Transactions Letters

Representations and Routing for Cayley Graphs

Bruce W. Arden and K. Wendy Tang

Abstract—**In the search for regular, undirected dense graphs for interconnection networks, Chudnovsky *et al.* found certain Cayley graphs that are the densest degree-four graphs known for an interesting range of diameters [1]. However, the group theoretic representation of Cayley graphs makes the development of effective routing algorithms difficult. This paper shows that all finite Cayley graphs can be represented by generalized chordal rings (GCR) and provides a sufficient condition for Cayley graphs to have chordal ring (CR) representations. Once a Cayley graph is represented in the modular integer domain of GCR or CR, existing routing algorithms can be applied. These include a progressive algorithm that finds a shortest path in incremental steps and a recursive algorithm that finds the entire path in a single computation.**

I. Introduction

SYMMETRIC, *regular, undirected* graphs are useful models for the interconnection of multicomputer systems. *Dense* graphs of this sort are particularly attractive. Here *density* means that there are a large number of vertices for a given *degree* and graph *diameter*. The degree of a regular graph is the uniform number of incident edges at each vertex and the diameter is the maximum of the minimum number of edges between any pair of vertices. A degree of four is emphasized in this paper because of its importance for practical interconnection.

Cayley graphs, based on group theoretic constructions, are in this category of graphs. Of special interest are Cayley graphs based on subgroups of the general linear 2×2 matrices where the group operation is modular matrix multiplication. These matrices are not convenient as labels for a computer address space. Hence it is useful to map these matrix elements into integers, preserving the inherent symmetry or *vertex-transitivity,* to the extent possible. This paper shows that all Cayley graphs can be represented as generalized chordal rings (GCR), which have integer labels and are symmetrical. Thus these representations are candidates for practical implementation, including the development of routing algorithms.

Paper approved by the Editor for Network Management of the IEEE Communications Society. Manuscript received August 22, 1989; revised May 3, 1990. This paper was presented at the 1990 ACM 18th Annual Computer Science Conference, Washington, DC, February 20–22, 1990.

B. W. Arden is with the Department of Electrical Engineering, University of Rochester, Rochester, NY. 14627.

K. W. Tang is with the Department of Electrical Engineering, SUNY at Stony Brook, Stony Brook, NY 11794.

IEEE Log Number 9102281.

II. Cayley Graphs

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

Definition 1: A graph $\boldsymbol{C} = (\boldsymbol{V}, \boldsymbol{G})$ is a Cayley graph with vertex set $\boldsymbol{V}$ if two vertices $v_1, v_2 \in \boldsymbol{V}$ are adjacent $\Leftrightarrow v_1 = v_2 * g$ for some $g \in \boldsymbol{G}$ where $(\boldsymbol{V},^*)$ is a finite group and $\boldsymbol{G} \subset \boldsymbol{V} \setminus \{I\}$. $\boldsymbol{G}$ is called the generator set of the graph.

Note that the identity element I is excluded from $\boldsymbol{G}$. This prevents the graph from having self-loops. A Cayley graph is undirected if $\boldsymbol{G}$ is closed under inversion, and the graph's degree is $|G|$. In this paper, we are interested in undirected, degree-4 Cayley graphs. In other words, we are dealing with Cayley graphs whose generator set consists of two group elements and their inverses.

The definition of Cayley graphs requires vertices to be elements of a group but does not specify a particular group. The flexibility of choosing different groups in the construction allows Cayley graphs to be defined in different domains. Carlsson [2], Akers [3], Margulis [4], and Chudnovsky [1] have defined Cayley graphs in various domains. Despite the wide range of possible Cayley graphs, all Cayley graphs share the following property:

Theorem 1: All Cayley graphs are vertex-transitive.

The proof of the theorem can be found in [5] and is not repeated here.

An immediate consequence of this theorem is stated in the following corollary:

Corollary 1: Let $\boldsymbol{C} = (\boldsymbol{V}, \boldsymbol{G})$ be a Cayley graph as defined;

$$a, b \in \boldsymbol{V} \text{ are adjacent } \Leftrightarrow a', b' \text{ are adjacent and } a', b' \in \boldsymbol{V}$$

where $a' = T * a$ and $b' = T * b$ for any $T \in \boldsymbol{V}$.

Proof:

$$a, b \text{ are adjacent } \Leftrightarrow b = a * g \text{ for some } g \in \boldsymbol{G}$$

$$b' = T * b = T * a * g = a' * g \Leftrightarrow a', b' \text{ are adjacent;}$$

a' and b' are in $\boldsymbol{V}$ because $\boldsymbol{V}$ is closed under *. □

We refer to this property as the *transform property* of Cayley graphs and the element T as the *transform element.* It is this transform property that allows Cayley graphs in the group domain to be transformed to the modular integer domain of GCR, as discussed in Section III.

TABLE I
SIZE OF DEGREE-4 GRAPHS FOR CERTAIN DIAMETERS

Diameter	Moore Bound	Known Graphs (1987)	New Cayley Graphs
3	53	40	36
4	161	95	90
5	485	364	320
6	1457	731	730
7	4373	856	1081
8	13121	1872	2943
9	39365	4352	7439
10	118 097	13056	15657
11	354 293	—	38764
12	1 062 881	—	82901
13	3 118 645	—	140607

Among the various Cayley graphs, we have a special interest in Cayley graphs constructed by Margulis and Chudnovsky. In these two cases, subgroups of the general linear 2×2 matrices $\boldsymbol{GL_2(Z_p)}$ and modular matrix multiplication are chosen and the vertex set and the group operation, respectively. The vertices of these graphs are 2×2 matrices whose elements are in $\boldsymbol{Z_p}$ ($\boldsymbol{Z_p}$ is the ring of integers $\{0, 1, \cdots, p-1\}$ and p is prime). The group operation is the modular prime p matrix multiplication and the generators are two matrices and their inverses. Cayley graphs constructed by Chudnovsky are among the densest. That is, the number of vertices for a degree-4 graph of a given diameter is larger than previously known graphs of the same degree and diameter (Table I). The generally unrealizable Moore bound shown is obtained by considering four, degree-3 trees joined at a common root vertex. In the following subsections, we discuss the Cayley graphs of these two subgroups separately.

A. Cayley Graph over $\boldsymbol{SL_2(Z_p)}$

Margulis [4] gave an explicit construction of Cayley graphs $\boldsymbol{C}$ over the group of simple linear 2×2 matrices, $\boldsymbol{SL_2(Z_p)}$:

$$\boldsymbol{C} = (\boldsymbol{V}, \boldsymbol{G})$$

where $\boldsymbol{V} = \boldsymbol{SL_2(Z_p)}$ and $\boldsymbol{G} = \{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}^{-1}, \boldsymbol{B}^{-1}\}$ with $\boldsymbol{A} = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\boldsymbol{B} = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$.

The group of simple linear 2×2 matrices $\boldsymbol{SL_2(Z_p)}$, consists of *unimodular* (mod p) 2×2 matrices whose elements are in $\boldsymbol{Z_p}$. Note that a matrix is unimodular (mod p) if its determinant is one (mod p). A Cayley graph constructed over this group has $n = |\boldsymbol{V}| = p(p^2 - 1)$ elements because there are $p^2(p-1)$ matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a \neq 0$ and $p(p-1)$ matrices with $a = 0$.

One of the features of these Cayley graphs is the regularity of their cycle structure. Since $\boldsymbol{A}^p = \boldsymbol{B}^p = \boldsymbol{I}$, all cycles generated solely by $\boldsymbol{A}$ or $\boldsymbol{B}$ have length p. As examples, for $p = 3$, there are 24 vertices and the diameter is 4; and for $p = 5$, there are 120 vertices and the diameter is 6. These graphs are not the densest for their degree and diameter. However, they stimulate investigation of Cayley graphs over subgroups of the general 2×2 matrices.

B. Cayley Graphs over $\boldsymbol{BL_2(Z_p)}$

Chudnovsky *et al.* constructed some of the densest (degree-4, diameter-D) graphs as Cayley graphs over the Borel subgroup, denoted as $\boldsymbol{BL_2(Z_p)}$, of the group of general linear 2×2 matrices. In this section, we provide the definition of $\boldsymbol{BL_2(Z_p)}$.

Definition 2: If $\boldsymbol{V}$ is a Borel subgroup of $\boldsymbol{GL_2(Z_p)}$ with a parameter a, $a \in \boldsymbol{Z_p} \backslash \{0, 1\}$, then

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

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 linear 2×2 matrices that satisfy the definition of a Borel subgroup, and modular matrix multiplication is chosen as the group operation *. Note that $n = |\boldsymbol{V}| = p \times k$. By choosing specific generators, Chudnovsky *et al.* [1] showed that Cayley graphs constructed over $\boldsymbol{BL_2(Z_p)}$ are the densest, nonrandom degree-4 graphs currently known for diameter 7 to 13 (Table I).

Interestingly, the densest degree-4 graphs have been shown by Bollobas [6] to have a random structure and to have asymptotic diameter of $\log_3 n + \log_3 0.5(\log_3 n) + 1$. By comparison, all but one of Chudnovsky's degree-4 Cayley graphs have a diameter less than this bound [1]. Apparently the modular arithmetic introduces a pseudo-random connectivity that contributes to the favorable diameters. Strictly random graphs are obviously not symmetric whereas Cayley graphs have the distinct advantages of explicit construction and vertex-transitive symmetry. These properties can lead to an efficient routing algorithm.

III. REPRESENTATIONS

In this section we recall the definition of GCR [7], which is defined in the modular integer domain. We prove that all finite Cayley graphs can be transformed into the integer domain of GCR. We also provide a sufficient condition for a general Cayley graph to be represented by a special kind of GCR, called a chordal ring (CR) [8].

A. GCR Representations

In section 2, we provided the definition of Cayley graphs and discussed the transform property. Such a transform property is analogous to the definition of a GCR [7] which is restated as follows:

Definition 3: A graph $\boldsymbol{R}$ is a generalized chordal ring (GCR) if vertices of $\boldsymbol{R}$ can be labeled with integers mod n (n is the number of vertices), and there is a divisor q of n such that vertex i is connected to vertex j iff vertex $i + q \pmod{n}$ is connected to vertex $j + q \pmod{n}$.

According to this definition, vertices of a GCR are numbered from 0 to $n - 1$ and are classified into q classes. The classification is based on modulo q arithmetic. In other words, two vertices having the same residue (mod q) are considered to be in the same class. The connection rules of a vertex can be defined according to its class. Each class has a set of connection rules or connection constants. In short, a GCR can be characterized by its class structure and the modulo n addition that defines the connection rules for each class.

In the following proposition, we prove that for all finite Cayley graphs there exists an isomorphic mapping of the vertices of a Cayley graph $\boldsymbol{C}$ from the group element domain to the GCR integer $(\bmod\ n)$ domain. The graph obtained after the mapping is thus a GCR representation of $\boldsymbol{C}$ in the modular integer domain. The GCR representation, with integer labels and modular connectivity rules, is not a Cayley graph because the group theoretic definition does not apply in this domain. But, importantly, the connectivity, and hence the diameter, of the Cayley graph is preserved. We state our proposition as follows:

Proposition 1: For any Cayley graph $\boldsymbol{C} = (\boldsymbol{v}, \boldsymbol{G})$ as defined, a generalized chordal ring (GCR) representation of $\boldsymbol{C}$ is always possible if $\boldsymbol{V}$ is a finite group.

Proof: Since $\boldsymbol{V}$ is finite, any T in $\boldsymbol{V}$ satisfies $T^m = I$ and $n = |\boldsymbol{V}| = mq$ for some integer q. This implies the elements of $\boldsymbol{V}$ can be partitioned into q classes: $\boldsymbol{N}(a_0), \boldsymbol{N}(a_1), \cdots, \boldsymbol{N}(a_{q-1})$, such that

$$\boldsymbol{N}(a_0) = \{a_0, T * a_o, \cdots, T^{m-1} * a_o\}$$
$$\boldsymbol{N}(a_1) = \{a_1, T * a_1, \cdots, T^{m-1} * a_1\}$$
$$\vdots$$
$$\boldsymbol{N}(a_{q-1}) = \{a_{q-1}, T * a_{q-1}, \cdots, T^{m-1} * a_{q-1}\}.$$

i.e., For any $a \in \boldsymbol{V}$

$$a = T^s * a_i \text{ for some } s = 0, 1, \cdots, (m-1) \quad \text{and} \quad i = 0, 1, \cdots, (q-1).$$

Consider the following function f from the group domain to the integer domain:

$$f : a \to i + sq.$$

Note that, for $s = 0$

$$a \to i$$
$$\Rightarrow T * a \to i + q.$$

Hence the connection of a Cayley graph after transforming into a GCR is preserved under this mapping. Also the function f is one-to-one:

For any two distinct $a, b \in \boldsymbol{V}$ $a = T^s * a_i,\ b = T^{s'} * a_{i'}$ for some $s, s' = 0, \cdots, (m-1)$ and $i, i' = 0, \cdots, (q-1)$.

$$\text{i.e., } a \to i + sq, \quad b \to i' + s'q.$$
$$a \neq b \Rightarrow s \neq s' \quad \text{or} \quad i \neq i' \quad \text{or both.}$$
$$\Rightarrow i + sq \neq i' + s'q$$
$$\Rightarrow f \text{ is one-to-one.} \qquad \square$$

The facts that f is one-to-one and preserves the transform property imply that the graph obtained after the mapping is a GCR with divisor q. Hence we proved that GCR representations exist for all finite Cayley graphs and the divisor of the GCR depends on the choice of the transformation element T. In the course of proving the proposition, we have essentially constructed an algorithm that finds a GCR representation of the graph. By definition, a GCR graph is partially vertex-transitive among vertices of the same class because i connects to j implies $i + q(\bmod\ n)$ connects to $j + q(\bmod\ n)$. However it is unclear that the general vertex-transitive property of the original Cayley graph is readily expressed in GCR representations. We deal with this issue in a separate report. In [9], we formulate a framework for expressing a Cayley graph's vertex-transitive property in the integer domain of a GCR.

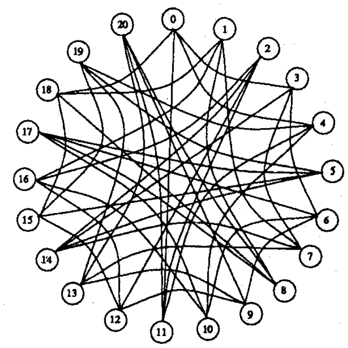

Fig. 1. GCR representation of $\boldsymbol{BL}_2(Z_7)$.

B. Example of GCR Representation

In this section, we show an example of GCR representation from $\boldsymbol{BL}_2(\boldsymbol{Z}_p)$.

We consider the Cayley graphs over $\boldsymbol{BL}_2(\boldsymbol{Z}_p)$ with $a = 2$ and $p = 7$. $\boldsymbol{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \boldsymbol{B} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ and their inverses are the generators. Note that is this case we have $k = 3$, $p = 7$, $n = p \times k = 21$, and the diameter is 3. We choose $\boldsymbol{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ with $\boldsymbol{T}^7 = \boldsymbol{I}$ to produce a GCR representation. The divisor $q = 3$.

Let $\boldsymbol{V} = \{0, 1, \cdots, 20\}$. For any $i \in \boldsymbol{V}$, if $i \bmod 3 =$:

"0" : i is connected to $i+3, i-3, i+4, i-10$; mod n
"1" : i is connected to $i+6, i-6, i+7, i-4$; mod n
"2" : i is connected to $i-9, i+9, i+10, i-7$.mod n(10)

We show such a GCR representation of the graph in Fig. 1.

C. CR Representations

In Section III-A, we have proved that all finite Cayley graphs possess GCR representations. It is tempting to think of the possibility of representing a Cayley graph in a special case of GCR. When the peripheral vertices are each connected to their nearest neighbor (i.e., each class has a $+1$ and a -1 connection to other vertices), we have a special case of GCR, called a chordal ring (CR) [8]. Clearly for a CR to exist the graph must have a Hamiltonian cycle. The following proposition provides a sufficient condition for representing a Cayley graph by a CR.

Proposition 2: Let A, B be two distinct generators of a finite Cayley graph $\boldsymbol{C}$. Assume $A \neq B^{-1}$, $A^q = I$ and $m = n/q$. If $(AB)^m = I$ or $(A^{-1}B)^m = I$ then CR representations with divisor q exist; and the transform element $T = AB$ or $A^{-1}B$.

Proof: $A^q = I$ and $n = mq$ implies that there are m cycles, each with q elements, generated solely by A. If all these m cycles are connected by another generator B, we have a Hamiltonian cycle. This is equivalent to either $(AB)^m = I$ or $(A^{-1}B)^m = I$. To obtain the CR representation, we choose the transformation element $T = (AB)$ or $(A^{-1}B)$, such that $T^m = I$. This choice insures that all q elements in each of the m cycles are named consecutively and hence are a CR representation. □

IV. Routing

In Section III, we proved that all finite Cayley graphs have GCR representations and provided a sufficient condition for Cayley graphs to have CR representations. By transformation to a GCR or CR, the vertices of a Cayley graph are necessarily given integer labels and are hence ordered as integers modulo n. Furthermore, the "class-connection" rules of a GCR or CR provide concise formulae for describing connections in Cayley graphs. Such a description facilitates the construction of routing algorithms. In this section we summarize a progressive routing algorithm [10] and reference a recursive routing algorithm [11]. We emphasize that the application of these algorithms for Cayley graphs is made possible because of the transformation to GCR or CR.

In [10], Reed and Fujimoto suggested a routing algorithm based on table lookup procedures for irregular networks. The idea is to produce a *routing table* of size $(n-1) \times \delta$ at each vertex (δ is the degree and n is the number of vertices). The table consists of $(n-1)$ rows and there are δ bits in each row, corresponding to the number of available links at each vertex. At vertex i, the 1-bit locations on row j of the table indicate the communication links that lead to shortest paths from vertices i to j. For example, if there are two shortest paths from vertex i to vertex j, and one corresponds to taking link 1 and the other corresponds to taking link 3, then at vertex i, row j of the routing table would have only the first and the third bit marked as 1.

In essence, the algorithm assumes that an incoming message, whether originating at the vertex or in transit from another vertex, contains the address of its ultimate destination. When such a message with ultimate destination j arrives at vertex i, row j of the routing table will be used to route the message to an appropriate outgoing link leading to a shortest path between i and j. In other words, this table lookup scheme finds shortest path(s) between any two vertices and works for any network. Routing is achieved through a routing table, which identifies outgoing links for any incoming message according to its destination. The space complexity of the algorithm is of $O(n^2)$ for the entire network because each vertex needs $(n-1) \times \delta$ bits and there are n vertices in the network. Since the time complexity for a single table lookup scheme is $O(1)$, it is $O(D)$ overall, where D is the graph diameter. This algorithm is progressive in that an incremental path computation is done at each vertex. Since alternative shortest paths are included in the tables, the algorithm is useful for the avoidance of contention. However, in some instances it is desirable to determine an entire shortest path in one step. This would be true when computation at vertices is separated from the message-passing function or when the path is of intrinsic interest.

There is a straight forward augmentation of the table look-up procedure to permit the determination of a complete, shortest path. Each vertex would contain a table of size $nD\lceil \log_2 \delta \rceil$ where each entry specifies an entire shortest path to the desired destination. This requires more space than the progressive approach by roughly a factor of D. Whenever entire paths are generated at the source, the resultant algorithm is necessarily *oblivious* or insensitive to routing alternatives at intermediate vertices.

The preceding schemes could be accomplished with any mapping of group elements into integers, but the symmetry of Cayley graphs suggests that it ought to be possible to determine complete paths through the repeated use of an identical, length $(n-1)$ table stored at each vertex. However, in order to accomplish this, and thus achieve complexity measures of the same order as the progressive algorithm, the relationship between the integer vertex labels in the GCR representation must be carefully constructed. As it turns out, such a construction is always possible for Cayley graphs based on Borel subgroups [9]. This is fortuitous because instances of these graphs are among the densest known [1].

There is yet another algorithm for complete path determination which leads to a space complexity of $O(n^2 q \log_2 D)$, where q is the number of classes [11]. This tree-matching, recursive algorithm has a parallel time complexity of $O(\log_2 D)$ or a serial complexity of $O(D)$. However, the algorithm does not necessarily produce a shortest path. Instead it generates a path whose length is bounded by $2^{s-1} <$ path length $\leq 2^s$, where the length of the shortest path S is similarly bounded, i.e., $2^{s-1} < S \leq 2^s$.

V. Conclusion

In this paper we analyze a special class of interconnection networks, derived from group theoretic Cayley graphs. These regular, undirected graphs are vertex-transitive, or symmetric, and some examples are among the densest known. Due to their vertex-transitivity, any Cayley graph can be represented as a generalized chordal ring (GCR). The graph vertices can thus be labeled with integers (modulo n), a more tractable addressing scheme for computer application.

An example Borel Cayley graph is used to illustrate the generation of GCR representations. Also a sufficient condition is given for the representation of a Cayley graph as an important special case of a GCR, namely a chordal ring (CR). Interestingly, this representation is always possible for Borel Cayley graphs [12].

With the integer (modulo n) labeling of GCR representations, a straight forward, progressive routing algorithm based on table look-up is summarized. The algorithm has a time complexity of $O(D)$ and a space complexity of $O(n^2)$. This algorithm is readily extended to one for total path determination but in the general case the space complexity becomes $O(n^2 D)$.

REFERENCES

[1] D. V. Chudnovsky, G. V. Chudnovsky, and M. M. Denneau, "Regular graphs with small diameter as models for interconnection networks," Tech. Rep. RC 13484-60281, IBM Res. Division, Feb. 1988.

[2] G. E. Carlsson, J. E. Cruthirds, and H. B. Sexton, "Interconnection networks based on a generalization of cube-connected cycles," *IEEE Trans. Comput.,* vol. 34, pp. 769–772, Aug. 1985.

[3] S. B. Akers and B. Krishnamurthy, "A group-theoretic model for symmetric interconnection networks," *IEEE Trans. Comput.,* vol. 38, pp. 555–565, Apr. 1989.

[4] G. A. Margulis, "Explicit construction of graphs without short cycles and low density codes," *Combinatorica,* vol. 2, no. 1, pp. 71–78, 1982.

[5] N. Biggs, *Algebric Graph Theory.* London, England: Cambridge University Press, 1974.

[6] B. Bollobas and W. Fernandex De La Vega, "The diameter of random regular graphs," *Combinatorica 2,* vol. 2, pp. 125–134, 1982.

[7] J. C. Bermond, C. Delorme, and J. J. Quisquater, "Tables of large graphs with given degree and diameter," *Inform. Processing Lett.,* vol. 15, no. 1, pp. 10–13, 1982.

[8] B. W. Arden and H. Lee, "Analysis of chordal ring network,: *IEEE Trans. Comput.,* vol. 30, 291–295, Apr. 1981.

[9] K.-M. W. Tang and B. W. Arden, "Vertex-transitivity and routing for Cayley graphs in GCR representations," Tech. Rep. EE-90-01, Dep. Elec. Eng. Univ. Rochester, Rochester, NY, Mar. 1990, to be published.

[10] D. A. Reed and R. M. Fujimoto, *Multi-Computer Networks.* Cambridge MA: MIT Press 1987.

[11] B. W. Arden and K-M. W. Tang. "Routing for generalized chordal rings," in *Proc. ACM 18th Comput. Sci. Conf.,* Washington, DC, Feb. 20–22 1990.

[12] K.-M. W. Tang and B. W. Arden, "Representation and routing of Borel Cayley graphs," Tech. Rep. EL-89-07, Dep. Elec. Eng., Univ. Rochester, Rochester, NY, 1989, to be published.