Hamilton circuits in the directed wrapped Butterfly network [1]

J-C. Bermond [a], E. Darrot [a], O. Delmas [a], S. Perennes [a]

[a] *SLOOP project, INRIA Sophia Antipolis – 2004, route des Lucioles BP 93 – 06902 Sophia Antipolis Cedex (France)* [2]

Abstract

In this paper, we prove that the wrapped Butterfly digraph $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ of degree d and dimension n contains at least $d-1$ arc-disjoint Hamilton circuits, answering a conjecture of Barth [5]. We also conjecture that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ can be decomposed into d Hamilton circuits, except for $\{d=2$ and $n=2\}$, $\{d=2$ and $n=3\}$ and $\{d=3$ and $n=2\}$. We show that it suffices to prove this conjecture for d prime and $n=2$. Then, we give such a Hamilton decomposition for all primes to 12000 by a clever computer search, and so, as a corollary, we have a Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ for any d divisible by a number q, with $4 \le q \le 12000$.

Key words: Butterfly digraph, graph theory, Hamilton decomposition, Hamilton cycle, Hamilton circuit, perfect matching.

1 Introduction and notation

1.1 Butterfly networks

Many interconnection networks have been proposed as suitable topologies for parallel computers. Among them, *Butterfly networks* have received particular attention, due to their interesting structure.

[1] This work has been supported by the CEFIPRA (french-indian collaboration) and the european project HCM MAP.

[2] SLOOP (Simulation, Object Oriented Languages and Parallelism) is a common project with the CNRS/University of Nice - Sophia Antipolis (I3S laboratory) and the INRIA.

First, we have to warn the reader that under the name *Butterfly* and with the same notation, different networks are described in the literature. Indeed, while some authors consider the *Butterfly networks* to be multistage networks used to route permutations, others consider them to be point-to-point networks. In what follows, we will use the term *Butterfly* for the multistage version and we will use Leighton's terminology [13], namely *wrapped Butterfly*, for the point-to-point version. Furthermore, these networks can be considered either as undirected or directed. To be complete, we recall that some authors consider only *binary Butterfly networks* − the restricted class of networks obtained when the out-degree is 2 (directed case) or the degree is 4 (undirected case).

In this article, we will use the following definitions and notation, where $\mathbb{Z}_q$ denotes the set of integers modulo q (for definitions not given here see [15]).

Definition 1 *The* **Butterfly digraph** *of degree d and dimension n, denoted $\vec{\mathcal{BF}}(d,n)$, has as vertices the ordered pairs (x,l), where x is an element of $\mathbb{Z}_d^n$, that is a word $x_{n-1}x_{n-2}\cdots x_1x_0$ where the letters belong to $\mathbb{Z}_d$ and $0 \le l \le n$ (l is called the level). For $l < n$, a vertex $(x_{n-1}x_{n-2}\cdots x_1x_0, l)$ is joined by an arc to the d vertices $(x_{n-1}\cdots x_{l+1}\ \alpha\ x_{l-1}\cdots x_0, l+1)$ where α is any element of $\mathbb{Z}_d$.*

$\vec{\mathcal{BF}}(d,n)$ has $(n+1)d^n$ vertices. Each vertex in level $l < n$ has out-degree d. This digraph is not strongly connected. It is mainly used as a multistage interconnection network (the levels corresponding to the stages) in order to route some one-to-one mapping of d^n inputs (nodes at level 0) to d^n outputs (nodes at level n).

The underlying undirected graph obtained by ignoring the orientation will be denoted $\mathcal{BF}(d,n)$.

Figure (**1**) shows simultaneously $\mathcal{BF}(3,2)$ and $\vec{\mathcal{BF}}(3,2)$. The orientation on $\vec{\mathcal{BF}}(d,n)$ is obtained by directing the edges from left to right.

Note that $\vec{\mathcal{BF}}(d,n)$ is often represented (for example in [13,15]) in an opposite way to our drawing as the authors denote the nodes $(x_0x_1\cdots x_{n-1})$. We have chosen the representation which most emphasizes the recursive decomposition of $\vec{\mathcal{BF}}(d,n)$ and provides us with an easy representation of our inductive construction (see section 3).

Definition 2 *The* **wrapped Butterfly digraph***, denoted $\mathcal{W}\vec{\mathcal{BF}}(d,n)$, is obtained from $\vec{\mathcal{BF}}(d,n)$ by identifying the vertices of the last and first levels, namely (x,n) with $(x,0)$. In other words, the vertices are the ordered pairs (x,l) where x is an element of $\mathbb{Z}_d^n$, that is a word $x_{n-1}x_{n-2}\cdots x_1x_0$ where the letters belong to $\mathbb{Z}_d$ and $l \in \mathbb{Z}_n$ (l is called the level). For any l, a vertex $(x_{n-1}x_{n-2}\cdots x_1x_0, l)$ is joined by an arc to the d vertices $(x_{n-1}\cdots x_{l+1}\ \alpha\ x_{l-1}\cdots x_0,\ l+1)$ where α is any element of $\mathbb{Z}_d$.*

Usually, to represent the wrapped Butterfly (di)graph we use the representation of $\vec{\mathcal{BF}}(d,n)$ by repeating level 0 at the end. Hence the reader has to remember that levels 0 and n are identified for $\mathcal{W}\vec{\mathcal{BF}}(d,n)$. $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ is a d-regular digraph with nd^n vertices; its diameter is $2n-1$. The underlying wrapped Butterfly network will be denoted $\mathcal{WBF}(d,n)$; it is easy to see that this graph is regular of degree $2d$ and has diameter $\lfloor \frac{3n}{2} \rfloor$.

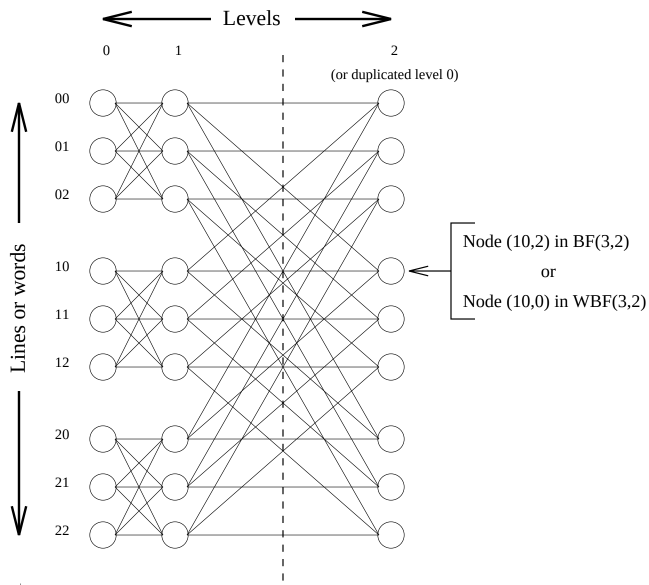

Fig. 1. *The graphs* $\mathcal{BF}(3,2)$ *(multistage version) with 3 levels, or* $\mathcal{WBF}(3,2)$ *(point-to-point version with level* 0 *duplicated). For digraphs* $\vec{\mathcal{BF}}(3,2)$ *or* $\mathcal{W}\vec{\mathcal{BF}}(3,2)$*, the edges must be arcs directed from left to right .*

1.2 Other definitions and general results

- $\mathcal{K}_d$ will denote the complete graph on d vertices.
- $\mathcal{K}_{d,d}$ will denote the complete bipartite graph where each set of the bipartition has size d.
- G^* will denote the symmetric digraph obtained from an undirected graph G by replacing each edge by two opposite arcs. In particular $\mathcal{K}_d^*$ (*resp.* $\mathcal{K}_{d,d}^*$) will denote the complete symmetric (*resp. bipartite*) digraph on d (*resp.* $d \times d$) vertices.
- $\mathcal{K}_d^+$ will denote the complete symmetric digraph with a loop on each vertex.
- A circuit, or directed cycle, of length n will be denoted $\vec{C}_n$ and a dipath of length n will be denoted $\vec{P}_n$.
- $\vec{\mathcal{K}}_{d,d}$ will denote the digraph obtained from $\mathcal{K}_{d,d}$ by orienting each edge from one part of the bipartition, called *left part*, to the other, called *right part*.

Definition 3 *(see [15]) Let G be a directed graph. The* **line digraph of** G*, denoted $L(G)$, is the directed graph whose vertices correspond to the arcs of G and whose arcs are defined as follows: there is an arc from a vertex e to a vertex f in $L(G)$ if and only if, in G, the initial vertex of f is the end vertex of e.*

Note that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,1)$ is just $\mathcal{K}_d^+$ and that $\mathcal{B}\vec{\mathcal{F}}(d,1)$ is $\vec{\mathcal{K}}_{d,d}$. We will see in section 4 (corollary (**38**)) that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$ is the line digraph of $\mathcal{K}^*_{d,d}$.

Definition 4 *A* **1-difactor** *of a digraph G is a spanning subgraph of G with in- and out-degree 1. It corresponds to a partition of the vertices of G into circuits.*

Definition 5 *A* **Hamilton cycle** (resp. **circuit**) *of a graph* (resp. **digraph**) *is a cycle* (resp. circuit) *which contains every vertex exactly once.*

Definition 6 *We will say that a graph* (resp. digraph) *has a* **Hamilton decomposition** *or* **can be decomposed into Hamilton cycles** (resp. **circuits**) *if its edges* (resp. arcs) *can be partitioned into Hamilton cycles* (resp. circuits)*.*

Remark 7 *A Hamilton circuit is a connected 1-difactor.*

The existence of one and if possible many edge(arc)-disjoint Hamilton cycles (circuits) in a network is advantageous for algorithms that make use of a ring structure. Furthermore, the existence of a Hamilton decomposition also allows the message traffic to be evenly distributed across the network. Various results have been obtained about the existence of Hamilton cycles in classical networks (see for example the surveys [2,11]). For example, it is well-known that any Cayley graph on an abelian group is Hamiltonian. Furthermore, it has been conjectured by Alspach [1] that:

Conjecture 8 (Alspach) *Every connected Cayley graph on an abelian group has a Hamilton decomposition.*

This conjecture has been verified for all connected 4-regular graphs on abelian groups in [9]. This includes in particular the toroidal meshes (grids). It is also known that $\mathcal{H}(2d)$, the hypercube of dimension $2d$, can be decomposed into d Hamilton cycles (see [2,3]).

Concerning line digraphs, it has been shown in [12] that d-regular line digraphs always admit $\lfloor \frac{d}{2} \rfloor$ Hamilton circuits. In the case of de Bruijn and Kautz digraphs which are the simplest line digraphs, partial results have been obtained successively in [14] and [6] respectively, and near optimal results have been obtained for undirected de Bruijn and Kautz graphs [4].

The wrapped Butterfly (di)graph is actually a Cayley graph (on a non abelian group) and a line digraph. So, the decomposition into Hamilton cycles (*resp. circuits*) of this graph (*resp. digraph*) has received some attention. First, it is well-known that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ is Hamiltonian (see [13, page 465] for a proof in the case $d = 2$). In [7], Barth and Raspaud proved that $\mathcal{WBF}(2,n)$ has a Hamilton decomposition, answering a conjecture of Rowley and Sotteau (private communication).

Theorem 9 (Barth, Raspaud) *$\mathcal{WBF}(2,n)$ can be decomposed into 2 Hamilton cycles.*

They also gave the following conjecture:

Conjecture 10 (Barth, Raspaud) *For $n \geq 2$, $\mathcal{WBF}(d,n)$ can be decomposed into d Hamilton cycles.*

In his thesis [5] , Barth also stated the following conjecture for the directed case:

Conjecture 11 (Barth) *For $n \geq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Recall that for $n = 1$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,1)$ is just $\mathcal{K}_d^+$ which itself is the arc-disjoint sum of $\mathcal{K}_d^*$ and loops. So conjecture (**11**) can be seen as an extension of a theorem of Tillson [17].

Theorem 12 (Tillson) *The complete symmetric digraph $\mathcal{K}_d^*$ can be decomposed into $d-1$ Hamilton circuits, except for $d = 4$ and 6.*

In this paper we focus mainly on the decomposition of the wrapped Butterfly digraph $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$. Our main result implies that the number of arc-disjoint Hamilton circuits contained in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ can only increase when n increases.

Proposition 13 *For any $n' \geq n$, if $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains p arc-disjoint Hamilton circuits, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n')$ also contains at least p arc-disjoint Hamilton circuits.*

This proposition, with Tillson's theorem and a special study for $d = 4$ and 6, implies conjecture (**11**).

Theorem 14 *For $n \geq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Furthermore, it appears that, except for three cases, for all small values of d, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ can be decomposed into d Hamilton circuits. So, we conjecture that:

Conjecture 15 *For $n \geq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ can be decomposed into d Hamilton circuits, except for ($d = 2$ and $n = 2$ or 3) and ($d = 3$ and $n = 2$).*

By proposition (**13**), it suffices to prove the conjecture for $n = 2$. Using results of section 4 on the conjunction of graphs, we have been able to reduce the study to prime degrees. So, conjecture (**15**) would follow from conjecture (**16**).

Conjecture 16 *For any prime number $p > 3$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p,2)$ can be decomposed into p Hamilton circuits.*

With a clever computer search, we have been able to prove conjecture (**16**) for any prime less than 12000, leading to the following statement:

Theorem 17 *If d is divisible by any number q, such that $4 \leq q \leq 12000$, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$, and consequently $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$, has a Hamilton decomposition.*

Finally, the methods used in this paper are combined with other ideas and applied to the undirected case to prove conjecture (**10**) in a forthcoming paper [8].

Theorem 18 *For $n \geq 2$, $\mathcal{WBF}(d,n)$ can be decomposed into d Hamilton cycles.*

2 Circuits and Permutations

2.1 More definitions

First, we will show that the existence of k arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$, is equivalent to the ability to route k *compatible cyclic realizable* permutations between levels 0 and n in $\vec{\mathcal{B}}\mathcal{F}(d,n)$. For this purpose, we need some specific definitions.

In this paper, π will always denote a permutation of $\mathbb{Z}_d^n$ which associates the element $\pi(x)$ with x. The **composition** $\pi \cdot \pi'$ **of two permutations** π and π' is the permutation which associates with the element a the element $\pi(\pi'(a))$.

Definition 19 *A permutation π is* **cyclic** *if, for some x, all the elements $\pi^i(x)$ are distinct, for $0 \leq i < d^n$.*

Remark 20 *Note that if π is cyclic, then, for every x, the elements $\pi^i(x)$ are all distinct. In fact, to verify that π is cyclic, it suffices to verify that for a given x, $\pi^i(x) \neq x$, for $1 \leq i < d^n$. Indeed, if there exists j and k, with $j > k$, such that $\pi^j(x) = \pi^k(x)$, then $\pi^{j-k}(x) = x$.*

For example, the permutation π which associates with a the element $a + 1$ is clearly cyclic, as $\pi^i(a) = a + i$.

It follows from the definition of $\vec{\mathcal{BF}}(d, n)$ that there exists a unique dipath connecting a vertex $(x, 0)$ to a vertex (y, n). So, we can associate with a permutation π of $\mathbb{Z}_d^n$ a set of dipaths in $\vec{\mathcal{BF}}(d, n)$ connecting vertex $(x, 0)$ to vertex $(\pi(x), n)$ for any x in $\mathbb{Z}_d^n$.

Following the terminology used in multistage interconnection networks, where one wants to connect inputs to outputs via disjoint paths, we introduce the notation of realizable permutations.

Definition 21 *A permutation π is* **realizable** *in $\vec{\mathcal{BF}}(d, n)$, or equivalently $\vec{\mathcal{BF}}(d, n)$* **realizes the permutation** *π, if the d^n associated dipaths from the inputs to the outputs are vertex-disjoint.*

Finally, following the terminology of Eulerian graph theory, we say:

Definition 22 *A set of k permutations $\pi_0, \pi_1, \cdots, \pi_{k-1}$ realizable in $\vec{\mathcal{BF}}(d, n)$ is* **compatible** *if the kd^n dipaths from $(x, 0)$ to $(\pi_j(x), n)$, for x in $\mathbb{Z}_d^n$ and $0 \leq j \leq k - 1$, are arc-disjoint. We will also say that $\vec{\mathcal{BF}}(d, n)$ realizes k compatible permutations.*

Warning - In the whole paper we are working with permutations which are mathematical objects independent of the graph for which they can be either realizable or compatible. In contrary, the realizability or compatibility is a property related to the graphs on which it applies.

2.2 Hamilton circuits and permutations

We are now ready to prove that there is an immediate connection between the existence of compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d, n)$ and that of arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{BF}}(d, n)$.

Lemma 23 *$\mathcal{W}\vec{\mathcal{BF}}(d, n)$ contains k arc-disjoint Hamilton circuits if and only if $\vec{\mathcal{BF}}(d, n)$ realizes k compatible cyclic permutations.*

Proof. First, let us show how to associate with a cyclic permutation π, realizable in $\vec{\mathcal{BF}}(d,n)$, a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ and conversely.

Let π be a cyclic permutation of $\mathbb{Z}_d^n$. Let x be a given element of $\mathbb{Z}_d^n$ and let P_i be the unique dipath of $\vec{\mathcal{BF}}(d,n)$ joining $(\pi^i(x),0)$ to $(\pi^{i+1}(x),n)$. As π is cyclic, all the $\pi^i(x)$ are distinct. So, if π is realizable, the dipaths P_i are vertex-disjoint. Let P'_i be the dipath of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ obtained from P_i by identifying $(\pi^{i+1}(x),n)$ with $(\pi^{i+1}(x),0)$. Now, the end vertex of P'_i is the initial of P'_{i+1} and so, as the $(\pi^i(x),0)$ span the set of vertices of level 0, the concatenation of the dipaths P'_i, with $0 \leq i < d^n - 1$, forms a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$.

Conversely, let H be a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$. Let $(x_0,0)$, $(x_1,0)$, $\ldots$, $(x_i,0)$, $\ldots$, $(x_{d^n-1},0)$ be the vertices we meet successively on level 0 by following the cycle H. Let us consider the permutation defined by $\pi(x_i) = x_{i+1}$. As H is a Hamilton circuit, all the x_i's are distinct so π is cyclic; furthermore, all the inside dipaths are vertex-disjoint, so π is a cyclic realizable permutation in $\vec{\mathcal{BF}}(d,n)$.

To prove the lemma, it suffices to note that the definition of compatible permutations has been done in order that the dipaths associated with the permutation are arc-disjoint, and so their concatenation form arc-disjoint Hamilton circuits, and conversely (see Figure (**2**)). $\square$

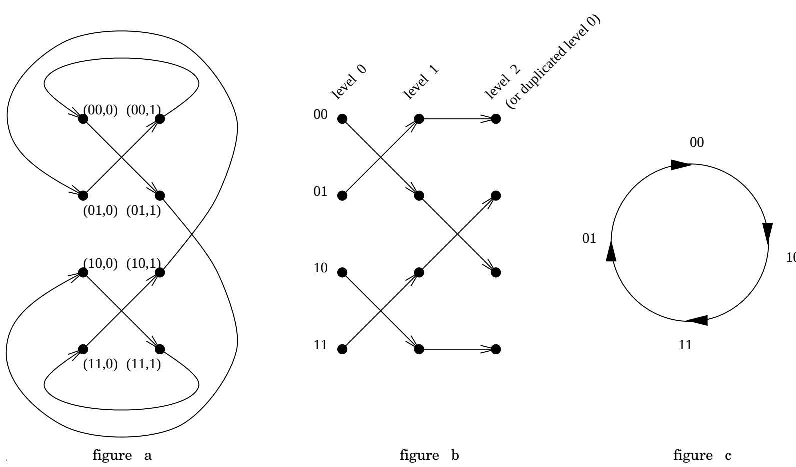

Fig. 2. *A Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(2,2)$ (figure a) or equivalently the associated permutation realizable in $\vec{\mathcal{BF}}(2,2)$ (figure b) and the cyclic permutation which is used (figure c).*

3 Recursive construction

3.1 Recursive decomposition of $\vec{\mathcal{BF}}(d,n)$

The permutation network $\vec{\mathcal{BF}}(d,n)$ has a simple recursive property: the $n+1$ first levels of $\vec{\mathcal{BF}}(d,n+1)$ form d vertex-disjoint subgraphs isomorphic to $\vec{\mathcal{BF}}(d,n)$. We shall call them *left Butterflies*. If the elements of $\mathbb{Z}_d^{n+1}$ are denoted $y=(ax)\in\mathbb{Z}_d\times\mathbb{Z}_d^n$, then each left Butterfly connects the set of vertices having the same left part a. So we will label a left Butterfly by $\mathcal{B}_{\text{Left}}(a)$. In the same way, the two last levels of $\vec{\mathcal{BF}}(d,n+1)$ are built with d^n disjoint subgraphs isomorphic to $\vec{\mathcal{BF}}(d,1)=\vec{\mathcal{K}}_{d,d}$, that we shall call *right Butterflies*; each right Butterfly connects all the vertices having the same right part x and we will label it by $\vec{\mathcal{K}}_{d,d}(x)$.

We can summarize the situation as follows:

- vertices of $\vec{\mathcal{BF}}(d,n+1)$ are denoted (ax,l),
- the left Butterfly labeled by $a\in\mathbb{Z}_d$ is formed by the vertices $a*$ of the $n+1$ first levels. It is denoted $\mathcal{B}_{\text{Left}}(a)$,
- the right Butterfly with label $x\in\mathbb{Z}_d^n$ is formed by the vertices $*x$ of the 2 last levels. It is denoted $\vec{\mathcal{K}}_{d,d}(x)$.

Remark 24 *In $\vec{\mathcal{BF}}(d,n+1)$, vertices of level n are shared by the left and right Butterflies, the outputs of the left Butterflies being considered as the inputs of the right Butterflies. Moreover, all the subgraphs defined above are arc-disjoint.*

Figure (**3**) displays such a recursive decomposition.

3.2 Iterative Construction

We will now give a simple construction which enables us to construct p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d,n+1)$ from p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d,n)$.

In what follows, we will use the letter M to indicate a permutation of $\mathbb{Z}_d$ and M_x to denote a permutation realizable in the right Butterfly $\vec{\mathcal{K}}_{d,d}(x)$. If M_x is a permutation of $\mathbb{Z}_d$ realizable in $\vec{\mathcal{K}}_{d,d}(x)$, then the arcs joining the vertices ax on level n of $\vec{\mathcal{BF}}(d,n+1)$ to the vertices $M_x(a)x$ on level $n+1$ are disjoint and form a perfect matching in $\vec{\mathcal{K}}_{d,d}(x)$.

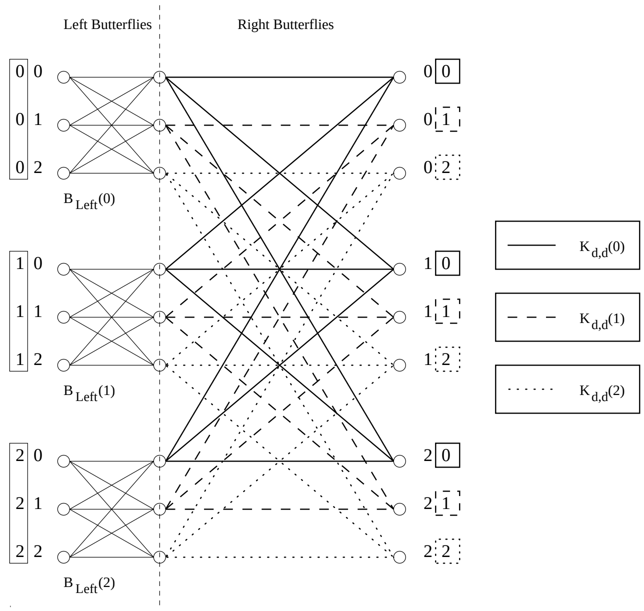

Fig. 3. *The recursive decomposition of $\mathcal{BF}(3,2)$. To obtain the directed version $\overrightarrow{\mathcal{BF}}(3,2)$ the edges must be changed into arcs directed from left to right. The vertices are denoted $y = (ax) \in \mathbb{Z}_3 \times \mathbb{Z}_3^1$. In $\overrightarrow{\mathcal{BF}}(3,2)$, the 2 first levels form 3 vertex-disjoint subgraphs, each one isomorphic to $\overrightarrow{\mathcal{BF}}(3,2-1)$. These 3 subgraphs are labeled $\mathcal{B}_{Left}(a)$. In the same way, the 2 last levels of $\overrightarrow{\mathcal{BF}}(3,2)$ are built with 3^1 disjoint subgraphs isomorphic to $\overrightarrow{\mathcal{BF}}(3,1) = \overrightarrow{\mathcal{K}}_{d,d}$, labeled $\overrightarrow{\mathcal{K}}_{d,d}(x)$.*

To be able to prove an inductive lemma, we need another definition:

Definition 25 *A* **family** *(or* **multi-set***)* **of permutations** *satisfies the* ***cyclic property*** *if the composition of the permutations of the family is a cyclic permutation for any order of the composition.*

We use the word "family" because the permutations are not necessarily different. This is the case in the following useful example, where all the permutations are identical except one:

Example 26 *Let the family $\mathcal{M}_j$ consist of the d^n permutations $M_{x,j}$ of $\mathbb{Z}_d$, such that $x \in \mathbb{Z}_d^n$, $M_{x,j}(a) = a + j$, for $x \neq 0$, and $M_{x,j}(a) = a + j + 1$, for $x = 0$. Then, the family $\mathcal{M}_j$ satisfies the cyclic property. Indeed, consider a permutation obtained by the composition of these d^n permutations in any order; this permutation associates with the element a of $\mathbb{Z}_d$ the element $a + (d^n - 1)j + j + 1 = a + d^n j + 1 = a + 1$ and so is clearly a cyclic permutation of $\mathbb{Z}_d$.*

Lemma 27 (inductive lemma) *Let π be a cyclic permutation realizable in $\overrightarrow{\mathcal{BF}}(d,n)$ and let $\mathcal{M} = (M_x,\, x \in \mathbb{Z}_d^n)$ be a family of d^n permutations satisfying the cyclic property and such that M_x is realizable in $\overrightarrow{\mathcal{K}}_{d,d}(x)$. Then, the permutation $f_{(\pi,\mathcal{M})}$ of $\mathbb{Z}_d^{n+1}$ defined by $f_{(\pi,\mathcal{M})}(ax) = b\pi(x)$, where $b = M_{\pi(x)}(a)$, is a cyclic permutation realizable in $\overrightarrow{\mathcal{BF}}(d, n+1)$.*

Proof. First, let us show that $f_{(\pi,\mathcal{M})}$ is a cyclic permutation. To show that $f_{(\pi,\mathcal{M})}$ is cyclic, it suffices, by remark (**20**), to show that $f^i_{(\pi,\mathcal{M})}(ax) \neq ax$, for $1 \leq i \leq d^{n+1}-1$. Suppose that $f^i_{(\pi,\mathcal{M})}(ax) = ax$ for some i. By definition, $f^i_{(\pi,\mathcal{M})}(ax) = a'\pi^i(x)$. So, $\pi^i(x) = x$, which implies that $i = kd^n$. If $i = d^n$, a' is the image of a by the composition of the d^n elements of $\mathcal{M}$, in some order and since $\mathcal{M}$ has the cyclic property, $a' = \sigma(a)$, where σ is a cyclic permutation. Therefore, $f^{kd^n}_{(\pi,\mathcal{M})}(ax) = \sigma^k(a)x \neq ax$, for $1 \leq k < d$. So, for any i, $1 \leq i \leq d^{n+1}-1$, $f^i_{(\pi,\mathcal{M})}(ax) \neq ax$.

It remains to show that $f_{(\pi,\mathcal{M})}$ is realizable in $\vec{\mathcal{BF}}(d,n+1)$. The dipath associated with $f_{(\pi,\mathcal{M})}$ from $(ax,0)$ to $(b\pi(x),n+1)$ consists of the dipath from $(ax,0)$ to $(a\pi(x),n)$ in $\mathcal{B}_{\text{Left}}(a)$ associated with the permutation π of $\mathcal{B}_{\text{Left}}(a)$ (which is isomorphic to $\vec{\mathcal{BF}}(d,n)$) followed by the arc joining $(a\pi(x),n)$ with $(b\pi(x),n+1)$ in $\vec{\mathcal{K}}_{d,d}(\pi(x))$ defined by the matching associated with the permutation $M_{\pi(x)}$, that is $b = M_{\pi(x)}(a)$. We claim that the dipaths joining two distinct inputs $(ax,0)$ and $(a'x',0)$ to their outputs are vertex-disjoint and so $f_{(\pi,\mathcal{M})}$ is realizable. Indeed, if $a \neq a'$ their first parts are in two different $\mathcal{B}_{\text{Left}}(a)$ and $\mathcal{B}_{\text{Left}}(a')$ and the last arcs are disjoint as either $x \neq x'$ or $x = x'$ and $M_{\pi(x)}$ is realizable in $\vec{\mathcal{K}}_{d,d}(\pi(x))$. If $a = a'$, then, since π is realizable, the first dipaths are vertex-disjoint and since $x \neq x'$, the last arcs belong to two different $\vec{\mathcal{K}}_{d,d}$. □

Corollary 28 *If there exist p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d,n)$, then there exist p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d,n+1)$.*

Proof. Let $\mathcal{M}_j$ $(0 \leq j \leq p-1)$ be the family of d^n permutations $M_{x,j}$ defined in example (**26**), that is $M_{x,j}(a) = a+j$, for $x \neq 0$, and $M_{x,j}(a) = a+j+1$, for $x = 0$. Note that the permutation $M_{x,j}$ is realizable in $\vec{\mathcal{K}}_{d,d}(x)$. Let π_0, $\dots$, π_j, $\dots$, π_{p-1} be p compatible cyclic realizable permutations of $\vec{\mathcal{BF}}(d,n)$. By lemma (**27**), the permutation $f_{(\pi_j,\mathcal{M}_j)}$, $0 \leq j \leq p-1$, are cyclic realizable permutations of $\vec{\mathcal{BF}}(d,n+1)$. It remains to show that these permutations are compatible. First, the associated dipaths are arc-disjoint in the left Butterflies $\mathcal{B}_{\text{Left}}(a)$ because the π_j are compatible. Secondly, for any given x, the permutations $M_{x,j}$, with $0 \leq j \leq p-1$, are compatible (i.e. the associated matchings are arc-disjoint). Indeed, for $x \neq 0$ the arcs $(a, a+j)$ and $(a, a+j')$ are arc-disjoint (since $j \neq j'$, $0 \leq j \leq p-1 \leq d-1$ and $0 \leq j' \leq p-1 \leq d-1$). Similarly, for $x = 0$, the arcs $(a, a+j+1)$ and $(a, a+j'+1)$ are disjoint. □

Now, we are ready to prove our main proposition, stated in the introduction:

Proposition 29 (main proposition) *For any $n' \geq n$, if $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ contains p arc-disjoint Hamilton circuits, then $\mathcal{W}\vec{\mathcal{BF}}(d,n')$ contains at least p arc-disjoint Hamilton circuits.*

Proof. The result for $n' = n+1$ follows from corollary (**28**) and lemma (**23**). A recursive application of this property gives the above proposition. $\square$

For an example of the construction see Figure (**4**).

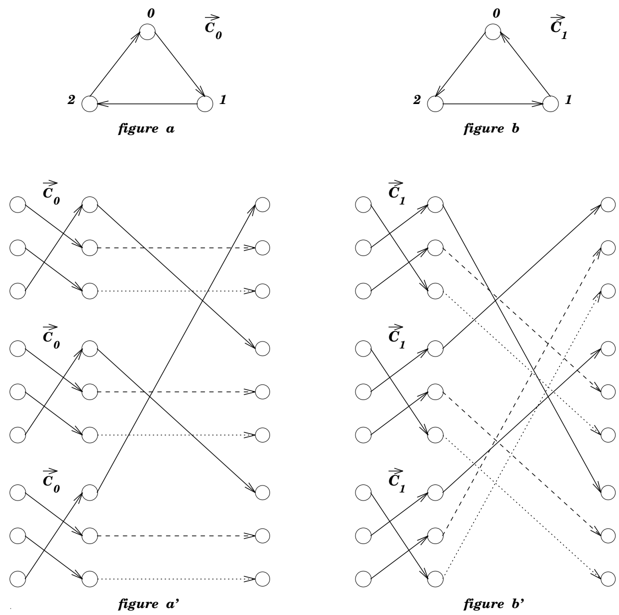

Fig. 4. *Two Hamilton circuits (figures (a') and (b')) of* $\vec{\mathcal{BF}}(3,2)$ *are obtained from two Hamilton circuits of* $\mathcal{W}\vec{\mathcal{BF}}(3,1) = \mathcal{K}_3^+$ *by the construction of lemma (**27**). The figures (a) and (b) show two arc-disjoint Hamilton circuits of* $\mathcal{K}_3^+$*: the circuits* $\{\vec{C}_0 \mid x \to x+1 \pmod 3\}$ *and* $\{\vec{C}_1 \mid x \to x+2 \pmod 3\}$*. This example uses the families* $\mathcal{M}_0$ *(figure (a')) and* $\mathcal{M}_1$ *(figure (b')) defined in the proof of corollary (**28**).*

3.3 Consequences

Corollary 30 $\mathcal{W}\vec{\mathcal{BF}}(2,n)$ *can be decomposed into* 2 *Hamilton circuits as soon as* $n \geq 4$*. For* $1 \leq n \leq 3$*,* $\mathcal{W}\vec{\mathcal{BF}}(2,n)$ *admits only one Hamilton circuit.*

Proof. A computer search has given a decomposition of $\mathcal{W}\vec{\mathcal{BF}}(2,4)$ into 2 arc-disjoint Hamilton circuits. Therefore, by proposition (**29**) $\mathcal{W}\vec{\mathcal{BF}}(2,n)$ has a Hamilton decomposition for any $n \geq 4$. For $1 \leq n \leq 3$, an exhaustive computer search shows that there cannot exist two arc-disjoint Hamilton circuits. $\square$

Corollary 31 $\mathcal{W}\vec{\mathcal{BF}}(3,n)$ *can be decomposed into* 3 *Hamilton circuits as soon as* $n \geq 3$*. For* $1 \leq n \leq 2$*,* $\mathcal{W}\vec{\mathcal{BF}}(3,n)$ *admits only two arc-disjoint Hamilton circuits.*

Proof. For $n \geq 3$, this follows from the existence of a Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3,3)$ obtained by computer (figures of decompositions available on demand). For $n = 1$ and 2, an exhaustive search (by computer) shows that there exist only two arc-disjoint Hamilton circuits. □

Now, we are able to prove Barth's conjecture (conjecture (**11**)):

Theorem 32 *For $n \geq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Proof. By Tillson's decomposition (theorem (**12**)), for $d \neq 4$ and $d \neq 6$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,1) = \mathcal{K}_d^+$ contains $d-1$ arc-disjoint Hamilton circuits. So, by proposition (**29**), for $d \neq 4$ and $d \neq 6$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains at least $d-1$ arc-disjoint Hamilton circuits. For $d = 4$ (*resp.* $d = 6$), we have found, by computer search, 4 (*resp. 6*) arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4,2)$ (*resp.* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(6,2)$). So, by proposition (**29**), $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4,n)$ (*resp.* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(6,n)$) contains 4 (*resp. 6*) arc-disjoint Hamilton circuits. □

As seen in the proof above, there exists a Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ for $n \geq 2$ and $d = 4$ or 6. These results and those of the next section lead us to propose the following conjecture, which would completely close the study of the Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$.

Conjecture 33 *For $d \geq 4$ and $n \geq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ can be decomposed into Hamilton circuits.*

By proposition (**29**), it suffices to prove the conjecture for $n = 2$ or equivalently, as $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2) = L(\mathcal{K}^*_{d,d})$ (see corollary (**38**)), that $\mathcal{K}^*_{d,d}$ admits d compatible Eulerian tours (see [12]).

4 Decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$ into Hamilton circuits

4.1 Line digraphs and conjunction

We need some more definitions and results concerning *conjunction*, *line digraphs* and *de Bruijn digraphs.*

Definitions 34 (see [2])

(1) The **conjunction** *$G_1 \cdot G_2$ of two digraphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the digraph with vertex-set $V_1 \times V_2$ and an arc joining (u_1, u_2) to (v_1, v_2) if and only if there is an arc joining u_1 to v_1 in G_1 and an arc joining u_2 to v_2 in G_2.*

(2) If A and B are two digraphs defined on the same set of vertices with no arc in common, we denote by $A \oplus B$ the **arc-disjoint union (sum)** *of them, that is the digraph on the same set of vertices having as arcs the union of those of A and B.*

(3) cG will denote the digraph made of c disjoint copies of G.

(4) $L^k(G) = L(L^{k-1}(G))$ will denote the k iterated line digraph of G.

For example, $\mathcal{K}^*_{d,d} = \mathcal{K}^+_d \cdot \vec{C}_2$ and $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,4) = A \oplus B$, if A and B are the two arc-disjoint Hamilton circuits of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,4)$.

Properties 35

$$F \cdot G = G \cdot F$$

$$L(F \cdot G) = L(F) \cdot L(G)$$

$$(F \cdot G) \cdot H = F \cdot (G \cdot H) = F \cdot G \cdot H$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C) = A \oplus B \oplus C$$

$$(A \oplus B) \cdot F = (A \cdot F) \oplus (B \cdot F)$$

Proof. These results are clear from the definitions. □

There is a very strong connection between the *de Bruijn* digraph and the wrapped Butterfly digraph. We recall the definition of the de Bruijn digraph:

Definition 36 *The* **de Bruijn digraph** *of out-degree d and diameter n is denoted $\vec{\mathcal{B}}(d,n)$ and has as vertices the words of length n on an alphabet of d letters. A vertex $x_0 \cdots x_{n-1}$ is joined by an arc to the vertices $x_1 \cdots x_{n-1}\alpha$, where α is any letter from the alphabet.*

Propositions 37

$$\vec{\mathcal{B}}(d,n) = L^{n-1}(\mathcal{K}^+_d) \tag{1}$$

$$\vec{\mathcal{B}}(d_1 d_2, n) = \vec{\mathcal{B}}(d_1, n) \cdot \vec{\mathcal{B}}(d_2, n) \tag{2}$$

$$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n) = \vec{\mathcal{B}}(d,n) \cdot \vec{C}_n = L^{n-1}(\mathcal{K}^+_d \cdot \vec{C}_n) \tag{3}$$

$$\vec{\mathcal{BF}}(d,n) = \vec{\mathcal{B}}(d,n) \cdot \vec{P}_n \quad (4)$$

$$\mathcal{W}\vec{\mathcal{BF}}(d_1 d_2, n) = \mathcal{W}\vec{\mathcal{BF}}(d_1, n) \cdot \vec{\mathcal{B}}(d_2, n) \quad (5)$$

Proof. Equality (**1**) is well known, and even sometimes considered as the proper definition of de Bruijn digraphs (see [10,15]).

Result (**2**) can be found in [16] and can be proved as follows: from (**1**), $\vec{\mathcal{B}}(d_1 d_2, n) = L^{n-1}(\mathcal{K}^+_{d_1 d_2})$. As $\mathcal{K}^+_{d_1 d_2} = \mathcal{K}^+_{d_1} \cdot \mathcal{K}^+_{d_2}$, we deduce from properties (**35**) that $L^{n-1}(\mathcal{K}^+_{d_1} \cdot \mathcal{K}^+_{d_2}) = L^{n-1}(\mathcal{K}^+_{d_1}) \cdot L^{n-1}(\mathcal{K}^+_{d_2})$, which is indeed $\vec{\mathcal{B}}(d_1, n) \cdot \vec{\mathcal{B}}(d_2, n)$.

Result (**3**) is implicit in different papers. It can be obtained by considering the following isomorphism from $\vec{\mathcal{B}}(d,n) \cdot \vec{C}_n$ to $\mathcal{W}\vec{\mathcal{BF}}(d,n)$: with the vertex (x,l) in $\vec{\mathcal{B}}(d,n) \cdot \vec{C}_n$, where $x = x_0 x_1 \cdots x_{n-1}$ and $l \in \mathbb{Z}_n$, we associate the vertex $\phi((x,l)) = (x', l)$ in $\mathcal{W}\vec{\mathcal{BF}}(d,n)$, where $x' = x'_{n-1} x'_{n-2} \cdots x'_0$ and $x'_i = x_{i-l}$. By definitions (**34**)-**1** and (**36**), the out-neighbors of (x,l) in $\vec{\mathcal{B}}(d,n) \cdot \vec{C}_n$ are the vertices $(y, l+1)$ with $y = y_0 y_1 \cdots y_{n-1}$ such that $y_i = x_{i+1}$, for $i \neq n-1$, and $y_{n-1} = \alpha$, α being any letter from the alphabet. The associated vertices in $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ are $\phi((y, l+1)) = (y', l+1)$ where $y' = y'_{n-1} y'_{n-2} \cdots y'_0$ and $y'_i = y_{i-l-1}$. For $i - l - 1 \neq n-1$, or equivalently $i \neq l$, $y'_i = x_{i-l} = x'_i$, and for $i = l$, $y'_i = \alpha$. So, by definition (**2**), the vertices $(y', l+1)$ are exactly the out-neighbors of (x', l) in $\mathcal{W}\vec{\mathcal{BF}}(d,n)$. The second part of the equality is due to the fact that $L^{n-1}(\vec{C}_n) = \vec{C}_n$; hence, $L^{n-1}(\mathcal{K}^+_d) \cdot \vec{C}_n = L^{n-1}(\mathcal{K}^+_d) \cdot L^{n-1}(\vec{C}_n) = L^{n-1}(\mathcal{K}^+_d \cdot \vec{C}_n)$. An example is displayed in Figure (**5**).

Result (**4**) can be proved in the same way as (**3**).

The last equality follows directly from (**2**) and (**3**). □

Corollary 38 $\mathcal{W}\vec{\mathcal{BF}}(d,2) = L(\mathcal{K}^*_{d,d})$.

Proof. Follows from proposition (**37**) equality (**3**) with $n = 2$. □

Lemma 39 *When r and s are relatively prime, $\vec{C}_{qs} \cdot \vec{C}_{qr} = q\vec{C}_{qsr}$.*

Proof. $\vec{C}_{qs} \cdot \vec{C}_{qr}$ is a regular digraph with in- and out-degree 1. So, it is the union of circuits. Starting from a vertex (u,v), we find at distance i the vertex $(u+i, v+i)$ where $u+i$ (*resp.* $v+i$) has to be taken modulo qs (*resp.* qr). So, the length of any circuit is the smallest common multiple of qs and qr, that is qrs, as r and s are relatively prime. As the number of vertices in the digraph is $q^2 rs$, there are q such cycles. □

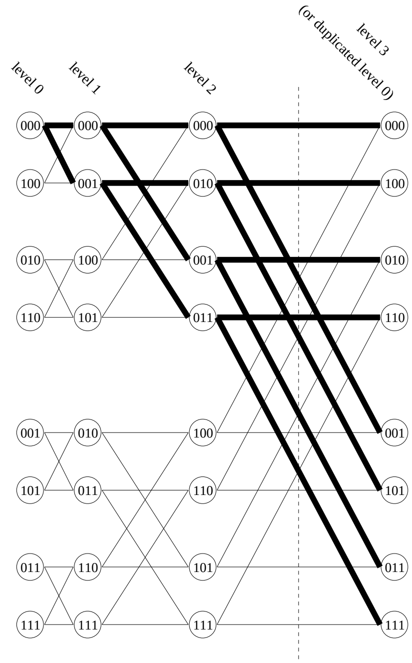

Fig. 5. *The graph* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,3)$ *as a conjunction of* $\vec{\mathcal{B}}(2,3)$ *and* $\vec{C}_3$.

Proposition 40 $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)\cdot\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n) = n\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$.

Proof. Let $G = \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)\cdot\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n)$. By proposition (**37**)-(**3**), we have $G = (\vec{\mathcal{B}}(d_1,n)\cdot\vec{C}_n)\cdot(\vec{\mathcal{B}}(d_2,n)\cdot\vec{C}_n)$. As $\vec{C}_n\cdot\vec{C}_n = n\vec{C}_n$ (from lemma (**39**), with $q = n$ and $s = r = 1$), we obtain: $G = \vec{\mathcal{B}}(d_1,n)\cdot\vec{\mathcal{B}}(d_2,n)\cdot(n\vec{C}_n) = n(\vec{\mathcal{B}}(d_1,n)\cdot\vec{\mathcal{B}}(d_2,n)\cdot\vec{C}_n) = n\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$. $\square$

Corollary 41 *If* d_1 *and* d_2 *are relatively prime, and if* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)$ (resp. $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n)$) *admits* a_1 (resp. a_2) *arc-disjoint Hamilton circuits, then* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$ *admits* a_1a_2 *arc-disjoint Hamilton circuits.*

Proof. Let $\vec{C}_{nd_1^n}$ (*resp.* $\vec{C}_{nd_2^n}$) be a Hamilton circuit in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)$ (*resp.* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n)$). From lemma (**39**), the conjunction $\vec{C}_{nd_1^n}\cdot\vec{C}_{nd_2^n}$ is a set of n circuits of length $nd_1^nd_2^n$. As $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$ has $nd_1^nd_2^n$ vertices, the 1-difactor $\vec{C}_{nd_1^n}\cdot\vec{C}_{nd_2^n}$ consists of n circuits, each one being a Hamilton circuit of a connected component of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)\cdot\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n)$ isomorphic to $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$. So, the conjunction of one Hamilton circuit of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n)$ with one Hamilton circuit of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2,n)$ provides one Hamilton circuit in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$. Applying this results to the a_1a_2 different ordered pairs of circuits provides a_1a_2 arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2,n)$. $\square$

So, by corollary (**41**), it is enough to prove conjecture (**33**) for every power p^i of a prime number p.

4.2 Reduction to the case where p is prime

We would like to prove that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2) = \vec{\mathcal{B}}(d,2)\cdot\vec{C}_2$ has a Hamilton decomposition. But this appears to be quite difficult. However, we will prove that for $n \geq 3$, $\vec{\mathcal{B}}(d,2)\cdot\vec{C}_n$ has a Hamilton decomposition. Such a decomposition will then be sufficient to reduce the problem to the case of prime degrees.

Lemma 42 *For any number $n \geq 3$ and any prime p, $\vec{\mathcal{B}}(p,2)\cdot\vec{C}_n$ can be decomposed into p Hamilton circuits.*

Proof. Let the nodes of $\vec{\mathcal{B}}(p,2)\cdot\vec{C}_n$ be labeled (xy,l), with $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_p$ and $l \in \mathbb{Z}_n$. The digraph $\vec{\mathcal{B}}(p,2)\cdot\vec{C}_n$ is similar to the wrapped Butterfly digraph, and we can define a multistage network by duplicating level 0 to obtain level n. Formally, this multistage network is $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$, where $\vec{P}_n$ is a directed path of length n (i.e. with $n+1$ vertices); its vertices will be labeled (xy,l), with $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_p$ and $l \in \{0,1,\dots,n\}$.

Like in section 2, we can define a notion of realizable permutation in the graph $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$, except that now there is more than one dipath connecting $(xy,0)$ to $(\pi(xy),n)$. We will say that $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$ realizes k compatible permutations $\pi_0, \pi_1, \dots, \pi_{k-1}$ of $\mathbb{Z}_p^2$, if there exist kp^2 dipaths $P_j(xy)$, with $xy \in \mathbb{Z}_p^2$ and $0 \leq j \leq k-1$, where $P_j(xy)$ connects $(xy,0)$ to $(\pi_j(xy),n)$ in $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$, satisfying the following properties: for a given j, the p^2 dipaths $P_j(xy)$ are vertex-disjoint (realizability property) and all the kp^2 dipaths $P_j(xy)$ are arc-disjoint (compatibility property).

Using the same argument as in lemma (**23**), we can establish that $\vec{\mathcal{B}}(p,2)\cdot\vec{C}_n$ can be decomposed into p Hamilton circuits if and only if $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$ realizes p compatible cyclic permutations.

We will show by induction that $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$ realizes p compatible cyclic permutations; more exactly, we will prove that if the property is true for n, it is also true for $n+3$. First, we give, for $n \in \{3,4,5\}$, the dipaths $P_j(xy)$ associated with compatible cyclic permutations.

In all the dipaths that we consider, a vertex (xy,l) is followed by a vertex $(yx',l+1)$ with $x' = g_l(x,y,j) = ax + f(y) + cj$, where a, f and c depend on the level l and where $0 \leq j \leq p-1$.

- For any j, the dipaths $P_j(xy)$ are vertex-disjoint if and only if, at each level, two distinct vertices (x_1y_1, l) and (x_2y_2, l) are followed by two distinct vertices $(y_1x'_1, l+1)$ and $(y_2x'_2, l+1)$. As p is a prime, this is realized if and only if the coefficient a of x in $g_l(x, y, j)$ is different from 0. Indeed, if $y_2x'_2 = y_1x'_1$ then, $y_2 = y_1$ and $x'_2 = x'_1$. So, $ax_2 + f(y_2) + cj = ax_1 + f(y_1) + cj$ and as $y_2 = y_1$. This implies $ax_2 = ax_1$, which in turn implies (as p is a prime number) either $a = 0$ or $x_2 = x_1$.
- Similarly, the dipaths $P_j(xy)$ are arc-disjoint if and only if, for given l, x, y: $g_l(x, y, j) = g_l(x, y', j)$ are different. This is satisfied if and only if $c \neq 0$, as p is a prime number.

Since a vertex of level l is always followed by a vertex of level $l+1$, we will simplify the notation in the following, by omitting the values of the levels from the labels of the vertices.

4.2.1 Initial constructions

Let δ_0 denote the function of $\mathbb{Z}_p$ into $\{0, 1\}$: $\delta_0(x) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x \neq 0 \end{cases}$

$\boldsymbol{n = 3}$

$$P_j(xy) = xy \quad y(x+y+j) \quad (x+y+j)(x+1) \quad (x+1)(y+\delta_0(x+1))$$

$\boldsymbol{n = 4}$

$$P_j(xy) = xy \quad y(x+j) \quad (x+j)(y+j) \quad (y+j)(x+1) \quad (x+1)(y+\delta_0(x+1))$$

Figure (**6**) shows one decomposition of $\vec{\mathcal{B}}(3, 2) \cdot \vec{C}_4$ into circuits. To produce a clearer figure, vertices ab on odd levels are ranked lexicographically and those on even levels in the following order: $ab < a'b'$ if $b < b'$ or $b = b'$ and $a < a'$.

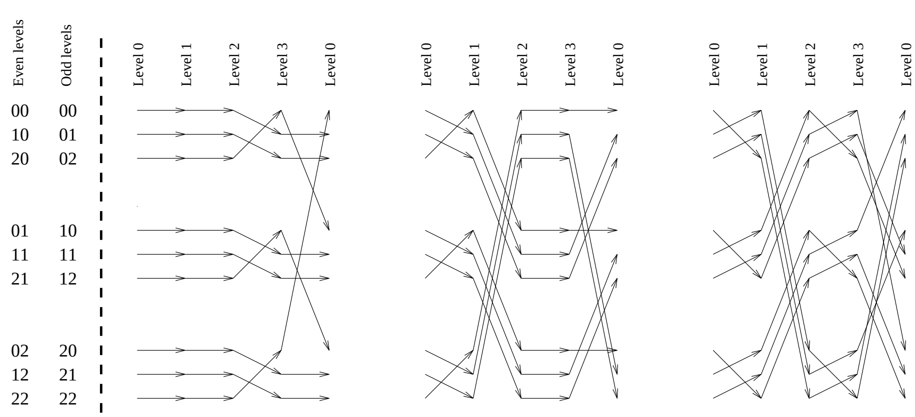

Fig. 6. *A decomposition of $\vec{\mathcal{B}}(3, 2) \cdot \vec{C}_4$, presented with a special ranking of the vertices.*

$n = 5$ and $p \neq 2$ $\quad P_j(xy) =$

$xy \;\; y(x+y+j) \;\; (x+y+j)(x+2j) \;\; (x+2j)y \;\; y(x+1) \;\; (x+1)(y+j+\delta_0(x+1))$

$n = 5$ and $p = 2$ $\quad P_j(xy) =$

$xy \;\; y(x+y+j+1) \;\; (x+y+j+1)(y+j) \;\; (y+j)(x+j+1) \;\; (x+j+1)y \;\; y(x+1)$

In all the cases, one can easily verify that the functions $g_l(x, y, j)$ are of the form $ax + f(y) + cj$ with, $a \neq 0$ and $c \neq 0$. For example, in the construction for $n = 3$, the functions implicitly defined are:

$$\begin{array}{rcl} (X,\ Y) & \overset{X' = aX+f(Y)+cj}{\rightarrow} & (Y,\ \ X') \\ (x,\ \ y) & \overset{X' = X+Y+j}{\rightarrow} & (y,\ \ x+y+j) \\ (y,\ \ x+y+j) & \overset{X' = Y-X-j+1}{\rightarrow} & (x+y+j,\ \ x+1) \\ (x+y+j,\ \ x+1) & \overset{X' = X-Y-j+1+\delta_0(Y)}{\rightarrow} & (x+1,\ \ y+\delta_0(x+1)) \end{array}$$

To complete the proof, it remains to note that in the three first cases, the permutation induced by the construction $\pi(xy) = (x+1)(y+cj+\delta_0(x+1))$ is cyclic, and that in the case $n = 5$ and $p = 2$, $\pi(xy) = y(x+1)$ is also cyclic, as $p = 2$.

4.2.2 Induction step

The induction step follows from two facts. First, it can be easily seen that $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_{n+m}$ realizes p compatible permutations π_j, $0 \leq j \leq p-1$, if and only if there exist two sets of permutations π'_j and π''_j, $0 \leq j \leq p-1$, such that:

- for $0 \leq j \leq p-1$, $\pi_j = \pi'_j \pi''_j$,
- $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_n$ realizes the p compatible permutations π'_j, $0 \leq j \leq p-1$,
- $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_m$ realizes the p compatible permutations π''_j, $0 \leq j \leq p-1$.

Secondly, $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_3$ realizes p compatible permutations π_j, $0 \leq j \leq p-1$, such that each $\pi_j = e$ is the identity permutation. Indeed, let us consider the dipaths:

$$P_j(xy) = xy \;\; y(x+y+j) \;\; (x+y+j)x \;\; xy$$

Once again, a vertex XY of level l is joined to a vertex YX' of level $l+1$, with $X' = g_l(X, Y, j) = aX + f(Y) + cj$, $a \neq 0$ and $c \neq 0$. So, if $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_n$ realizes p compatible permutations π'_j, then $\vec{\mathcal{B}}(p, 2) \cdot \vec{P}_{n+3}$ realizes the same compatible permutations.

So, we can conclude by induction that $\vec{\mathcal{B}}(p, 2) \cdot \vec{C}_n$ can be decomposed into p Hamilton circuits for any number $n \geq 3$. $\square$

Theorem 43 *If a digraph G, with at least 3 vertices, contains k arc-disjoint Hamilton circuits, then $\vec{\mathcal{B}}(d,2)\cdot G$ contains dk arc-disjoint Hamilton circuits.*

Proof. First, we prove the result for d prime. By hypothesis, $G \supset \bigoplus_{0\le i<k-1} \vec{C}_l^i$, where l is the number of vertices of G and $l \geq 3$. Hence:

$$\vec{\mathcal{B}}(d,2)\cdot G \supset \vec{\mathcal{B}}(d,2)\cdot \bigoplus_{0\le i<k-1} \vec{C}_l^i = \bigoplus_{0\le i<k-1} \vec{\mathcal{B}}(d,2)\cdot \vec{C}_l^i$$

From lemma (**42**), we have $\vec{\mathcal{B}}(d,2)\cdot \vec{C}_l = \bigoplus_{0\le j\le d-1} \vec{C}^j_{d^2l}$. So:

$$\vec{\mathcal{B}}(d,2)\cdot G \supset \bigoplus_{0\le i<k-1}\ \bigoplus_{0\le j\le d-1} \vec{C}^{i,j}_{d^2l} \iff \vec{\mathcal{B}}(d,2)\cdot G \supset \bigoplus_{0\le m\le kd-1} \vec{C}^{m}_{d^2l}$$

Suppose now that the result holds for all integers strictly less than d. If d is prime, we have just proved the result. Otherwise, $d = d_1 p$, where p is a prime and $d_1 < d$. By proposition **(37)-2**, $\vec{\mathcal{B}}(d,2) = \vec{\mathcal{B}}(p,2)\cdot\vec{\mathcal{B}}(d_1,2)$. As a consequence, $\vec{\mathcal{B}}(d,2)\cdot G = \vec{\mathcal{B}}(p,2)\cdot(\vec{\mathcal{B}}(d_1,2)\cdot G)$. By induction, $G' = \vec{\mathcal{B}}(d_1,2)\cdot G$ contains at least d_1k arc-disjoint Hamilton circuits. Moreover, since p is prime, $G = \vec{\mathcal{B}}(p,2)\cdot G'$ will contain $pd_1k = dk$ arc-disjoint Hamilton circuits. $\square$

When G can be decomposed into Hamilton circuits, the above theorem can be restated as:

Theorem 44 *If G has more than 3 vertices and can be decomposed into Hamilton circuits, then $\vec{\mathcal{B}}(d,2)\cdot G$ can also be decomposed into Hamilton circuits.*

Corollary 45 *If $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$, with $d \neq 1$, can be decomposed into Hamilton circuits, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(qd,2)$ can also be decomposed into Hamilton circuits for any integer q.*

Proof. Just apply theorem (**44**) to $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(qd,2)$ which is $\vec{\mathcal{B}}(q,2)\cdot\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$ by proposition (**37**). Note that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(1,2)$ has only 2 vertices. So, the corollary cannot be applied for $d = 1$. $\square$

Example 46 *Since $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4,2)$ has a Hamilton decomposition, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4q,2)$ also has a Hamilton decomposition for any integer q. In particular, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2^i,2)$ has a Hamilton decomposition for $i \geq 2$.*

Corollary 47 *To prove conjecture (**33**), it suffices to prove that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p,2)$ has a Hamilton decomposition, for any prime $p \geq 5$.*

Proof. Let d be a non prime number. If d has a prime factor $p \notin \{2, 3\}$, by corollary (**45**), it suffices to prove the conjecture for $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p, 2)$. If $d \geq 4$ has only prime factors equal to 2 or 3, then $d = 2^i 3^j$ with $i + j \geq 2$. A computer search shows that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4, 2)$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(6, 2)$ and $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(9, 2)$ have a Hamilton decomposition. So, according to corollary (**45**), $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2^i 3^j, 2)$, with $i + j \geq 2$ has a Hamilton decomposition. □

Remark 48 *Although it is not the purpose of this article, proposition (***43***) can be used to improve results about the decomposition of de Bruijn digraphs into Hamilton circuits:*

Propositions 49

- *If p is the greatest prime dividing d, then $\vec{\mathcal{B}}(d, 2)$ contains $\frac{p-1}{p}d$ Hamilton circuits.*
- *$\vec{\mathcal{B}}(2^i q, 2)$ contains $(2^i - 1)q$ Hamilton circuits.*

Proof. The first result holds for $p = 1$. For $p > 1$, by a result of Barth, Bond and Raspaud [6], we know that, for p a prime, $\vec{\mathcal{B}}(p, 2)$ contains $p - 1$ arc-disjoint Hamilton circuits and has at least 4 vertices. Hence, theorem (**43**) implies that $\vec{\mathcal{B}}(d, 2)$ contains $(p - 1)d_1$ arc-disjoint Hamilton circuits, as we have $\vec{\mathcal{B}}(d, 2) = \vec{\mathcal{B}}(pd_1, 2) = \vec{\mathcal{B}}(d_1, 2) \cdot \vec{\mathcal{B}}(p, 2)$. Similarly, the second result follows from a result of Rowley and Bose [14], stating that $\vec{\mathcal{B}}(2^i, 2)$ contains $2^i - 1$ Hamilton circuits. □

4.3 Exhaustive Search for Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p, 2)$

As seen above, the problem has been reduced to finding a Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p, 2) = L(\vec{\mathcal{K}}_{p,p})$, for any prime $p \geq 5$. In order to provide ideas and to strengthen our conjecture, we have performed some exhaustive searches. The complexity of an exhaustive search being exponential, we have restricted the set of solutions to those for which *the i-th circuit H_i is obtained from H_0 by applying the automorphism ϕ_i of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p, 2)$ which sends vertex (ab, l) to vertex $(a(b + i), l)$*. Furthermore, we want solutions such that H_0 is Hamiltonian and the Hamilton circuits $H_i = \phi_i(H_0)$, with $0 \leq i \leq p - 1$ are arc-disjoint. However, the search space is still exponential in p and a computer search (with normal computation resources) cannot be successful for p greater than 7. So, we restricted the search space again to *"nearly linear"* solutions. This restriction gave us solutions for small primes strictly less than 29.

For example, for $p = 5$, we found the cycle H_0 given by the following set of arcs:

$$\begin{aligned}
(ab, 0) &\to (a(2b), 1) \qquad (a \notin \{0, 1\}) \\
(0b, 0) &\to (0(2b+1), 1) \\
(1b, 0) &\to (1(2b+2), 1) \\
(ab, 1) &\to ((2a+b)b, 0)
\end{aligned}$$

It induces the following cyclic permutation on level 0:

$$(00, 11, 14, 20, 40, 30, 10, 42, 24, 23, 01, 33, 21, 12, 31, 32, 04, 44, 13, 03, 22, 34, 43, 41, 02)$$

Finally, we looked for very special Hamilton circuits H_0. This enabled us to find a solution for every prime p between 7 and 12000. More precisely, we searched for parameters α and β in $\mathbb{Z}_p$, such that H_0 is given by the following set of arcs:

$$\begin{aligned}
(ab, 0) &\to (a(\alpha b), 1) \qquad (a \neq 0) \\
(0b, 0) &\to (0(\alpha b + \beta), 1) \\
(ab, 1) &\to ((a+b+1)b, 0)
\end{aligned}$$

One can easily check that if $\alpha \neq 1$, the H_i's are arc-disjoint. So, we only have to find α and β such that H_0 is a Hamilton circuit. In particular, we need $\alpha \neq 0$ (condition to obtain a one difactor) and $\beta \neq 0$ (otherwise we obtain a circuit of length p starting at vertex $(0, 0)$). We conjecture that:

Conjecture 50 *For any prime $p > 5$, there exist $\alpha \notin \{0, 1\}$ and $\beta \neq 0$ such that the permutation π of $\mathbb{Z}_p^2$ defined by the following is cyclic:*

$$\begin{aligned}
\pi(ab) &= (a + \alpha b + 1, \alpha b) \qquad (a \neq 0) \\
\pi(0b) &= (\beta + \alpha b + 1, \beta + \alpha b)
\end{aligned}$$

The number of possible solutions is then only p^2. So, we have been able to verify the conjecture by a computer search for large values of p (≤ 12000). Below, we give some solutions for p less than 100.

p	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
α	2	3	4	2	6	2	7	2	3	2	4	3	4	3	4	6	2	2	2	3	2	2
β	3	7	4	14	4	13	28	11	19	25	22	18	29	1	25	14	28	27	51	37	25	16

For example, for $p = 7$, $\alpha = 2$ and $\beta = 3$, we obtain the following cyclic permutation on level 0:

$$(00, 43, 46, 35, 03, 32, 14, 31, 62, 44, 61, 22, 04, 54, 01, 65, 33, 36, 25, 63, 66, 55, 23, 26, 15, 53, 56, 45, 13, 16, 05, 06, 21, 52, 34, 51, 12, 64, 11, 42, 24, 41, 02, 10, 20, 30, 40, 50, 60)$$

So, using corollary (**45**), we have:

Theorem 51 *If d is divisible by any number q, such that $4 \leq q \leq 12000$, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, 2)$, and consequently $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, n)$, has a Hamilton decomposition.*

This result can be strengthened in the case of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, 4)$. Indeed, we know that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2, 4)$ and $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3, 4)$ have a Hamilton decomposition and we have been able to generalize lemma (**42**) for $\vec{\mathcal{B}}(p, 4) \cdot \vec{C}_n$ when p is an odd prime and $n \geq 5$.

Theorem 52 *If d is divisible by any number q, such that $2 \leq q \leq 12000$, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, 4)$, and consequently $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, n)$ for $n \geq 4$, has a Hamilton decomposition.*

As a consequence, the Butterfly digraphs $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2p, n)$ have a Hamilton decomposition, for $n \geq 4$.

5 Conclusion

In this paper, we have shown that in a lot of cases, Butterfly digraphs have a Hamilton decomposition and give strong evidence that the only exceptions are $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2, 2)$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2, 3)$ and $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3, 2)$. We have furthermore reduced the problem to checking if $L(\vec{\mathcal{K}}_{p,p})$ has a Hamilton decomposition for p prime (or equivalently that $\vec{\mathcal{K}}_{p,p}$ has an Eulerian compatible decomposition). We have also shown that such a decomposition will follow from the solution of a problem (conjecture (**50**)) in number theory.

Our interest came from a conjecture of Barth and Raspaud [7], concerning the decomposition of Butterfly networks into undirected Hamilton cycles. This conjecture is solved in [8], by generalizing the techniques of section 3.2.

Finally, we have seen in proposition (**49**) that the techniques can be applied to obtain results on the Hamilton decomposition of de Bruijn digraphs. In this spirit it will be interesting to solve the following problem:

Problem 53 *Determine the smallest integer $f_d(n)$ such that $\vec{\mathcal{B}}(d, n) \cdot \vec{C}_{f_d(n)}$ has a Hamilton decomposition.*

A proof similar to that of lemma (**42**) should lead to $f_d(n) \leq n + 1$. Conjecture (**33**) is, for a given d, equivalent to $f_d(n) \leq n$.

Note added in proof

Helen Verrall [3] has informed us that she has been able to prove conjecture (**16**), thus closing the problem.

Acknowledgments

We thank very much J. Bond, R. Klasing, P. Paulraja, J.G. Peters and A. Raspaud for their numerous remarks and comments.

References

[1] B. Alspach. Research problem 59. *Discrete Mathematics*, 50:115, 1984.

[2] B. Alspach, J-C. Bermond, and D. Sotteau. Decomposition into cycles I: Hamilton decompositions. In G. Hahn et al., editor, *Cycles and Rays, Proceeding Colloquium Montréal, 1987*, NATO ASI Ser. C, pages 9–18, Dordrecht, 1990. Kluwer Academic Publishers.

[3] J. Aubert and B. Schneider. Décomposition de la somme cartésienne d'un cycle et de l'union de deux cycles en cycles hamiltoniens. *Discrete Mathematics*, 38:7–16, 1982.

[4] R. Balakrishnan, J-C. Bermond, and P. Paulraja. On the decomposition of de bruijn graphs into hamiltonian cycles. Manuscript.

[5] D. Barth. *Réseaux d'interconnection: structures et communications*. PhD thesis, Université de Bordeaux I, 1994.

[6] D. Barth, J. Bond, and A. Raspaud. Compatible eulerian circuits in K_n^{**}. *Discrete Applied Mathematics*, 56:127–136, 1995.

[7] D. Barth and A. Raspaud. Two edge-disjoint hamiltonian cycles in the Butterfly graph. *Information Processing Letters*, 51:175–179, 1994.

[8] J-C. Bermond, E. Darrot, O. Delmas, and S. Perennes. Hamilton cycle decomposition of the Butterfly network. Technical Report RR-2920, Inria - Sophia Antipolis - Projet SLOOP (CNRS/INRIA/UNSA), June 1996. To appear in Parallel Processing Letters.

[9] J-C. Bermond, O. Favaron, and M. Maheo. Hamiltonian decomposition of Cayley graphs of degree 4. *Journal of Combinatorial Theory, Series B*, 46(2):142–153, 1989.

[3] Department of Mathematics and Statistics, Simon Fraser University - Canada.

[10] J-C. Bermond and C. Peyrat. Broadcasting in de Bruijn networks. In Proceedings of the 19th S-E conference on Combinatorics, editor, *Congressus Numerantium 66*, pages 283–292. Graph theory, and Computing, Florida, 1988.

[11] S.J. Curran and J.A. Gallian. Hamilton cycles and paths in Cayley graphs and digraphs - a survey. To appear in Discrete Mathematics.

[12] H. Fleischner and B. Jackson. Compatible euler tours in eulerian digraphs. In G. Hahn et al., editor, *Cycles and Rays, Proceeding Colloquium Montréal, 1987*, pages 95–100. NATO ASI Ser. C, Kluwer Academic Publishers, Dordrecht, 1990.

[13] F. Thomson Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays . Trees . Hypercubes.* Computer Science, Mathematics Electrical Engineering. Morgan Kaufmann Publishers, 1992.

[14] R. Rowley and B. Bose. On the number of arc-disjoint hamiltonian circuits in the de Bruijn graph. *Parallel Processing Letters*, 3(4):375–380, 1993.

[15] Jean de Rumeur. *Communication dans les réseaux de processeurs.* Collection Etudes et Recherches en Informatique. Masson, 1994. (English version to appear).

[16] M. Syska. *Communications dans les architectures à mémoire distribuée.* PhD thesis, Université de Nice Sophia Antipolis, 1992.

[17] T. Tillson. A Hamiltonian decomposition of K^*_{2m}, $2m \geq 8$. *Journal of Combinatorial Theory, Series B*, 29:68–74, 1980.