_{i=0}^{2d-1}\{a^{(i+1)t_2-t_1}-a^{it_2-t_1}+a^{(i+1)t_2}-a^{it_2}\}$$

$$= (a^{-t_1}+1)(a^{2dt_2}-1)$$

$$= 2^{2dt_2-t_1}-a^{-t_1}+a^{2dt_2}-1$$

$$\Rightarrow\quad a^{(2d+1)t_2-t_1}-a^{t_2-t_1} = a^{2dt_2}-1$$

$$\Rightarrow\quad a^{t_2-t_1}(a^{2dt_2}-1) = a^{2dt_2}-1$$

$$\Rightarrow\quad (a^{t_2-t_1}-1)(a^{(t_1-1)t_2}-1) = 0 \qquad \text{(because } 2d=t_1-1\text{)}.$$

That is, $\mathbf{T}=\mathbf{I}\Rightarrow t_1=t_2$ or $t_1=1$ or $t_2=0$, which contradict $(t_1,t_2)=1$, $(t_1,k)\neq 1$, and $t_1,t_2\neq 0$. Hence $\mathbf{T}\neq\mathbf{I}$. Similar to Case 1, we can now construct a GCR with divisor $q=k$ and choose the representing elements according to (6). That is, the representing element of class j is the composition of the first j elements in (6). Specifically,

$$\begin{aligned}
a_0 &= \mathbf{I};\\
a_1 &= \mathbf{B};\\
a_2 &= \mathbf{B}^2;\\
&\vdots\\
a_{t_1-1} &= \mathbf{B}^{t_1-1};\\
a_{t_1} &= \mathbf{B}^{t_1-1}\mathbf{A};\\
a_{t_1+1} &= \mathbf{B}^{t_1-1}\mathbf{A}^2;\\
&\vdots\\
a_{t_1+k_1-2} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1};\\
a_{t_1+k_1-1} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1};\\
a_{t_1+k_1} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}\mathbf{A}^{-1};\\
a_{t_1+k_1+1} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}(\mathbf{A}^{-1})^2;\\
&\vdots\\
a_{q-1} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d.
\end{aligned}$$

Again, we assume that the representing element of class j is

$$\begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix}.$$

With these choices, the superscript i spans the set of $\{0,1,\ldots,k-1\}$. Furthermore, the following representing elements are connected to each other: $a_0\sim a_1\sim\cdots\sim a_{q-1}\sim \mathbf{T}*a_0$. Hence we have a CR representation.

Subcase 2. t_1 is even. We define the integer $d=(t_1/2)-1$. In this case, we consider a GCR with

$$\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-1}. \tag{12}$$

Again, using similar techniques as in Subcase 1, we can prove that

$$\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$$

for some $y' \in \mathbf{Z}_p$ and $y' \neq 0$. A GCR with divisor $q = k$ can then be constructed with class representing elements, $a_o, a_1, \ldots, a_{q-1}$, determined from the composition of the first j elements in (12). That is,

$$\begin{aligned} a_0 &= \mathbf{I}; \\ a_1 &= \mathbf{B}; \\ a_2 &= \mathbf{B}^2; \\ &\vdots \\ a_{q-1} &= \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}. \end{aligned}$$

As before, the superscripts of the first element of all class representing elements span the set of $\{0, 1, \ldots, k-1\}$. Also, the representing elements are connected to each other: $a_0 \sim a_1 \sim \cdots \sim a_{q-1} \sim \mathbf{T} * a_0$. Hence we have a CR representation.

Case 3. $t_1 = 0$ In this case, we can assume that $(t_2, k) = 1$ (t_2 and k are relatively prime); otherwise the graph is disconnected. According to Proposition 3, $t_1 = 0 \Rightarrow \mathbf{A}^p = \mathbf{I}$. Consider

$$\mathbf{A}^{-1}\mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 - y_1 \\ 0 & 1 \end{pmatrix},$$

$$(\mathbf{A}^{-1}\mathbf{B})^m = \mathbf{I} \Rightarrow m = \frac{\text{LCM}\,(t_2, k)}{t_2} = k.$$

Hence $m = n/p = k = \text{LCM}\,(t_2, k)/t_2$. According to the sufficient condition in Proposition 2, we choose $\mathbf{T} = \mathbf{A}^{-1}\mathbf{B}$ and the representing element of class i, $a_i = \mathbf{A}^i$ $(i = 0, \ldots, p-1)$ to construct a CR representation with divisor $q = p$. □

In the above proposition, we proved that all degree-4 Borel Cayley graphs have CR representations. In the course of proving the proposition, we provided an algorithm for the construction of a CR representation. This algorithm is summarized in Table 3. For simplicity, Table 3 only shows one possible way of constructing a CR representation in Case 1, even though an alternate way exists.

4. Examples. In this section, we use three examples to illustrate the three cases discussed in the constructive proof of CR representations (§3). Again, we assume a degree-4 Borel Cayley graph with parameters n, p, a, k as defined in Definition 3. Furthermore, $n = p \times k$ and $\mathbf{A}, \mathbf{B}, \mathbf{A}^{-1}, \mathbf{B}^{-1}$ are the generators, where

$$\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix},$$

$t_1, t_2 \in \{0, \ldots, k-1\}$, and $y_1, y_2 \in \{0, \ldots, p-1\}$.

TABLE 3
An algorithm to generate a CR *representation.*

For any degree-4 Borel Cayley graph with $n = |\mathbf{V}| = p \times k$, assume $\mathbf{A}$, $\mathbf{B}$, and their inverses are generators

$$\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}.$$

In each of the following cases, we construct a CR representation with divisor q, by following the procedure summarized in Table 2. Instead of using arbitrary transform element and class representing elements, we have specific choices.

Case 1. $t_1, t_2 \neq 0$ and $(t_1, k) = 1$.
Assume $t_2 = mt_1$ for some integer m;

$$\mathbf{T} = \mathbf{B}\,\mathbf{A}^{k-1-m}\,\mathbf{B}\,(\mathbf{A}^{-1})^{m-1}.$$

The representing element of class 0 is $\mathbf{I}$ and of class j is the composition of the first j elements in the above equation. With these choices, there are $q = k$ classes.

Case 2. $t_1, t_2 \neq 0$ and $(t_1, k) \neq 1$ and $(t_2, k) \neq 1$. Assume $\mathbf{A}^{k_1} = \mathbf{I}$
Subcase 1. t_1 is odd, let $d = (t_1 - 1)/2$;

$$\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^{d}\mathbf{A}.$$

The representing element of class 0 is $\mathbf{I}$ and of class j is the composition of the first j elements in the above equation. With these choices, there are $q = k$ classes.

Subcase 2. t_1 is even, let $d = t_1/2 - 1$;

$$\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^{d}\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-1}.$$

The representing element of class 0 is $\mathbf{I}$ and of class j is the composition of the first j elements in the above equation. With these choices, there are $q = k$ classes.

Case 3. $t_1 = 0$.
In this case, we can have a CR with $q = p$ classes and the transform element and class representing elements are

$$\mathbf{T} = \mathbf{A}^{-1}\mathbf{B} \quad \text{and} \quad a_j = \mathbf{A}^j, \quad j = 0, 1, \ldots, q-1.$$

4.1. Case 1. We consider a Borel subgroup with $p = 13$, $k = 12$, $a = 2$, $n = 156$. We choose parameters for the generators as $t_1 = 5$, $t_2 = 2$, $y_1 = 1$, $y_2 = 1$. That is, $\mathbf{A} = \left(\begin{smallmatrix} 6 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{B} = \left(\begin{smallmatrix} 4 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. For this set of generators, diameter $D = 5$. Since $t_1, t_2 \neq 0$ and $(t_1, k) = 1$, the conditions for Case 1 in Table 3 are satisfied. Furthermore, $t_2 = 10\ t_1 \pmod{k}$. Accordingly, we choose

$$\mathbf{T} = \mathbf{B}\,\mathbf{A}\,\mathbf{B}\,(\mathbf{A}^{-1})^9 = \begin{pmatrix} 1 & 10 \\ 0 & 1 \end{pmatrix}.$$

We thus have a CR representation with divisor $q = k = 12$. For any $i \in \mathbf{V}$, if $i \bmod 12 =$:
"0" : i is connected to $i + 1, i - 1, i + 14, i - 38 \pmod{n}$;
"1" : i is connected to $i + 1, i - 1, i - 22, i - 69 \pmod{n}$;
"2" : i is connected to $i + 1, i - 1, i - 14, i - 57 \pmod{n}$;
"3" : i is connected to $i + 1, i - 1, i + 22, i - 58 \pmod{n}$;

"4" : i is connected to $i+1, i-1, i-34, i-69 \pmod n$;
"5" : i is connected to $i+1, i-1, i+74, i+58 \pmod n$;
"6" : i is connected to $i+1, i-1, i+14, i+34 \pmod n$;
"7" : i is connected to $i+1, i-1, i-22, i-74 \pmod n$;
"8" : i is connected to $i+1, i-1, i+50, i-14 \pmod n$;
"9" : i is connected to $i+1, i-1, i+62, i+22 \pmod n$;
"10" : i is connected to $i+1, i-1, i+38, i-50 \pmod n$;
"11" : i is connected to $i+1, i-1, i-57, i-62 \pmod n$.

4.2. Case 2. We consider the same Borel group as in Case 1, but with a different set of generators. The parameters for the generators are $t_1 = 2$, $t_2 = 3$, $y_1 = 1$, $y_2 = 1$. That is, $\mathbf{A} = \left(\begin{smallmatrix} 4 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{B} = \left(\begin{smallmatrix} 8 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. For this set of generators, diameter $D = 6$. Since $t_1, t_2 \neq 0$, $(t_1, k) \neq 1$, and $(t_2, k) \neq 1$, the conditions for Case 2 in Table 3 are satisfied. Furthermore, $k_1 = 6$, and $t_1 = 2$ is even. Accordingly, we choose

$$\mathbf{T} = \mathbf{B}\,\mathbf{A}^4\,\mathbf{B}^{-1}\,(\mathbf{A}^{-1})^4 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.$$

We thus have a CR representation with divisor $q = k = 12$. For any $i \in \mathbf{V}$, if $i \bmod 12 =$:
"0" : i is connected to $i+1, i-1, i-5, i+64 \pmod n$;
"1" : i is connected to $i+1, i-1, i+5, i-16 \pmod n$;
"2" : i is connected to $i+1, i-1, i+54, i-51 \pmod n$;
"3" : i is connected to $i+1, i-1, i+28, i+67 \pmod n$;
"4" : i is connected to $i+1, i-1, i-64, i+77 \pmod n$;
"5" : i is connected to $i+1, i-1, i+18, i-33 \pmod n$;
"6" : i is connected to $i+1, i-1, i-5, i+40 \pmod n$;
"7" : i is connected to $i+1, i-1, i+5, i-28 \pmod n$;
"8" : i is connected to $i+1, i-1, i+33, i-54 \pmod n$;
"9" : i is connected to $i+1, i-1, i-77, i+16 \pmod n$;
"10" : i is connected to $i+1, i-1, i-67, i-40 \pmod n$;
"11" : i is connected to $i+1, i-1, i+51, i-18 \pmod n$.

4.3. Case 3. We consider a smaller Borel Cayley graph with $a = 2$, $p = 7$, $k = 3$, $n = 21$, diameter $D = 3$, and the generators $\mathbf{A} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{B} = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Note that, in this case, we have $t_1 = 0$, $t_2 = 1$, $q = p = 7$, and $n/q = \text{LCM}\,(t_2 - t_1, k)/(t_2 - t_1) = 3$. According to Table 3, we choose $\mathbf{T} = (\mathbf{A}^{-1}\mathbf{B})$, $a_j = \mathbf{A}^j$ to produce a CR representation with divisor, $q = p = 7$. Let $\mathbf{V} = \{0, 1, \ldots, 20\}$. For any $i \in \mathbf{V}$, if $i \bmod 7 =$:
"0" : i is connected to $i+1, i-1, i-10, i+6 \pmod n$;
"1" : i is connected to $i+1, i-1, i+7, i-7 \pmod n$;
"2" : i is connected to $i+1, i-1, i+10, i-6 \pmod n$;
"3" : i is connected to $i+1, i-1, i+6, i-5 \pmod n$;
"4" : i is connected to $i+1, i-1, i+9, i+10 \pmod n$;
"5" : i is connected to $i+1, i-1, i+5, i-10 \pmod n$;
"6" : i is connected to $i+1, i-1, i-6, i-9 \pmod n$.
We show this CR representation of the graph in Fig. 5.

5. Conclusions. Dense, symmetric graphs are good candidates for the interconnection topology of a multicomputer system. Being a class of symmetric graphs, Cayley graphs are attractive. In our earlier research effort, we discussed the representations and routing of Cayley graphs [2]. In this paper, we analyzed a special class of Cayley graphs, the *Borel Cayley graphs*, which generates the densest known, constructive, degree-4 graphs with diameter $D = 7, \ldots, 13$.

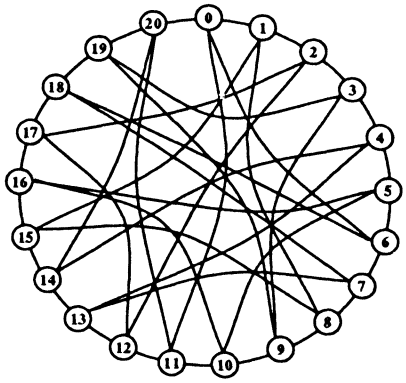

FIG. 5. *CR representation of* $\mathbf{BL}_2(\mathbf{Z}_7)$.

Borel Cayley graphs are defined over a group of matrices, the *Borel matrices*. That is, nodes are labeled as matrices. There is no inherent, simple ordering of node labels and no known computational routing algorithm with a constant or O(1) space commitment. GCRs and CRs, on the other hand, are two existing topologies defined in the integer domain and have systematic structure.

By transforming into GCRs [2], Cayley graphs have a systematic representation. Furthermore, an optimal, time-efficient routing algorithm, called *vertex-transitive routing*, is developed for Borel Cayley graphs [18]. However, the goal of developing an optimal, space-efficient, distance-reduction routing algorithm is still elusive.

Through the discovery of inherent properties of degree-4 Borel Cayley graphs, we proved that CR representations always exist for these graphs. A step-by-step algorithm and examples are used to illustrate the transformation to CR representations. This special case of a GCR includes a Hamiltonian cycle formed by edges connecting adjacent integers in the modulo n labels, thus permitting a distance-reduction routing algorithm, called *CR routing*. Given a Borel Cayley graph with $n = pk$ nodes (p is a prime and k is a factor of $p - 1$), this distance-reduction algorithm requires a small table of O(k). However, the algorithm is *suboptimal* in the sense that a shortest path is not guaranteed. Readers interested in CR routing are referred to [17].

Aside from facilitating the development of a space-efficient routing algorithm, the existence of a CR representation for any degree-4 Borel Cayley graphs also partially proved the long-standing conjecture that all Cayley graphs have Hamiltonian cycles [19]. Obviously, a CR graph, by definition, contains a Hamiltonian cycle. In fact, its class structure and connection rules impose a stronger condition. By providing a CR representaion, we have thus shown that all connected, degree-4 Borel Cayley graphs have Hamiltonian cycles.

REFERENCES

[1] D. V. CHUDNOVSKY, G. V. CHUDNOVSKY, AND M. M. DENNEAU, *Regular Graphs with Small Diameter as Models for Interconnection Networks*, Tech. Report RC 13484(60281), IBM Research Division, T. J. Watson Research Center, Yorktown Heights, NY, February 1988.

[2] B. W. ARDEN AND K. W. TANG, *Representations and routing of Cayley graphs*, IEEE Trans. Comm., 39 (1991), pp. 1533–1537.

[3] D. A. REED AND R. M. FUJIMOTO, *Multicomputer Networks*, MIT Press, Cambridge, MA, 1987.

[4] L. D. WITTIE, *Communication structures for large networks of microcomputers*, IEEE Trans. Comput., 30 (1981), pp. 264–273.

[5] J. A. BONDY AND U. S. R. MURTY, *Graph Theory with Applications*, North–Holland, New York, 1979.
[6] J. C. BERMOND, C. DELORME, AND J. J. QUISQUATER, *Tables of large graphs with given degree and diameter*, Inform. Process. Lett., 15 (1982), pp. 10–13.
[7] T. Y. FENG, *A survey of interconnection networks*, Computer, 14 (1981), pp. 12–27.
[8] G. H. BARNES, *The* ILLIAC IV *computer*, IEEE Trans. Comput., 17 (1968), pp. 746–757.
[9] J. P. HAYES ET AL., *Architecture of a hypercube supercomputer*, in Proc. of the 1986 Internat. Conf. on Parallel Processing, St. Charles, IL, August 1986, pp. 653–660.
[10] B. W. ARDEN AND H. LEE, *Analysis of chordal ring network*, IEEE Trans. Comput., 30 (1981), pp. 291–295.
[11] F. P. PREPARATA AND J. VUILLEMIN, *The cube-connected cycles: A versatile network for parallel computation*, Comm. Assoc. Comput. Mach., May 1981, pp. 300–309.
[12] J. C. BERMOND AND C. DELORME, *Strategies for interconnection networks: Some methods from graph theory*, J. Parallel Distributed Comput., 3 (1986), pp. 433–449.
[13] M. HOMEWOOD, D. MAY, D. SHEPHERD, AND R. SHEPHERD, *The* IMS T800 *transputer*, IEEE MICRO, October 1987, pp. 10–26.
[14] S. B. AKERS AND B. KRISHNAMURTHY, *A group-theoretic model for symmetric interconnection networks*, IEEE Trans. Comput., 38 (1989), pp. 555–565.
[15] G. E. CARLSSON, J. E. CRUTHIRDS, AND H. B. SEXTON, *Interconnection networks based on a generalization of cube-connected cycles*, IEEE Trans. Comput., 34 (1985), pp. 769–772.
[16] K. W. TANG AND B. W. ARDEN, *Representations and routing for Borel Cayley graphs*, in Proc. of Internat. Conf. on Information Technology, Tokyo, Japan, October 1990, pp. 27–31.
[17] ———, *Class-congruence property and two-phase routing for Borel Cayley graphs*, IEEE Trans. Comput., February 1993, submitted.
[18] ———, *Vertex-transitivity and routing for Cayley graphs in* GCR *representations*, in Proc. of 1992 Sympos. on Applied Computing, Kansas City, MO, March 1992, pp. 1180–1187.
[19] D. WITTE AND J. A. GALLIAN, *A survey: Hamiltonian cycles in Cayley graphs*, Discrete Math., 51 (1984), pp. 293–304.
[20] M. J. DINNEEN, *Algebraic Methods for Efficient Network Constructions*, Master thesis, Department of Computer Science, University of Victoria, Victoria, BC, Canada, 1991.
[21] L. CAMPBELL ET AL., *Small diameter symmetric networks from linear groups*, IEEE Trans. Comput., 41 (1992), pp. 218–220.
[22] K. W. TANG AND B. W. ARDEN, *Pseudo-Random Formulation of Borel Cayley Graphs*, Technical Report #661, College of Engineering and Applied Sciences, State University of New York at Stony Brook, Stony Brook, NY, March 1993.