AN ABSTRACT OF THE THESIS OF

Megan E. Lytle for the degree of Honors Baccalaureate of Science in Mathematics presented on June 06, 2013. Title: Edge-Disjoint Hamiltonian Cycles in De Bruijn Graphs.

Abstract Approved:

____

Mary Flahive

The purpose of this thesis is to examine the number of edge-disjoint Hamiltonian cycles in de Bruijn graphs using ideas from finite field theory, particularly linear recurring sequences. It is known that the de Bruijn graph B(d,n) admits d-1 disjoint Hamiltonian cycles when d is a power of 2, and it is conjectured that all de Bruijn graphs B(d,n) admit d-1 disjoint Hamiltonian cycles. The conjecture also states that for every de Bruijn graph there exists a Hamiltonian cycle to which a particular function, defined in chapter 4, can be applied to obtain d-2 additional Hamiltonian cycles. I have shown for several specific de Bruijn graphs that this method does not work on Hamiltonian cycles obtained using linear recurring sequences.

Key words: de Bruijn graphs, Hamiltonian cycles, interconnection networks, linear recurring sequences

Corresponding e-mail address: lytlem@onid.orst.edu

Edge-Disjoint Hamiltonian Cycles in De Bruijn Graphs

by

Megan E. Lytle

A PROJECT

submitted to

Oregon State University

University Honors College

in partial fulfillment of
the degree requirements for the
degree of

Honors Baccalaureate of Science in Mathematics (Honors Scholar)

Presented June 06, 2013
Commencement June 2013

Contents

Edge-Disjoint Hamiltonian Cycles in De Bruijn Graphs

1 Introduction

The d-ary de Bruijn graph B(d, n) consists of nodes corresponding to n-tuples over a d-letter alphabet Σ. There is a directed edge from the node $x_1, ..., x_n$ to the node $y_1, ..., y_n$ if and only if $y_1 = x_2, y_2 = x_3, ..., y_{n-1} = x_n, y_n = \alpha$ with $\alpha \in \Sigma$.For example, the following is a graph of B(2,3):

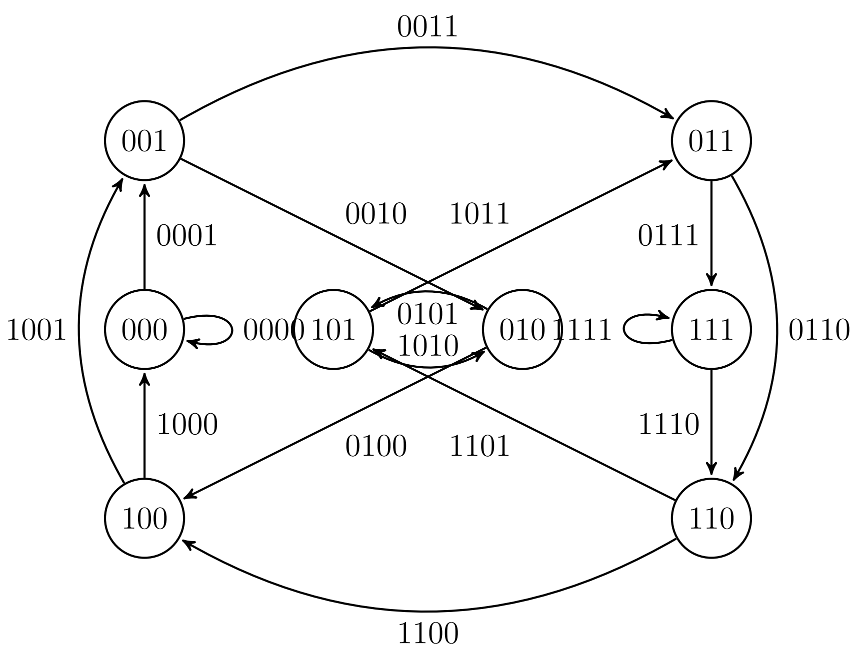

Figure 1: The de Bruijn Graph B(2,3).

De Bruijn graphs are often used as interconnection networks for parallel computing clusters and multicore processors. The nodes of the de Bruijn graph represent individual processors that communicate with each other via the edges of the graph. One processor can send information to another processor if and only if there is a directed edge from the sending processor to the receiving processor.

A Hamiltonian cycle is a path that starts and ends at the same node and visits each node exactly once. Two Hamiltonian cycles are edge-disjoint if they do not use any of the same edges. If a graph admits n disjoint Hamiltonian cycles, then there are at least n disjoint paths in each direction between any two nodes in the graph. It is desirable to have multiple disjoint Hamiltonian cycles in an interconnection network because individual edges are not always available for use. For example, a processor might not be able to receive data because it is busy with another task. In this situation, the busy processor could be avoided by sending the desired information via a different Hamiltonian cycle.

It has been proven that the de Bruijn Graph B(d,n) admits d-1 disjoint Hamiltonian cycles when d is a power of 2. Chapter 3 summarizes this result. It has also been conjectured that the de Bruijn graph B(d,n) always admits d-1 disjoint Hamiltonian cycles. This conjecture, which is explained in more detail in chapter 4, involves applying a function to one Hamiltonian cycle to obtain d-2 additional Hamiltonian cycles.

The purpose of my work has been to use the method of linear recurring sequences to learn more about the number of disjoint Hamiltonian cycles in de Bruijn graphs. Linear recurring sequences are explained in chapter 2. So far I have shown for several specific de Bruijn graphs that Hamiltonian cycles obtained using linear recurring sequences are not effective candidates for the method of finding disjoint Hamiltonian cycles described in chapter 4. This finding is explained in chapter 5.

2 Linear Recurring Sequences

The following information about linear recurring sequences comes from the book *Finite Fields*, by Lidl and Niederreiter.

A kth-order linear recurring sequence is a sequence (x_i) for which

$$x_{n+k} = a_{k-1}x_{n+k-1} + a_{k-2}x_{n+k-2} + ... + a_0x_n$$

where k is a positive integer, $x_0, \cdots, x_{k-1}$ are fixed and the a_i are given elements of a finite field GF(d). The function

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_0$$

is called the characteristic polynomial of the linear recurring sequence given above.

The matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{bmatrix}$$

is called the companion matrix of the characteristic polynomial. Let X_n denote the state vector $[x_nx_{n+1}\cdots x_{n+k-1}]$. Notice that $X_nA = X_{n+1}$ and that $X_0A^n = X_n$. If $a_0 \neq 0$ then the determinant of A is nonzero and A is an element of the group GL(k, GF(d)), the group of invertible kxk matrices with entries in GF(d) under matrix multiplication. Let e be the order A in GL(k, GF(d)). Since $A^e = I_k$, $X_0A^e = X_0$ and therefore $X_0 = X_e$. Since the sequence (x_i) satisfies a kth-order linear recurrence, the preceding fact implies that x_i is perodic with period e. In fact, it can be shown that if $X_0 = [0, 0, \cdots, 1]$ then e is the least period of (x_i) .

Let r be the least period of (x_i). Then for any state vector X_m, $X_m = X_{m+r}$ and therefore $X_m = X_m A^r$. Note that $\{X_0, X_1, \cdots X_k\}$ forms a basis for a k-dimensional vector space over GF(d) when $X_0 = [0, 0, \cdots, 1]$ because each $X_i, 0 \leq i \leq k$ will have zero for the first $k - i$ entries and a 1 for the $k - i + 1$ entry. It follows that $A^r = I_k$, so the order of A in GL(k, GF(d)) is less than or equal to r. We conclude that the least period of (x_i) is the order of A in GL(k, GF(d)).

Let the circular sequence $[x_0, ..., x_{r-n}]$ denote a closed path with length (r-n) in B(d,n) for which the node $(x_i, x_{i+1}, ..., x_{i+n-1})$ is connected to the node $(x_{i+1}, x_{i+2}, ..., x_{i+n})$. For example in the De Bruijn Graph B(2,3), the circular sequence [0, 1, 1, 0] would denote the the cycle

$$(011) \to (110) \to (100) \to (001) \to (011).$$

It turns out that if the characteristic polynomial of (X_i) is a primitive polynomia of degree n over GF(d)l, defined below, then the least period of (X_i) will be $d^n - 1$.

The minimal polynomial of α is defined as the product

$$m(x) = \prod_{\sigma \in conj(\alpha)} (x - \sigma)$$

where σ is in $conj(\alpha)$ if and only if $\sigma = \alpha^{d^k}$ for some k. The elements of $conj(\alpha)$ are called the conjugates of α. Notice that the roots of m(x) are exactly the conjugates of α. A primitive element of GF(d) is an element α for which $\{0, 1, \alpha, \alpha^2, ..., \alpha^{k-2}\}$ is the entire field. The minimal polynomial of a primitive element of the field $GF(d^n)$ is called a primitive polynomial of degree n over GF(d). If α is primitive, then the order of a conjugate $\sigma = \alpha^{d^k}$ is equal to

$$\frac{(d-1)}{gcd(d^k, d-1)} = d - 1$$

because d^k and d-1 are relatively prime. Therefore, if α is primitive, so are its conjugates. We can conclude that all roots of a primitive polynomial are primitive elements. y For example, let's find a primitive polynomial of degree 2 over GF(2). First we need to find a primitive element of $GF(2^2) = GF(4)$. GF(4) is given by $\mathbb{Z}_2[y]/(y^2 + y + 1)$, or the equivalency classes of the polynomials with coefficients in $\mathbb{Z}_2$, modulo $(y^2 + y + 1)$. The elements of GF(4) are 0, 1, y, and (y+1). Note that $y^2 = y + 1$ and $y^3 = y^2 + y = 1$, so $GF(4) = \{0, y^2, y^3\}$. Therefore y is a primitive element of GF(4). Now we need to find the minimal polynomial of y with respect to GF(4). We see that $conj(y) = \{y, y + 1\}$ because $y^2 = y + 1$ and $y^4 = y$. The minimal polynomial of y is thus

$$(x - y)(x - y - 1) = x^2 - 2xy + y^2 + y - x.$$

Since $2xy = 0$ modulo 2, and $y^2 - y = 1$ modulo $(y^2 + y + 1)$, the minimal polynomial of y is given by

$$x^2 + x + 1.$$

This is a primitive polynomial over GF(2).

Theorem 1. *(from Lidl and Niederreiter) If the characteristic polynomial of the linear recurring sequence (x_i) is a primitive polynomial of degree n over GF(d), then the least period of (x_i) is $d^n - 1$, and the cycle $[x_0, x_1, \cdot, x_{r-n}]$ visits every nonzero node of B(d,n).*

Proof. If A is the companion matrix of the charateristic polynomial f(x), then f(A)=0. Every root of a primitive polynomial is a primitive element in the field $GF(d^n)$.Therefore if f(x) is a primitive polynomial then A has order $d^n - 1$. We conclude that the linear recurring sequence $(x_i)$with characteristic polynomial f(x) has least period $d^n - 1$ if $X_0 = [0, 0, \cdots, 1]$, and the cycle $[x_0, x_1, \cdot, x_{r-n}]$ visits every node of B(d,n) except for one. It is clear that the node excluded from the cycle has to be the zero node, because the linear recurrence would map the zero node to itself, leading to a least period of 1. Notice that snce the cycle visits every nonzero node of B(d,n), it is not necessary for the sequene to start at $[0, 0, \cdots, 1]$. □

A cycle obtained using a primitive polynomial can be made Hamiltonian by inserting a 0 into the inear recurring sequence following a string of (n-1) 0s. This is equivalent to replacing one edge that bypasses the zero node with two edges: one that enters the zero node, and one that exits the zero node.

3 Proving that B(d,n) has d-1 Disjoint Hamiltonian Cycles When d is a Power of 2

In their paper ”On the Number of Disjoint Hamiltonian Circuits in the De Bruijn Graph,” Rowley and Bose show that the de Bruijn Graph B(d, n) admits d-1 disjoint Hamiltonian cycles when d is a power of 2. Notice that each node in a de Bruijn graph has indegree and outdegree d, and n-tuples of the form $(\sigma\ , ..., \sigma)$ have loops. A cycle containing a loop cannot be Hamiltonian because it visits the same node twice, so the presence of these loops guarantees that B(d, n) can admit at most d-1 disjoint Hamiltonian cycles.

Rowley and Bose start by using a linear recurring sequence to find a cycle C of length $d^n - 1$ in the de Bruijn graph B(d,n) that visits every nonzero node of the graph. Notice thatthe polynomial

$$f(x) = x^3 - x - 1$$

is primitive over GF(2) because it is the minimal polynomial of the primitive element x with respect to $\mathbb{Z}_2[y]/(y^3 - y - 1)$. Therefore we can generate a cycle containing every nonzero node of B(2,3) using the recurrence $c_{i+3} = c_{i+1} + c_i$. To do this, we start with any nonzero node of B(2,3). That is, any node other that (0, 0, 0). let's choose (0, 0, 1). Then $c_1 = 0, c_2 = 0, c_3 = 1$ becomes the beginning of our sequence and we use our recurrence to find that $c_4 = 0, c_5 = 1, c_6 = 1, c_7 = 1$. After this point, the sequence repeats and we are left with the circular sequence $C = [0, 0, 1, 0, 1, 1, 1]$ which denotes the cycle $(0, 0, 1) \rightarrow (0, 1, 0) \rightarrow (1, 0, 1) \rightarrow (0, 1, 1) \rightarrow (1, 1, 1) \rightarrow (1, 1, 0) \rightarrow (1, 0, 0) \rightarrow (0, 0, 1)$. C visits every nonzero node of B(2,3) and satisfies the linear recurrence $c_i = c_{i-2} + c_{i-3}$.

Let $C = [c_0, ..., c_{k-1}]$ be a circuit satisfying the conditions above and let

$$s + C = [s + c_0, ..., s + c_{k-1}]$$

where s is an element of GF(d). Then s + C is a new cycle of length $k = d^n - 1$. The following lemmas show that the cycles of $(s + C : s \in GF(d))$ are mutually disjoint.

Lemma 1. *(from Rowley and Bose) The circuit*

$$s + C = [y_0, ..., y_{k-1}], s \in GF(d),$$

satisfies

$$y_i = L(y_{i-n}, ..., y_{i-1}) + s(1 - L(1^n)),$$

where (1^n) *denotes the n-tuple (1, ... , 1).*

Proof. Since

$$c_i = L(c_{i-n}, ..., c_{i-1})$$

and

$$x_j = y_j - s$$

for all j, it follows that

$$y_j - s = L((y_{i-n} - s), ..., (y_{i-1} - s)).$$

By adding s to both sides and using the linearity of L to separate it into two functions, we see that

$$y_i = L(y_{i-n}, ..., y_{i-1}) - L(s^n) + s,$$

and factoring an s out of the last two terms we can conclude that

$$y_i = L(y_{i-n}, ..., y_{i-1}) + s(1 - L(1^n)).$$

□

Lemma 2. *(from Rowley and Bose) The circuits of* $(s+C : s \in GF(d))$ *are mutually disjoint.*

Proof. Assume that s + C and t + C have a common edge and $s \neq t$. Then by Lemma 1,

$$L(X) + s(1 - L(1^n)) = L(X) + t(1 - L(1^n))$$

for some n-tuple X. Subtracting L(X) from both sides we find

$$s(1 - L(1^n)) = t(1 - L(1^n)).$$

Since $s \neq t$ and GF(d) is a field (and therefore has no zero divisors), it follows that

$$(1 - L(1^n)) = 0.$$

Therefore

$$L(1^n) = 1$$

and L maps $(1, ..., 1) \to (1, ..., 1)$. This contradicts the assumption that C visits every nonzero node exactly once. We conclude that s and t do not have a common edge and the circuits of $(s + C : s \in GF(q)$ are mutually disjoint. □

Now we have constructed d cycles that are nearly Hamiltonian and our goal is to extend them to create d-1 edge-disjoint Hamiltonian cycles. Since the cycle C contains every node of B(d, n) except for 0^n, each cycle s+C will contain every node except for s^n.

Node s^n can be inserted into s+C by replacing any (n+1)-tuple of the form $\alpha s^{n-1}\beta$ by the (n+2)-tuple $\alpha s^n\beta$. This is equivalent to replacing the arc $(\alpha, s, ..., s)$ with two arcs $(\alpha, s, ..., s) \to (s, ..., s) \to (s, ..., \beta)$. Rowley and Bose show that the edges used to extend the cycles $\{s + C : s \in GF(d), s \neq 0\}$ can be selected so that they all come from the original cycle C. This ensures that the other d-1 Hamiltonian cycles will be edge-disjoint.

Notice that the number of non-loop edges in the graph B(d,n) is

$$d^{n+1} - d = d(d^n - 1).$$

Since each of the d arc-disjoint cycles that we have constructed contain $d^n - 1$ edges, none of which are loops, these cycles partition the nonloop edges of B(d,n). Therefore the edges αs^n and $s^n\beta$ that we used to extend the cycle s + C to a Hamiltonian cycle must lie in circuits (s+k)+C and (s+k')+C for some nonzero k and k'.

Recall from Lemma 1 that $y_i = L(y_{i-n}, ...y_{i-1}) + s(1 - L(1^n))$. So, since $\alpha s^{n-1}\beta$ is an edge in s+C, we have

$$\beta = L(\alpha s^{n-1}) + s(1 - L(1^n)). \tag{1}$$

And since αs^n is an edge in (s+k)+C, we have

$$s = L(\alpha s^{n-1}) + (s + k)(1 - L(1^n)). \tag{2}$$

Finally, since $s^n\beta$ is an edge in (s+k')+C, we have

$$\beta = L(s^n) + (s + k')(1 - L(1^n)). \tag{3}$$

Subtracting (1) from (2), we see that

$$s = \beta + k(1 - L(1^n)), \tag{4}$$

and simplifyng (3) we see that

$$\beta = s + k'(1 - L(1^n)). \tag{5}$$

Substituting the (4) into (5) we derive that k = -k'. Therefore if $\alpha s^{n-1}\beta$ is an edge in s+C, and αs^n is an edge in (s+k)+C, then $s^n\beta$ will be an edge in (s-k)+C.

Since every cycle we have created besides s+C will contain the edge $s^n\beta$ for some β, and the cycle s+C contains the node $s^{n-1}\beta$ for every $\beta \neq s$, we can choose β such that $s^n\beta$ will be an edge in (s-s)+C. That is, we can choose k = s. Then αs^n will be an edge in (s+s)+C. So the edges used to extend s+C will lie in C and 2s+C.

If d is a power of 2, then we are working in a field of characteristic 2, and 2s=0. Therefore, we can extend all of our cycles of the form s+C, $s \neq 0$, using edges in C. The edges that we use to extend distinct cycles will not be the same because if $s \neq t$ then $\alpha s^n \neq \alpha t^n$, and $s^n\beta \neq t^n\beta$. Therefore we can use the d-1 disjoint cycles to create d-1 disjoint Hamiltonian cycles.

For example, let's use this strategy to find three disjoint Hamiltonian cycles in B(4,2). Recall that

$$GF(4) = \mathbb{Z}_2[y]/(y^2 + y + 1) = \{0, 1, y, y + 1\}$$

Since $x^2 + x + (y + 1)$ is a primitive polynomial over GF(4), we can use the linear recurrence relation $x_{i+2} = x_{i+1} + (y+1)x_i$ to find a nearly-Hamiltonian cycle in B(4,2).

Starting with the node (0 1), we obtain the cycle:

$$C = [0, 1, 1, y, 1, 0, (y+1), (y+1), 1, (y+1), 0, y, y, (y+1), y].$$

We find three more nearly-Hamiltonian cycles by adding the field elements to C.

$$1 + C = [1, 0, 0, (y+1), 0, 1, y, y, 0, y, 1, (y+1), (y+1), y, (y+1)].$$

$$y + C = [y, (y+1), (y+1), 0, (y+1), y, 1, 1, (y+1), 1, y, 0, 0, 1, 0].$$

$$(y+1) + C = [(y+1), y, y, 1, y, (y+1), 0, 0, y, 0, (y+1), 1, 1, 0, 1].$$

We can make the cycle 1 + C Hamiltonan by replacing the edge (0, 1, y) with the edges (0, 1, 1) and (1, 1, y). Both of these edges come from C. The resulting Hamiltonian cycle is

$$[1, 0, 0, (y+1), 0, 1, 1, y, y, 0, y, 1, (y+1), (y+1), y, (y+1)].$$

Similarly, we can make the cycles y + C and (y+1) + C Hamiltonian by replacing the edge $((y+1), y, 1)$ with the edges $((y+1), y, y)$ and $(y, y, 1)$, and the edge $(1, (y+1), y)$ with the edges $(1, (y+1), (y+1))$ and $((y+1), (y+1), y)$. The resulting Hamiltonian cycles are

$$[y, (y+1), (y+1), 0, (y+1), y, y, 1, 1, (y+1), 1, y, 0, 0, 1, 0]$$

and

$$[(y+1), y, y, 1, y, (y+1), 0, 0, y, 0, (y+1), 1, 1, 0, 1, (y+1)].$$

These three cycles don't use any of the same edges, so we have found three edge-disjoint Hamiltonian cycles in B(4,2).

4 The Conjecture that all De Bruijn Graphs have d-1 Dijoint Hamiltonian Cycles

In the paper *On Arc-Disjoint Hamiltonian Cycles in De Bruijn Graphs*, Kása presents a conjecture that all de Bruijn Graphs B(d,n) have d-1 disjoint Hamiltonian cycles. The paper defines a function μ on words over the alphabet $\{0, 1, \cdots, q-1\}$, considered modulo q, as follows:

$$\mu(0) = 0$$

$$\mu(i) = i + 1, 1 \leq i < q - 1$$

$$\mu(q-1) = 1$$

For example in the de Bruijn graph B(3,2), $\mu([0, 1, 1, 2, 0, 2, 2, 1]) = [0, 2, 2, 1, 0, 1, 1, 2]$.

The conjecture further states that for every de Bruijn graph B(d,n) there exists a Hamiltonian cycle C such that $C, \mu(C), \mu^2(C), \cdots \mu^{d-2}(C)$ are all edge-disjoint Hamiltonian cycles. In the paper, examples of such cycles are provided for B(3,2), B(3,3), B(4,2), and B(5,2).

The cycles given for B(4,2) are

$$C = [0, 0, 1, 0, 2, 1, 1, 3, 2, 3, 0, 3, 3, 1, 2, 2, 0]$$

$$\mu(C) = [0, 0, 2, 0, 3, 2, 2, 1, 3, 1, 0, 1, 1, 2, 3, 3, 0]$$

$$\mu^2(C) = [0, 0, 3, 0, 1, 3, 3, 2, 1, 2, 0, 2, 2, 3, 1, 1, 0].$$

Notice that the three Hamiltonian cycles do not have any edges (3-tuples) in common with each other.

5 Applying Kása's Function to Hamiltonian Cycles Obtained from Linear Recurring Sequences

I've tried applying Kása's function to Hamiltonian cycles obtained using linear recurring sequences such as the ones in chapters 2 and 3. So far I have checked the cycles obtained from every primitive polynomial of degree 2 and 3 over the fields GF(3) and GF(4). I was not able to find d-1 disjoint Hamiltonian cycles in B(d,n) by applying μ to any of them. For every Hamiltonian cycle C that I obtained from a linear recurring sequence, at least one of the cycles $\mu^x(C), 1 < x \leq d-2$ had edges in common with the original cycle, C.

For example let's look at the Hamiltonian cycle of B(4,2) we found in chapter 3.

$$C = [0, 1, 1, y, 1, 0, (y+1), (y+1), 1, (y+1), 0, y, y, (y+1), y].$$

Let y = 2 and (y+1) = 3 so that $\mu(C)$ is defined. Then we have

$$C = [0, 1, 1, 2, 1, 0, 3, 3, 1, 3, 0, 2, 2, 3, 2]$$

$$\mu(C) = [0, 2, 2, 3, 2, 0, 1, 1, 2, 1, 0, 3, 3, 1, 3]$$

Notice that there are multiple edges in common between these two cycles, for example the edges (2, 2, 3), and (1, 1, 2) are used in both C and $\mu(C)$.

6 Conclusion

Identifying edge-disjoint Hamiltonian cycles in de Bruijn graphs improves the efficiency of de Bruijn interconnection networks because each disjoint Hamiltonian cycle corresponds to two distinct paths between any pair of nodes in the network. It is known that the de Bruijn graph B(d,n) admits d-1 disjoint Hamiltonian cycles when d is a power of 2, and it is conjectured that all de Bruijn graphs B(d,n) admit d-1 disjoint Hamiltonian cycles. It is also known that for the graphs B(3,2), B(3,3), B(4,2), and B(5,2), there exists a Hamiltonian cyce to which Kása's function can be applied to obtan d-2 additional disjoint Hamiltonian cycles. This is believed to be true in general. I have shown that for the graphs B(3,2), B(3,3), B(4,2), and B(4,3), applying Kása's function to a Hamiltonian cycle satisfying a linear recurrence relation does not yield d-1 disjoint Hamiltonian cycles. If this is proved to be true in general, it could provide insight into the kind of Hamiltonian cycles that actually do work for Kása's method. Perhaps this could lead to a proof of Kása's conjecture and a reliable procedure for finding the d-1 disjoint Hamiltonian cycles in the general de Bruijn graph B(d,n).

7 Bibliography

[1] Kása, Z. *On arc-disjoint Hamiltonian Cycles in De Bruijn Graphs* 5th Joint Conference on Mathematics and Computer Science June 2004: 1-5 Print.

[2] Lidl, Rudolph and Niederreiter, Harald. *Finite Fields* Encyclopedia of Mathematics and its Applications 20 1997: 394-410 Print.

[3] Rowley, Robert and Bose, Bella *On the Number of Arc-Disjoint Hamiltonian Circuits in the De Bruijn Graph* Parallel Processing Letters Volume 3 Number 4 1993: Print.