International Journal of Computer Mathematics
Vol. 82, No. 5, May 2005, 521–528

Some mathematical properties of Cayley digraphs with applications to interconnection network design

WENJUN XIAO†‡ and BEHROOZ PARHAMI*§

†Department of Mathematics, Xiamen University, Xiamen 361005
‡Department of Computer Science, South China University of Technology, Guangzhou 510641, P.R. China
§Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA 93106-9560, USA

(Received 30 July 2004; in final form 23 August 2004)

We consider the relationships between Cayley digraphs and their coset graphs with respect to subgroups and obtain some general results on homomorphism and broadcasting between them. We also derive a general factorization theorem on subgraphs of Cayley digraphs by their automorphism groups. We discuss the applications of these results to well-known interconnection networks such as the butterfly network, the de Bruijn network, the cube-connected cycles network and the shuffle-exchange network.

Keywords: Broadcasting; Cayley digraphs; Coset graphs; Cross-product graphs; Digraphs; Graph factorization; Homomorphism; Interconnection networks; Parallel processing

C.R. Categories: B.4.3; G.2.2

1. Introduction

It is known that Cayley (di)graphs and coset graphs are excellent models for interconnection networks [1–3]. Many well-known interconnection networks are Cayley (di)graphs or coset graphs. For example, hypercube, butterfly, and cube-connected cycles networks are Cayley graphs, while de Bruijn and shuffle-exchange networks are coset graphs [3].

As suggested by Heydemann [3], general theorems are lacking for Cayley digraphs and more group theory has to be exploited to find their properties. In this paper, we consider the relationships between Cayley digraphs and their coset graphs with respect to subgroups and obtain some general results on homomorphism and broadcasting between them. We also derive a general factorization theorem on subgraphs of Cayley digraphs by their automorphism groups. We provide several applications of these results to well-known interconnection networks such as butterfly, de Bruijn, cube-connected cycles and shuffle-exchange networks.

Before proceeding further, we introduce some definitions and notations related to interconnection networks and (di)graphs, in particular, Cayley (di)graphs. For more definitions and

*Corresponding author. Email: parhami@ece.ucsb.edu

International Journal of Computer Mathematics
ISSN 0020-7160 print/ISSN 1029-0265 online
http://www.tandf.co.uk/journals
DOI: 10.1080/00207160512331331101

Table 1. Key notation.

Unless explicitly specified, all graphs in this paper are directed graphs (digraphs)

$\bullet \le \bullet$	Subgroup relationship	BF_q	Butterfly network of order q
$\bullet \lhd \bullet$	Normal subgroup relationship	C_k	Cycle (ring network) of size k
$\bullet/\bullet$	Set of (right) cosets	C_k^+	Cycle with self-loop at each vertex
$\bullet \times \bullet$	Graph or set cross-product	Cay( )	Cayley graph
$\bullet$ wr $\bullet$	Wreath product	CCC_q	Cube-connected cycles of order q
$\bullet \oplus \bullet$	Graph composition	Cos( )	Coset graph
$\bullet^{(i)}$	The symbol $\bullet$ repeated i times	d, d^+, d^-	Degree, out-degree, in-degree
$(\bullet, \bullet)$	Directed edge ($\bullet \to \bullet$)	DB_d^q	de Bruijn network
$[\bullet, \bullet]$	Undirected edge ($\bullet$—$\bullet$)	$E(\,)$	Edge set of a graph
$\to$	Mapping	G, H	Groups
$\mapsto$	Bijection	K, N	Subgroups
Γ, Δ, Σ	Graphs or digraphs	R_i	Orbits of a group
Φ	Empty set	S, T	Generator sets, subsets of G
σ	Right-rotation operator	SE_d^q	Shuffle-exchange network
τ	Communication time to neighbour	$\mathrm{U}\Gamma$	Undirected form of Γ (e.g., UBF_q)
1	Identity element of a group	$V(\,)$	Vertex set of a graph
$A(\,)$	Adjacency matrix of a graph	Z_q	Cyclic group of order q
Aut( )	Automorphism	Z_d^q	Elementary abelian d-group of order d^q
b_M	Broadcast time under the model M		

basic results on graphs and groups we refer the reader to [4], for instance, and for interconnection networks to [5, 6]. Unless noted otherwise, all graphs in this paper are digraphs. Notation is shown in table 1.

A digraph $\Gamma = (V, E)$ is defined by a set V of vertices and a set E of arcs or directed edges. The set E is a subset of elements (u, v) of $V \times V$. If the subset E is symmetric, *i.e.*, $(u, v) \in E$ implies $(v, u) \in E$, we identify two opposite arcs (u, v) and (v, u) by the undirected edge $[u, v]$. We then obtain a graph. The out-degree (or in-degree) of a vertex u of a digraph Γ is the number of arcs (u, v) (or (v, u)) of Γ and is denoted by $d^+(u)$ (or $d^-(u)$). A digraph Γ is said to be regular of out-degree d if $d^+(u) = d^-(u)$ for every vertex u of Γ.

Let G be a finite group and S a subset of G. The subset S is said to be a generating set for G, and the elements of S are called generators of G, if every element of G can be expressed as a finite product of their powers. We also say that G is generated by S. The Cayley digraph of the group G and the subset S, denoted by Cay(G, S), has vertices that are elements of G and arcs that are ordered pairs (g, gs) for $g \in G$, $s \in S$. If S is a generating set of G then we will say that Cay(G, S) is the Cayley digraph of G generated by S. If $1 \notin S$ (1 is the identity element of G) and $S = S^{-1}$, then Cay(G, S) is a simple graph.

2. Some example networks

Let Z_q be a cyclic group of order q and Z_2^q the elementary abelian 2-group of order 2^q for some integer q. Now we can proceed to define four well-known interconnection networks: the butterfly network BF, the de Bruijn network DB, the cube-connected cycles network CCC and the shuffle-exchange network SE. These examples, and their associated formal definitions, set the stage for our discussions in the following sections.

The (wrapped, directed) butterfly network of order q, denoted BF_q, has $2^q q$ vertices that are the elements of group G which is the wreath product ($Z_2 \,\mathrm{wr}\, Z_q$) of Z_2 and Z_q, *i.e.*, a particular semidirect product of Z_2^q by Z_q. The elements of G are (x, l), where $l \in Z_q$ and $x = x_0 x_1 \ldots x_{q-1}$, with $x_i \in Z_2$ for $0 \le i \le q-1$. The identity of G is $(0^{(q)}, 0)$. The homomorphism h from the group Z_q into the automorphism group of the group Z_2^q, used

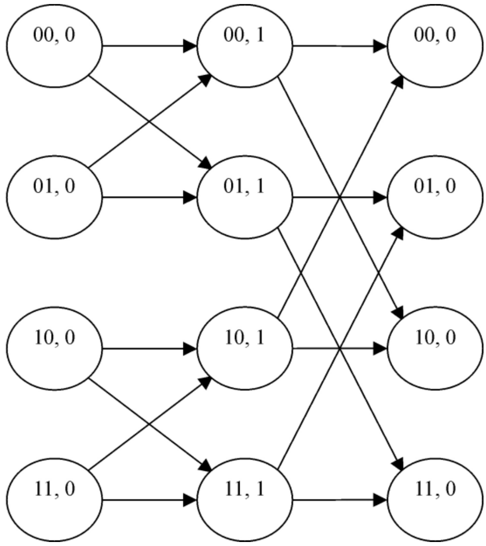

Figure 1. The (wrapped) butterfly network BF_2, with 2-cycles in rows unwrapped to avoid clutter.

in the semidirect product above, is defined by $l \to \{y \mapsto \sigma^l(y)\}$, where $\sigma(y_0y_1 \ldots y_{q-1}) = (y_{q-1}y_0 \ldots y_{q-2})$. Thus the product is given by

$$(x, l)(y, t) = (x + \sigma^l(y), l + t) = ((x_0 + y_{q-l})(x_1 + y_{q-l+1}) \ldots (x_{q-1} + y_{q-l-1}), l + t).$$

Let $S = \{(0^{(q)}, 1), (0^{(q-1)}1, 1)\}$. Then, according to [3], we have $BF_q = \mathrm{Cay}(G, S)$. Figure 1 depicts the BF_2 network, with vertices $(x_1x_0, 0)$ duplicated on the two sides to avoid clutter; this also explains the designation 'wrapped butterfly' which is sometimes used.

The de Bruijn network, denoted DB_d^q, has the vertex set Z_d^q and the arc set

$$\{(x_0x_1 \ldots x_{q-1}, x_1 \ldots x_{q-1}x_q) | x_i \in Z_d, 0 \le i \le q\}.$$

It is known that DB_d^q is regular of out-degree d. Figure 2 depicts the DB_2^3 network.

The (directed) cube-connected cycles network, denoted CCC_q, is a Cayley digraph whose vertex set, like that of BF_q, is $G = Z_2$ wr Z_q but has the generator set $S' = \{(0^{(q)}, 1), (0^{(q-1)}1, 0)\}$. Thus $CCC_q = \mathrm{Cay}(G, S')$. Figure 3 depicts the CCC_2 network using a layout of vertices that exposes its relationship to the butterfly network BF_2 in figure 1.

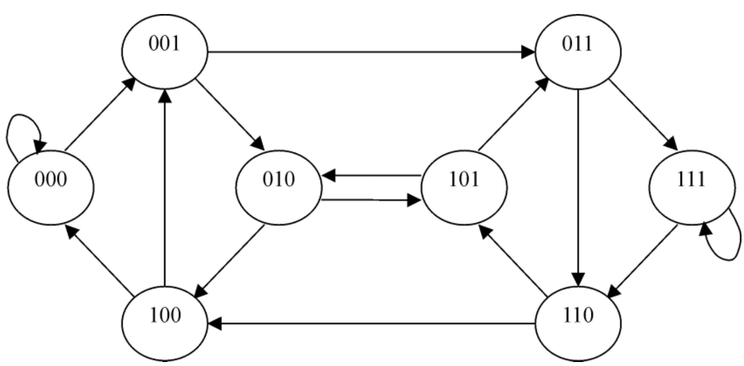

Figure 2. The de Bruijn network DB_2^3.

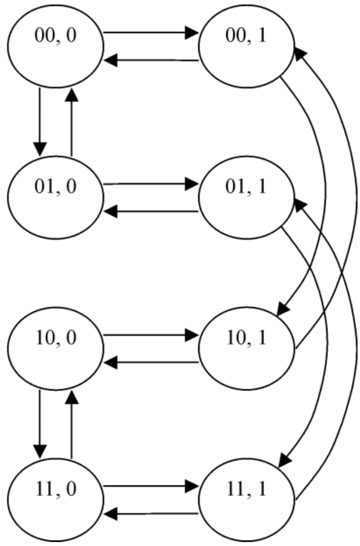

Figure 3. The cube-connected cycles network CCC_2. This is really an 8-node bidirectional cycle which is drawn in this way to facilitate understanding of the general structure and its correspondence to the butterfly network in figure 1.

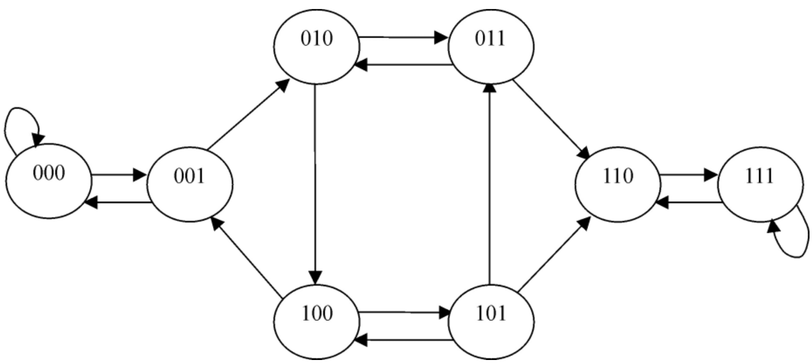

Figure 4. The shuffle-exchange network SE_2^3.

The shuffle-exchange network, denoted SE_d^q, has the vertex set Z_d^q and the arc set

$$\{(x_0x_1 \dots x_{q-1}, x_1 \dots x_{q-1}x_0), (x_0 \dots x_{q-2}x_{q-1}, x_0 \dots x_{q-2}(x_{q-1} + y)) | x_i \in Z_d, \\ 0 \le i \le q-1, y \in Z_d, y \ne 0\}.$$

Figure 4 depicts the shuffle-exchange network SE_2^3 as an example.

3. Cayley coset graphs

Assume that Γ and Σ are two digraphs. The mapping ϕ of $V(\Gamma)$ to $V(\Sigma)$ is a homomorphism from Γ to Σ if, for any $(u, v) \in E(\Gamma)$ we have $(\phi(u), \phi(v)) \in E(\Sigma)$. The tensor product $\Gamma \times \Sigma$ denotes the digraph with the vertex set $V(\Gamma) \times V(\Sigma)$ and the arc set

$$\{((x_1, x_2), (y_1, y_2)) | (x_1, y_1) \in E(\Gamma), (x_2, y_2) \in E(\Sigma)\}.$$

Let G be a finite group and S a subset of G. Assume that K is a subgroup of G (denoted as $K \leq G$). Let G/K denote the set of the right cosets of K in G. The (right) coset graph of G with respect to the subgroup K and subset S, denoted by $\mathrm{Cos}(G, K, S)$, is the digraph with the vertex set G/K such that there exists an arc (Kg, Kg') if and only if there exists $s \in S$ and $Kgs = Kg'$.

It is known [3] that the de Bruijn network DB_2^q is isomorphic to the coset graph of the butterfly network BF_q, *i.e.*, $\mathrm{DB}_2^q = \mathrm{Cos}(Z_2 \text{ wr } Z_q, Z_q, S)$, with $S = \{(0^{(q)}, 1), (0^{(q-1)}1, 1)\}$. Similarly, the shuffle-exchange network SE_2^q is isomorphic to the coset graph of the cube-connected cycles network CCC_q, *i.e.*, $\mathrm{SE}_2^q = \mathrm{Cos}(Z_2 \text{ wr } Z_q, Z_q, S')$, with $S' = \{(0^{(q)}, 1), (0^{(q-1)}1, 0)\}$.

3.1 *Mathematical properties*

Let us assume that the group G satisfies $G = NK$, where N is a normal subgroup of G (denoted by $N \lhd G$), $K \leq G$, and $N \cap K = 1$, *i.e.*, G is the semidirect product of N by K. Let $\Gamma = \mathrm{Cay}(G, S)$, $\Sigma = \mathrm{Cay}(G/N, NS/N)$ and $\Delta = \mathrm{Cos}(G, K, S)$, where S is a generating set of the group G. Then any element g of G can be uniquely expressed as $g = kn$ with $n \in N$, $k \in K$. Define the corresponding ϕ: $kn \mapsto (Kn, Nk)$ of $V(\Gamma) = G$ to $V(\Delta \times \Sigma)$. Then it is easily verified that ϕ is a bijection, and we have the following result.

THEOREM 1 *The mapping ϕ is a homomorphism of the digraph Γ to the digraph $\Delta \times \Sigma$.*

Proof Consider the diagram,

$$\begin{array}{ccc} kn & \xrightarrow{\phi} & (Kn, Nk) \\ \downarrow & & \downarrow \\ kns & \xrightarrow{\phi} & (Kn_1, Nk_1) \end{array}$$

where $kns = k_1 n_1$, $k_1 \in K$, $n_1 \in N$, $s \in S$ and (kn, kns) is any arc of the digraph Γ. Thus by virtue of $N \lhd G$, we obtain $Kn_1 = Kk_1n_1 = Kkns = Kns$ and $Nk_1 = Nk_1n_1 = Nkns = Nks$. Therefore $((Kn, Nk), (Kn_1, Nk_1))$ is an arc of the digraph $\Delta \times \Sigma$ and ϕ is a homomorphism of Γ to $\Delta \times \Sigma$. ■

As applications of theorem 1, we consider the following two examples.

Example 1 We relate the butterfly network BF_q to the de Bruijn network DB_2^q. Let $N = Z_2^q$ and $K = Z_q$. Then $G = Z_2 \text{ wr } Z_q$ is a semidirect product of N by K. Assuming $S = \{(0^{(q)}, 1), (0^{(q-1)}1, 1)\}$, we have $\Gamma = \mathrm{Cay}(G, S) = \mathrm{BF}_q$, $\Sigma = \mathrm{Cay}(G/N, NS/N) = \mathrm{C}_q$, where C_q is a directed cycle of order q, and $\Delta = \mathrm{Cos}(G, K, S) = \mathrm{DB}_2^q$. Thus we have a homomorphism ϕ from BF_q to $\mathrm{DB}_2^q \times \mathrm{C}_q$. In fact, it is easily shown that ϕ is an isomorphism and $\mathrm{BF}_q = \mathrm{DB}_2^q \times \mathrm{C}_q$.

Example 2 We relate the cube-connected cycles CCC_q and the shuffle-exchange network SE_2^q. Assume $N = Z_2^q$, $K = Z_q$ and $G = Z_2 \text{ wr } Z_q$, as in example 1. Let $S' = \{(0^{(q)}, 1), (0^{(q-1)}1, 0)\}$. Then $\Gamma = \mathrm{Cay}(G, S') = \mathrm{CCC}_q$, $\Sigma = \mathrm{Cay}(G/N, NS'/N) = \mathrm{C}_q^+$, where C_q^+ is a directed cycle of order q with a loop at every vertex, and $\Delta = \mathrm{Cos}(G, K, S') = \mathrm{SE}_2^q$. In this way, we obtain a homomorphism ϕ of CCC_q to $\mathrm{SE}_2^q \times \mathrm{C}_q^+$.

The diameter of a digraph is the maximum of (directed) distances between any two vertices. Based on the above, we note that using Cayley digraphs on groups that are semidirect products leads to a general method of constructing interconnection networks in the form of Cayley digraphs with small degrees and diameters.

(1) Pick a group N such that the diameter of the Cayley digraph Cay(N, T) is small for any generating set T.
(2) Choose a subgroup K of the automorphism group of N and construct the semidirect product $G = NK$.
(3) Choose a small generating set S of the group G and construct the Cayley digraph Cay(G, S).

The butterfly network BF_q and the cube-connected cycles CCC_q are two examples constructed in this manner. Following this method, we can derive many other new interconnection networks with small degrees and diameters.

3.2 *Application to broadcasting*

We now consider the broadcasting problem for interconnection networks. Broadcasting, a communication operation whereby a message is sent from one processor to all others, is a basic building block in the synthesis of parallel algorithms. The time τ to send a message from a processor to a neighbouring one depends on the communication model assumed, with linear- and constant-time models being the two main choices. We assume the constant-time model, wherein communication between adjacent processors needs one time unit.

In addition to communication delay, other assumptions relating to the communication mode are needed. We assume that messages are sent in store-and-forward mode where a processor cannot use the contents of a message, or send it on to another processor, until it has been received in its entirety. Given a connected graph G (representing an interconnection network) and a message originator u, the broadcast time $b_M(u)$ of the vertex u is the minimum time required to complete broadcasting from vertex u under the model M. The broadcast time $b_M(G)$ of G under M is defined as the maximum broadcast time of any vertex u in G, *i.e.* $b_M(G) = \max\{b_M(u) | u \in V(G)\}$. For more details, we refer the reader to [7].

Now let G be a finite group and $K \le G$. Assume that $\Gamma = \mathrm{Cay}(G, S)$ and $\Delta = \mathrm{Cos}(G, K, S)$ for some generating set S of G. For a communication model M, let $b_M(\Gamma_K)$ be the minimum time required to complete broadcasting in the vertices of K from the identity element 1 (which is the message originator). Our main result in this subsection is as follows.

THEOREM 2 $b_M(\Gamma) \le b_M(\Delta) + b_M(\Gamma_K)$.

Proof Let the message originator be the identity element 1. We first broadcast the message to all vertices of subgroup K of group G under the model M. The minimum time required to complete broadcasting in the vertices of K is $b_M(\Gamma_K)$. Consider now two cosets K and Ks of K in G for some $s \in S \setminus K$. Then (k, ks) is an arc of the graph Γ for any $k \in K$. For two different elements k and k_1 of K and $s \in S \setminus K$, (k, ks) and $(k_1, k_1 s)$ are parallel arcs of Γ. Hence the message can be forwarded from K to all vertices of Ks in only one step. Let Ku be any coset of K in G. Then, given that S is a generating set of G, we can assume that $Ku = Ks_1 s_2 \dots s_t$ for $s_1, s_2, \dots, s_t \in S$. Thus the message can be sent from K to all vertices of Ku in only t steps. The fact that $t \le b_M(\Delta)$ leads to the desired conclusion $b_M(\Gamma) \le b_M(\Delta) + b_M(\Gamma_K)$. ∎

As applications of theorem 2, we revisit examples 1 and 2.

Example 3 Consider the butterfly network BF_q and the de Bruijn network DB_2^q. By example 1, we know that $\Gamma = \mathrm{BF}_q$, $\Delta = \mathrm{DB}_2^q$. It is easily shown that $b_M(\Gamma_K) \le b_M(\mathrm{C}_q)$. Hence we obtain

$b_M(\Gamma) \leq b_M(\Delta) + b_M(\mathrm{C}_q)$. In general, $b_M(\mathrm{C}_q)$ is easily derived. For example, under the unit-time store-and-forward communication model, we have $b_M(\mathrm{C}_q) = q - 1$. Therefore we can obtain an upper bound on $b_M(\Gamma)$ when we know some upper bound on $b_M(\Delta)$. Similarly, any known lower bound on $b_M(\Gamma)$ leads to a corresponding lower bound on $b_M(\Delta)$.

Example 4 Consider the cube-connected cycles CCC_q and the shuffle-exchange network SE_2^q. By example 2, we have $b_M(\Gamma) \leq b_M(\Delta) + b_M(\mathrm{C}_q)$, where $\Gamma = \mathrm{CCC}_q$, $\Delta = \mathrm{SE}_2^q$. Therefore the observations made in example 3 also apply here.

The methods of this section can be extended to the other communication problems and to undirected graphs. For example, for the undirected butterfly network UBF_q and the undirected de Bruijn network UDB_2^q in [7], we have $b_M(\mathrm{UBF}_q) \leq b_M(\mathrm{UDB}_2^q) + b_M(\mathrm{UC}_q)$, where UC_q is an undirected cycle of order q.

4. Subgraph factorization

In this section, we assume that Γ is a finite digraph (possibly with loops) having the vertex set $V(\Gamma) = \{1, 2, \ldots, n\}$ and the arc set $E(\Gamma) = R$. Let $G = \mathrm{Aut}(\Gamma)$ be the automorphism group and $A(\Gamma)$ the adjacency matrix of the digraph Γ. Suppose that R_i, $1 \leq i \leq r$, are orbits of the group G acting on $V(\Gamma) \times V(\Gamma)$ such that $(x, y)^g = (x^g, y^g)$ for $x, y \in V(\Gamma)$ and $g \in G$. Let Γ_i be the digraph with the vertex set $V(\Gamma)$ and the arc set R_i for $1 \leq i \leq r$. Then we have $G = \bigcap_{i=1}^{r} \mathrm{Aut}(\Gamma_i)$. Let Φ denote the empty set. It is easily verified that

$$\begin{aligned} A(\Gamma) &= \Sigma\{A(\Gamma_i) | R \cap R_i \neq \Phi, 1 \leq i \leq r\} \\ R_i \cap R_j &= \Phi \text{ for } i \neq j \\ R &= \cup\{R_i | R \cap R_i \neq \Phi, 1 \leq i \leq r\} \end{aligned}$$

We denote the above as $\Gamma = \oplus\{\Gamma_i | R \cap R_i \neq \Phi, 1 \leq i \leq r\}$. Let Γ be a Cayley digraph Cay(H, S) for a finite group H and its generating set S. Then H can be regarded as the left regular automorphism group of Γ. Because $H \leq G \leq \mathrm{Aut}(\Gamma_i)$, the digraph Γ_i is a Cayley digraph [7]. In fact, it is easily proved that $\Gamma_i = \mathrm{Cay}(H, S_i)$ and $S_i = \{(x^g)^{-1} y^g | (x, y) \in R_i, g \in G\}$. Thus we obtain the following factorization theorem and associated examples.

THEOREM 3 *Cay*$(H, S) = \oplus\{$*Cay*$(H, S_i) | R \cap R_i \neq \Phi, 1 \leq i \leq r\}$.

Example 5 For the butterfly network BF_q, we have

$$\mathrm{BF}_q = \mathrm{Cay}(Z_2 \text{ wr } Z_q, \{(0^{(q)}, 1)\}) \oplus \mathrm{Cay}(Z_2 \text{ wr } Z_q, \{(0^{(q-1)}1, 1)\}).$$

Example 6 For the cube-connected cycles CCC_q, we have

$$\mathrm{CCC}_q = \mathrm{Cay}(Z_2 \text{ wr } Z_q, \{(0^{(q)}, 1)\}) \oplus \mathrm{Cay}(Z_2 \text{ wr } Z_q, \{(0^{(q-1)}1, 0)\}).$$

5. Conclusion

In this paper, we have supplied general theorems on homomorphism and broadcasting between Cayley digraphs and their coset graphs, and a factorization theorem on subgraphs of Cayley digraphs. We have also shown the applications of these results to some well-known interconnection networks: the butterfly network, the de Bruijn network, the cube-connected cycles network and the shuffle-exchange network. Many other useful directed and undirected networks can be similarly formulated and studied.

Because of the generality of these theorems, we believe that they will have further applications to interconnection networks, providing an interesting area for further research. In particular, the design of scalable interconnection networks for parallel processing [8], offering the desirable properties of simple routing algorithms, balanced communication traffic and resilience to node and link failures, can benefit from our results.

Acknowledgements

Wenjun Xiao's research was supported by the Natural Science Foundation of China and Fujian Province.

References

[1] Akers, S.B. and Krishnamurthy, B., 1989, A group theoretic model for symmetric interconnection networks. *IEEE Trans. Comput.*, **38**, 555–566.
[2] Annexstein, F., Baumslag, M. and Rosenberg, A.L., 1990, Group action graphs and parallel architectures. *SIAM J. Comput.*, **19**, 544–569.
[3] Heydemann, M., 1997, Cayley graphs and interconnection networks. In: G. Hahn and G. Sabidussi (Eds), *Graph Symmetry: Algebraic Methods and Applications*, pp. 167–224.
[4] Biggs, N., 1993, *Algebraic Graph Theory* (Cambridge: Cambridge University Press).
[5] Leighton, F.T., 1992, *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes* (San Mateo, California: Morgan Kaufmann).
[6] Parhami, B., 1999, *Introduction to Parallel Processing: Algorithms and Architectures* (New York: Plenum Press).
[7] Fraigniaud, P. and Lazard, E., 1994, Methods and problems of communication in usual networks. *Discrete Appl. Math.*, **53**, 79–133.
[8] Parhami, B., 2000, Challenges in interconnection network design in the era of multiprocessor and massively parallel microchips. *Proc. Int. Conf. on Communications in Computing* (Las Vegas, Nevoda: CSREA Press), pp. 241–246.