Representations of Borel Cayley Graphs

K. Wendy Tang
Department of Electrical Engineering
SUNY at Stony Brook
Stony Brook, NY 11794

Bruce W. Arden
Department of Electrical Engineering
University of Rochester
Rochester, NY 14627

Abstract

There is a continuing search for dense (δ, D) interconnection graphs, that is, regular, bidirectional, degree δ graphs with diameter D and having a large number of nodes. Cayley graphs formed by the Borel subgroup currently contribute to some of the densest $(\delta = 4, D)$ 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, we showed that all Cayley graphs have generalized chordal ring (GCR) representations [2]. In this paper, we show that all degree-4 Borel Cayley graphs can also be represented by more restrictive chordal rings (CR) through a constructive proof. A step-by-step algorithm to transform any degree-4 Borel Cayley graph into CR graphs is provided. Examples are used to illustrate this concept.

1 Introduction

Amid the many interconnection models for multicomputers, a special class of symmetric graphs, Cayley graphs, is an attractive candidate [1, 3, 4]. Besides their symmetric property, Cayley graphs from the Borel subgroup, *Borel Cayley graphs*, are the densest known degree-4 graphs for a range of diameters ($D = 8, \ldots, 12$) [1, 5]. In other words, these degree-4 graphs interconnect the largest number of nodes for this degree and range of diameter ($D = 8, \ldots, 12$), and 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*. 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 makes the development of routing algorithms difficult.

Generalized Chordal Rings (GCR) [6] and the more specialized *Chordal Rings (CR)* [7], on the other hand, are two existing topologies that are defined in the integer domain and have a systematic and regular structure. Their definitions are reviewed in Section 2. In an earlier report, we proved and provided an algorithm to transform *any* Cayley graphs into Generalized Chordal Rings (GCR). We also provided a sufficient condition for Cayley graphs to have Chordal Ring (CR) representations [2]. By transforming into GCR [2], Cayley graphs have a systematic representation. Furthermore, an optimal, *time-efficient* routing algorithm, called *Vertex-Transitive routing*, is developed for Borel Cayley graphs [8]. However, the goal of developing an optimal, *space-efficient*, distance-reduction routing algorithm is still elusive.

This paper concentrates on representations of degree-4 *Borel Cayley graphs*. Through the discovery of inherent properties of these graphs, we prove another interesting proposition. Specifically, *all* bidirectional, degree-4 Borel Cayley graphs have the more restrictive CR representations and hence Hamiltonian cycles *always* exist for these graphs. In the course of proving this proposition, a step-by-step algorithm is constructed to transform *any* Borel Cayley graph to a CR representation.

Besides providing a systematic structure for Borel Cayley graphs, this result on Borel Cayley graphs has an impact on routing. A Chordal Ring graph includes a Hamiltonian cycle formed by edges connecting adjacent integers in the modulo n labels, and 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 *sub-optimal* in the sense that a shortest path is not guaranteed. Simulation shows that a more dynamic approach produces path lengths closer to optimal [9].

This paper is organized as follows: In section 2, we review the definitions of GCR, CR, 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 section 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 Chordal Rings. Finally in section 5, we present a summary and conclusions.

2 Reviews

In this section we review the definitions of generalized chordal rings (GCR), chordal rings (CR), Cayley graphs in general and Borel Cayley graphs in particular. We begin with the definition of a GCR:

Definition 1 A graph is a generalized chordal ring (GCR) if its nodes can be labeled with integers mod n, the number of nodes, and there is a divisor q of n such that node i is connected to node j iff node $i + q \pmod n$ is connected to node $j + q \pmod n$.

According to this definition, nodes of a GCR are classified into q classes, each class with n/q elements. The classification is based on modulo q arithmetic. Two nodes having the same residue (mod q) are considered to be in the same class. That is, class i consists of the following nodes: i, $i+q$, $i+2q$, ..., $i+(m-1)q \pmod n$, where $m = n/q$; and node i is the *representing element* of class i. Since i connects to j implies $i+q$ 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, Figure 1 shows a degree 4 GCR with 10 nodes and $q = 2$ classes. The connection rules for these classes can be defined as: Let $V = \{0, 1, \ldots, 9\}$. For any $i \in V$, if $i \bmod 2 =$:
"0" : i is connected to $i+2$, $i+3$, $i-1$, $i-2 \pmod{10}$;
"1" : i is connected to $i+1$, $i+4$, $i-4$, $i-3 \pmod{10}$.

0-8186-2772-7/92 $3.00 © 1992 IEEE

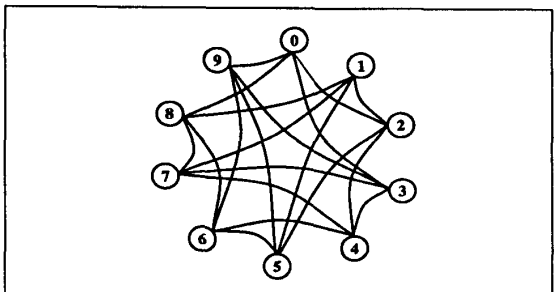

Figure 1: *A Degree-4 GCR ($n = 10$ $q = 2$)*

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.

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

A Chordal Ring (CR) is a special case of a 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 in the circumference of the ring are connected to form a Hamiltonian cycle.

Figure 2 shows a degree 4 CR with 10 nodes and $q = 2$ classes. The connection rules for these classes can be defined as: Let $\mathbf{V} = \{0, 1, \ldots, 9\}$. For any $i \in \mathbf{V}$, if $i \bmod 2 =$:
"0" : i is connected to $i+1$, $i-1$, $i+2$, $i-2 \pmod{10}$;
"1" : i is connected to $i+1$, $i-1$, $i+4$, $i-4 \pmod{10}$.
Note that every class has $+1$ and -1 as GCR constants and nodes on the circumference of the ring are connected.

The construction of Cayley graphs is described by finite (algebraic) group theory. Recall that a group $(\mathbf{V}, *)$ consists of a set $\mathbf{V}$ 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 $\mathbf{V}$.

Definition 2 A graph $\mathbf{C} = (\mathbf{V}, \mathbf{G})$ is a Cayley graph with vertex set $\mathbf{V}$ 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 $(\mathbf{V}, *)$ is a finite group and $\mathbf{G} \subset \mathbf{V} \backslash \{I\}$. $\mathbf{G}$ is called the generator set of the graph and I is the identity element of the finite group $(\mathbf{V}, *)$.

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 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, vertices 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 et al. [1] showed that these Borel Cayley graphs are the densest, nonrandom ($\delta = 4, D$) graphs known for $D = 8, \ldots, 12$ (Table 1). The *Moore Bound* shown in Table 1 is an upper bound for the number of nodes in a degree-4 graph with diameter D. 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 non-existent except for the cases where $D = 2$, $\delta = 3$, the Peterson graph; or $D = 2$, $\delta = 7$, the Hoffman-Singleton graph; and possibly for $D = 2$, $\delta = 57$ [6]. Given this general impossibility of constructing Moore graphs, there has been a longstanding 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 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 $D = 11$, $\delta = 4$.

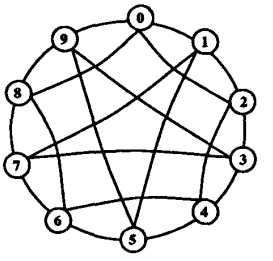

Figure 2: *A Degree-4 CR ($n = 10$ $q = 2$)*

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 non-adjacent nodes is non-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 [10]. 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 $n = \mid \mathbf{V} \mid$.

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 Chordal Ring (CR) representations.

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

Proposition 2 Let A, B be two distinct generators of a finite Cayley graph $\mathbf{C}$. Assume $A \neq B^{-1}, A^q = I$ and

Diameter	Cayley Graphs	Moore Bound	1987 Graphs
7	1,152	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	140,868	3,118,643	-

Table 1: *Comparisons of Degree-4 Graphs*

$m = n/q$. 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, bidirectional Borel Cayley graphs have Chordal Ring (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 $\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}$. Furthermore, the orders 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

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

where LCM(t,k) stands for "the Least Common Multiple of t and k".

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

$\mathbf{X}^q = \mathbf{I}$

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

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

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

Hence $\mathbf{X}^q = \mathbf{I} \Rightarrow qt = 0 \pmod k \Rightarrow q = \frac{\text{LCM}(t,k)}{t}$.

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

Also, $(a^{(q-1)t} + a^{(q-2)t} + \ldots + a^0) = 0 \pmod p$

$\Rightarrow \quad q = 0 \pmod p \Rightarrow q = p$ □

Proposition 4 $\mathbf{B} \neq \mathbf{A}^m$ 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 $\mathbf{A}$. □

Proposition 5

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

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: $\mathbf{N}(a) = \{x \in \mathbf{V} : x = T^s a\}$ $s = 0, 1, \ldots, (m-1)$.

1. Construct $\mathbf{N}(a_i)$, $i = 0, \ldots, (q-1)$ by picking arbitrary $a_i \in V/\mathbf{N}(a_0)/\ldots/\mathbf{N}(a_{i-1})$. $a_0, a_1, \ldots, a_{q-1}$ are the initial representative elements in partitions $\mathbf{N}(a_0), \mathbf{N}(a_1), \ldots, \mathbf{N}(a_{q-1})$.
2. Associate $a_i \rightarrow i$, $i = 0, 1, \ldots, (q-1)$ 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 $w + j + sq - i$.

Table 2: *GCR Algorithm*

The proof of this proposition is a straight forward 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 m_2 as the net number of generator $\mathbf{B}$, $\mathbf{X} = \mathbf{A}^{m_1}\mathbf{B}^{m_2}$, where

$$m_1 = \text{number of } \mathbf{A} - \text{number of } \mathbf{A}^{-1} \pmod{k_1}$$
$$m_2 = \text{number of } \mathbf{B} - \text{number of } \mathbf{B}^{-1} \pmod{k_2}$$

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

$$\mathbf{X} = \underbrace{\ldots\ldots}_{m_1' A,\ (m_2'-l)B} \mathbf{AB}^l$$
$$= \mathbf{A}^{m_1'}\mathbf{B}^{m_2'-l}\mathbf{AB}^l \text{ (by assumption)}$$

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

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 $\mathbf{AB} = \mathbf{BA} \Leftrightarrow$ the graph is disconnected.

Proof: From Proposition 6, an element $\mathbf{X}$ in the graph is represented as $\mathbf{X} = \mathbf{I}$, or $\mathbf{A}^{m_1}$, or $\mathbf{B}^{m_2}$, or $\mathbf{A}^{m_1}\mathbf{B}^{m_2}$, where $m_1 = 1, \ldots, k_1 - 1$, $m_2 = 1, \ldots, k_2 - 1$. In other words, there are at most

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

different $\mathbf{X}$. Since k is a factor of $p - 1$ (Definition 3), $n = p \times k > k^2$ which implies 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: $t_1 = t_2 = 0 \Rightarrow (1-a^{t_2})y_1 = (1-a^{t_1})y_2$
$\Leftrightarrow \mathbf{AB} = \mathbf{BA}$ (by Equation 1)
which implies the graph is disconnected by Corollary 1. □

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

Proof: $y_1 = y_2 = 0 \Rightarrow (1-a^{t_2})y_1 = (1-a^{t_1})y_2$
$\Leftrightarrow \mathbf{AB} = \mathbf{BA}$ (by Equation 1)
which implies 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 $\mathbf{B}^{-1}$,

$$\mathbf{X} = \begin{pmatrix} a^{<it_1+jt_2>_k} & < gy_1 + hy_2 >_p \\ 0 & 1 \end{pmatrix}$$
$$\Rightarrow \quad (1-a^{t_1})g + (1-a^{t_2})h = 1 - a^{it_1+jt_2} \pmod p$$

Proof: We prove this proposition by induction on the length of the path. For the single step path $\mathbf{X} = \mathbf{A}$,
$i = 1,\ j = 0,\ g = 1,\ h = 0,\ (1-a^{t_1})g = 1 - a^{t_1}$
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 $\mathbf{X}'$. Hence

$$\mathbf{X}' = \begin{pmatrix} a^{<i't_1+j't_2>_k} & < g'y_1 + h'y_2 >_p \\ 0 & 1 \end{pmatrix} \text{ and}$$
$$(1-a^{t_1})g' + (1-a^{t_2})h' = 1 - a^{i't_1+j't_2} \pmod p$$

Consider the path $\mathbf{X}'\mathbf{A}$

$$= \begin{pmatrix} a^{<(i'+1)t_1+j't_2>_k} & < (g' + a^{i't_1+j't_2})y_1 + h'y_2 >_p \\ 0 & 1 \end{pmatrix}.$$

By assumption,

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

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

$$\mathbf{X} = \begin{pmatrix} a^{<it_1+jt_2>_k} & < gy_1 + hy_2 >_p \\ 0 & 1 \end{pmatrix}$$
$$\mathbf{Y} = \begin{pmatrix} a^{<i't_1+j't_2>_k} & < g'y_1 + h'y_2 >_p \\ 0 & 1 \end{pmatrix}.$$

Then

$$\mathbf{X} = \mathbf{Y} \Leftrightarrow it_1 + jt_2 = i't_1 + j't_2 \pmod k$$
$$\text{and} \quad \begin{cases} g = g' \text{and } h = h' & \pmod p \quad \text{or} \\ (1-a^{t_2})y_1 = (1-a^{t_1})y_2 & \pmod p \end{cases}$$

Proof: From Proposition 7,

$$(1-a^{t_1})g + (1-a^{t_2})h = 1 - a^{it_1+jt_2} \pmod p$$
$$(1-a^{t_1})g' + (1-a^{t_2})h' = 1 - a^{i't_1+j't_2} \pmod p \qquad (2)$$

($\Rightarrow$) $\mathbf{X} = \mathbf{Y}$

$$\Rightarrow it_1 + jt_2 = i't_1 + j't_2 \pmod k$$
$$\Rightarrow (1-a^{t_1})(g-g') = (1-a^{t_2})(h'-h) \pmod p \qquad (3)$$

Also $\mathbf{X} = \mathbf{Y}$

$$\Rightarrow \quad gy_1 + hy_2 = g'y_1 + h'y_2 \pmod p$$
$$\Rightarrow \quad (g-g')y_1 = (h'-h)y_2 \pmod p \qquad (4)$$

From Equations 3 and 4, we have

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

($\Leftarrow$) Obviously,

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

On the other hand, from Eq. 2

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

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

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

Corollary 4 Let $\mathbf{X}$, $\mathbf{Y}$ as defined in Proposition 8. Then

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

Proof: From Proposition 8,

$$\begin{aligned} & \mathbf{X} = \mathbf{Y} \\ \Leftrightarrow \ & it_1 + jt_2 = i't_1 + j't_2 \pmod k \\ \text{and} \ & \begin{cases} g = g' \quad \text{and} \quad h = h' & \pmod p \quad \text{or} \\ (1-a^{t_2})y_1 = (1-a^{t_1})y_2 & \pmod p \end{cases} \end{aligned}$$

However, from Proposition 5 and Corollary 1

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

Hence for a connected degree-4 Borel Cayley graph,

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

We are now ready to state our proposition:

Proposition 9 All bidirectional, 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 $\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$, $y' \neq 0$, and the representing element of class j to be $a_j = \begin{pmatrix} a^i & \bar{y}_j \\ 0 & 1 \end{pmatrix}$, where $i,\ j = 0, \ldots, k-1$ 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:

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

(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 produce a CR representation.

Case 1: $t_1, t_2 \neq 0$ and either $(t_1, k) = 1$ or $(t_2, k) = 1$. Without lost of generality, we assume that $(t_1, k) = 1$, (t_1 and k are relatively prime). In other words, multiples of t_1 span the set { 1, ..., (k-1) }. Since $t_2 \in \{1, \ldots, (k-1)\}$, we have $m\ t_1 = t_2$ for some $m = 1, \ldots, (k-1)$. We consider a GCR with

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

Claim: $\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$ 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 $\mathbf{A}$ and $\mathbf{B}$ that composed the matrix. As an example, for matrix $\mathbf{X} = \mathbf{AB}$, its t value is $t_1 + t_2$. Counting the net number of generators $\mathbf{A}$ and $\mathbf{B}$ in

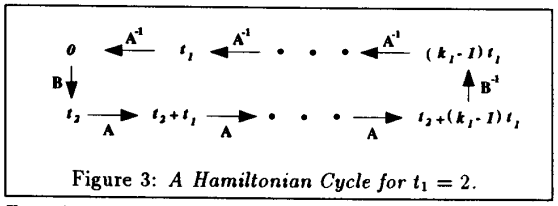

Figure 3: *A Hamiltonian Cycle for* $t_1 = 2$.

Equation 5,

$$t_2 + (k-1-m)t_1 + t_2 + (m-1)(k-t_1) = 0,$$

hence the first element of $\mathbf{T}$ is 1. We proceed to prove that $\mathbf{T} \neq \mathbf{I}$. Since $mt_1 = t_2$, we let $\mathbf{B} = \mathbf{H}\mathbf{A}^m$ where $\mathbf{H} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ for some $z \in \mathbf{Z}_p$ and $z \neq 0$ because $\mathbf{B} \neq \mathbf{A}^m$, as stated in Proposition 4. Also, assume $\mathbf{A}^{-1} = \begin{pmatrix} 1 & z' \\ 0 & 1 \end{pmatrix}$ where $z' = -a^{-t_1} y_1 \pmod p$.

$$\begin{aligned}
& & \mathbf{T} &= \mathbf{I} \\
\Rightarrow & & \mathbf{B}\mathbf{A}^{k-1-m}\mathbf{B} &= \mathbf{A}^{m-1} \\
\Rightarrow & & \mathbf{H}\mathbf{A}^m\mathbf{A}^{k-1-m}\mathbf{H}\mathbf{A}^m &= \mathbf{A}^{m-1} \\
\Rightarrow & & \mathbf{H}\mathbf{A}^{-1}\mathbf{H} &= \mathbf{A}^{-1} \\
\Rightarrow & \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix} \\
\Rightarrow & \begin{pmatrix} a^{k-t_1} & (a^{k-t_1}+1)z + z' \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a^{k-t_1} & z' \\ 0 & 1 \end{pmatrix} \\
\Rightarrow & & (a^{k-t_1}+1)z &= 0 \mod p \\
\Rightarrow & & a^{k-t_1} &= -1 \mod p \\
\Rightarrow & & 2(k-t_1) &= 0 \mod k \\
\Rightarrow & & (t_1, k) &\neq 1,
\end{aligned}$$

which contradicts to the assumption that t_1 and k are relatively prime. 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 Equation 5. That is, the representing element of class j is the composition of the first j elements in Equation 5. Specifically,

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

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 $t_2 = mt_1$. 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.

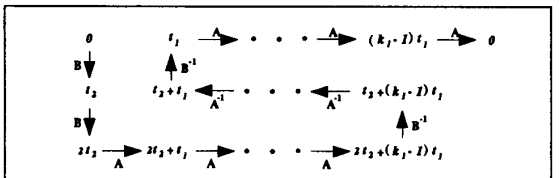

Figure 4: *A Hamiltonian Cycle for* $t_1 = 3$.

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 not all the k values can be generated and the graph is disconnected. Furthermore, $t_1 k_1 = t_2 k_2 = k$. Since t_1 and t_2 are relatively prime, t_1 is a factor of k_2, and $k_2 \geq t_1$, which implies that we can divide the set $\{0, \ldots, k-1\}$ into t_1 distinct subsets each with k_1 elements:

$$\begin{array}{llll}
\{0, & t_1, & \ldots, & (k_1-1)t_1\}, \\
\{t_2, & t_2+t_1, & \ldots, & t_2+(k_1-1)t_1\}, \\
\vdots & \vdots & \vdots & \vdots \\
\multicolumn{4}{l}{\{(t_1-1)t_2,\ (t_1-1)t_2+t_1,\ \ldots,\ (t_1-1)t_2+(k_1-1)t_1\}.}
\end{array}$$

As discussed in the outset of this proof, the idea is to construct a specific GCR by choosing the transform element $\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$, $y' \neq 0$, 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 $\{0, 1, \ldots, k-1\}$. If each number in the subsets represents the superscript i of a class representing element, 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 $\mathbf{B}$. The problem of finding proper 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" these k numbers, 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 $d = \frac{t_1-1}{2}$. In this case, we consider a GCR with

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

Claim: $\mathbf{T} = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$ for some $y' \in \mathbf{Z}_p$ and $y' \neq 0$.

Proof: By counting the net numbers of $\mathbf{A}$ and $\mathbf{B}$ in Equation 6,

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

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

$$\begin{aligned}
& \mathbf{T} &&= \mathbf{I} \\
\Rightarrow\ & \begin{pmatrix} 1 & gy_1 + hy_2 \\ 0 & 1 \end{pmatrix} &&= \begin{pmatrix} 1 & 0y_1 + 0y_2 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

where

$$\begin{aligned}
g = {} & -a^{2dt_2-t_1} + \textstyle\sum_{i=1}^{d}\{a^{(2i-1)t_2-t_1} + a^{(2i-1)t_2} \\
& -a^{2(i-1)t_2} - a^{2(i-1)t_2-t_1}\} + a^{-t_1} \pmod p
\end{aligned} \quad (7)$$

$$h = \sum_{i=0}^{2d-1} a^{it_2} - \sum_{i=1}^{d}\{a^{(2i-1)t_2-t_1} + a^{2(i-1)t_2+t_1}\} \pmod p \quad (8)$$

For any degree-4 Borel Cayley graph with $n = |\mathbf{V}| = p \times k$, assume $\mathbf{A}$, $\mathbf{B}$, and their inverses are generators: $\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}$.

In each of the following cases, we construct a CR representation with divisor q, by following the procedure summarized in Table 2. But 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: $\mathbf{T} = \mathbf{A}^{-1}\mathbf{B}$, $a_i = \mathbf{A}^i$, $i = 0, \ldots, q-1$.

Table 3: *CR Algorithm.*

Equations 7 and 8 are obtained by observing that

$$\mathbf{T} = \mathbf{B}^{2d}\mathbf{A}^{-1}\{\mathbf{B}^{-1}\mathbf{A}^2\mathbf{B}^{-1}\mathbf{A}^{-2}\}^d\mathbf{A}$$

and

$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{A} = \begin{pmatrix} a^{t+t_1} & < y + a^t y_1 >_p \\ 0 & 1 \end{pmatrix};$$
$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{A}^{-1} = \begin{pmatrix} a^{t-t_1} & < y - a^{t-t_1} y_1 >_p \\ 0 & 1 \end{pmatrix};$$
$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{B} = \begin{pmatrix} a^{t+t_2} & < y + a^t y_2 >_p \\ 0 & 1 \end{pmatrix};$$
$$\begin{pmatrix} a^t & y \\ 0 & 1 \end{pmatrix}\mathbf{B}^{-1} = \begin{pmatrix} a^{t-t_2} & < y - a^{t-t_2} y_2 >_p \\ 0 & 1 \end{pmatrix}.$$

According to Corollary 4, $g = h = 0 \pmod p$. That is,

$$\begin{aligned} & g = 0 \pmod p \\ \Rightarrow\ & a^{2dt_2-t_1} - a^{-t_1} \\ =\ & \sum_{i=1}^{d}\left\{a^{(2i-1)t_2-t_1} - a^{2(i-1)t_2-t_1}\right\} \\ & + \sum_{i=1}^{d}\left\{a^{(2i-1)t_2} - a^{2(i-1)t_2}\right\} \pmod p \\ =\ & (a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2-t_1} \\ & + (a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p \\ =\ & (a^{-t_1}+1)(a^{t_2}-1)\sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p \qquad (9) \end{aligned}$$

Similarly,

$$\begin{aligned} & h = 0 \pmod p \\ \Rightarrow\ & \sum_{i=0}^{2d-1} a^{it_2} \\ =\ & (a^{t_2-t_1} + a^{t_1})\sum_{i=1}^{d} a^{2(i-1)t_2} \pmod p \\ \Rightarrow\ & \sum_{i=1}^{d} a^{2(i-1)t_2} \\ =\ & (a^{t_2-t_1} + a^{t_1})^{-1}\sum_{i=0}^{2d-1} a^{it_2} \pmod p \qquad (10) \end{aligned}$$

Using Equations 9 and 10, we have

$$\begin{aligned} & (a^{t_2-t_1} + a^{t_1})\,(a^{2dt_2-t_1} - a^{-t_1}) \\ & = (a^{-t_1}+1)\,(a^{t_2}-1)\sum_{i=0}^{2d-1} a^{it_2} \pmod p \\ \Rightarrow\ & a^{(2d+1)t_2-2t_1} - a^{t_2-2t_1} + a^{2dt_2} - 1 \\ & = (a^{t_2-t_1} - a^{-t_1} + a^{t_2} - 1)\sum_{i=0}^{2d-1} a^{it_2} \\ & = \sum_{i=0}^{2d-1}\{a^{(i+1)t_2-t_1} - a^{it_2-t_1} + a^{(i+1)t_2} - a^{it_2}\} \\ & = (a^{-t_1}+1)(a^{2dt_2}-1) \\ & = 2^{2dt_2-t_1} - a^{-t_1} + a^{2dt_2} - 1 \\ \Rightarrow\ & a^{(2d+1)t_2-t_1} - a^{t_2-t_1} = a^{2dt_2} - 1 \\ \Rightarrow\ & a^{t_2-t_1}(a^{2dt_2}-1) = a^{2dt_2} - 1 \\ \Rightarrow\ & (a^{t_2-t_1}-1)(a^{(t_1-1)t_2}-1) = 0 \text{ (since } 2d = t_1 - 1) \end{aligned}$$

That is, $\mathbf{T} = \mathbf{I} \Rightarrow t_1 = t_2$ or $t_1 = 1$ or $t_2 = 0$ which contradict to $(t_1, t_2) = 1$, $(t_1, k) \neq 1$ 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 Equation 6. That is, the representing element of class j is the composition of the first j elements in Equation 6. Specifically,

$$\begin{aligned} a_0 &\rightarrow \mathbf{I}; \\ a_1 &\rightarrow \mathbf{B}; \\ a_2 &\rightarrow \mathbf{B}^2; \\ &\vdots \\ a_{t_1-1} &\rightarrow \mathbf{B}^{t_1-1}; \\ a_{t_1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}; \\ a_{t_1+1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^2; \\ &\vdots \\ a_{t_1+k_1-2} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}; \\ a_{t_1+k_1-1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}; \\ a_{t_1+k_1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}\mathbf{A}^{-1}; \\ a_{t_1+k_1+1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\mathbf{B}^{-1}(\mathbf{A}^{-1})^2; \\ &\vdots \\ a_{q_1-1} &\rightarrow \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d. \end{aligned}$$

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 representing elements are connected to each other: $a_0 \sim a_1 \sim \ldots \sim a_{q-1} \sim \mathbf{T} * a_0$. Hence we have a CR representation.

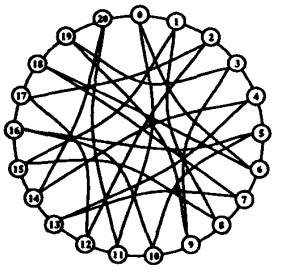

Figure 5: *CR Representation of* $\mathbf{BL}_2(\mathbf{Z}_7)$

Subcase 2: t_1 is even. We define the integer $d = \frac{t_1}{2} - 1$. In this case, we consider a GCR with

$$\mathbf{T} = \mathbf{B}^{t_1-1}\mathbf{A}^{k_1-1}\{\mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-2}\mathbf{B}^{-1}\mathbf{A}^{k_1-2}\}^d \mathbf{B}^{-1}(\mathbf{A}^{-1})^{k_1-1} \quad (11)$$

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 $y' \neq 0$.

Similar to Subcase 1, we can now construct a GCR with divisor $q = k$, and choose the representing elements to be: $a_o, a_1, \ldots, a_{q-1}$ according to Equation 11. The representing element of class j is determined from the compositon of the first j elements in Equation 11. That is,

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

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: $a_0 \sim a_1 \sim \ldots \sim a_{q-1} \sim \mathbf{T} * a_0$. 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 not all k values can be generated and 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 $m = n/p = k = \frac{\text{LCM}(t_2,k)}{t_2}$. 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 bidirectional, 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.

4 Examples

In this section, we use three examples to illustrate the three cases discussed in the constructive proof of CR representations (section 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 $\mathbf{A} = \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}$, $t_1, t_2 \in \{0, \ldots, k-1\}$, $y_1, y_2 \in \{0, \ldots, p-1\}$, and $k_1, k_2 \in \{0, \ldots, k-1\}$ are the orders of $\mathbf{A}$ and $\mathbf{B}$.

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, $\mathbf{A} = \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}$. 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, $\mathbf{A} = \begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 8 & 1 \\ 0 & 1 \end{pmatrix}$. 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 $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$.

Note that in this case we have $t_1 = 0$, $t_2 = 1$, $q = p = 7$, and $n/q = \frac{\text{LCM}(t_2 - t_1, k)}{t_2 - t_1} = 3$. According to Table 3, we choose $\mathbf{T} = (\mathbf{A}^{-1}\mathbf{B})$ to produce a CR representation with divisor, $q = 7$. Let $\mathbf{V} = \{0, 1, \ldots, 20\}$. For any $i \in \mathbf{V}$, if $i \bmod 7 =$:

"0" : i is connected to $i+1$, $i-1$, $i-10$, $i+6$ (mod n);
"1" : i is connected to $i+1$, $i-1$, $i+7$, $i-7$ (mod n);
"2" : i is connected to $i+1$, $i-1$, $i+10$, $i-6$ (mod n);
"3" : i is connected to $i+1$, $i-1$, $i+6$, $i-5$ (mod n);
"4" : i is connected to $i+1$, $i-1$, $i+9$, $i+10$ (mod n);
"5" : i is connected to $i+1$, $i-1$, $i+5$, $i-10$ (mod n);
"6" : i is connected to $i+1$, $i-1$, $i-6$, $i-9$ (mod n).
We show this CR representation of the graph in Figure 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, 8]. In this paper, we analyzed a special class of Cayley graphs, the *Borel Cayley graphs* which generates the densest known, constructive graphs (degree-4) with diameter $D = 8, \ldots, 12$.

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. Generalized Chordal Rings (GCR) and Chordal Rings (CR), on the other hand, are two existing topologies defined in the integer domain and have systematic structure.

By transforming into GCR [2], Cayley graphs have a systematic representation. Furthermore, an optimal, time-efficient routing algorithm, called *Vertex-Transitive routing*, is developed for Borel Cayley graphs [8]. 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 and hence Hamiltonian cycles 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, and 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 *sub-optimal* in the sense that a shortest path is not guaranteed. Readers who are interested in CR routing are referred to [10].

References

[1] D.V. Chudnovsky, G.V. Chudnovsky, and M.M. Denneau. Regular Graphs with Small Diameter as Models for Interconnection Networks. Technical Report RC 13484(60281), IBM Research Division, February 1988.

[2] B.W. Arden and K.W. Tang. Representation and Routing of Cayley Graphs. *IEEE Transactions on Communications*, 39(11):1533–1537, November 1991.

[3] S.B. Akers and B. Krishnamurthy. "A Group-Theoretic Model for Symmetric Interconnection Networks". *IEEE Transactions on Computers*, 38(4):555–565, April 1989.

[4] G.E. Carlsson, J.E. Cruthirds, and H.B. Sexton. "Interconnection Networks Based on a Generalization of Cube-Connected Cycles". *IEEE Transactions on Computers*, 34(8):769–772, August 1985.

[5] M.J. Dinneen. Algebraic methods for efficient network constructions. Master's thesis, Department of Computer Science, University of Victoria, Victoria, B.C., Canada, 1991.

[6] J.C. Bermond and C. Delorme. "Strategies for Interconnection Networks: Some Methods from Graph Theory". *Journal of Parallel and Distributed Computing*, 3:433–449, 1986.

[7] B.W. Arden and H. Lee. "Analysis of Chordal Ring Network". *IEEE Transactions on Computers*, 30(4):291–295, April 1981.

[8] K.W. Tang and B.W. Arden. Vertex-Transitivity and Routing for Cayley Graphs in GCR Representations. In *Proceedings of 1992 Symposium on Applied Computing*, pages 1180–1187, Kansas City, MO, March 1-3 1992.

[9] K.W. Tang and B.W. Arden. Routing for Borel Cayley Graphs. Technical Report EE-91-07, Department of Electiral Engineering, University of Rochester, July 1991. (Submitted for publication.).

[10] K.W. Tang and B.W. Arden. Representations and Routing for Borel Cayley Graphs. In *Proceedings of The International Conference on Information Technology*, pages 27–31, Tokyo, Japan, October 1-5 1990.

[11] B.W. Arden and K.W. Tang. "Routing for Generalized Chordal Rings". In *Proceedings of the ACM:18th Computer Science Conference*, Washington, D.C., February 20-22 1990.