Department of Electrical Engineering
College of Engineering and Applied Sciences
State University of New York at Stony Brook
Stony Brook, New York 11794-2350

Pseudo-Random Formulation of Borel Cayley Graphs

by

K. Wendy Tang and Bruce W. Arden

Technical Report # 661

March 1, 1993

Pseudo-Random Formulation of Borel Cayley Graphs

K. WENDY TANG* and BRUCE W. ARDEN†

*Department of Electrical Engineering
SUNY at Stony Brook, Stony Brook, NY 11794.

†Department of Electrical Engineering
University of Rochester, Rochester NY 14627.

ABSTRACT *Dense, symmetric graphs are good candidates for effective interconnection networks. Recently, Cayley graphs have received much attention [1]--[6]. Specifically, Cayley graphs formed by Borel subgroups are the densest, vertex-transitive degree-4 graphs known for a range of diameters [1]. In this paper, we propose a new and simpler formulation for these graphs. With this formulation, these graphs resemble the generation of pseudo-random numbers and hence the name, pseudo-random formulation. Furthermore, this new formulation demonstrates that Borel Cayley graphs are isomorphic to a special case of Cayley graphs proposed in [3].*

1 Introduction

There is an increasing interest in a special class of graphs based on group theory, known as Cayley graphs [1]--[6]. Basically, a Cayley graph is constructed from a finite group. The vertices of the graph are the elements of the group. Connections between vertices are defined by the group operation and a set of generators. (The formal definition of Cayley graphs is reviewed in Section 2.) There is no restriction in the choice of the underlying group. We can construct a Cayley graph over an arbitrary finite group and hence there are many varieties of Cayley graphs. It is known that all Cayley graphs are vertex-transitive [8]. Mathematically, this implies that for any two vertices u and v, there is an automorphism that maps u to v. Informally, this means the graph looks the same from any vertex. Such node symmetry allows identical processing/communicating elements at every node incorporating the same routing algorithm and therefore is desirable in a multicomputer system. The attractiveness of Cayley graphs was further enhanced when Chudnovsky et. al discovered that certain Borel Cayley graphs, i.e., Cayley graphs based on Borel subgroups, are the densest degree-4, non-random graphs known for an interesting range of diameters [1].

The definition of a Cayley graph requires vertices to be elements of a group but does not specify a particular group. A family of Cayley graphs that includes some of the densest degree 4 graphs are formed 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:

Definition 2 If $\mathbf{V}$ is a Borel subgroup, $\mathbf{BL}_2(\mathbf{Z}_p)$, of $\mathbf{GL}_2(\mathbf{Z}_p)$ with a parameter a, $a \in \mathbf{Z}_p \setminus \{0, 1\}$, 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 p is prime and k is the smallest positive integer such that $a^k = 1 \pmod{p}$.

The vertices of *Borel Cayley graphs* are 2×2 matrices that satisfy the definition of Borel subgroup, and modular p matrix multiplication is chosen as the group operation *. Note that $N = |\mathbf{V}| = p \times k$, where k is a factor of $p - 1$ and p is a prime number. By choosing specific generators, Chudnovsky et al. [1] constructed the densest, nonrandom $(\delta = 4, D)$ graphs known for $D = 7, \ldots, 13$ from Borel Cayley graphs (Table 1).

Table 1 compares the size of these graphs with that of the known graphs and the Moore bounds. It is clear that these Borel Cayley graphs show significant improvements in density. However, many questions about these graphs are not addressed in [1]. Most importantly, the question of how the choice of parameters contributes to improvements in density. Motivated by this question, our research focuses on Borel Cayley graphs and this paper presents some of our findings. 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 $D = 11$, $\delta = 4$.

In a separate research effort, Dinneen proposed a Cayley graph constructed over a semi-direct product group [3]. The definition of this group is summarized as follows.

Definition 3 Given two cyclic groups Z_m and Z_n, the semi-direct product group $SG = Z_m \times_\sigma Z_n$ is defined by a homomorphism $\sigma : Z_m \to Aut(Z_n)$. Let an element r be chosen

Diameter	Moore Bound	Known Graphs (1987)	Borel Cayley Graphs	Dinneen Cayley Graphs
7	4,373	856	1,081	1,081
8	13,121	1,872	2,943	2,943
9	39,365	4,352	7,439	7,439
10	118,097	13,056	15,657	15,657
11	354,293	–	41,831	–
12	1,062,881	–	82,901	–
13	3,118,645	–	140,607	–

Table 1: *Size of Degree 4 Graphs for Certain Diameters*

from the group of units $U(Z_n)$. Define a mapping $\sigma'(k) = (r^c)^k = r^{ck}$ where c is chosen such that $r^{cm} = 1$. The group SG has its multiplication table defined by

$$(a_0, a_1) *_\sigma (b_0, b_1) = (a_0 + b_0 \bmod m, a_1 + \sigma'(a_0)b_1 \bmod n). \tag{1}$$

Using this group, Dinneen constructed some largest known Cayley graphs (Appendix A of [3]). For the reader's convenience, these graphs are summarized in Table 1. Interestingly, for the cases of $\delta = 4, D = 7, \ldots, 10$, these graphs have the same number of nodes as the Borel Cayley graphs in Table 1. In section 4, we show that the Borel group is actually a special case of this semi-direct product group and the dense Cayley graphs produced by Dinneen are isomorphic to the Borel Cayley graphs in Table 1.

3 Parameters of Degree-4 Borel Cayley Graphs

For ease of description, we assume a size N, degree-4 Borel Cayley graph with generators $\mathbf{A}, \mathbf{B}, \mathbf{A}^{-1}$, and $\mathbf{B}^{-1}$. Furthermore,

$$\begin{aligned} \mathbf{A} &= \begin{pmatrix} a^{t_1} & y_1 \\ 0 & 1 \end{pmatrix}, \quad & \mathbf{A}^{-1} &= \begin{pmatrix} a^{k-t_1} & < -a^{k-t_1} y_1 >_p \\ 0 & 1 \end{pmatrix} \\ \mathbf{B} &= \begin{pmatrix} a^{t_2} & y_2 \\ 0 & 1 \end{pmatrix}, \quad & \mathbf{B}^{-1} &= \begin{pmatrix} a^{k-t_2} & < -a^{k-t_2} y_2 >_p \\ 0 & 1 \end{pmatrix}, \end{aligned} \tag{2}$$

where $< x >_p$ denotes x mod p. We note that $N = p \times k$ and the parameters: p, a, k, t_1, t_2, y_1 and y_2 are needed to specify a particular Borel Cayley graph. Among

N	p	k	a	t_1	t_2	y_1	y_2	D
1081	47	23	2	1	7	0	1	7
				2	10	0	1	7
				7	8	0	1	8
				3	6	0	1	9
2943	109	27	7	1	6	0	1	8
7439	173	43	16	4	10	0	1	9
15657	307	51	4	2	16	0	1	10
				2	12	0	1	10
				1	4	0	1	11
				4	13	0	1	12
				1	2	0	1	15
82901	911	91	2	31	34	0	1	12

Table 2: *Parameters of Borel Cayley Graphs*

these parameters, p, a, k, related by $a^k = 1 \pmod{p}$, are responsible for the determination of a Borel group (Definition 2). However, connections and hence the diameter are determined by the generators $\mathbf{A}, \mathbf{B}$ and their inverses, characterized by t_1, t_2, y_1, and y_2. In our research effort, we investigate how these parameters affect each other and the diameter of the graph. Table 2 illustrates the variations in diameter D as a result of different parameter values. In particular, the choices of t_1 and t_2 have a significant effect on the diameter D. For instance, a graph with size $N = 1081$ have diameters ranging from 7 to 9, depending on t_1 and t_2. In the following subsections, we summarize our results.

3.1 Parameters: p, a, k

As stated before, $N = p \times k$. That is, the size of a graph is determined by p and k. Furthermore, k is the *order* of $a \pmod{p}$, which implies that k divides $p-1$. However the reason to choose a particular value of a is not clear. Particularly, we have the following questions: (1) Is k the smallest or largest order for all possible a? (2) How many a have

order k? (3) For those a of the same order, do they generate the same set of numbers? In this section, we address these questions.

For any element $a \in \mathbf{Z}_p$, the smallest order is always 1, when $a = 1$; and the biggest order is always $p - 1$, when a is a *primitive root* of p. Furthermore, the possible values of k are the factors of $p - 1$. For example, when $p = 47$, $p - 1 = 2 \times 23$, and the possible values of k are 1, 2, 23 and 46.

The number of a with order k is given by the Euler function $\phi(k)$. Furthermore, these a generate the same set of numbers. These observations are supported by existing theorems [15]. They are summarized as follows:

Theorem 1 The number of a with order k is $\phi(k)$, where $\phi()$ is the Euler function. That is, for $k = p_1^{c_1} \times p_2^{c_2} \times p_3^{c_3} \times \ldots$

$$\phi(k) = k \times (1 - 1/p_1) \times (1 - 1/p_2) \times (1 - 1/p_3) \times \ldots$$

where $p_1, p_2, p_3, \ldots$ are prime numbers.

Theorem 2 For a prime p, if k divides $p - 1$, then $x^k = 1 \pmod{p}$ has exactly k roots.

The fact that different a generate the same set of numbers, implies that the choice of a has no effect on the group or the graph. Once p and k are being fixed, the size of the graph is determined, and any a with order k can be chosen.

3.2 Parameters: t_1, t_2, y_1, y_2

The parameters t_1, t_2, y_1, y_2 define the generators $\mathbf{A}, \mathbf{B}, \mathbf{A}^{-1}$ and $\mathbf{B}^{-1}$, which in turn define the connections and hence the diameter of the graph. From Table 2, it is clear that the choices of t_1 and t_2 play a crucial part in the determination of diameter. Furthermore, our computer analysis indicates that changing y_1 and y_2 do not change the diameter. This empirical observation is verified through the establishment of the following propositions. Again, we assume the generators of the degree-4 Borel Cayley graphs are $\mathbf{A}, \mathbf{B}, \mathbf{A}^{-1}, \mathbf{B}^{-1}$, according to Equation 2.

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

The proof of this proposition is a straight forward substitution and is omitted.

Proposition 2 For any paths $\mathbf{X}$, $\mathbf{Y}$, composed of generators $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}^{-1}$ and $\mathbf{B}^{-1}$, let

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

where $< x >_p$ denotes $x \pmod p$. Then

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

The proof of this proposition is included in [12] and is not repeated here. From this result, if $\mathbf{A}\ \mathbf{B} \neq \mathbf{B}\ \mathbf{A}$,

$$\mathbf{X} = \mathbf{Y} \Leftrightarrow \begin{cases} it_1 + jt_2 = i't_1 + j't_2 \pmod k \\ g = g' \text{and } h = h' \pmod p \end{cases} \text{ and} \tag{3}$$

The determination of the diameter of a graph basically involves generating the entire set of vertices from different compositions of generators. Equation 3 shows that, whether two different compositions, $\mathbf{X}$, $\mathbf{Y}$ correspond to the same node is independent of the values of y_1 and y_2. In other words, we have a useful corollary:

Corollary 1 The values of y_1 and y_2 do not affect the diameter, iff $\mathbf{A}\ \mathbf{B} \neq \mathbf{B}\ \mathbf{A}$.

4 A Pseudo-Random Formulation

In section 3.1 and 3.2, we have shown that the choices of a, y_1 and y_2 do not affect the connections of a Borel Cayley graph. The parameters that determine a Borel Cayley graph are: p, k, t_1, t_2. Based on this finding, we can use a constrained, simpler formulation of a Borel group. Assume a Borel group as defined in Definition 2. we define a *Borel coordinate group* $\mathbf{B}_{p,k}$ as follows:

Definition 4 For any prime number p and a factor of $p-1$, k, choose any a such that $a^k = 1 \pmod{p}$. We have a $\mathbf{B}_{p,k}$ with size $N = p \times k$ and

$$\mathbf{B}_{p,k} = \{(t, y) : t \in \mathbf{Z}_k,\ y \in \mathbf{Z}_p\}$$

For any (t, y), $(t', y') \in \mathbf{B}_{p,k}$, the group operation * is defined as:

$$(t, y) * (t', y') = (< t + t' >_k,\ < a^t y' + y >_p). \tag{4}$$

Accordingly, the generators $\mathbf{A}$, $\mathbf{B}$ in the group can be defined as:

$$\begin{array}{ll} \mathbf{A} = (t_1,\ y_1), & \mathbf{A}^{-1} = (k - t_1,\ < -a^{k-t_1} y_1 >_p) \\ \mathbf{B} = (t_2,\ y_2), & \mathbf{B}^{-1} = (k - t_2,\ < -a^{k-t_2} y_2 >_p) \end{array}$$

Since y_1 and y_2 do not affect the diameter, the simplest choices for y_1 and y_2 are

$$y_1 = \begin{cases} 0 \text{ if } t_1 \neq 0 \\ 1 \text{ if } t_1 = 0 \end{cases} \qquad y_2 = \begin{cases} 0 & \text{if } t_2 \neq 0 \text{ and } y_1 \neq 0 \\ 1 & \text{if } t_2 = 0 \text{ or } y_1 = 0 \end{cases}$$

Basically this new formulation has eliminated non-essential parameters and retained the properties of the original group. In this new formulation, only two integers are needed to specify an element; while in the original group, an element is represented by a 2×2 matrix, which requires four integers to specify. However, we observe that the elements on the second row of a Borel matrix are always 0 and 1, which implies that such a formulation carries redundant information. In our new formulation, modular integer arithmetic has replaced the more complicated, modular matrix multiplication of the original group.

Furthermore, the new group operation * (Equation 4) resembles the generation of pseudo-random numbers. The generation of pseudo-random numbers by digital computers has been well studied. The almost universally used method is the *mixed congruential scheme*, given by

$$x_{i+1} = \lambda x_i + c \pmod{T} \tag{5}$$

where λ and c are fixed odd integers and the $x_i < T$ are the sequence of random numbers. We observed that the operation on the y-coordinate in Equation 4 is similar to the mixed congruential scheme, Equation 5. Because of such similarity, we called this new formulation, a *pseudo-random formulation* of Borel Cayley graphs.

In comparing Equations 4 and 1, we also found a striking resemblance. Indeed, the Borel coordinate group, $\mathbf{B}_{p,k}$, defined in Definition 4 is a sub-class of the semi-direct product group SG proposed by Dinneen and defined in Definition 3. More specifically, if we choose, $m = k, n = p, r^c = a$ (Definition 3), $SG = Z_m \times_\sigma Z_k = \mathbf{B}_{p,k}$, where a has order k in Z_p. It is therefore not surprising that the densest known degree-4 Cayley graphs provided in [3] have the same number of nodes as that of Table 1. Using a computer program, we have also verified that the generators listed in [3] produce the same diameter in our pseudo-random formulation of the corresponding Borel Cayley graph.

5 Conclusions

Dense, symmetric graphs are good candidates for the interconnection topology of a multicomputer system. Borel Cayley graphs are attractive since they are symmetric and provide densest known degree-4 graphs for a range of diameters [6]. These graphs are constructed over a group of matrices. Connections of the graph are defined by postmultiplying vertices with generators in the generator set. Appropriate choices of generators are critical to the diameter of the graph.

Despite the increasing interest of Borel Cayley graphs as interconnection models, little is known about the parameters of these graphs. Most importantly, the relationship between the generators and the diameter of the graph is unknown. Currently, identification of "good" generators are achieved through random or extensive systematic search of all possibilities [4]. In an effort to resolve this problem, we investigate the parameters of Borel Cayley graphs. This technical report summarizes our findings.

By eliminating redundant information, we propose a new and simpler formulation of Borel Cayley graphs. This new formulation is defined in the integer domain and the group operation resembles the generation of pseudo-random numbers, hence the name *pseudo-random formulation.* In this new formulation, elements of the group are defined as coordinate pairs. For a degree-4 Borel Cayley graph, the generators are now considered as $\mathbf{A} = (t_1, y_1)$ and $\mathbf{B} = (t_2, y_2)$.

Through the establishment of propositions and corollaries, we proved that the values of y_1 and y_2 do not affect the diameter if and only if $\mathbf{AB} \neq \mathbf{BA}$. This result provides a guideline in choosing appropriate generators and thus reducing the computation time in the search of "good" generators. Using this new formulation, we also show that Borel Cayley graphs are isomorphic to the dense Cayley graphs proposed by Dinneen [3].

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

[3] M.J. Dinneen. *Algebraic Methods for Efficient Network Constructions.* Master's thesis, Department of Computer Science, University of Victoria, Victoria, B.C., Canada, 1991.

[4] L. Campbell et al. "Small Diameter Symmetric Networks from Linear Groups". *IEEE Transactions on Computers*, 41(2):218–220, February 1992.

[5] 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.

[6] K. Wendy Tang. *Dense Symmetric Interconnection Networks.* PhD thesis, Electrical Engineering Department, College of Engineering and Applied Science, University of Rochester, Rochester, New York, 1991.

[7] 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.

[8] N. Biggs. *Algebric Graph Theory.* Cambridge University Press, London, 1974.

[9] F. Annexstein, M. Baumslag, and A.L. Rosenberg. "Group Action Graphs and Parallel Architectures". *To be appeared in SIAM Journal of Computing*, 1990.

[10] K.D. Blaha. Algorithms for Permutation Groups and Cayley Networks. Technical Report CIS-TR-89-14, Department of Computer and Information Science, University of Oregon, September 1989.

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

[12] K.W. Tang and B.W. Arden. "Representations for Borel Cayley Graphs'. *SIAM Journal on Discrete Mathematics*, 1993. (accepted for publication).

[13] 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.

[14] K.W. Tang and B.W. Arden. "Class-Congruence Property and Two-Phase Routing for Borel Cayley Graphs'. *IEEE Transactions on Computers*, 1993. (submitted for publication).

[15] G.H. Hardy and E.M. Wright. *An Introduction To The Theory of Numbers.* Oxford University Press, Oxford, England, 1979.