SIAM J. COMPUT.
Vol. 35, No. 3, pp. 741–765

MAPPING CYCLES AND TREES ON WRAP-AROUND BUTTERFLY GRAPHS*

MEGHANAD D. WAGH† AND OSMAN GUZIDE‡

Abstract. We give a new algebraic representation for the wrap-around butterfly interconnection network. This new representation is based on the direct product of groups and finite fields and allows an algebraic expression of the network connectivity. The abstract algebraic tools may then be employed to explore the structural properties of the butterfly. In this paper we exploit this model to map guest graphs on the butterfly. In particular, we provide designs of unit dilation mappings of all possible length cycles on butterflies. We also map the largest possible binary trees on butterfly networks with a dilation 2 if the network degree is less than 16, 3 if it is less than 32, and 4 if it is less than 64. This is a great improvement over previous results.

Key words. butterfly graphs, mathematical model, finite field, mapping, cycles, trees

AMS subject classifications. 68M07, 05C62, 68M10, 05C38

DOI. 10.1137/S0097539799365462

1. Introduction.

Distributed memory parallel architectures rely upon interconnection networks to communicate data and intermediate results between processors. With the rapid advances in semiconductor technology, the computational speeds of processors have far surpassed the improvements in communication speeds. Consequently, communication between processors is threatening to become a bottleneck in parallel processing.

Improving the communication characteristics of a parallel machine is a challenging problem because of the many conflicting demands on the interconnection networks. For example, scalability and cost issues force one to have a small (and, if possible, fixed) node degree and a small number of total edges. On the other hand, performance demands a large number of processors, a small network diameter, symmetry, and the possibility of mapping of common parallel algorithm skeletons on the architecture.

The *wrap-around butterfly network* represents a good trade-off between the cost and the performance of a parallel machine. It has a large number of processors, fixed node degree, low diameter, symmetry, and ability to support a variety of parallel algorithms. A *wrap-around butterfly network* of degree $n \geq 3$, B_n, is a graph with node set $Z_n \times \{0,1\}^n$ [7]. A node $(m,\ V)$ of B_n is connected to the four nodes shown in Figure 1.1. Note that in this figure, since $m \in Z_n$, $m+1$ and $m-1$ are evaluated modulo n. V is an n-bit binary vector $v_{n-1}, v_{n-2}, \ldots, v_0$, and 2^m refers to a length n vector with 1 in position m and 0's everywhere else. Thus an exclusive OR operation with 2^m alters exactly the mth bit of vector V. B_n is often visualized as an $n \times 2^n$ array of nodes with node (m, V) located in the mth row and Vth column of the array. Each node is connected only to nodes in the neighboring rows (except for the *wrap-around* links between the nodes of the 0th and the $(n-1)$th rows). The edges between nodes in the same row (same m) are often called *straight edges*, and those between nodes in different rows are the *diagonal edges*.

*Received by the editors December 5, 1999; accepted for publication (in revised form) July 21, 2005; published electronically February 3, 2006.
http://www.siam.org/journals/sicomp/35-3/36546.html
†Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA 18015 (mdw0@lehigh.edu).
‡Department of Computer and Information Sciences, Shepherd University, Shepherdstown, WV 25443 (oguzide@sheperd.edu).

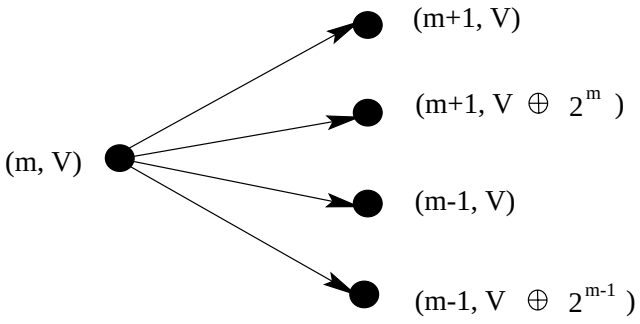

FIG. 1.1. *Connections from node* $(m,\ V)$ *in the butterfly network.*

The edges in a butterfly network are bidirectional, i.e., corresponding to an edge from $(m_1,\ V_1)$ to $(m_2,\ V_2)$, there is also an edge from $(m_2,\ V_2)$ to $(m_1,\ V_1)$. B_n is node symmetric and has $n2^n$ nodes and $n2^{n+1}$ edges. Its node degree is 4 and its diameter is $\lfloor 3n/2 \rfloor$. The degree 4 Cayley graph, proposed recently [13], is identical to B_n [3]. Cube connected cycles are a subgraph of B_n [4]. B_n supports many parallel algorithms well [7, 5, 8, 9, 10, 12]. It is shown that one can map cycles and trees on B_n with relatively low dilation [11, 6, 2].

This paper provides a new model for the wrap-around butterfly graph using a direct product of groups and finite fields. In this model, node connectivity can be expressed as an algebraic relationship between the node labels. This allows one to explore the structural properties of the butterfly network in much more direct fashion using powerful algebraic techniques. This paper investigates the mapping of guest graphs of cycles and trees to the butterfly host graph with the help of this new model. All our mappings have unit *load*; i.e., each vertex of a guest graph is mapped to a unique butterfly node. Our mappings also have a low *dilation*; i.e., neighboring vertices of the guest graphs are mapped either to neighboring butterfly nodes (unit dilation) or on nodes between whom paths of relatively small length exists. Unit load and low dilation characterize an efficient mapping. In the case of constant node degree networks such as the wrap-around butterflies, unit load and constant dilation imply a constant congestion. Further, a unit load and unit dilation mapping is a subgraph of the host graph of butterfly.

The rest of this paper is organized as follows. In section 2, we provide the details of our new representation of B_n and prove its isomorphism to the binary node labels. Section 3 is devoted to mapping of cycles to B_n. We enumerate cycles which can *never* be subgraphs of a wrap-around butterfly graph and then provide simple procedures to design all the remaining cycle subgraphs. In particular, we show that barring a few exceptions, it is possible to map (with unit dilation) an arbitrary length cycle to B_n when n is odd, and any even length cycle when n is even. Section 4 deals with mapping trees to B_n. We show that when n is less than 16, one can map the maximal binary balanced tree to B_n with a dilation of 2. Results for larger size networks are also provided. Finally, section 5 presents our conclusions.

2. Alternate representation of the butterfly. This section presents a new model of the wrap-around butterfly using the direct product of finite groups and fields. We show that in this model, network connectivity is expressed as a simple algebraic relationship (Theorem 2.1), thereby providing powerful algebraic tools to investigate its structural properties.

In the proposed representation, nodes of B_n are labeled with the elements of $Z_n \times GF(2^n)$.[1] Thus the new node labels would be $(m,\ X)$, where $m \in Z_n$ and $X \in GF(2^n)$. Integer m and the field element X would be referred to as the first and second indices of the node, respectively. We will provide the exact equivalence between the new node labels and the ones using the binary notation later, but first we summarize important properties of finite fields used in this paper. Reader is referred to [1] for detailed description of the algebraic notions used here.

The finite field $GF(2^n)$ is an extension of $GF(2)$. Similar to $GF(2)$, it uses modulo 2 addition; i.e., for any $X \in GF(2^n)$, $X + X = 0$. Elements of $GF(2^n)$ may be enumerated as $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^n-2}\}$, where the element α is known as the *primitive element*. $\alpha^{2^n-1} = 1$ and thus the elements of $GF(2^n)$ are closed under multiplication. The minimum degree polynomial (over $GF(2)$) of which α is a root, is called the *primitive polynomial*. Primitive polynomial has degree n and plays a central role in the design of $GF(2^n)$. Because α is a root of this degree n polynomial, elements of $GF(2^n)$ may also be expressed as polynomials (of degree at most $n-1$) in α over $GF(2)$. One can therefore view $GF(2^n)$ as a vector space over $GF(2)$ with basis $\langle \alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1\rangle$.

Fields $GF(2^4)$ and $GF(2^5)$ are illustrated in Tables 2.1 and 2.2, respectively. Expressing each element of $GF(2^n)$ in basis $\langle \alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1\rangle$ is fairly straightforward. For example, in Table 2.1, elements 1, α, α^2, and α^3 are already the basis elements. α^4 can be expressed using lower powers of α using the fact that α is the root of the primitive polynomial $x^4 + x + 1$. Thus $\alpha^4 + \alpha + 1 = 0$, or $\alpha^4 = \alpha + 1$. (Recall that $GF(2^n)$ uses modulo 2 additions.) The expressions for successive higher powers of α are obtained by multiplying the expressions for lower powers by α and replacing any α^4, thus created, by $\alpha + 1$. Tables 2.1 and 2.2 are important to simplify additions between field elements. For example, using Table 2.1, one may easily add α^{10} and α^{11} in $GF(2^4)$ as $\alpha^{10} + \alpha^{11} = (\alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) = \alpha^3 + \alpha = \alpha^{14}$.

Alternately, the elements of $GF(2^n)$ can be expressed over $GF(2)$ using the *dual basis* $\langle \beta_{n-1}, \beta_{n-2}, \ldots, \beta_0\rangle$. The dual basis is unique and its component β_i is defined as that element of $GF(2^n)$ which satisfies

$$\mathrm{Tr}(\alpha^j \beta_i) = \begin{cases} 1 & \text{if } j = i, \\ 0 & \text{otherwise,} \end{cases} \tag{2.1}$$

where the *Trace* function $\mathrm{Tr}(\cdot) : GF(2^n) \to GF(2)$ is computed as [1]

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + x^{2^3} + \cdots + x^{2^{n-1}}.$$

Tr(.) is a linear function over $GF(2)$, i.e.,

$$\mathrm{Tr}(aX + bY) = aTr(X) + bTr(Y), \qquad a, b \in GF(2), \quad X, Y \in GF(2^n).$$

Structure of the primitive polynomial governs the relationships between the dual basis elements. For the purposes of this paper, we will need only the relationship

$$\beta_{n-1} = \alpha\beta_0. \tag{2.2}$$

[1]Here, Z_n denotes the set of integers $\{0, 1, \ldots, n-1\}$ under the operation of addition modulo n and $GF(2^n)$ denotes the finite field of 2^n elements with characteristic 2.

TABLE 2.1
Structure of $GF(2^4)$.

Primitive polynomial: $x^4 + x + 1$ Elements and their relationships:	
0	$\alpha^7 = \alpha^3 + \alpha + 1$
1	$\alpha^8 = \alpha^2 + 1$
α	$\alpha^9 = \alpha^3 + \alpha$
α^2	$\alpha^{10} = \alpha^2 + \alpha + 1$
α^3	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 = \alpha + 1$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{14} = \alpha^3 + 1$
Dual base $\langle \beta_3, \beta_2, \beta_1, \beta_0 \rangle = \langle 1, \alpha, \alpha^2, \alpha^{14} \rangle$	

TABLE 2.2
Structure of $GF(2^5)$.

Primitive polynomial: $x^5 + x^4 + x^3 + x^2 + 1$ Elements and their relationships:	
0	$\alpha^{15} = \alpha^4 + \alpha^3 + \alpha + 1$
1	$\alpha^{16} = \alpha^3 + \alpha + 1$
α	$\alpha^{17} = \alpha^4 + \alpha^2 + \alpha$
α^2	$\alpha^{18} = \alpha^4 + 1$
α^3	$\alpha^{19} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$
α^4	$\alpha^{20} = \alpha + 1$
$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha^{21} = \alpha^2 + \alpha$
$\alpha^6 = \alpha^2 + \alpha + 1$	$\alpha^{22} = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{23} = \alpha^4 + \alpha^3$
$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2$	$\alpha^{24} = \alpha^3 + \alpha^2 + 1$
$\alpha^9 = \alpha^2 + 1$	$\alpha^{25} = \alpha^4 + \alpha^3 + \alpha$
$\alpha^{10} = \alpha^3 + \alpha$	$\alpha^{26} = \alpha^3 + 1$
$\alpha^{11} = \alpha^4 + \alpha^2$	$\alpha^{27} = \alpha^4 + \alpha$
$\alpha^{12} = \alpha^4 + \alpha^2 + 1$	$\alpha^{28} = \alpha^4 + \alpha^3 + 1$
$\alpha^{13} = \alpha^4 + \alpha^2 + \alpha + 1$	$\alpha^{29} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{14} = \alpha^4 + \alpha + 1$	$\alpha^{30} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
Dual base $\langle \beta_4, \beta_3, \beta_2, \beta_1, \beta_0 \rangle = \langle \alpha^{20}, \alpha^9, \alpha^{26}, \alpha^{18}, \alpha^{19} \rangle$	

In order to establish the equivalence between the binary labels used in section 1 and the new labels, we use the mapping $\psi : Z_n \times \{0,1\}^n \to Z_n \times GF(2^n)$,

$$\psi(m,\ v_{n-1}v_{n-2}\dots v_1v_0) = \left(m,\ \sum_{i=0}^{n-1} v_{(i+m) \bmod n}\ \beta_i\right). \tag{2.3}$$

Mapping ψ is one-to-one and onto because $\langle \beta_{n-1}, \beta_{n-2}, \dots, \beta_0 \rangle$ is a basis of $GF(2^n)$. We will show in Theorem 2.1 that ψ also preserves the connectivity of B_n.

Further, using the properties of β_i's one can show the inverse of ψ to be

$$\psi^{-1}(m, X) = (m,\ v_{n-1}v_{n-2}\dots v_1v_0),$$

where

$$v_i = \mathrm{Tr}(\alpha^{(i-m) \bmod n} X). \tag{2.4}$$

TABLE 2.3
Equivalence between the nodes of B_5 and graph $Z_5 \times GF(2^5)$.

Label	$(m,\ x)$
(0, 00000)	$(0,0)$
(0, 00001)	$(0,\alpha^{19})$
(0, 00010)	$(0,\alpha^{18})$
(0, 00011)	$(0,\alpha^{7})$
(0, 00100)	$(0,\alpha^{26})$
(0, 00101)	$(0,\alpha^{17})$
(0, 00110)	$(0,\alpha^{23})$
(0, 00111)	$(0,\alpha^{6})$
(0, 01000)	$(0,\alpha^{9})$
(0, 01001)	$(0,\alpha^{25})$
(0, 01010)	$(0,\alpha^{11})$
(0, 01011)	$(0,\alpha^{16})$
(0, 01100)	$(0,\alpha^{22})$
(0, 01101)	$(0,\alpha^{14})$
(0, 01110)	$(0,\alpha^{5})$
(0, 01111)	$(0,\alpha)$
(0, 10000)	$(0,\alpha^{20})$
(0, 10001)	$(0,\alpha^{8})$
(0, 10010)	$(0,\alpha^{27})$
(0, 10011)	$(0,\alpha^{24})$
(0, 10100)	$(0,\alpha^{10})$
(0, 10101)	$(0,\alpha^{12})$
(0, 10110)	$(0,\alpha^{15})$
(0, 10111)	$(0,\alpha^{2})$
(0, 11000)	$(0,\alpha^{21})$
(0, 11001)	$(0,\alpha^{28})$
(0, 11010)	$(0,\alpha^{13})$
(0, 11011)	$(0,\alpha^{3})$
(0, 11100)	$(0,\alpha^{29})$
(0, 11101)	$(0,\alpha^{4})$
(0, 11110)	$(0,\alpha^{30})$
(0, 11111)	$(0,1)$
(1, 00000)	$(1,0)$
(1, 00001)	$(1,\alpha^{20})$
(1, 00010)	$(1,\alpha^{19})$
(1, 00011)	$(1,\alpha^{8})$
(1, 00100)	$(1,\alpha^{18})$
(1, 00101)	$(1,\alpha^{27})$
(1, 00110)	$(1,\alpha^{7})$
(1, 00111)	$(1,\alpha^{24})$
(1, 01000)	$(1,\alpha^{26})$
(1, 01001)	$(1,\alpha^{10})$
(1, 01010)	$(1,\alpha^{17})$
(1, 01011)	$(1,\alpha^{12})$
(1, 01100)	$(1,\alpha^{23})$
(1, 01101)	$(1,\alpha^{15})$
(1, 01110)	$(1,\alpha^{6})$
(1, 01111)	$(1,\alpha^{2})$
(1, 10000)	$(1,\alpha^{9})$
(1, 10001)	$(1,\alpha^{21})$
(1, 10010)	$(1,\alpha^{25})$
(1, 10011)	$(1,\alpha^{28})$
(1, 10100)	$(1,\alpha^{11})$
(1, 10101)	$(1,\alpha^{13})$
(1, 10110)	$(1,\alpha^{16})$
(1, 10111)	$(1,\alpha^{3})$
(1, 11000)	$(1,\alpha^{22})$
(1, 11001)	$(1,\alpha^{29})$
(1, 11010)	$(1,\alpha^{14})$
(1, 11011)	$(1,\alpha^{4})$
(1, 11100)	$(1,\alpha^{5})$
(1, 11101)	$(1,\alpha^{30})$
(1, 11110)	$(1,\alpha)$
(1, 11111)	$(1,1)$
(2, 00000)	$(2,0)$
(2, 00001)	$(2,\alpha^{9})$
(2, 00010)	$(2,\alpha^{20})$
(2, 00011)	$(2,\alpha^{21})$
(2, 00100)	$(2,\alpha^{19})$
(2, 00101)	$(2,\alpha^{25})$
(2, 00110)	$(2,\alpha^{8})$
(2, 00111)	$(2,\alpha^{28})$
(2, 01000)	$(2,\alpha^{18})$
(2, 01001)	$(2,\alpha^{11})$
(2, 01010)	$(2,\alpha^{27})$
(2, 01011)	$(2,\alpha^{13})$
(2, 01100)	$(2,\alpha^{7})$
(2, 01101)	$(2,\alpha^{16})$
(2, 01110)	$(2,\alpha^{24})$
(2, 01111)	$(2,\alpha^{3})$
(2, 10000)	$(2,\alpha^{26})$
(2, 10001)	$(2,\alpha^{22})$
(2, 10010)	$(2,\alpha^{10})$
(2, 10011)	$(2,\alpha^{29})$
(2, 10100)	$(2,\alpha^{17})$
(2, 10101)	$(2,\alpha^{14})$
(2, 10110)	$(2,\alpha^{12})$
(2, 10111)	$(2,\alpha^{4})$
(2, 11000)	$(2,\alpha^{23})$
(2, 11001)	$(2,\alpha^{5})$
(2, 11010)	$(2,\alpha^{15})$
(2, 11011)	$(2,\alpha^{30})$
(2, 11100)	$(2,\alpha^{6})$
(2, 11101)	$(2,\alpha)$
(2, 11110)	$(2,\alpha^{2})$
(2, 11111)	$(2,1)$
(3, 00000)	$(3,0)$
(3, 00001)	$(3,\alpha^{26})$
(3, 00010)	$(3,\alpha^{9})$
(3, 00011)	$(3,\alpha^{22})$
(3, 00100)	$(3,\alpha^{20})$
(3, 00101)	$(3,\alpha^{10})$
(3, 00110)	$(3,\alpha^{21})$
(3, 00111)	$(3,\alpha^{29})$
(3, 01000)	$(3,\alpha^{19})$
(3, 01001)	$(3,\alpha^{17})$
(3, 01010)	$(3,\alpha^{25})$
(3, 01011)	$(3,\alpha^{14})$
(3, 01100)	$(3,\alpha^{8})$
(3, 01101)	$(3,\alpha^{12})$
(3, 01110)	$(3,\alpha^{28})$
(3, 01111)	$(3,\alpha^{4})$
(3, 10000)	$(3,\alpha^{18})$
(3, 10001)	$(3,\alpha^{23})$
(3, 10010)	$(3,\alpha^{11})$
(3, 10011)	$(3,\alpha^{5})$
(3, 10100)	$(3,\alpha^{27})$
(3, 10101)	$(3,\alpha^{15})$
(3, 10110)	$(3,\alpha^{13})$
(3, 10111)	$(3,\alpha^{30})$
(3, 11000)	$(3,\alpha^{7})$
(3, 11001)	$(3,\alpha^{6})$
(3, 11010)	$(3,\alpha^{16})$
(3, 11011)	$(3,\alpha)$
(3, 11100)	$(3,\alpha^{24})$
(3, 11101)	$(3,\alpha^{2})$
(3, 11110)	$(3,\alpha^{3})$
(3, 11111)	$(3,1)$
(4, 00000)	$(4,0)$
(4, 00001)	$(4,\alpha^{18})$
(4, 00010)	$(4,\alpha^{26})$
(4, 00011)	$(4,\alpha^{23})$
(4, 00100)	$(4,\alpha^{9})$
(4, 00101)	$(4,\alpha^{11})$
(4, 00110)	$(4,\alpha^{22})$
(4, 00111)	$(4,\alpha^{5})$
(4, 01000)	$(4,\alpha^{20})$
(4, 01001)	$(4,\alpha^{27})$
(4, 01010)	$(4,\alpha^{10})$
(4, 01011)	$(4,\alpha^{15})$
(4, 01100)	$(4,\alpha^{21})$
(4, 01101)	$(4,\alpha^{13})$
(4, 01110)	$(4,\alpha^{29})$
(4, 01111)	$(4,\alpha^{30})$
(4, 10000)	$(4,\alpha^{19})$
(4, 10001)	$(4,\alpha^{7})$
(4, 10010)	$(4,\alpha^{17})$
(4, 10011)	$(4,\alpha^{6})$
(4, 10100)	$(4,\alpha^{25})$
(4, 10101)	$(4,\alpha^{16})$
(4, 10110)	$(4,\alpha^{14})$
(4, 10111)	$(4,\alpha)$
(4, 11000)	$(4,\alpha^{8})$
(4, 11001)	$(4,\alpha^{24})$
(4, 11010)	$(4,\alpha^{12})$
(4, 11011)	$(4,\alpha^{2})$
(4, 11100)	$(4,\alpha^{28})$
(4, 11101)	$(4,\alpha^{3})$
(4, 11110)	$(4,\alpha^{4})$
(4, 11111)	$(4,1)$

Table 2.3 provides the mapping ψ between the two representations of B_5. In

order to illustrate the entries in this table, consider mapping of a butterfly node $(0,\ 01011) \in Z_n \times \{0,1\}^n$ to its new algebraic setting. The dual basis of $GF(2^5)$ given in Table 2.2 is $\langle \alpha^{20}, \alpha^9, \alpha^{26}, \alpha^{18}, \alpha^{19} \rangle$. Thus

$$\begin{aligned}\psi(0,\ 01011) &= (0,\ \alpha^9 + \alpha^{18} + \alpha^{19}) \\ &= (0,\ (\alpha^2+1) + (\alpha^4+1) + (\alpha^4+\alpha^3+\alpha^2+\alpha+1)) \\ &= (0,\ \alpha^3+\alpha+1) \ = \ (0,\ \alpha^{16}).\end{aligned}$$

Thus the butterfly node with binary label $(0,\ 01011)$ is renamed in the new algebraic notation as $(0,\ \alpha^{16})$.

We now state the central result of this section which expresses the connectivity of B_n through algebraic relationships between node labels.

THEOREM 2.1 (connectivity). *In B_n, a graph node (m, X) is connected to the four nodes $(m+1, \alpha X)$, $(m-1, \alpha^{-1}X)$, $(m+1, \alpha X+\beta_{n-1})$, and $(m-1, \alpha^{-1}X+\beta_0)$.*

Proof. Let

$$\psi(m,\ v_{n-1}v_{n-2}\dots v_1v_0) = (m,\ X) \qquad \text{and}$$
$$\psi(m+1,\ v'_{n-1}v'_{n-2}\dots v'_1v'_0) = (m+1,\ \alpha X).$$

Components v_i of the binary vector are related to m and X as in (2.4). Similar equation for v'_i gives

$$v'_i = \mathrm{Tr}(\alpha^{(i-m-1)\ mod\ n}\alpha X). \tag{2.5}$$

Now, if $i \neq m$, then $(i-m-1)\mathrm{mod}\ \ n \ < \ n-1$ and consequently $\alpha^{(i-m-1)\ mod\ n}\alpha = \alpha^{(i-m)\ mod\ n}$. On the other hand, if $i = m$, then $\alpha^{(i-m-1)\ mod\ n}\alpha = \alpha^n$. Using this in (2.5) gives the values of v'_i as

$$v'_i = \begin{cases} \mathrm{Tr}(\alpha^{(i-m)\ mod\ n}X) & \text{if } i \neq m, \\ \mathrm{Tr}(\alpha^n X) & \text{if } i = m. \end{cases} \tag{2.6}$$

Comparing (2.4) and (2.6) one now gets

$$v'_i = \begin{cases} v_i & \text{if } i \neq m, \\ v_m \text{ or } v_m \oplus 1 & \text{if } i = m. \end{cases} \tag{2.7}$$

The second line of (2.7) is obtained by noting that the $\mathrm{Tr}(\alpha^n X)$ is either 0 or 1, and therefore equals either v_m or $v_m \oplus 1$. Since the binary vectors $(v_{n-1}v_{n-2}\dots v_1v_0)$ and $(v'_{n-1}v'_{n-2}\dots v'_1v'_0)$ are equal, except possibly in the mth bit, Figure 1.1 shows that nodes $(m,\ v_{n-1}v_{n-2}\dots v_1v_0)$ and $(m+1,\ v'_{n-1}v'_{n-2}\dots v'_1v'_0)$ are connected. Thus $(m,\ X)$ is connected to $(m,\ \alpha X)$.

To show that $(m+1,\ \alpha X + \beta_{n-1})$ is connected to $(m,\ X)$, suppose

$$\psi(m+1,\ v'_{n-1}v'_{n-2}\dots v'_1v'_0) = (m+1,\ \alpha X + \beta_{n-1}).$$

In this case, v'_i is obtained as

$$v'_i = \mathrm{Tr}(\alpha^{(i-m-1)\ \mathrm{mod}\ n}(\alpha X + \beta_{n-1})). \tag{2.8}$$

As before, if $i \neq m$, $(i-m-1)\ \mathrm{mod}\ n \ < \ n-1$. Using this and the linearity of the trace function in (2.8) gives

$$v'_i = \begin{cases} \mathrm{Tr}(\alpha^{(i-m)\ \mathrm{mod}\ n}X) + \mathrm{Tr}(\alpha^{i-m-1\ mod\ n}\beta_{n-1}) & \text{if } i \neq m, \\ \mathrm{Tr}(\alpha^n X) + \mathrm{Tr}(\alpha^{n-1}\beta_{n-1}) & \text{if } i = m. \end{cases} \tag{2.9}$$

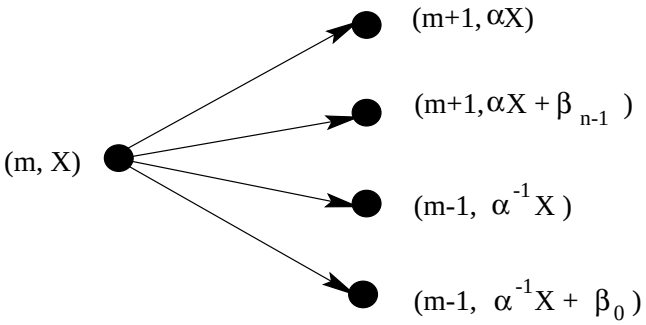

FIG. 2.1. *Connections from node* $(m,\ X) \in Z_n \times GF(2^n)$ *in the butterfly network.*

Employing the definition of β_{n-1}, (see (2.1)), this becomes

$$v_i' = \begin{cases} v_i & \text{if } i \neq m, \\ v_m \text{ or } v_m \oplus 1 & \text{if } i = m. \end{cases}$$

As before, $\mathrm{Tr}(\alpha^n X) + 1$ in the second line of (2.9) is replaced by v_m or $v_m \oplus 1$ because it is either 0 or 1. Therefore from Figure 1.1, $(m,\ X)$ is connected to $(m,\ \alpha X + \beta_{n-1})$.

The other two connections specified in the theorem can be proved similarly by substituting α^{-1} and β_0 in place of α and β_{n-1}, respectively. □

The four edges from $(m,\ X) \in Z_n \times GF(2^n)$ are shown in Figure 2.1. Because of (2.2), these edges are bidirectional. It should be pointed out here that even though the four edges in Figure 2.1 map to the four edges in Figure 1.1, the exact correspondence between them is dependent upon the source node $(m,\ X)$ and, in particular, on the equality of $\mathrm{Tr}(\alpha^n X)$ and the bit v_m of binary vector V. An edge from node $(m,\ X)$ to $(m{+}1,\ \alpha X)$ is sometimes a *straight edge* and sometimes a *diagonal edge*. For example, as can be seen from Table 2.3, the edge between nodes $(1,\ \alpha^{22})$ and $(2,\ \alpha^{23})$ in B_5 is a straight edge since the binary labels of these nodes are (0, 01100) and (1, 01100), respectively. On the other hand, the edge between nodes $(1,\ \alpha^{23})$ and $(2,\ \alpha^{24})$ is a diagonal edge since the binary labels of these nodes are (1, 01100) and (2, 01110), respectively. Thus the correspondence between the binary labels and their algebraic counterparts is more intricate than one might initially suppose.

Redefining B_n in the new algebraic notation allows use of simple but powerful algebraic techniques to study its structure. Also, unlike the binary representation (Figure 1.1), in the new algebraic notation (Figure 2.1) the two indices of a node change independently between connected nodes. This independence further simplifies our investigation.

3. Mapping cycles on the butterfly. This section provides comprehensive results about cycles as subgraphs of B_n. We first prove exactly which cycles are *not* subgraphs of B_n (Theorem 3.1). Then we provide simple procedures to map to B_n all the permissible cycles, i.e., those that are not enumerated in Theorem 3.1 (Theorems 3.3, 3.6, and 3.7). Earlier, Rosenberg [11] has given mappings of cycles of lengths $L = n$ or $L = n2^n - (n-2)c$, $1 \leq k \leq n$, $0 \leq c \leq 2^k$, on B_n. His results map at most $n + 2^{n+1} - 1$ cycles of different lengths on B_n when n is even and exactly $n + 2^{n+1} - 1$ cycles when n is odd. On the other hand, we give constructions of all the cycle subgraphs of B_n that are ever possible. Thus our methods map as many as

$n2^n - (n+5)/2$ cycles of different lengths on B_n when n is odd and at least $n2^{n-1} - 3$, when n is even.

We begin by specifying which cycles can *never* be subgraphs of B_n.

THEOREM 3.1 (impossible cycles). *Simple cycles (i.e., cycles with distinct nodes) of the following lengths L are* never *subgraphs of B_n:*

(a) *odd L when n is even,*

(b) *odd L less than n,*

(c) *$L = 6$ when $n = 5$ or $n \geq 7$,*

(d) *$L = 10$ when $n = 7$, $n = 9$, or $n \geq 11$.*

Proof. (a). From Figure 2.1, if n is even and $(m,\ X)$ is connected to $(m',\ X')$, then exactly one of m and m' is odd and the other is even. This implies that for even n, B_n is a *bipartite graph*, and therefore an odd-length cycle cannot be its subgraph.

(b). Note that because of the connectivity described in Figure 2.1, the first indices of all the nodes in the cycle may be translated by the same amount to get another equivalent cycle. Thus when $L < n$, the solution can be embedded on a butterfly *without* using any wrap-around edges. But an unwrapped butterfly is a bipartite graph and therefore cannot have an odd-length cycle subgraph.

(c) and (d). These cases may be proved by enumerating all possibilities of mapping the cycle and then illustrating contradictions in each case. First note that it is impossible to have the first indices of any five consecutive nodes in a cycle to be m, $m+1$, m, $m+1$, and m. Because if $(m, X) \to (m+1, X_1) \to (m, X_2) \to (m+1, X_3) \to (m, X_4)$ are the five connected nodes, then from Figure 2.1, $X_1 = \alpha X + c\beta_{n-1}$, $c \in \{0, 1\}$. This gives $X_2 = X + \beta_0$. Clearly, the only choices for X_3 are $\alpha X + \beta_{n-1}$ and αX, giving X_4 equal to $X + \beta_0$ or X. Thus node (m, X_4) is not distinct and the assumed chain of five nodes does not exist.

We can now demonstrate the impossibility of cycle mapping for $L = 6$. The case of $L = 10$ can be proved similarly. Let, if possible,

$$(m_0, X_0) \to (m_1, X_1) \to (m_2, X_2) \to (m_3, X_3) \to (m_4, X_4) \to (m_5, X_5) \to (m_0, X_0)$$

denote the length 6 cycle which is a subgraph of B_n, $n \geq 7$. Clearly, the first index of all cycle nodes can be increased or decreased by the same amount, or the direction of the cycle traversal may be reversed without disturbing the connectivity. Therefore, without loss of generality, one may choose $m_0 = 0$ and $m_1 = 1$. Clearly $m_5 = 1$ as well, because one cannot go from $m_1 = 1$ to $m_5 = n - 1$ in only 4 hops since $n \geq 7$. Indices m_2, m_3, and m_4 should satisfy two conditions: (1) cyclically successive values in the sequence $(m_0, m_1, m_2, m_3, m_4, m_5)$ change only by 1; (2) no five cyclically consecutive values in the sequence are $(m, m+1, m, m+1, m)$. It can be verified that under these conditions, the only possible set of values for m_0 through m_5 are $(0, 1, 2, 3, 2, 1)$. Without loss of generality, let $X_0 = X$, $X_1 = \alpha X$, and $X_5 = \alpha X + \beta_{n-1}$. Then for $c_i \in \{0, 1\}$, following successive links, one gets $X_2 = \alpha^2 X + c_1\beta_{n-1}$, $X_3 = \alpha^3 X + c_1\alpha\beta_{n-1} + c_2\beta_{n-1}$, $X_4 = \alpha^2 X + c_1\beta_{n-1} + c_2\alpha^{-1}\beta_{n-1} + c_3\beta_0$, and $X_5 = \alpha X + c_1\alpha^{-1}\beta_{n-1} + c_2\alpha^{-2}\beta_{n-1} + c_3\alpha^{-1}\beta_0 + c_4\beta_0$. Equating the two values of X_5 and then using $\beta_{n-1} = \alpha\beta_0$ give

$$\alpha^2 + (c_1 + c_4)\alpha + (c_2 + c_3) = 0.$$

But this is impossible since α cannot satisfy an equation of degree smaller than n.

When $L = 6$ and $n = 5$, the only possible set of values of m_0 through m_5 that need to be considered are $(0, 1, 2, 3, 2, 1)$, $(0, 1, 0, 4, 3, 4)$, $(0, 1, 2, 1, 0, 4)$, and $(0, 4, 3, 2, 3, 4)$. Note that if all the indices in any set are increased by a constant amount, then the

set transforms into a rotated version of the first set. For example, by adding 2 to each index of the second set, one gets set $(2, 3, 2, 1, 0, 1)$, which is simply the first set rotated left twice. Thus by dealing with only the first set, no generality is lost. But we demonstrated earlier that this first set does not produce a valid cycle of length 6. Therefore it is impossible to have a length 6 cycle as a subgraph of B_n when $n \geq 7$ or $n = 5$. □

To obtain cycle mappings for lengths not specified in Theorem 3.1 we proceed as follows. Theorem 3.3 gives the mappings when the cycle length L is divisible by n.[2] This also includes the Hamiltonian cycle. For other lengths that may be expressed as $L = Kn + 2t \leq n2^n$, for some $K > 0$ and $0 \leq t < n$, Theorem 3.6 shows that one can first design a cycle of length Kn and then attach t pairs of new nodes to it. Finally, an alternate procedure to map cycles of lengths less than $4n$ (except 6 and 10) is provided in Theorem 3.7.

In order to prove the existence of cycles in butterfly networks, we need the following lemma.

LEMMA 3.2. *$n \nmid (2^n - 1)$ for any integer $n > 1$.*

Proof. The lemma is obvious when n is an even integer. Further, when n is an odd prime, according to *Fermat's little theorem*, $2^n = 2 \bmod n$ which shows that for prime n, $n \nmid (2^n - 1)$. If possible, let n be the smallest odd integer such that $n \mid (2^n - 1)$. Clearly n must be composite. Let p denote the largest odd prime in n, i.e., $n = p^t p_1^{t_1} p_2^{t_2} \cdots$, where $p, p_1, p_2, \ldots$ are distinct primes, $p > p_1, p_2, \ldots$. Consider the group G of integers less than n and relatively prime to n under the operation of multiplication modulo n. The Euler phi-function $\phi(n)$ which represents the number of elements in G is given by

$$\phi(n) = (p-1)p^{t-1}(p_1 - 1)p_1^{t_1 - 1}(p_2 - 1)p_2^{t_2 - 1} \cdots . \tag{3.1}$$

As $2 \in G$, it satisfies

$$2^{\phi(n)} = 1 \bmod n. \tag{3.2}$$

Now, if $n \mid (2^n - 1)$, then

$$2^n = 1 \bmod n. \tag{3.3}$$

Equations (3.2) and (3.3) imply that

$$2^{gcd(\phi(n), n)} = 1 \bmod n. \tag{3.4}$$

Since p is the largest prime in n, the power of p in $\phi(n)$ according to (3.1) is $t - 1$. Therefore

$$\gcd(\phi(n), n) \mid (n/p). \tag{3.5}$$

From (3.4) and (3.5) one gets

$$2^{(n/p)} = 1 \bmod n,$$

and consequently,

$$2^{(n/p)} = 1 \bmod (n/p). \tag{3.6}$$

[2] We use the notation $n|L$ to indicate that L is a multiple of n, and $n \nmid L$ to indicate that L is *not* a multiple of n.

But this is contradictory to the assumption that n is the smallest integer satisfying $n \mid (2^n - 1)$. Hence there is no such n. ∎

We can now state the theorems on cycles in butterfly networks.

THEOREM 3.3 (cycles of length divisible by n). *Suppose L is an arbitrary multiple of n and $L \leq n2^n$. Then cycle of length L can be mapped to B_n with dilation 1.*

Proof. Let $g = \gcd(n, 2^n - 1)$. From Lemma 3.2, one gets $n/g \geq 2$. We consider the following two cases based on the magnitude of L.

Case 1. $L \leq n(2^n - 1)/g$. If $L = n(2^n - 1)/g$, choose any nonzero $X \in GF(2^n)$. Otherwise, $\alpha^L \neq 1$ in $GF(2^n)$; choose X as

$$X = \beta_{n-1}(1 + \alpha^L)^{-1}. \tag{3.7}$$

The required cycle may then be constructed as

$$(0,\ X) \to (1,\ \alpha X) \to (2,\ \alpha^2 X) \to \cdots \to ((L-1) \bmod n,\ \alpha^{L-1} X) \to (0,\ X). \tag{3.8}$$

From the graph connectivity described earlier, each node on this cycle is connected to the next. Observe that (3.7) implies that $\alpha^L X = X + \beta_{n-1}$, so the last edge in (3.8) also is valid. Further, the first component of the node label repeats with periodicity of n and the second, with periodicity $(2^n - 1)$. Therefore the same label will repeat only with a periodicity of $n(2^n - 1)/g$. Thus for $L \leq n(2^n - 1)/g$, all the nodes in the cycle are distinct.

Case 2. $L > n(2^n - 1)/g$. Partition L as

$$L = n + L_1 + L_2 + \cdots + L_t, \qquad \text{where } (2^n - 1) \leq L_i \leq n(2^n - 1)/g \text{ and } n | L_i. \tag{3.9}$$

One way to achieve this partition is to choose

$$t = \left\lceil \frac{g(L-n)}{n(2^n - 1)} \right\rceil, \tag{3.10}$$

set $L_i = n(2^n - 1)/g$ for $1 \leq i < t$, and adjust L_t to make up the total to L. If this $L_t < 2^n - 1$, then reduce L_{t-1} by some amount and increase L_t by the same amount. Since $n/g \geq 2$, $L_{t-1} \geq 2(2^n - 1)$. Therefore, one can always find an appropriate amount to shift from L_{t-1} to L_t so as to make both $L_{t-1}, L_t \geq 2^n - 1$.

To build the required cycle, first obtain t disjoint cycles C_i of lengths L_i as in Case 1. Cycles of length $n(2^n - 1)/g$ may be constructed by starting from arbitrary nonzero nodes not used in previous cycles and always going from $(m,\ x)$ to $(m{+}1,\ \alpha x)$. To create cycles of length less than $n(2^n - 1)/g$, compute the second index X of the starting node according to (3.7). Use a first index such that the node has not appeared in previous cycles. Note that this is possible because a node with the same second index repeats in a cycle only with a period of $2^n - 1$. In each cycle of length less than or equal to $n(2^n - 1)/g$, such labels occur at most n/g times. Since the number of cycles, t, is at most g (see (3.10)), unused labels (m, X) will be available to start new cycles.

Finally, build a cycle C_0 of length n as

$$(0,\ 0) \to (1,\ 0) \to (2,\ 0) \to \cdots \to (n-1,\ 0) \to (0,\ 0).$$

It is easy to see that the neighboring nodes in C_0 are connected and are distinct from those in the previous t cycles.

These $t + 1$ cycles can be merged together to form a single cycle as follows. Since each $L_i \geq 2^n - 1$, each cycle C_i, $1 \leq i \leq t$, contains consecutive elements

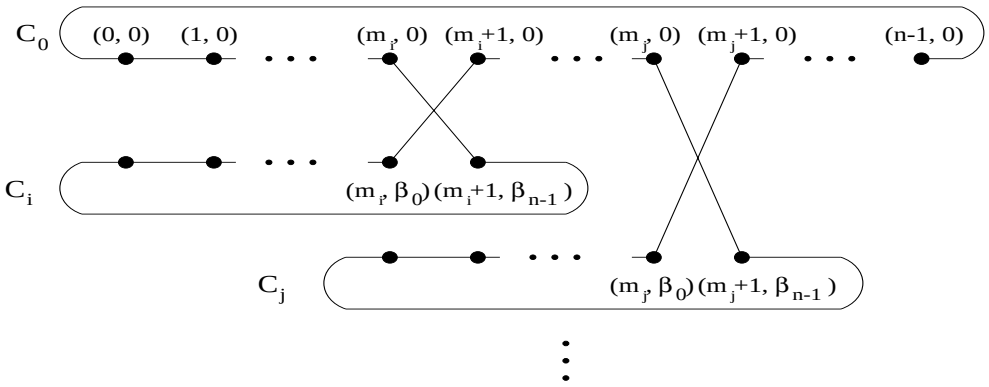

FIG. 3.1. *Merging C_0 and C_i's into a single cycle.*

$(m_i,\ \beta_0)$ and $(m_i+1,\ \beta_{n-1})$ for some $0 \le m_i < n$. To combine C_i and C_0, add edges $(m_i,\ \beta_0) \to (m_i+1,\ 0)$ and $(m_i+1,\ \beta_{n-1}) \to (m_i, 0)$ and remove edges $(m_i,\ \beta_0) \to (m_i+1,\ \beta_{n-1})$ and $(m_i,\ 0) \to (m_i+1,\ 0)$. Since the m_i for each C_i is different, each C_i can be joined with C_0 at a different place. This process of cycle merging is sketched in Figure 3.1. The resultant cycle thus has the desired length L. □

Note that for most values of n, we have $g = 1$. In fact, for $n \le 20$, the only values of n for which $g > 1$ are 6, 12, and 18. Case 2 of Theorem 3.3 is mostly useful for these n's. Using techniques similar to those of Theorem 3.3, it is also possible to map many disjoint cycles to B_n simultaneously. This is shown in the following corollary.

COROLLARY 3.4 (multiple cycles). *If $n|L$ and $L \le t(2^n-1)$ for some t, $0 < t < (n/g)$, one can map $g\lfloor n/(gt)\rfloor$ disjoint cycles of length L to B_n with dilation 1.*

Proof. Obtain X from (3.7) corresponding to the given L. Let h represent $(2^n - 1) \bmod n$. Begin the required cycles from

$$(hti_1 + i_2,\ X), \qquad 0 \le i_1 < \lfloor n/(tg)\rfloor,\ \ 0 \le i_2 < g, \tag{3.11}$$

and use the edges $(m,\ x) \to (m+1, \alpha x)$ repeatedly until each cycle is complete.

From Theorem 3.3, it is clear that length of each cycle is L. We need only to prove that the nodes used in each cycle are distinct. Assume that, if possible, the ith node of the cycle beginning at $(hti_1 + i_2,\ X)$ is the same as the i'th node of the cycle beginning at $(hti_1' + i_2',\ X)$, i.e.,

$$(hti_1 + i_2 + i,\ \alpha^i X) = (hti_1' + i_2' + i',\ \alpha^{i'} X). \tag{3.12}$$

We will show that this implies that the two starting nodes are identical, i.e., $i_1 = i_1'$ and $i_2 = i_2'$. This being contradictory to the construction described above, we conclude that the cycles are disjoint.

By comparing the second indices of the nodes in (3.12) we get

$$i - i' = q(2^n - 1) \qquad \text{for some integer } q. \tag{3.13}$$

Note that since $0 \le i, i' < L = t(2^n - 1)$, one has $q < t$. Comparison of the first indices in (3.12) yields

$$ht(i_1 - i_1') + (i_2 - i_2') + q(2^n - 1) \equiv 0 \pmod{n}$$

or

$$h(t(i_1 - i_1') + q) + (i_2 - i_2') \equiv 0 \pmod{n}. \tag{3.14}$$

Note now from the definition of h that

$$g = \gcd(2^n - 1,\ n) = \gcd((2^n - 1) \bmod n,\ n) = \gcd(h,\ n). \tag{3.15}$$

By reducing each term in (3.14) modulo g (a factor of n and h), one gets

$$i_2 \equiv i_2' \pmod{g}.$$

But since each $i_2,\ i_2' < g$,

$$i_2 = i_2'. \tag{3.16}$$

Combining this with (3.14) and using (3.15) give

$$i_1 t + q \equiv i_1' t \pmod{(n/g)}. \tag{3.17}$$

However, because of the bounds on i_1, i_1', t, and q, one can verify that $i_1 t + q < (n/g)$ as well as $i_1' t < (n/g)$. Therefore,

$$i_1 t + q = i_1' t.$$

Since $q < t$, this gives

$$i_1 = i_1'. \qquad \square$$

Corollary 3.4 allows one to efficiently utilize the butterfly architectures for concurrent computation of multiple algorithms, each having a cyclic communication structure. Thus, for example, in the case of B_6, one can have 6 disjoint cycles of any length (divisible by 6) up to 60, or 3 disjoint cycles of any length (divisible by 6) up to 126.

We illustrate the construction by mapping four length 12 cycles to B_4. To do this, we compute X from (3.7) in field $GF(2^4)$ as (refer to Table 2.1)

$$X = 1 \cdot (1 + \alpha^{12})^{-1} = \alpha^4.$$

The four disjoint cycles are then directly given by

$$\begin{aligned}
&(0, \alpha^4) \to (1, \alpha^5) \to (2, \alpha^6) \to (3, \alpha^7) \to (0, \alpha^8) \to (1, \alpha^9) \to (2, \alpha^{10}) \\
&\qquad \to (3, \alpha^{11}) \to (0, \alpha^{12}) \to (1, \alpha^{13}) \to (2, \alpha^{14}) \to (3, 1) \to (0, \alpha^4). \\
&(3, \alpha^4) \to (0, \alpha^5) \to (1, \alpha^6) \to (2, \alpha^7) \to (3, \alpha^8) \to (0, \alpha^9) \to (1, \alpha^{10}) \\
&\qquad \to (2, \alpha^{11}) \to (3, \alpha^{12}) \to (0, \alpha^{13}) \to (1, \alpha^{14}) \to (2, 1) \to (3, \alpha^4). \\
&(2, \alpha^4) \to (3, \alpha^5) \to (0, \alpha^6) \to (1, \alpha^7) \to (2, \alpha^8) \to (3, \alpha^9) \to (0, \alpha^{10}) \\
&\qquad \to (1, \alpha^{11}) \to (2, \alpha^{12}) \to (3, \alpha^{13}) \to (0, \alpha^{14}) \to (1, 1) \to (2, \alpha^4). \\
&(1, \alpha^4) \to (2, \alpha^5) \to (3, \alpha^6) \to (0, \alpha^7) \to (1, \alpha^8) \to (2, \alpha^9) \to (3, \alpha^{10}) \\
&\qquad \to (0, \alpha^{11}) \to (1, \alpha^{12}) \to (2, \alpha^{13}) \to (3, \alpha^{14}) \to (0, 1) \to (1, \alpha^4).
\end{aligned}$$

There is also another simple configuration of multiple cycles on B_n when $g = 1$. A cycle of length $L < n(2^n - 1)$, $n|L$, is given by

$$(0,\ X) \to (1,\ \alpha X) \to (2,\ \alpha^2 X) \to \cdots \to ((L-1),\ \alpha^{L-1} X) \to (0,\ X),$$

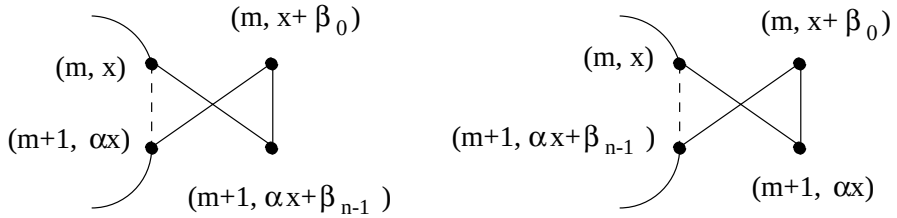

FIG. 3.2. *Two cases of adding a pair of outside nodes to a cycle.*

where

$$X = \beta_{n-1}(1 + \alpha^L)^{-1}.$$

It is easy to verify that all but n of the remaining nodes in B_n are also linked as a cycle. This *complementary cycle* of length $n2^n - n - L$ is given by

$$(L,\ \alpha^L X) \to (L+1,\ \alpha^{L+1}X) \to (L+2,\ \alpha^{L+2}X) \to \cdots$$
$$\to (n(2^n-1)-1,\ \alpha^{n(2^n-1)-1}X) \to (L,\ \alpha^L X).$$

One should also note that the only nodes which are not part of either the cycle of length L or its complementary cycle form a third cycle C_0 described earlier in Figure 3.1. Thus, when $g = 1$, the nodes of B_n can be partitioned into three cycles of lengths n, L, and $n2^n - L - n$ with the only condition on L being that it should be a multiple of n.

When $g > 1$ and cycle length $L \le (2^n - 1)n/g$ is a multiple of n, one can similarly show that the nodes of B_n may be partitioned into g cycles of length L, g cycles of length $(2^n - 1)n/g - L$, and one cycle of length n.

We now present the result about mapping cycles of lengths that are *not* multiples of n. Our methodology is rather simple. We first form a cycle of a smaller length which is a multiple of n. Then we attach appropriately chosen pairs of outside nodes to this cycle. This process is illustrated in Figure 3.2. As shown in the figure, if the cycle link shown by the dashed line is removed and three new links are added, then the outside pair of nodes can be incorporated in the cycle. We will refer to this process as *attaching a node pair at* (m, x). Further, the pair of nodes, $(m,\ x)$ and $(m,\ x + \beta_0)$, which plays a crucial role in this process, will be called the pair of *companion nodes*. Note that the companion node labels have the same first index, and their second indices differ by β_0.

For this method to succeed, it is necessary to find enough nodes in the cycle with their companion nodes outside the cycle. Lemma 3.5, to be presented later, will help us count (or in some cases, bound) the number of companion node pairs. This lemma will then be used to prove Theorem 3.6, which guarantees that there are, indeed, the required number of companion node pairs to construct cycles of any length.

For any $(m, X) \in Z_n \times GF(2^n)$, $X \neq 0$, define a *chain* starting from (m, X) to mean a set of distinct nodes

$$\{(m, X), (m+1, \alpha X), (m+2, \alpha^2 X), \ldots, (m+T-1, \alpha^{T-1}X)\}.$$

The number of nodes in the chain, T, will be called the length of the chain. The maximum value of T is $(2^n - 1)n/g$. Butterfly connectivity described in Figure 2.1 shows that the consecutive nodes in a chain are connected.

Let $(m,\ \alpha^i)$ be any node of B_n. We refer to the quantity $(i-m) \bmod g$ as the *partition index* of that node. Clearly, all the nodes (m_i, α^i) of a chain have the same partition index. This is because from one node to the next, m_i increases by 1 mod n and the power of α, by 1 mod (2^n-1). The $n(2^n-1)$ nodes of B_n with nonzero second index may be separated into g partitions based on their partition index. Each partition has exactly $n(2^n-1)/g$ nodes. Each chain is confined to a single partition. Chains of length $n(2^n-1)/g$ occupy a complete partition.

In the light of this new terminology, one can see that when $g=1$, a cycle formed as in (3.8) is also a chain. Further, for $g \neq 1$, cycles $C_1, C_2, \ldots, C_t$ described in Theorem 3.3 can also be viewed as chains in distinct partitions. Therefore, the number of companion node pairs that may be used to extend the cycle length can be obtained by studying companion node pairs in relation to chains. We call a companion node pair to be *within a chain* if both its nodes are in the same chain. If the two nodes are in different chains, we call that companion node pair to be *across chains*. The following lemma explores the bounds on these numbers.

LEMMA 3.5 (companion node pairs within and across chains).

(a) *The number of companion node pairs, $\Gamma(T)$, confined to a chain of length T satisfies*

$$\Gamma(T) \leq \begin{cases} \lfloor (T-1)/n \rfloor & \text{if } T \leq 2^n-1, \\ \lfloor (T-1)/n \rfloor \ + \ \Gamma(T-(2^n-1)) & \text{otherwise.} \end{cases} \tag{3.18}$$

(b) *The number of companion node pairs across two disjoint chains of lengths $T_1, T_2 \leq 2^n-1$ is at most $\lfloor (T_1+T_2)/n \rfloor + 1$.*

(c) *The number of companion pairs across the two chains (not necessarily disjoint) of lengths $T_1 = 2^n-1$ and $T_2 = (2^n-1)n/g$, is exactly $(2^n-1)/g$ or $[(2^n-1)/g]-1$.*

Proof. (a) Let the chain begin at (m, X). Consider a companion pair $(m+i, \alpha^i X)$ and $(m+j, \alpha^j X)$, $i<j$. By distance between the nodes of a companion pair we will mean the quantity $j-i$. Because these nodes are companions,

$$i \equiv j \pmod{n} \tag{3.19}$$

and

$$\alpha^i X + \alpha^j X = \beta_0. \tag{3.20}$$

From (3.20) one gets

$$\alpha^{j-i} X + X = \alpha^{-i} \beta_0. \tag{3.21}$$

Consider now another distinct companion node pair $(m+i', \alpha^{i'} X)$ and $(m+j', \alpha^{j'} X)$, $i'<j'$. For this pair, one could similarly show that

$$\alpha^{j'-i'} X + X = \alpha^{-i'} \beta_0. \tag{3.22}$$

If $i, i' < 2^n-1$, then (3.21) and (3.22) imply that the distance $j'-i'$ must be different from $j-i$; or else α^i would equal $\alpha^{i'}$, which is impossible for $i, i' < 2^n-1$. Further, from (3.19), the distances must always take values that are multiples of n. Therefore there are at most $\lfloor (T-1)/n \rfloor$ companion node pairs when $T \leq 2^n-1$.

For larger values of T, either the first node of the pair is within the first 2^n-1 nodes of the chain, or the pair is entirely confined to the last $T-(2^n-1)$ elements of

the chain. Since the number of companion node pairs of these two kinds are at most $\lfloor (T-1)/n \rfloor$) and $\Gamma(T-(2^n-1))$, respectively, we get the stated bound.

(b) Let the two chains begin at (m, X) and (m', X'). Consider a companion pair $(m+i, \alpha^i X)$ and $(m'+j, \alpha^j X')$ across the chains. By arguments similar to part (a), $j-i$ must be a multiple of n. Since $-T_1 \leq j-i \leq T_2$, we get the specified bound on the number of pairs.

(c) Let $T_1 = 2^n - 1$ and $T_2 = (2^n-1)n/g$. Denote by g_1 and g_2, the partition indices of the nodes in the two chains. Let (m, α^i) be a typical node of the first chain, $0 \leq i \leq 2^n - 2$. We want to determine if its companion (m, α^j) is in the second chain. Since the second chain occupies a whole partition, the companion will belong to it if its partition index is g_2. When $\alpha^i = \beta_0$, the companion, $(m, 0)$, is clearly not a member of the second chain. When $\alpha^i \neq \beta_0$, from the companion relationship between nodes $(m,\ \alpha^i)$ and $(m,\ \alpha^j)$, one gets $\alpha^{j-i} = 1 + \alpha^{-i}\beta_0$. Thus for each of the $2^n - 2$ values of i (excluding the one corresponding to $\alpha^i = \beta_0$), $j - i \bmod (2^n - 1)$ takes a different value. Consequently it assumes all the values from 0 to $2^n - 2$ except one. Now, one has

$$\begin{aligned} \text{partition index of } (m, \alpha^j) &= j - m \bmod g \\ &= ((j-i) \bmod (2^n - 1)\ +\ g_1) \bmod g. \end{aligned}$$

Since $(j-i) \bmod (2^n-1)$ takes all values from 0 to $2^n - 2$ except one, the partition index of (m, α^j) will assume value g_2 exactly $(2^n-1)/g$ or $[(2^n-1)/g] - 1$ times, showing that there exist exactly these many companion node pairs between the two chains. □

Note that the two chains of part (c) of Lemma 3.5 may overlap, unlike those of part (b).

We now state Theorem 3.6 relating to mapping cycles of all allowed lengths larger than $2n$ to B_n. (Actually, odd lengths between n and $2n$ are also covered by this result.) Because of Lemma 3.5, this theorem only needs to prove the existence of sufficient number of external node pairs to attach to the cycle constructed as per Theorem 3.3.

THEOREM 3.6 (arbitrary length cycles of lengths $\geq n$).

(a) *For odd n, a cycle of any length L, $n \leq L \leq n2^n$, excluding even values of L less than $2n$, can be mapped to B_n with dilation 1.*

(b) *For even n, a cycle of any even length L, $n \leq L \leq n2^n$, can be mapped to B_n with dilation 1.*

Proof. If $n|L$, the desired cycle is already addressed in Theorem 3.3. For other L values, first form a cycle of length Kn using Theorem 3.3, where K is the largest possible number such that $Kn < L$ and $L - Kn$ is even. We will call this cycle the primary cycle. By adding up to $n-1$ pairs of outside nodes to the primary cycle we get the required cycle of length L. (If $K = 2^n - 1$, one needs to add only up to $\lfloor n/2 \rfloor$ pairs to get the largest required length.)

We will show that there are sufficient number of nodes in the primary cycle without their companion nodes. Following the method of Figure 3.2, one can attach a pair of external nodes at each of these nodes. We first prove the theorem when $g = 1$ (Case 1). Cases 2, 3, and 4 deal with $g > 1$, and assume $n \geq 6$ since it is the smallest n for which $g \neq 1$. The parameter that distinguishes these cases is t, the number of smaller cycles $C_1, C_2, \ldots, C_t$ that are merged as in Theorem 3.3 to obtain the primary cycle.

Case 1. $g = 1$. If $K = 1$, then each node of the primary cycle is without its companion node, and each new added node pair is distinct. The first part of this is true because companion node pairs must have a distance of at least n. To see the second part, compare the pairs added at two consecutive cycle nodes, say, (m, X) and $(m+1, \alpha X)$. The outside pair added at the first node is $(m, X+\beta_0) \to (m+1, \alpha X + \beta_{n-1})$, and the one added at the second node is $(m+1, \alpha X+\beta_0) \to (m+2, \alpha^2 X+\beta_{n-1})$. Clearly all these four new nodes are distinct. In a similar fashion, one can show that up to $n-1$ new distinct pairs of nodes may be added to the cycle.

When $K = 2^n - 1$, the primary cycle consists of all the nodes (m, X), $0 \le m < n$, $X \in GF(2^n)$, $X \neq 0$. In this case, at each node (m, β_0) in the cycle, one can attach an outside pair $(m, 0) \to (m+1, 0)$. Distinctness of the new pairs can be ensured by using only even values of m. In this manner, up to $\lfloor n/2 \rfloor$ pairs of outside nodes may be attached to the cycle to achieve the required length.

Unfortunately, when $2 \le K \le 2^n - 2$, the second node of a pair may, at times, turn out to be the same as the first node of another pair. We therefore would not be able to add both these pairs to the cycle at the same time. However, if we have $2(n-1)$ nodes without their companion nodes, we can guarantee adding at least half of the outside node pairs, i.e., $(n-1)$ pairs. We will now show that the primary cycle, indeed, contains $2(n-1)$ nodes without their companion nodes. We will prove this for $Kn \le n(2^n - 1)/2$ only. For larger Kn values, one may consider the complementary cycle of length $n(2^n - 1) - Kn$ and prove similarly the existence of at least $2(n-1)$ nodes therein, which have their companion nodes outside, i.e., in the original cycle of length Kn.

Using Lemma 3.5(a) we can find the maximum number of companion node pairs within the cycle of length Kn. Subtracting these nodes from the total number of nodes in the cycle, we find that at least

$$Kn - 2\Gamma(Kn) \tag{3.23}$$

cycle nodes have companion nodes outside the cycle. For $Kn \le 2^n - 1$, use of Lemma 3.5(a) in (3.23) gives

$$\begin{aligned} \text{number of nodes with external companions} &\ge Kn - 2(K-1) \\ &= (2n-2) \ + \ (n-2)(K-2) \\ &> 2n-2. \end{aligned}$$

This proves that there are sufficient number of companion node pairs in the primary cycle where new node pairs may be attached.

To prove the result for $Kn > 2^n - 1$ by mathematical induction, assume its truth for length $Kn - (2^n - 1)$; i.e., assume that

$$[Kn - (2^n - 1)] - 2\Gamma(Kn - (2^n - 1)) \ge 2n - 2.$$

Recall that we need only to prove the result for $Kn \le n(2^n - 1)/2$. One now gets for the primary cycle of length Kn,

$$\begin{aligned} \text{no. of nodes with external companions} &\ge Kn - 2[\lfloor (Kn-1)/n \rfloor + \Gamma(Kn - (2^n - 1))] \\ &\ge (2n-2) + (2^n - 1) - 2(K-1) \\ &\ge (2n-2) + 2 \\ &> 2n - 2. \end{aligned}$$

Case 2. $g > 1$ and $t < g$. If the primary cycle length $Kn \leq 2^n - 1$, the situation is similar to that of Case 1. For $Kn > 2^n - 1$, we proceed as follows. Since $t < g$, at least one partition representing a chain of length $n(2^n - 1)/g$ is not used in the primary cycle. Consider this chain and a chain of length $2^n - 1$ in C_1 of nodes used in the primary cycle. From Lemma 3.5(c), there are at least $[(2^n - 1)/g] - 1$ companion node pairs across them. But note that for $n \geq 6$, $2^n - 1 > n^2$. Further, $g \leq n/2$. Therefore $[(2^n - 1)/g] - 1 > 2n - 2$ showing that at least $2n - 2$ companion node pairs exist between the primary cycle and the remaining nodes.

Case 3. $g > 1$, $t = g$ and cycles $C_1, C_2, \ldots, C_{t-1}$ have lengths $n(2^n - 1)/g$. If the number of nodes left out of the primary cycle is less than or equal to $2^n - 1$, then one can prove this case in a manner similar to Case 1 except that the focus will now be on the nodes that are *not* in the cycle rather than those that are part of the cycle. But the final consequence is the same: there are enough companion pairs between the nodes in the cycle and those outside. If the number of nodes outside the primary cycle is more than $2^n - 1$, then a chain of length $2^n - 1$ of these outside elements will have at least $[(2^n - 1)/g] - 1$ companion nodes within C_1. (Lemma 3.5(c)). This number is greater than $2n - 2$ (for $n \geq 6$) showing that there are enough companion node pairs between the primary cycle and the outside nodes.

Case 4. $g > 1$, $t = g$ and cycles $C_1, C_2, \ldots, C_{t-2}$ have lengths $n(2^n - 1)/g$. First note that because g is odd, when $g \neq 1$, $g \geq 3$. Thus, in this case, cycle C_1 of $n(2^n - 1)/g$ nodes is part of the primary cycle. Further, from the construction in Theorem 3.3, for this case to exist, the number of unused nodes in partitions of C_{t-1} and C_t—call them R_1 and R_2, respectively—must satisfy

$$R_1 + R_2 > (2^n - 1)(n/g - 1). \tag{3.24}$$

Without loss of generality, let $R_1 \leq R_2$. Clearly, both these sets of unused elements form chains. If either of these chains has at least $2^n - 1$ elements, then at least $(2^n - 1)/g$ of them will have companion nodes in C_1. Thus as in Case 3, there are enough companion node pairs between the nodes of the companion cycle and those outside. On the other hand, if both $R_1, R_2 < 2^n - 1$, then from Lemma 3.5(a) and (b), one can see that there are at most $\lfloor (R_1 - 1)/n \rfloor$ and $\lfloor (R_2 - 1)/n \rfloor$ companion node pairs within these chains and $\lfloor (R_1 + R_2)/n \rfloor + 1$ across the two chains. Since there are a total of $R_1 + R_2$ nodes in these two chains, the rest of their nodes must have companions in the primary cycle. Since R_1 and R_2 are multiples of n, $\lfloor (R_1 - 1)/n \rfloor = (R_1/n) - 1$ and $\lfloor (R_2 - 1)/n \rfloor = (R_2/n) - 1$. Using (3.24) one thus gets that the number of companion node pairs between the primary cycle and those outside to be at least

$$\begin{aligned}
(R_1 + R_2) - 2[R_1/n - 1 + R_2/n - 1 + (R_1 + R_2)/n + 1] &= (R_1 + R_2)(1 - 4/n) + 2 \\
&> (2^n - 1)(n/g - 1)(1 - 4/n) + 2 \\
&\geq (2^n - 1)/3 + 2 \\
&> (2n - 2). \qquad (3.25)
\end{aligned}$$

The simplification in the third line of (3.25) is based on the fact that $(n/g) \geq 2$ and $(1 - 4/n) \geq 1/3$ for $n \geq 6$, while last line of (3.25) is true for any $n \geq 6$. □

Theorem 3.6 proves that there are sufficient number of nodes in the primary cycle where one can attach outside node pairs to obtain any desired length cycle as long as this length can be expressed as $Kn + 2t$. Construction of such a cycle is rather straightforward; once the primary cycle is obtained as per Theorem 3.3, one only needs to identify the required number of cycle nodes whose companions are outside

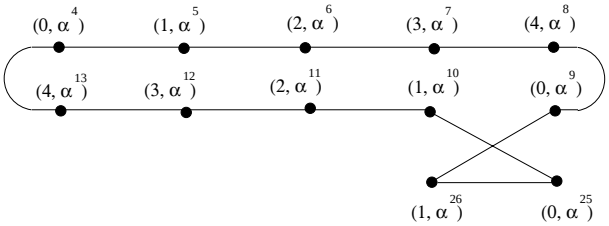

FIG. 3.3. *A length* 12 *cycle mapped to* $Z_5 \times GF(2^5)$ *with dilation* 1.

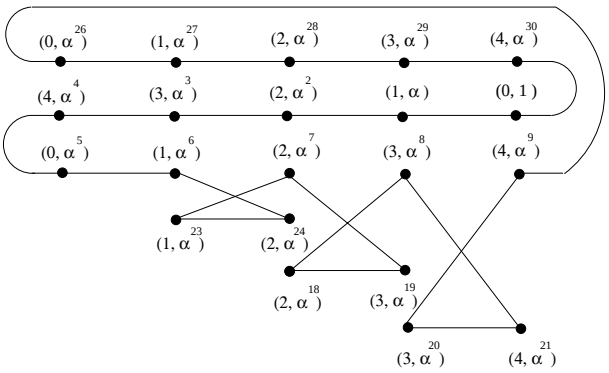

FIG. 3.4. *A length* 21 *cycle mapped to* $Z_5 \times GF(2^5)$ *with dilation* 1.

$$(0,\ 11101) \to (1,\ 11100) \to (2,\ 11100) \to (3,\ 00011) \to$$
$$(4,\ 11000) \to (0,\ 01000) \to (1,\ 01000) \to (0,\ 01001) \to$$
$$(1,\ 01001) \to (2,\ 01001) \to (3,\ 01101) \to (4,\ 01101) \to (0,\ 11101)$$

$$(0,\ 00100) \to (1,\ 00101) \to (2,\ 00111) \to (3,\ 00111) \to (4,\ 01111) \to$$
$$(0,\ 11111) \to (1,\ 11110) \to (2,\ 11110) \to (3,\ 11110) \to (4,\ 11110) \to$$
$$(0,\ 01110) \to (1,\ 01110) \to (2,\ 01110) \to (1,\ 01100) \to (2,\ 01100) \to$$
$$(3,\ 01000) \to (2,\ 01000) \to (3,\ 01100) \to (4,\ 01100) \to (3,\ 00100) \to$$
$$(4,\ 00100) \to (0,\ 00100)$$

FIG. 3.5. *Cycles of length* 12 *and* 21 *in* B_5.

the cycle. Finding a small number of these nodes is a relatively simple process. New node pairs may be attached at these nodes as in Figure 3.2 to get the desired cycle.

We illustrate this process by constructing length 12 and 21 cycles in B_5. The final construction is shown in Figures 3.3 and 3.4. To construct the cycle of length 12, one first uses Theorem 3.3 to create a primary cycle of length 10 (beginning at $(0,\ \alpha^4)$). Since $(0,\ \alpha^9)$ belongs to the cycle, but not its companion $(0,\ \alpha^9 + \beta_0) = (0,\ \alpha^{25})$, we add the indicated pair to get length 12 cycle. (Note that companions of none of the nodes in this length 10 cycle are present in it. Thus one could have added a new node pair at any of these nodes.) Similarly, a length 21 cycle is obtained by first creating a primary cycle of length 15 (beginning at $(0,\ \alpha^{26})$) and then adding pairs of new nodes at $(1,\ \alpha^6)$, $(2,\ \alpha^7)$, and $(3,\ \alpha^8)$. These cycles translated to binary notation using Table 2.3 are shown in Figure 3.5.

$$
\begin{array}{lll}
(0,0) & \to (1,0) & \cdots \to (K,0) \to \\
(K-1,\beta_0) & \to (K-2,\beta_0(\alpha^{-1}+1)) & \cdots \to (0,\beta_0 \textstyle\sum_{i=0}^{K-1} \alpha^{-i}) \to \\
(1,\beta_0 \textstyle\sum_{i=-1}^{K-2} \alpha^{-i}) & \to (2,\beta_0 \textstyle\sum_{i=-2}^{K-3} \alpha^{-i}) & \cdots \to (K,\beta_0 \textstyle\sum_{i=-K}^{-1} \alpha^{-i}) \to \\
(K-1,\beta_0 \textstyle\sum_{i=-(K-1)}^{-1} \alpha^{-i}) \to & (K-2,\beta_0 \textstyle\sum_{i=-(K-2)}^{-1} \alpha^{-i}) & \cdots \to (1,\beta_0 \textstyle\sum_{i=-1}^{-1} \alpha^{-i}) \to (0,0)
\end{array}
$$

FIG. 3.6. *Length $4K$ cycle mapping to B_n ($K < n$).*

Unfortunately, Theorem 3.6 does not cover all the cycles that can possibly be mapped to B_n. Particularly, when n is odd, Theorem 3.6 does not provide constructions of cycles of even lengths less than $2n$ and when n is even, it excludes even lengths less than n. We now illustrate a technique to cover these cases. Using this technique, one can easily map cycles of even lengths less than $4n$ (except possibly lengths 6 and 10) to B_n with dilation 1. This implies that all the cycles that are not proved to be impossible in Theorem 3.1 can indeed be mapped to B_n. This final result about cycles is stated in Theorem 3.7.

THEOREM 3.7 (comprehensive cycle mapping). *One can map to B_n all cycles, except those identified in Theorem* 3.1*, with dilation* 1.

Proof. Because of Theorem 3.6, the only cycles we need to map to B_n are those with even lengths less than $2n$. We can use the following construction for even lengths less than $4n$.

If $L = 4K$, $K < n$, construct the cycle as follows.

Start from node $(0,0)$. Let (m, X) denote the current node on the cycle. Use K times link $(m, X) \to (m+1, \alpha X)$. Then use K times link $(m, X) \to (m-1, \alpha^{-1}X+\beta_0)$. Follow it K times with link $(m, X) \to (m+1, \alpha X)$. Finally, K times, travel along $(m, X) \to (m-1, \alpha^{-1}X + \beta_0)$. This will bring you back to the starting node $0, 0)$. Figure 3.6 shows this length $4K$ cycle.

One can see from the connectivity of B_n, shown in Figure 2.1, that the consecutive nodes in the cycle above are indeed connected. We need only to show that they are distinct. The only two nodes in the cycle with the first index of the label 0 are $(0,0)$ and $(0, \beta_0 \sum_{i=0}^{K-1} \alpha^{-i})$. Clearly these are not the same since $K < n$. For the same reason, the two nodes with the first index of label being K, $(K,0)$ and $(K, \beta_0 \sum_{i=-K}^{-1} \alpha^{-i})$ are distinct. The four cycle nodes with the same first index m, $0 < m < K$, are $(m,0)$, $(m, \beta_0 \sum_{i=0}^{K-1-m} \alpha^{-i})$, $(m, \beta_0 \sum_{i=-m}^{K-1-m} \alpha^{-i})$, and $(m, \beta_0 \sum_{i=-m}^{-1} \alpha^{-i})$. One can see that the second indices of these four nodes are distinct because $K < n$ and α, being a primitive element of $GF(2^n)$, cannot satisfy any equation of degree less than n. Thus one can map all cycles of length $4K$, $K < n$, to B_n with dilation 1.

If $L = 4K + 2$ and $K > 2$, one can add a pair $(2, \beta_{n-1}) \to (1, \beta_0)$ of new nodes between the cycle nodes $(1,0) \to (2,0)$ as in Figure 3.2. Thus, replacing the first three elements in the cycle of Figure 3.6 by the five elements: $(0,0) \to (1,0) \to (2, \beta_{n-1}) \to (1, \beta_0) \to (2,0)$, one gets a new cycle of length $4K+2$. It is easy to verify that the new elements were indeed absent from the original cycle when $K > 2$. Thus one can map all cycles of length $4K + 2$, $2 < K < n$, to B_n with dilation 1. The only even-length cycles less than $4n$ excluded by this procedure have lengths 6 and 10. ∎

The construction of Theorem 3.7 may be illustrated by mapping a cycle of length 14 to B_5. Since $14 = 12 + 2$, we first construct a cycle of length 12 and then add a new pair to it. The final cycle and its binary translation are shown in Figures 3.7 and 3.8.

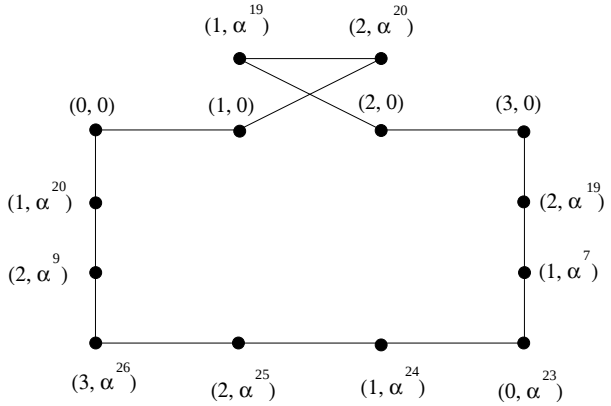

FIG. 3.7. *A length* 14 *cycle mapped to* $Z_5 \times GF(2^5)$.

$$(0,\ 00000) \to (1,\ 00000) \to (2,\ 00010) \to (1,\ 00010) \to (2,\ 00000) \to$$
$$(3,\ 00000) \to (2,\ 00100) \to (1,\ 00110) \to (0,\ 00110) \to (1,\ 00111) \to$$
$$(2,\ 00101) \to (3,\ 00001) \to (2,\ 00001) \to (1,\ 00001) \to (0,\ 00000)$$

FIG. 3.8. *A length* 14 *cycle in* B_5.

4. Mapping binary trees on the butterfly. This section presents two results about mapping trees to B_n. We first show that it is possible to map multiple nonoverlapping balanced binary trees with dilation 1 to this network (Theorem 4.1). Next, by combining these trees, we show that one can map the largest possible binary tree to B_n with a slightly higher dilation (Theorem 4.3). With the new model for B_n, both these tasks are relatively simple.

In the discussion that follows, we restrict ourselves to balanced binary trees. By level of a node in the tree we will mean its distance from the root. An m-level tree has nodes in levels $0, 1, \ldots, m-1$. Each parent has exactly two children. Thus the m-level tree has 2^{m-1} leaves and $2^m - 1$ total nodes. All the logarithms are assumed to be base 2.

THEOREM 4.1 (multiple trees). *One can map* n *nonoverlapping* n*-level binary trees to* B_n *with dilation* 1.

Proof. Choose node $(i,\ \beta_{n-1})$ to be the root of the ith tree, $0 \le i < n$. Construct each tree by the simple rule that the children of any node $(j,\ x)$ are nodes $(j+1,\ \alpha x)$ and $(j+1,\ \alpha x + \beta_{n-1})$.

Clearly, both the children in each tree node are connected to the parent by a direct edge (see Figure 2.1). We need only to prove that all the nodes in these trees are distinct. Note that, because of the way the trees are constructed, the nodes in level j of ith tree have labels $((i+j) \bmod n,\ \beta_{n-1} f(\alpha))$ where $f(\alpha)$ are distinct binary polynomials of α of degree j. Clearly, nodes on different levels of a tree are distinct since their first indices are unequal. Similarly, all nodes on the same level of a tree are also distinct; otherwise, their second indices, $\beta_{n-1} f_1(\alpha)$ and $\beta_{n-1} f_2(\alpha)$ will be equal, implying that $f_1(\alpha) - f_2(\alpha)$, a polynomial in α of degree less than n, equals zero. This is impossible since α is a primitive element of $GF(2^n)$. Finally, suppose a node $((i_1 + j_1) \bmod n,\ \beta_{n-1} f_1(\alpha))$ of tree i_1 is identical to the node $((i_2 + j_2) \bmod n,\ \beta_{n-1} f_2(\alpha))$ of a different tree i_2. Since the first indices of the two nodes are the same, $j_1 \ne j_2$. Thus, equality of the second index implies two polynomials

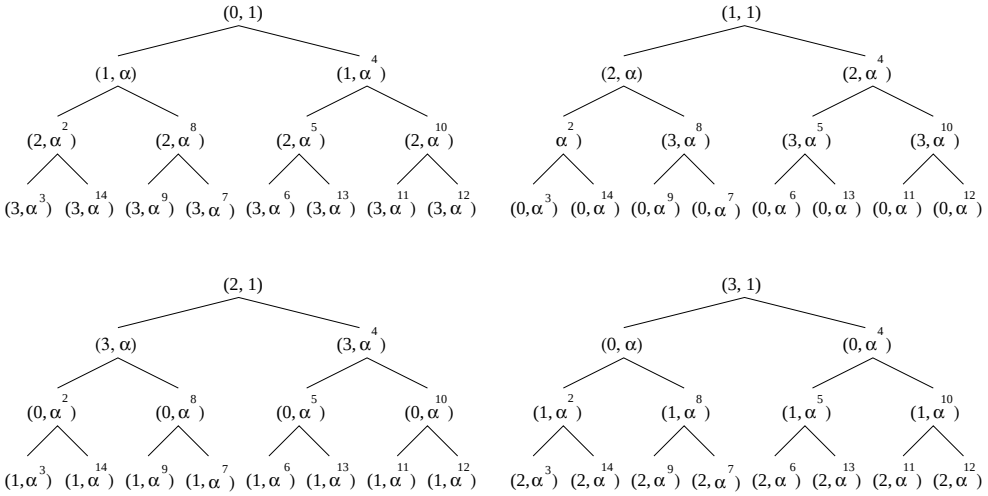

FIG. 4.1. *Four nonoverlapping* 4*-level trees mapped to* B_4 *with dilation* 1.

$f_1(\alpha)$ and $f_2(\alpha)$ of unequal degrees (and each less than n) are equal. This is again impossible in $GF(2^n)$. Therefore all nodes in all trees are distinct. □

Bhatt et al. [2] have previously proved the same result stated in Theorem 4.1. However, our construction is based on the butterfly modeled as $Z_n \times GF(2^n)$ and is necessary to obtain the mapping of the largest tree as given in Theorem 4.3.

Note that the mapping given in Theorem 4.1 is optimum in the sense that it describes the maximum number of nonoverlapping n-level binary trees that may be mapped to B_n. Clearly the unused n nodes, $\{(i,0) \mid 0 \le i < n\}$, do not support another n-level tree. Figure 4.1 shows mapping of four disjoint trees to B_4.

We now focus on mapping the single largest binary tree to B_n. Such a tree would have $n + \lfloor \log n \rfloor$ levels and would use $2^{\lfloor \log n \rfloor} 2^n - 1$ nodes of B_n. For n values which are powers of 2, such a tree would span all but one node of B_n. For other values of n, this is the largest tree that may be mapped to B_n, because increasing the number of tree levels even by 1 will imply more nodes than the number of nodes of B_n.

We create this tree by first designing the top $\lfloor \log n \rfloor$ levels using nodes unused in Theorem 4.1. Then two n-level trees generated as in Theorem 4.1 are attached at each leaf of this tree. Since a $\lfloor \log n \rfloor$-level tree has at most $n/2$ leaves, the n nonoverlapping trees obtained in Theorem 4.1 suffice. The top tree, however, needs to be designed carefully since its leaves should be able to connect (with low dilation) to the roots of the lower n-level trees which are very specific. Recall that the only nodes unused in Theorem 4.1 are $(i,\ 0)$, $0 \le i < n$. Lemma 4.2 provides the required mapping of the $\lfloor \log n \rfloor$-level tree to these nodes.

LEMMA 4.2. *One can map a* $\lfloor \log n \rfloor$*-level binary tree to nodes* $(i,\ 0)$, $0 \le i < n$, *of* B_n *such that all its leaves are mapped to* $(i,\ 0)$ *with odd* i. *Further, the dilation of this mapping is* $2^{\lfloor \log\ n \rfloor}/4$.

Proof. Let n' denote $\lfloor \log n \rfloor$. Number the tree levels 0 through $\lfloor \log n \rfloor - 1$ with the root at level 0. Map the tree root to node $(2^{n'-1}, 0)$. Map the children of a parent $(i,\ 0)$ at level l of the tree to nodes $(i - 2^{n'-2-l},\ 0)$ and $(i + 2^{n'-2-l},\ 0)$.

One can verify that this procedure maps 2^l tree vertices at level l to nodes $(2^{n'-1-l}p,\ 0)$, with odd p, $1 \le p \le 2^{l+1} - 1$. Thus all tree nodes are mapped to distinct nodes of B_n. The leaves of this tree are mapped to $(p,\ 0)$ as specified.

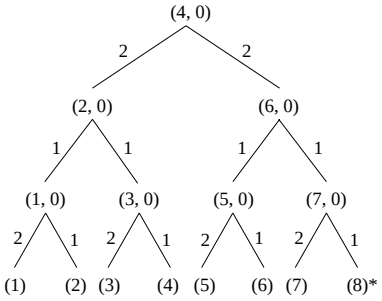

FIG. 4.2. *The top of the tree in B_n, $8 \le n < 16$ (with dilation marked on each edge). The last row contains the roots of n-level trees. (For brevity, a root $(i,\ \beta_{n-1})$ is shown only as (i). Further, $(8)^*$ denotes root $(0,\ \beta_{n-1})$ when $n = 8$.)*

Further, the paths from the image of a parent at level l to images of its children are of length $2^{n'-2-l}$. The longest of these paths gives the specified dilation of the mapping. □

The mapping of Lemma 4.2 exhibits a congestion of $(n' - 1)$; i.e., $(n' - 1)$ paths corresponding to tree edges pass through a single edge B_n. To see this, first note that all the paths in B_n corresponding to edges of any single tree level are disjoint. Thus the congestion cannot exceed $(n' - 1)$. One can also show that the B_n edge between nodes $(\lfloor 2^{n'}/3 \rfloor,\ 0)$ and $(\lfloor 2^{n'}/3 \rfloor + 1,\ 0)$ carries paths corresponding to a tree edge at every level. Thus this B_n edge has a congestion of $(n' - 1)$.

We now combine Theorem 4.1 and Lemma 4.2 to derive the central result of this section.

THEOREM 4.3 (tree mapping). *One can map a binary tree of $n + \lfloor \log\ n \rfloor$ levels to B_n with dilation 2 if $n < 16$, 3 if $16 \le n < 32$, 4 if $32 \le n < 64$, and $2^{\lfloor \log\ n \rfloor}/4$ if $n \ge 64$.*

Proof. We map the top $\lfloor \log\ n \rfloor$ levels of the tree as in Lemma 4.2. Note that the leaves of this $\lfloor \log\ n \rfloor$-level tree are mapped to $(i,\ 0)$ for odd i. At each leaf $(i,\ 0)$ we attach two n-level trees generated according to Theorem 4.1 with roots at $(i,\ \beta_{n-1})$ and $(i + 1,\ \beta_{n-1})$. Obviously all the nodes in the resultant $(n + \lfloor \log\ n \rfloor)$-level tree are distinct.

Further, the roots of the n-level tree are at distances 2 and 1 from the corresponding leaves of the $\lfloor \log\ n \rfloor$-level tree. The dilation within the lower n-level trees is 1. Therefore the overall dilation of the tree is dictated by the dilation within the top $\lfloor \log\ n \rfloor$ levels which, according to Lemma 4.2, is $2^{\lfloor \log\ n \rfloor}/4$.

As an example, the $\lfloor \log\ n \rfloor$-level tree for $8 \le n < 16$ is shown in Figure 4.2. The top three levels of this tree are generated from Lemma 4.2, and the fourth level shows the roots of n-level trees. When $16 \le n < 64$, one can use the top trees shown in Figures 4.3 and 4.4 rather than the ones obtained from Lemma 4.2. These trees are obtained by shuffling certain nodes of the tree obtained from Lemma 4.2 to reduce the dilation. Since in the new $\lfloor \log\ n \rfloor$-level trees the leaves are not necessarily at $(i,\ 0)$ with odd i's, the choice of the n-level trees attached to each leaf is also different. The last rows of these figures specify the roots of the n-level trees to be attached to each leaf. □

The tree mapping strategy presented here is interesting because of its extreme simplicity. The bottom n levels of the tree using $2^{\lfloor \log\ n \rfloor}(2^n - 1)$ nodes are mapped in a very systematic manner. The top $\lfloor \log\ n \rfloor$ levels of the tree using fewer than n nodes may also be algorithmically created using Lemma 4.2. The overall dilation is decided

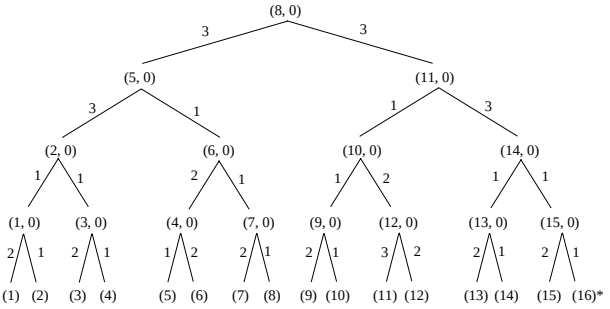

FIG. 4.3. *A* better *top for a tree in* B_n, $16 \leq n < 32$ *(with dilation marked on each edge). The last row contains the roots of the* n*-level trees. (For brevity, a root* $(i,\ \beta_{n-1})$ *is shown only as* (i)*. Further,* $(16)^*$ *denotes root* $(0,\ \beta_{n-1})$ *when* $n = 16$*.)*

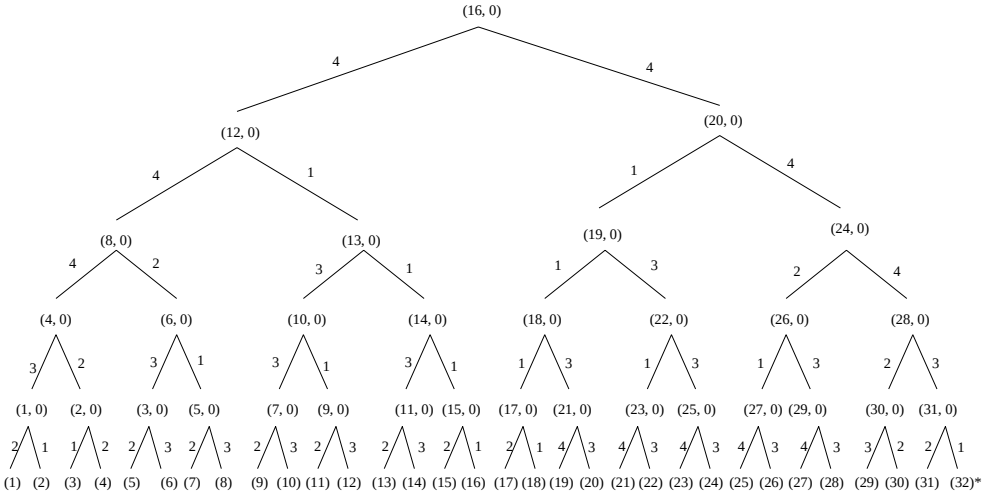

FIG. 4.4. *A* better *top for a tree in* B_n, $32 \leq n < 64$ *(with dilation marked on each edge). The last row contains the roots of the* n*-level trees. (For brevity, a root* $(i,\ \beta_{n-1})$ *is shown only as* (i)*. Further,* $(32)^*$ *denotes root* $(0,\ \beta_{n-1})$ *when* $n = 32$*.)*

by the dilation within these top levels. The dilation may be reduced by modifying the top tree. Fortunately, for every set of n values between two consecutive powers of 2, one needs to design a single top tree. We have altered the top tree to limit dilation to 3 when $16 \leq n < 32$ and to 4 when $16 \leq n < 32$. Such alterations may sometimes increase the congestion. The congestions of the top trees of Figures 4.2 and 4.3 are 2 and 3, respectively. These values are identical to the congestions of the same size top trees built using Lemma 4.2. But for the range $16 \leq n < 32$, the congestion of the top tree in Figure 4.4 is 6 as against the congestion of 4 for the top tree built using Lemma 4.2. Note that this increase in congestion yields a decrease of dilation from 8 to 4.

5. Conclusion. This paper has given a new model for the wrap-around butterfly networks and has demonstrated its utility to obtain mappings of cycles and trees.

Our results about cycle mappings are presented in Table 5.1. We have identified all cycles that could be subgraphs of butterfly networks and have provided their

TABLE 5.1
The existence of cycles as subgraphs of B_n.

Cycle length L	$3 \le L < n$	$n \le L < 2n$	$2n \le L \le n2^n$
n odd L even	Theorem 3.7*	Theorem 3.7 *	Theorem 3.6
n odd L odd	Impossible	Theorem 3.6	Theorem 3.6
n even L even	Theorem 3.7*	Theorem 3.6	Theorem 3.6
n even L odd	Impossible	Impossible	Impossible
* When $n = 5$ or $n \ge 7$, cycle of length 6 is not possible. When $n = 7, 9$ or $n \ge 11$, cycle of length 10 is not possible.			

TABLE 5.2
Mapping a tree of $2^{n+\lfloor \log\ n \rfloor} - 1$ nodes to a butterfly architecture.

Reference	Architecture size	Dilation	Conditions
Bhatt et al. [2]	$(n+3)2^{n+3}$	4	
Gupta et al. [6]	$(n+1)2^{n+1}$	4	even n
Gupta et al. [6]	$(n+2)2^{n+2}$	2	even n
This paper	$n2^n$	2	$n < 16$
This paper	$n2^n$	3	$16 \le n < 32$
This paper	$n2^n$	4	$32 \le n < 64$
This paper	$n2^n$	$2^{\lfloor \log\ n \rfloor}/4$	

mappings. We give two procedures for mapping cycles to B_n: one that is applicable to cycles of even lengths less than $4n$ and the other for larger lengths. In the first case, the cycle is established directly. In the second, one sets up a cycle of length divisible by n and then augments it with a small number of node pairs to make up the required length. Earlier results [11] about cycle mappings on B_n had identified $O(2^n)$ cycle subgraphs each with a different length, whereas we provide $O(n2^n)$ cycle subgraphs of different lengths.

Our results about tree mappings are listed in Table 5.2. Using our methods one can map the largest possible balanced binary tree to B_n, $n < 16$, with a small dilation of 2. One may note that B_{15}, the biggest butterfly network to which this result applies, has almost half a million nodes. We also give maximal tree mappings in larger butterflies with bounded dilation. For $16 \le n < 32$, the dilation is 3, and for $32 \le n < 64$, it is 4. Thus even though the tree mapping results presented here are asymptotically poor as compared to the earlier work [2, 6] (dilation and congestion $O(n)$ as against $O(1)$), for practical network sizes of up to $n = 64$, they have low dilation and congestion. Further, unlike the earlier mappings, ours does not require a larger size butterfly to ensure the one-to-one (load = 1) mapping. Thus to map the same tree, we use a butterfly with at most half the nodes as before. Our trees have unit dilation in their lower n levels. A larger dilation may be present only within the top $\lfloor \log\ n \rfloor + 1$ levels that employ fewer than n nodes.

The simplicity of the mappings obtained here is essentially due to our identification of the butterfly network with the direct product of a group and a finite field. We have shown that in the context of this model, the network connectivity may be expressed as an algebraic relationship between the node labels. One may then employ the powerful tools of abstract algebra to explore the structural properties of the network. Even though we have limited our investigation here to certain mappings, we

believe that these methods hold a lot of promise for other aspects of these networks as well.

Acknowledgment. The authors wish to thank anonymous referees for comments and suggestions that improved the paper tremendously.

REFERENCES

[1] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
[2] S. N. Bhatt, F. R. K. Chung, J. Hong, F. T. Leighton, B. Obrenic, A. L. Rosenberg, and E. J. Schwabe, *Optimal emulation by butterfly-like networks*, J. ACM, 43 (1996), pp. 293–330.
[3] G. Chen and C. M. Lau, *Comments on "A new family of Cayley graph interconnection networks of constant degree four",* IEEE Trans. Parallel Distrib. Syst., 8 (1997), pp. 1299–1300.
[4] R. Feldmann and W. Unger, *The cube-connected cycle is a subgraph of the butterfly network*, Parallel Process. Lett., 2 (1992), pp. 13–19.
[5] C. T. Gray, W. Liu, T. Hughes, and R. Cavin, *The design of a high-performance scalable architecture for image processing applications*, in Proceedings of the 1990 International Conference on Application Specific Array Processors, IEEE, Piscataway, NJ, 1991, pp. 722–733.
[6] A. Gupta and S. E. Hambrusch, *Embedding complete binary trees into butterfly networks*, IEEE Trans. Comput., 40 (1991), pp. 853–863.
[7] F. T. Leighton, *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*, Morgan Kaufman, San Mateo, CA, 1992.
[8] W. Lin, T. Sheu, C. R. Das, T. Feng, and C. Wu, *Fast data selection and broadcast on the butterfly network*, in Proceedings of the International Workshop on Future Trends of Distributed Computing Systems in the 1990s, 1998, pp. 65–72.
[9] A. Ranade, *Optimal speedup for backtrack search on a butterfly network*, Math. Systems Theory, 27 (1994), pp. 85–102.
[10] J. H. Reif and S. Sen, *Randomized algorithms for binary search and load balancing on fixed connection networks with geometric applications*, SIAM J. Comput., 23 (1994), pp. 633–651.
[11] A. L. Rosenberg, *Cycles in Networks*, Technical report 91–20, University of Massachusetts, Amherst, 1993.
[12] E. J. Schwabe, *Constant-slowdown simulations of normal hypercube algorithms on the butterfly network*, Inform. Process. Lett., 45 (1993), pp. 295–301.
[13] P. Vadapalli and K. Srimani, *A new family of Cayley graph interconnection networks of constant degree four*, IEEE Trans. Parallel Distrib. Syst., 17 (1996), pp. 26–32.