PB-232 598

VULNERABILITY OF DE BRUIJN COMMUNICATIONS NETWORKS

STANFORD UNIVERSITY

PREPARED FOR
NATIONAL SCIENCE FOUNDATION

MAY 1974

BIBLIOGRAPHIC DATA SHEET	1. Report No. Technical Report No. 81	2.	PB 232 598

4. Title and Subtitle	5. Report Date
Vulnerability of de Bruijn communications networks	May 1974
	6.
7. Author(s) Maurice Schlumberger	8. Performing Organization Rept. No.
9. Performing Organization Name and Address Stanford University Digital Systems Laboratory Stanford, California 94305	10. Project/Task/Work Unit No.
	11. Contract/Grant No. Grant NSF GJ-41093
12. Sponsoring Organization Name and Address National Science Foundation 1800 G Street, NW Washington, D.C. 20550	13. Type of Report & Period Covered technical
	14.

15. Supplementary Notes

STAN-CS-74-425

16. Abstracts

This report studies de Bruijn communications networks with faulty nodes. A de Bruijn communications networks is a communications network based on a de Bruijn graph. We show a method for messages to by-pass a faulty node in at most six steps when the out-degree d of the network is larger than two, or when the number of nodes n in the network is a multiple of d^2. In general less than $2 \cdot d^2$ nodes have less than $2 \cdot d$ distinct neighbors. Let the connectivity of the network be the minimum number of nodes that need to fail for the network to become disconnected. The connectivity of an unoriented de Bruijn network is at least d-1. If $n = d^k$, for some integer k, the connectivity of the unoriented network is at least d and that of the oriented network is d-1.

17. Key Words and Document Analysis. 17a. Descriptors

detours, connectivity, node-independent-paths, monotone paths, vulnerability, logarithmic network, fixed length detour.

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group

18. Availability Statement	19. Security Class (This Report)	21. No. of Pages
Approved for public release; distribution unlimited.	UNCLASSIFIED	68
	20. Security Class (This Page) UNCLASSIFIED	22. Price $3.75

STAN-CS-74-425

Vulnerability of de Bruijn communications networks

by

Maurice Schlumberger

April 1974

Technical Report No. 81

DIGITAL SYSTEMS LABORATORY

Stanford University

Stanford, California

This work was supported by the National Science Foundation under Grant GJ-41093.

I. Introduction

In an earlier report we have studied the routing of messages in a de Bruijn network [Sch74]. Messages go in a "store and forward" way from node to node before reaching their final destination. In a de Bruijn graph, a node of address M has for descendants the nodes of addresses

$$(d \cdot M + j) \bmod n, \text{ for each } j \text{ such that } 0 \leq j \leq d-1$$

and where n is the number of nodes in the network.

In the previous report, all nodes are operative all of the time. This report studies the possibilities of a network with a certain number of nodes that fail. A step is the operation that sends a message from one node to one of its neighbors. The distance between two nodes is the smallest number of steps needed for a message to go from one node to the other. The diameter of a network is the largest distance between any two nodes in the network. The number of directly accessible neighbors to a given node is, by definition, the degree of that node. The degree of a network is the largest degree of all nodes of that network.

We can use such a network in two ways, either oriented or unoriented. In an oriented network, the connections are unidirectional, going from a node to its descendants. In an unoriented network, the connections are bidirectional. This is the same as two unidirectional connections. We should then expect much better characteristics in an unoriented network than in an oriented one.

The degree of a de Bruijn network is the same as that of all the nodes. If the out-degree is d and the number of nodes in the network is n, the diameter of the oriented network is $\lceil \log_d n \rceil$. This diameter is the same when the network is unoriented.

When a single node is not working, we show schemes that reroute messages around that node in at most six steps, when $d>2$ or when $n = k \cdot d^2$.

We also study the vulnerability of the network. If the unoriented network has degree $2 \cdot d$ and n nodes, we show that the number of nodes with less than $2 \cdot d$ distinct neighbors is smaller than $2 \cdot d^2$, and that for sufficiently large networks, no node has less than $2 \cdot d-2$ distinct neighbors. We find an upper and lower bound for the connectivity of the network to be respectively $2 \cdot d-2$ and $d-1$. We know that the minimum number of node-independent paths between two points in a network is equal to the connectivity of the network. Looking then at node-independent paths between nodes in the network, we show how to construct such paths in a network with $d \cdot p$ nodes once we know how to construct them in a network with p nodes. Using such paths, we also show that the connectivity of an oriented network with d^k nodes is $d-1$. In a similar unoriented network, there are at least d node-independent paths between two nodes. In an unoriented network with degree 4, and an even number of nodes, there are at least two node independent paths between any two nodes.

II. By-passing a faulty node

When all nodes of a network are operative, the control of the message flow is done locally at each node, and is independent of what happens in the rest of the network. We would like this to also apply when only one node is faulty.

In some cases a node may become inoperative. It is overloaded, or some link to the node is out of service. This prevents the general routing scheme from working. We must find an alternate path that by-passes the faulty node. We show such a path, first when there are d^k nodes in the network, then in the general case. In general, there is a by-pass if $d > 2$, or if n is a multiple of d^2.

We show a by-pass around an inoperative node, six-steps long, when $d > 2$, or $n=k \cdot d^2$. This shows that when a node becomes inoperative, the maximum number of extra steps needed for a message to reach its destination is four. This also requires only local knowledge of the network as the detour has a finite number of steps. A message taking the detour should carry information about the detour path for the length of the detour.

A possible solution to the detour problem, although terribly wasteful, is to send the message to any neighbor but the bad node, and restart the routing of the message from there. This requires up to an extra k steps in a network with diameter k and does not insure that the bad node is not encountered again, or that the message reaches its destination in a finite time. We show here a by-pass of a bad node that takes only six

steps, or four more than the path through the bad node.

Suppose that the node with the following address is inoperative:

$$X_1X_2\ldots X_k \ .$$

and that there are d^k nodes in the network with degree 2.d. The message comes from:

$$X_0X_1X_2\ldots X_{k-1} \ .$$

and the path, going through the bad node, leads to:

$$X_2\ldots X_kX_{k+1} \ .$$

The path in Table 2-1 links the above two addresses without going through the bad node. One should note that this path does not follow the orientation of the edges, at some point the path requires an "ancestor" transformation instead of the "descendant" transformation used up to now.

The various restrictions on the right insure that no intermediate node has the same address as the inoperative node if $d > 1$. If the bad node is the final destination of the message, then not much can be done.

This shows in general for all networks with d^k nodes, the existance of a 6-step detour or an 8-step unoriented cycle. When messages in the system encounter a bad node, they go into a special "detour state", and go around the bad node before resuming normal routing. When the message encounters another bad node while in "detour state", we need a control stack to come back to the previous detour state once we are out of the new one. If there are too many bad nodes, the message may go into an

Table 2-1: Addresses of nodes in a detour.

step number	address	comments
0	$X_0X_1\cdots X_{k-1}$	
1	$X_1X_2\cdots X_{k-1}a$	$a \neq X_k$
2	$X_2X_3\cdots X_{k-1}am$	$m \neq X_k$
3	$bX_2\cdots X_{k-1}a$	$b \neq X_1$
4	$cbX_2\cdots X_{k-1}$	$c \neq X_1$
5	$bX_2\cdots X_{k-1}X_k$	
6	$X_2X_3\cdots X_{k}X_{k+1}$	

infinite loop.

When the number of nodes in the network is not a power of the out-degree, this detour mechanism does not always work. For example, let n=10, d=2, and assume we want to transit a message from node 4 to node 6 when node 8 is out of order. The scheme gives the nodes in Table 2-2. After 6 steps, the scheme does not route the message to its destination. In general the scheme works when the number of nodes in the network is a multiple of d^2, where d is the out-degree of the network, or when $d > 2$.

In order to prove the existence of detours in these cases, we study the graph consisting of the detours and the direct path between two nodes separated by one node. We count the number of node independent paths in this graph between the origin and destination nodes. Before studying this graph, we prove some lemmas related to the expression:

$$Y = x - ((x + r \cdot y) \bmod d) \qquad (2\text{-}1)$$

where x, y and r are integers between 0 and d-1.

Lemma 2-1:

When x is increased by one in (2-1), Y is either unchanged, or changes by an amount of d. This change occurs at most once, for x's in the interval $0 \leq x < d$.

Proof:

This proof shows where the change happens and that it is the only one.

Table 2-2: Addresses of nodes in a detour when n=10, d=2, from node 4 to node 6 when node 8 is inoperative.

step	addresses of the nodes	comments
0	4	origin
1	8,9	Descendants of Step 0; node 8 is not possible because of failure.
2	8 , 9	Descendants of Step 1; node 8 is not possible because of failure.
3	4 , 9	Ancestors of Step 2; node 9 is its own ancestor.
4	2,7 , 4,9	Ancestors of Step 3.
5	4 , 5 , 8 , 9	Descendants of Step 4; nodes 2 and 7 have nodes 4 and 9 as descendants, nodes 4 and 9 have nodes 8 and 9 as descendants and node 8 is not possible.
6	0 , 1 , 8 , 9	Descendants of Step 5; nodes 4 and 9 have nodes 8 and 9 as descendants, node 5 has nodes 0 and 1 as descendants.

The replacementof x by $x_1 = x+1$ in (2-1) gives:

$$Y = x_1 - ((x_1 + r \cdot y) \bmod d) ,$$

$$Y = x+1 - ((x+1 + r \cdot y) \bmod d) \qquad (2-2)$$

If $x+1 + r \cdot y \not\equiv 0 \bmod d$, then the value of Y in (2-2) is the same as in (2-1) as both terms of the right-hand-side have increased by one.

As x increases from 0 to d-1, there can be only one time where the value of Y changes when x increases. It is when:

$$x_1 + r \cdot y = 0 \qquad \bmod d .$$

When x is less than $(-r \cdot y \bmod d)$, then $Y = -(r \cdot y \bmod d)$, and otherwise, $Y = d - (r \cdot y \bmod d)$. When $r \cdot y \equiv 0 \bmod d$, Y is equal to zero for all x such that $0 \leq x < d$. Q.E.D.

Lemma 2-2:

In (2-1), $Y \leq 0$ for precisely $d-(r \cdot y \bmod d)$ x's in the interval $0 \leq x < d$.

Proof:

When x=0, Y is nonpositive, and equal to $-(r \cdot y \bmod d)$. As x increases, Y changes only for $x = d - (r \cdot y \bmod d)$. For all x's smaller than $d - (r \cdot y \bmod d)$, Y is nonpositive. This happens for $d - (r \cdot y \bmod d)$ values of x. When x is larger than this value, Y increases by d and becomes strictly positive. Q.E.D.

Lemma 2-3:

If, in (2-1), gcd(y,d) = g and d = g·δ, then the value of Y as a function of r, is periodic in r with period δ.

Proof:

The replacement of r by r+δ in (2-1) does not change the value of Y.

$x - ((x + r \cdot y + \delta \cdot y) \bmod d) = x - ((x + r \cdot y) \bmod d)$, as

$\delta \cdot y \equiv 0 \bmod d$. Q.E.D.

We can now study the detour scheme in general, between a node of address M and a node of address $d^2 \cdot M + d \cdot h + j$, with h and j between 0 and d-1. We first restate a result from a previous report on the connections between nodes.

Lemma 2-4:

The ancestors of a node with address M have as addresses:

$$\lfloor (M + k \cdot n)/d \rfloor \bmod n, \text{ with } 0 \leq k < d .$$

Proof:

The detailed proof is in a previous report [Sch74], and shows that one descendant from each of these addresses has M as an address. Q.E.D.

Table 2-3 shows the possible addresses of the nodes in the detour when $n = d^2 \cdot z + d \cdot y + x$. These addresses are derived from the definition of a de Bruijn network for the addresses of the descendants of a node and Lemma 2-4 for the addresses of the ancestors of a node. For example the addresses of the ancestors of the node with addresses $d^2 \cdot M + d \cdot p + q$

Table 2-3: Possible addresses for the nodes in a detour

when $n = d^2 \cdot z + d \cdot y + x$.

step	address modulo $n = d^2 \cdot z + d \cdot y + x$	comments
0	M	origin
1	$d \cdot M + p$	Descendants of Step 0; choose coefficient p.
2	$d^2 \cdot M + d \cdot p + q$	Descendants of Step 1; choose coefficient q.
3	$d \cdot M + p + r \cdot (d \cdot z+y) + \lfloor (q+r \cdot x)/d \rfloor$	Ancestors of Step 2; choose coefficient r.
4	$M+r \cdot z+s \cdot (d \cdot z+y) + \lfloor (p+r \cdot y+s \cdot x+\lfloor (q+r \cdot x)/d \rfloor)/d \rfloor$	Ancestors of Step 3; choose coefficient s.
5	$d \cdot M+r \cdot (d \cdot z+y)+\lfloor (q+r \cdot x)/d \rfloor +p-f+t$	Descendants of Step 4; choose coefficient t; here f is: $f = p+r \cdot y+s \cdot x+\lfloor (q+r \cdot x)/d \rfloor \bmod n$.
6	$d^2 \cdot M + d \cdot (p-f+t) + q-g+u$ $= d^2 \cdot M + d \cdot h + i$	Descendants of Step 5; choose coefficient u, this is the destination and g is: $g = q + r \cdot x \bmod d$.

We have the following inequalities: $0 \leq p,q,r,s,t,u,x,y < d$, as (p,q,r,s,t,u) are coefficients for the transformation of addresses between a node and its descendants or ancestors, and (x,y) come from the division of n by powers of d.

(in Step 4 of Table 2-3) are:

$$\lfloor (d^2 \cdot M + d \cdot p + q + r \cdot n)/d \rfloor \mod n ,$$

or, using the value of n, $n = d^2 \cdot z + d \cdot y + x$, and dividing when possible,

$$\lfloor d \cdot M + p + (q + r \cdot x)/d + r \cdot (d \cdot z + y) \rfloor \mod n ,$$

and, taking the integers out of the floor function we obtain the expression of the addresses of Step 3 in Table 2-3.

$$d \cdot M + p + r \cdot (d \cdot z + y) + \lfloor (q + r \cdot x)/d \rfloor \mod n .$$

There are a few obvious constraints on the coefficients in the steps of Table 2-3. The definitions of f and g in Steps 5 and 6 are:

$$f = p + r \cdot y + s \cdot x + \lfloor (q + r \cdot x)/d \rfloor \mod d \quad \text{and}$$

$$g = q + r \cdot x \mod d .$$

If the bad node has address $d \cdot M + h$ and the destination node has address $d^2 \cdot M + d \cdot h + i$, the constraints are:

$p \not\equiv h \mod n$, for Step 1 to avoid the faulty node (C-1)

$p - f + t \equiv h \mod n$, for Step 6 to be the destination (C-2)

$q - g + u \equiv i \mod n$, for Step 6 to be the destination (C-3)

$r \cdot (d \cdot z + y) + \lfloor (q + r \cdot x)/d \rfloor \not\equiv 0 \mod n$, for Step 5 to avoid the faulty node. (C-4)

We now prove a few lemmas related to the addresses in the detour before showing how many node-independent detours there are.

Lemma 2-5:

When $n \geq d$, constraint (C-4) is equivalent to $r \neq 0$.

Proof:

We first show that (C-4) implies $r \neq 0$, then that for $n \geq d$, $r \neq 0$ implies (C-4).

Let $r=0$ in (C-4). This gives:

$0 \cdot (d \cdot z+y) + \lfloor (q+0 \cdot x)/d \rfloor \not\equiv 0 \bmod n$, or, after simplifications

$$\lfloor q/d \rfloor \not\equiv \bmod n \ .$$

But q is by definition less than d, and the resulting contradiction implies $r \neq 0$.

In order to prove the converse part of the lemma, we show that $r \neq 0$ implies (C-4),

When $r \neq 0$, $r \cdot (d \cdot z+y) = r \cdot \lfloor n/d \rfloor \not\equiv 0 \bmod n$. So (C-4) can only be false when $r \neq 0$, if

$$r \cdot (d \cdot x+y) + \lfloor (q+r \cdot x)/d \rfloor \equiv 0 \mod n \qquad (2\text{-}3)$$

$$= k \cdot n, \text{ for some positive integer } k.$$

We show that the expression on the left-hand-side of (2-3) is always less than n when $n \geq d$, hence that (2-3) cannot be satisfied for $r \neq 0$. Let $A(x,y,z)$ be the expression on the left-hand-side of (2-3). By setting

r=q=d-1, we obtain an upper bound on A(x,y,z):

$$(d-1) \cdot (d \cdot z+y) + \lfloor (d-1) \cdot (x+1)/d \rfloor = U(x,y,z) \geq A(x,y,z) .$$

We now show that U(x,y,z) is less than $n = d^2 \cdot z+d \cdot y+x$.

$$U(x,y,z) = d^2 \cdot z+d \cdot y - (d \cdot z+y) + x+1 + \lfloor -(x+1)/d \rfloor .$$

$$= n - (d \cdot z+y) + 1 + \lfloor -(x+1)/d \rfloor$$

and as $1 \leq x+1 \leq d$, we have:

$$U(x,y,z) = n - (d \cdot z+y) .$$

$$< n, \text{ when } n \geq d .$$

Hence, when $n \geq d$, $A(x,y,z) < n$, and $r \neq 0$ implies (C-4). Q.E.D.

Lemma 2-6:

In the general detour scheme, at most one value of the parameter q yields addresses that do not satisfy (C-3).

Proof:

The destination address is:

$$d^2 \cdot M + d \cdot h + i = d^2 \cdot M + d \cdot (p-f+t) + q-g+u \mod n , \qquad (2-4)$$

where

$$f = p + r \cdot y + s \cdot x + \lfloor (q + r \cdot x)/d \rfloor \mod d, \text{ and}$$

$$g = q + r \cdot x \mod d .$$

Constraint (C-3) requires:

$$q-g+u = i \ .$$

If i=0, this implies that $q-g \leq 0$. The expression for q-g is:

$$q-g = q -((q + r*x) \bmod d) \ .$$

This is the same expression as (2-1), with a change of variables. Lemma 2-2 shows then that $q-g \leq 0$ for precisely $d-(r*x \bmod d)$ values of q.

If $\gcd(x,d) \neq 1$, we can always choose an r such that $q-g \leq 0$ for all values of q in $0 \leq q < d$, as there is an $r \neq 0$ such that $r*x \equiv 0 \bmod d$. If $\gcd(x,d) = 1$, then r=0 is the only r for which there are d values of q such that $q-g \leq 0$.

We have seen in Lemma 2-5 that r must be different from zero. However, by choosing r to be the solution of the congruence $r*x = 1 \bmod d$, which is possible as $\gcd(x,d) = 1$, it is possible to find d-1 values of q such that $q-g \leq 0$. There are then always at least d-1 values of q for which condition (C-3) is satisfied. Q.E.D.

We first show how to satisfy conditions (C-2) and (C-3) when h and i are equal to zero. We then show how to extend those results to any values of h and i less than d.

Lemma 2-7:

In the general detour scheme, there exists a one-to-one correspondence between values of the parameters q and r that satisfy condition (C-3).

Proof:

Lemma 2-6 has shown which values of r satisfy (C-3) for a given value of q. We now show that for each value of q we can assign a different value of r such that condition (C-3) is satisfied.

We do the correspondence sequentially, keeping (C-3) satisfied. Let gcd(x,d) = t. Using Lemma 2-3 and the proper change of variables, we know that (r·x) mod d and q-g in (2-4) are periodic in r with period d/t. This implies that (r·x) mod d takes d/t different values and each of these values is taken for t different values of r. We assign values of r to corresponding values of q in the following way that satisfies (C-3).

(0) Set i to zero. Let R and Q be respectively the sets of all possible values of r and q. Both these sets have cardinality d.

(1) Take, in R, the t values of r that maximize (r·x) mod d. They correspond to the values of q that have the least number of possible values of r so that (C-3) is satisfied. Associate these values of r arbitrarily with the values of q between i and i+t-1.

(2) Delete from R the values that have been assigned. Set i to i+1. If i·t = d then stop, all values have been assigned.

(3) go to Step 1.

We now have to show that, using this correspondence, the expression of q-g in (2-4) stays less than one. Using a change of variable, the proof of Lemma 2-2 shows that the first d-(r·x)mod d values of q satisfy

this condition. In Step 1, we associate with the t values of r that give the same value for $(r \cdot x) \bmod d$, t values of q between $d-((r \cdot x) \bmod d)-1$ and $d-t-(r \cdot x) \bmod d$. This association satisfies (C-3) . Q.E.D.

Table 2-4 shows an example of possible matches between the parameters q and r that satisfies (C-3) when t=1.

This correspondence has another property that is useful later, when finding a correspondence between parameters p and r of the detour.

Lemma 2-8:

Condition (C-3) gives a correspondence between the parameters q and r such that $\lfloor (q+r \cdot x)/d \rfloor = \lfloor (i+r \cdot x)/d \rfloor$, when i is the parameter of the destination in (C-3).

Proof:

We can write the addresses of Step 5 in two different ways, depending on the method used to obtain them. They are either a descendant of Step 4, or an ancestor of Step 5. This gives the equality:

$$d \cdot M + p-f+t + \lfloor (q+r \cdot x)/d \rfloor = d \cdot M + h + \lfloor (i+r \cdot x)/d \rfloor \bmod n .$$

As condition (C-2) implies that $p-f+t = h$, the equality becomes

$$\lfloor (q+r \cdot x)/d \rfloor = \lfloor (i+r \cdot x)/d \rfloor \qquad \text{Q.E.D.}$$

Using this correspondence between Q and R, we show what happens with condition (C-2). Once q or r is chosen this is very similar to (C-3), and we can find a one-to-one correspondence between the parameters

Table 2-4: Matching the parameters q and r when t=1.

The table shows the values of $q-(q+r\ x) \bmod d$, when x=1, d=7. The shaded areas indicate where there is no possible match. The matches in the one-to-one correspondence fall on a diagonal and encircled.

q \ r	0	1	2	3	4	5	6
0	0	-1	-2	-3	-4	-5	(-6)
1	0	-1	-2	-3	-4	(-5)	-6
2	0	-1	-2	-3	(-4)	2	1
3	0	-1	-2	(-3)	3	2	1
4	0	-1	(-2)	4	3	2	1
5	0	(-1)	5	4	3	2	1
6	(0)	6	5	4	3	2	1

p and r that satisfy conditions (C-2) and (C-3).

Let A(r) be the part in the expression of f that depends on q and r:

$$A(r) = (r \cdot y + \lfloor (q + r \cdot x)/d \rfloor) \bmod d \ . \qquad (2\text{-}5)$$

Condition (C-2) is satisfied if:

$$p - f \leq 0 \ , \text{ or, using } A(r)$$

$$p - (p + s \cdot x + A(r)) \bmod d \leq 0 \ .$$

We now show an important property on A(r), when $i < d/2$. By symmetry, a similar property is true when $i \geq d/2$.

Lemma 2-9:

When $i < d/2$, for all h less than t, there are at least h different values of $r \neq 0$ such that $A(r) \bmod t < h$.

Proof:

Let $Z(r) = A(r) \bmod t$. We have, using the correspondence of Lemma 2-7 between q and r and Lemma 2-8:

$$Z(r) = r \cdot y + \lfloor (i + r \cdot x)/d \rfloor \bmod t,$$

with $0 \leq x, y < d$. We can rewrite this as:

$$Z(r) = \lfloor (r \cdot (d \cdot y + x) + i)/d \rfloor \bmod t.$$

The expression within the floor function is less than h for:

$$r_j \leq r < r_j + \Delta_j \ , \qquad (2\text{-}6)$$

where

$$r_j = (j \cdot t \cdot d - 2 \cdot i)/(d \cdot y + x) \text{ , and}$$

$$\Delta_1 = h \cdot d/(d \cdot y + x) \text{ .}$$

We want to show that for all h less than t, there are at least h different integer r that satisfy (2-6). Let then

$$\gcd(d \cdot t, d \cdot y + x) = u \text{ .}$$

As $t = \gcd(d,x)$, we have $u \geq t$. Using u, we can express r_j differently. It is:

$$\begin{aligned} r_j &= j \cdot t \cdot d/(d \cdot y + x) - 2 \cdot i/(d \cdot y + x) \text{ ,} \\ &= s_j - \Delta_2, \text{ with } \Delta_2 = 2 \cdot i/(d \cdot y + x) \text{ ,} \\ &= \lfloor s_j \rfloor + (j \cdot t \cdot d \bmod (d \cdot y + x))/(d \cdot y + x) - \Delta_2 \text{ .} \\ &= \lfloor s_j \rfloor + m \cdot u/(d \cdot y + x) - \Delta_2, \text{ with the integer m such} \qquad (2\text{-}7) \\ &\qquad \text{that } 0 \leq m < (d \cdot y + x)/u, \text{ and m} \end{aligned}$$

can also be equal to zero when $u > 1$.

There are then at least u-1 different values of j for which there is an integer r satisfying (2-6) with h=1. These values of j correspond to those where m=0 in (2-7), and there is an integer satisfying (2-6) then as $d > 2 \cdot i$.

When u=1, the lemma is verified, as t is also equal to one. Assume now that $u > 1$. The integers satisfying (2-6) with m=0 in (2-7) are:

$$\lfloor s_j \rfloor = \lfloor j \cdot t \cdot d/(d \cdot y + x) \rfloor, \text{ for } j = k \cdot (d \cdot y + x)/(t \cdot u), \text{ and } k = 1, \ldots, u-1 .$$

If $u \leq d$, this gives u-1 different integers, hence at least t-1 of them, and the lemma is verified. If $u > d$, this gives d-1 different integers, and the lemma is also verified. Q.E.D.

We are now ready to show the existance of a one-to-one correspondence between the parameters p and r of the addresses of the nodes of the detour that satisfy conditions (C-1) to (C-4).

Lemma 2-10:

In the general detour scheme, there exists a one-to-one correspondence between the values of the parameters p, q and r that satisfy conditions (C-1) to (C-4), when the parameters h and i of the destination address are equal to zero.

Proof:

Lemma 2-7 has shown such a correspondence between the parameters q and r for condition (C-3). Condition (C-4) restricts the values of r to be nonzero, as shown in Lemma 2-5. We now focus on conditions (C-1) and (C-2).

Condition (C-2) is very similar to (C-3), it is satisfied if

$$p - f \leq 0, \text{ or using } A(r) \text{ in the expression of } f$$

$$p - (p + s \cdot x + A(r)) \bmod d \leq 0 . \qquad (2\text{-}8)$$

Lemma 2-2 and a change of variables show that (2-8) is satisfied for $(d - (s \cdot x + A(r)) \bmod d)$ values of p. By definition of t, $(s \cdot x + A(r)) \bmod d$, is periodic in s with period d/t. In order to be able to have all

the values of p and $r \neq 0$ corresponding, we must show that for any h less than d, $((s*x + A(r)) \bmod d)$ is less than h for r different values of $r \neq 0$. This is proven, for $s=k*t$, in Lemma 2-9. All values of $r \neq 0$ have a corresponding p. Because of the freedom of the choices of p, we can choose the p corresponding to r=0 to be the one avoided by condition (C-1). This shows the existence of a one-to-one correspondence between the d-1 nonzero values of r and the parameters p and q satisfying conditions (C-1) to (C-4). Q.E.D.

We now show that these results can be extended to values of the parameters of h and i other than zero.

Lemma 2-11:

The results of Lemmas 2-6, 2-7, 2-9 and 2-10, are also valid if the parameters h and i of the faulty node are different from zero.

Proof:

We prove this only for $i \neq 0$, as the proof for h is the same with a change of variables. We also restrict our proof to Lemma 2-7 as the others follow from it.

Condition (C-3) is equivalent to:

$$i-d < q-p \leq i \quad .$$

We know how to find a correspondence between values of q and r, that is one to one and satisfies (C-3) when i=0, or, by symmetry when i=d-1. The reason why we find a correspondence in this case, is because for any m less than d, there are at least m possible parameters q that have at least d-m possible matches in r. We show that this property is

kept when i increases from 0 to $\lfloor d/2 \rfloor$, or by symmetry, decreases from d-1 to $\lceil d/2 \rceil$. Let $t = \gcd(x,d)$. Let Q_j be the number of parameters q that have at least d-j·t possible matches in r that satisfy (C-3) for a given i. Lemma 2-7 uses the fact that for i=0, we have $Q_j = (j+1)\cdot t$. Let ":=" indicate an update. When i increases from zero to t, we have the following changes.

$$Q_j := Q_j + t, \text{ for } j = 1,\ldots,d/t - 2 ,$$

as t parameters r that could only be matched with d/t q's can now be matched only with the other d-d/t q's. Similarly, when i increases to i+t, the changes are, when $i+t < \lceil d/2 \rceil$:

$$Q_j := Q_j + t, \text{ for } j = 1 + i/t,\ldots,d/t - 2 - i/t .$$

As all these changes only increase the Q_j's, we keep the property that allowed for the one-to-one correspondence. Q.E.D.

Table 2-5 shows an example of possible matches between the parameters q and r that satisfy (C-3), when t=1, for various values of the parameter i.

We now show an example of a correspondence between the various parameters that satisfy (C-1) to (C-4) when h and i are nonzero.

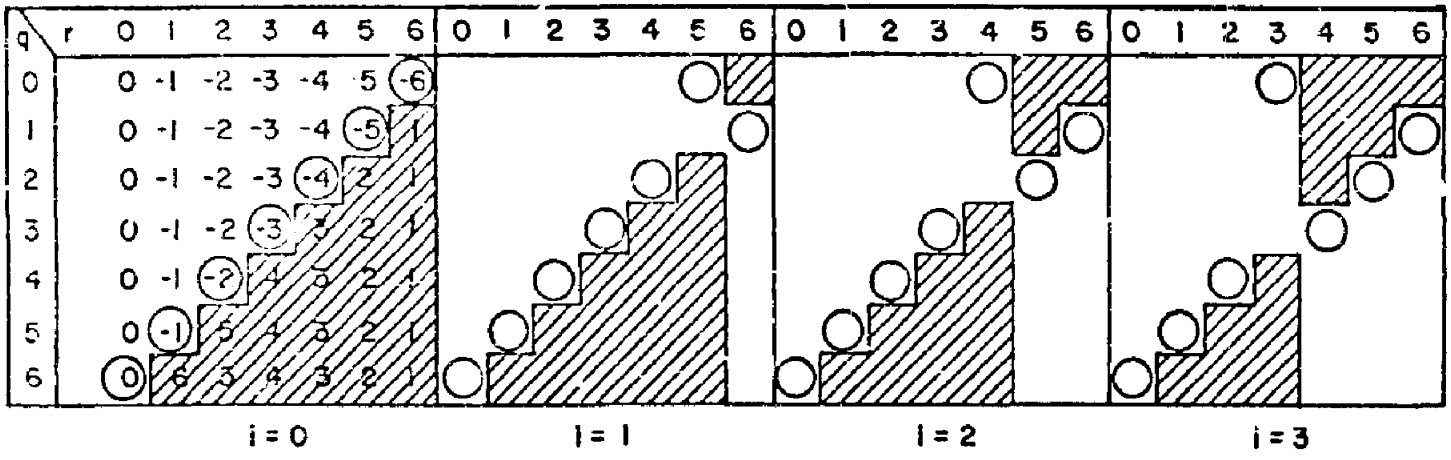
Example:

Take d=12, x=9, y=2, h=5, i=3 .

This gives t=3, j=4. We compute the values of r·x mod d, for $0 \le r < d$, then match the parameters q to each value of r. We then compute r·y mod d, $\lfloor (r\cdot x+i)/d \rfloor$ and A(r). We then show what values of p are impossible to

Table 2-5: Corresponding values of q and r when t=1.

We show the values of $q - (q \div r \cdot x) \bmod d$, when x=1, d=7 and indicate the areas of the table for which there is no possible match.



The shaded areas are those where there is no possible match. The circled squares are the corresponding values. The numbers in the table are the same for all i, but the circles and shaded areas depend on i.

associate to a given value of r, and choose the matches among the remaining ones, avoiding p=j. For each chosen value of p, we give a possible value for s. All this is summarized in Table 2-6.

In order to find how many node-independent detours there are, we first check what nodes may be common to two different steps of the detour.

Lemma 2-12:

If $n > d^2$, there is no common node between Steps 1, 3 and 5 of the detour.

Proof:

We show that the address of the nodes are different in each step. First we look for nodes common to Steps 1 and 3. This is possible when

$$d \cdot M + p = d \cdot M + p' + \lfloor (r \cdot n+q)/d \rfloor \mod n.$$

This gives, after simplifications:

$$p-p' = \lfloor (r \cdot n+q)/d \rfloor \mod n . \qquad (2-9)$$

As, in the detour (C-4) implies $r \neq 0$, (2-9) is impossible to satisfy for $n > d^2$.

There can be some nodes in common between Steps 1 and 5 if

$$d \cdot M + p = d \cdot M + h + \lfloor (r \cdot n+q)/d \rfloor \mod n .$$

As $r \neq 0$, this is also impossible, for $n > d^2$.

There can be some nodes in common between Steps 3 and 5 if

Table 2-6: Setting the parameters in order to by-pass a faulty node. d=12, x=9, y=2, h=5, i=3.

	r	0	1	2	3	4	5	6	7	8	9	10	11
9·r mod 12		0	9	6	3	0	9	6	3	0	9	6	3
	q	11	3	0	6	9	4	1	7	10	5	2	8
2·r mod 12		0	2	4	6	8	10	0	2	4	6	8	10
⌊(9·r+3)/12⌋		0	1	1	2	3	4	4	5	6	7	7	8
A(r)		0	3	5	8	11	2	4	7	10	1	3	6
impossible p's		/	11	/	/	/	/	11 10	11 10	11 10	11 10	11	11
	p	5	7	8	9	10	11	0	1	2	3	4	6
	s		0	1	0	1	1	0	0	1	0	0	0

$$d \cdot M + p + \lfloor (r \cdot n + q)/d \rfloor = d \cdot M + h + \lfloor (r' \cdot n + q')/d \rfloor \mod n.$$

As (C-1) requires $p \neq h$, this is impossible for $n > d^2$. Q.E.D.

We now study what happens when two steps have nodes in common. We start with one node in common between Steps 1 and 2.

Lemma 2-13:

When there is a node in common between Steps 1 and 2, there can be no other steps in the detour with nodes in common when n is larger than d^4.

Proof:

The relation satisfied by the address of a node common to Steps 1 and 2 is:

$$d \cdot M + p = d^2 \cdot M + d \cdot p' + q' \mod n. \qquad (2\text{-}10)$$

Lemma 2-11 has shown that there is no common node between Steps 1, 3 and 5 in the detour when $n > d^2$. If there were a node common to Steps 1 and 4, its address would satisfy the relation:

$$d \cdot M + p'' = M + \lfloor (h + s \cdot n + \lfloor (i + r \cdot n)/d \rfloor)/d \rfloor \mod n.$$

Multiplying this by d gives:

$$d^2 \cdot M + d \cdot p'' = d \cdot M + h + \lfloor (i + r \cdot n)/d \rfloor - f \mod n,$$

where f is less than d. This is impossible to satisfy along with (2-10) when $n > d^4$, as $r \neq 0$.

Similarly, as $r \neq 0$, there is no common node between Step 2 and Steps 3 and 5, or between Step 4 and Step 3 and 5, and between Steps 2 and 4. This finishes the proof as there is no other common node between two steps possible. Q.E.D.

We should note that the common node between Steps 1 and 2 may be the faulty node responsible for the detour. We now show a similar result when there is a node in common between Steps 1 and 4.

Lemma 2-14:

When there is a node in common between Steps 1 and 4, there can be no other node in common between two steps of the detour when $n \geq d^4 + d^3$.

Proof:

If there is a node in common to steps 1 and 4, its address satisfies the relation:

$$d \cdot M + p = M + \lfloor (h + s \cdot n + \lfloor (i + r \cdot n)/d \rfloor \mod n,$$

or multiplying both sides by d,

$$d^2 \cdot M + d \cdot p = d \cdot M + h + \lfloor (i + r \cdot n)/d \rfloor - f \mod n, \qquad (2\text{-}11)$$

where $f < d$.

Lemma 2-11 shows that there is no node in common between any two of the Steps 1, 3 or 5. Lemma 2-13 shows that there is no node in common between Steps 1 and 2. If there is a node in common between Steps 2 and 3, some set of parameters satisfies the following relation:

$$d^2 \cdot M + d \cdot p' + q' = d \cdot M + h + \lfloor (i + r'' \cdot n)/d \rfloor - f' \mod n,$$

where $f' < d$. If $n > d^4$, this can only be verified, along with (2-11), if they have the same set of parameters. This also implies that these nodes are the same. But we have seen that there is no common node between Steps 1 and 2, the relation cannot be satisfied. There is no common node between Steps 2 and 3.

Similarly, there is no common node between Steps 2 and 5 between Steps 3 and 4. By changing the orientation of the network, Step i is changed into Step 6-i, but the topology of the network is maintained. Lemma 2-13 shows then that there is no common node between Steps 4 and 5, as they correspond to Steps 1 and 2 in the other orientation.

If there is a node in common between Steps 2 and 4, there are parameters that satisfy:

$$d^2 \cdot M + d \cdot p' + q' = M + \lfloor (h + s'' \cdot n + \lfloor (i + r'' \cdot n)/d \rfloor)/d \rfloor \mod n. \quad (2\text{-}12)$$

Subtracting (2-12) from (2-11) gives:

$$d \cdot M + h + \lfloor (i + r \cdot n)/d \rfloor - f = d \cdot (p - p') - q' + M + \lfloor (h + s'' \cdot n + \lfloor (i + r'' \cdot n)/d \rfloor)/d \rfloor \mod n$$

This gives, after multiplication by d:

$$d^2 \cdot M + d \cdot (h - f) + i - g = d^2 \cdot (p - p') - d \cdot q' + d \cdot M + h + \lfloor (i + r'' \cdot n)/d \rfloor - g'' \mod n, \quad (2\text{-}13)$$

where g and g'' are less than d.

Subtracting (2-11) from (2-13) gives:

$$d\cdot(h-f-p) + i-g = d^2\cdot(p-p') - d\cdot q' + \lfloor(i+r''\cdot n)/d\rfloor - g'' -$$

$$\lfloor(i+r\cdot n)/d\rfloor \mod n.$$

This is impossible to satisfy, if $r \neq r''$ and $n > d^4 + d^3$, as the difference of the two floor functions is larger than the rest of the elements. This finishes the proof, showing that there is no common node to two steps, but the first one. Q.E.D.

This takes care of all the cases where Step 1 has some node in common with some other Step in the detour. By reciprocity, it also takes care of Step 5. We assume now that Steps 1 and 5 have no node in common with any other step.

Lemma 2-15:

When Step 1 has no common node with any other step, there can be at most one common node between Step 2 and any other step, either between Steps 2 and 3 or between Steps 2 and 4, when n is larger than $d^4 + d^3$.

Proof:

We consider what happens when we reverse the orientation of the network. The primed numbers denote step numbers when the orientation is reversed. Assume that there is a common node between Steps 2 and 3, or 3' and 4'.

There cannot be any new node in common between Steps 2 and 5, as this corresponds to 1' and 4', and this would contradict Lemma 2-14.

Similarly, a common node is impossible between Steps 4 and 5 (1' and 2'), because of Lemma 2-13.

A node in common between Steps 3 and 4 is the same as the node in common between Steps 2 and 3, as shown in Lemma 2-14. Assume now that there are both a node in common between Steps 2 and 3 and 2 and 4. This implies the existence of sets of parameters satisfying the equations:

$$d^2 \cdot M + d \cdot p + q = d \cdot M + p' + \lfloor r' \cdot n/d \rfloor \mod n, \qquad (2\text{-}14)$$

for a common node between Steps 2 and 3 and

$$d^2 \cdot M + d \cdot p'' + q'' = M + \lfloor (p_1 + s_1 \cdot n + \lfloor (r_1 \cdot n)/d \rfloor)/d \rfloor \mod n, \qquad (2\text{-}15)$$

for a common node between Steps 2 and 4.

Subtracting (2-14) from (2-15) gives:

$$d \cdot (p''-p) + q''-q + d \cdot M + p' + \lfloor r' \cdot n/d \rfloor =$$

$$M + \lfloor (p_1 + s_1 \cdot n + \lfloor (r_1 \cdot n)/d \rfloor)/d \rfloor \mod n.$$

We multiply this by d, and get:

$$d^2 \cdot (p''-p') + d \cdot (q''-q+p') + d^2 \cdot M - g' =$$

$$d \cdot M + p_1 + \lfloor r_1 \cdot n/d \rfloor - f_1 \mod n. \qquad (2\text{-}16)$$

Subtracting (2-14) from (2-16) gives:

$$d^2 \cdot (p''-p') + d \cdot (q''-q+p'-p) - g' - q =$$

$$p_1 - p' + \lfloor r_1 \cdot n/d \rfloor - f_1 - \lfloor r' \cdot n/d \rfloor \mod n.$$

This is impossible to satisfy, if $r' \neq r_1$ and $n > d^4 + d^3$, as the difference of the floor function is larger than the rest of the elements.

This finishes the proof, showing that there can only be one common node under those conditions, between Step 2 and either Step 3 or 4. Q.E.D.

If we assume that there is no common node between Steps 1 and 2 and the rest of the detour, we can, by reciprocity, assume the same of Steps 5 and 4, which takes care of all possible cases.

In summary, there can be only one node common to two different steps when $n > d^4 + d^3$. We can now count the number of node-independent detours.

Theorem 2-1:

In a de Bruijn network with out-degree $d > 2$, there are at least $d-2$ node-independent detours between a node with address M and a node with address $d^2 \cdot M + d \cdot h + i$, when the node with address $d \cdot M + h$ is inoperative, the addresses are taken modulo n -the number of nodes in the network-, $0 \leq h, i < d$ and there are at least $d^4 + d^3$ nodes in the network.

Proof:

We count how many nodes must fail in the detour graph before all detours can be cut. Frank and Frisch [Fra71], among others have shown that this is the number of node-independent paths between the origin and destination of such a graph.

Lemmas 2-13 to 2-15 show that when f nodes fail, at most f+2 paths may be cut, as at most two nodes are common to two different steps. In order to cut all detours, a minimum of d-3 nodes must then fail, as

Lemma 2-9 shows the existence of d-1 independent sets of parameters for the addresses of the detour. Q.E.D.

When n is a multiple of d^2, some of the restrictions for the detours disappear.

Theorem 2-2:

There exist d-1 node-independent six-step detours between a node of address M and a node of address $d^2 \cdot M + d \cdot h + 1$, with h and i between 0 and d-1, when the node $d \cdot M + h$ is inoperative, and when $n = k \cdot d^2$.

Proof:

We use the same notations as for the general detour. The steps are now as shown in Table 2-7.

If there is a total of S bad nodes in the detours, including the original bad node, there are at least d-S possible parameters possible for each step, when n is large enough so that nodes in Steps 1, 3, and 5 are distinct, except the original bad node. At least d-1 nodes need then to become inoperative before there is no detour left. There are then d-1 node-independent detours. Q.E.D.

We now show an example of detours around a faulty node, in the same case as Table 2-5. The parameters of the system are. n=24035, d=12, h=5, i=3. This gives the set of detours shown in Table 2-8. We use the parameters chosen in Table 2-5. We should note that there only are 10 independent detours, as the addresses of the node in Step 1 with p=8 is the same as the node in Step 2 with p=1.

Table 2-7: Possible addresses for the nodes in a detour when $n = k \cdot d^2$.

step	address	comments
0	M	origin
1	$d \cdot M + p$	$p \neq h$
2	$d^2 \cdot M + d \cdot p + q$	choose q
3	$d \cdot M + p + r \cdot d \cdot z$	
4	$M + r \cdot z + s \cdot d \cdot z$	choose s
5	$d \cdot M + h + r \cdot d \cdot z$	$r \neq 0$
6	$d^2 \cdot M + d \cdot h + i$	destination

Table 2-3: A set of detours when n = 24035, d = 12, M = 1892, $d^2 \cdot M + d \cdot h + i = 2236 \bmod n$.

p	Step	0	1	2	3	4	5	6
0			2184	2174	14201	1183	14206	
1			2185	2192	16205	1350	16209	
2			2186	2207	18209	3520	18212	
3			2187	2214	20213	1674	20215	
4			2188	2223	22217	1841	22218	
5		182	2189					2236
6			2190	2241	185	2008	186	
7			2191	2248	4194	349	4192	
8			2192	2257	6198	2519	6195	
9			2193	2275	8202	683	8198	
10			2194	2290	10205	2852	10200	
11			2195	2297	12209	3020	12203	

The entry for p=5 is not a detour, but the regular path between the nodes in Steps 0 and 6.

The method given here requires the edges of the network to be unoriented in order to by-pass a faulty node. Previous knowledge of the bad nodes within the detour is needed in order to avoid them, as shown in Theorems 2-1 and 2-2. However a limited knowledge of the state of the nodes in the network is needed, as all the nodes of a detour are at most 6 steps apart. This still insures the locality of the control.

If unoriented routing is used in general, another kind of detour is necessary as a message must by-pass in a small number of steps the node with address $d \cdot M + k$ on its way from M to $M + \lfloor (k+j \cdot n)/d \rfloor \mod n$.

The following theorems show the existence and the number of such detours.

Theorem 2-3:

There exist at least d-2 node-independent paths of six steps or less between a node of address M and a node of address $M + \lfloor (k+j \cdot n)/d \rfloor$, with k and j between 0 and d-1, and when there are at least d^2 nodes in the network.

Proof:

The two schemes below, used together, fulfill the conditions.

The first scheme gives d-gcd(d,n)-1 node-independent paths, the second one gives the remaining gcd(d,n)-1. The first scheme is two or four steps long. These steps are shown in Table 2-9.

Figure 2-1 shows an example of such a set of paths. The destination address is of the form:

Table 2-9: Possible addresses for the nodes in Theorem 2-3.

step	address modulo n	comments
0	M	origin
1	$d \cdot M + p$	
2	$M + \lfloor (p+q \cdot n)/d \rfloor$	may be the destination
3	$d \cdot M + p - f + r$	$f = (p + q \cdot n) \mod d$
4	$M + \lfloor (p-f+r + s \cdot n)/d \rfloor$	destination

Table 2-10: Possible addresses in the second scheme of Theorem 2-3.

step	address modulo n	comments
0	M	origin
1	$d \cdot M + p$	g possibilities
2	$M + q \cdot n/g$	could be M again
3	$\lfloor (M + q \cdot n/g + r \cdot n)/d \rfloor$	ancestor to $M + q \cdot n/g$ and $M + q \cdot n/g+h$, where $h=\pm 1$, depending on e.
4	$M + q \cdot n/g + h$	
5	$d \cdot M + t$	g unused descendants of the destination.
6	$M + \lfloor (j+k \cdot n)/d \rfloor$	destination

$$M + \lfloor (j+k\cdot n)/d \rfloor \mod n,$$

this gives a restriction on the possible values for p-f+r. For n large enough, p-f+r must be between e and e+d-1, where e is equal to

$$j - (j+k\cdot n \bmod d) .$$

If g is the gcd(n,d), we can write, using lemma 2-3:

$$e = -d + a\cdot g \text{ , with a between 1 and } (2\cdot d/g)-1 \text{ ,}$$

depending on the value of j.

Lemma 2-2 shows that the first g values of p-f, for all p's are less than one. If e is then larger than g there are at most d-g independent paths, as those that start with a p less than g cannot go to an address larger than $d\cdot M + d-1$.

The comment in Table 2-9 for Step 2 says that this address may be the destination. This happens when p is between e and e+d-1 and q=k. Steps 3 and 4 then become useless.

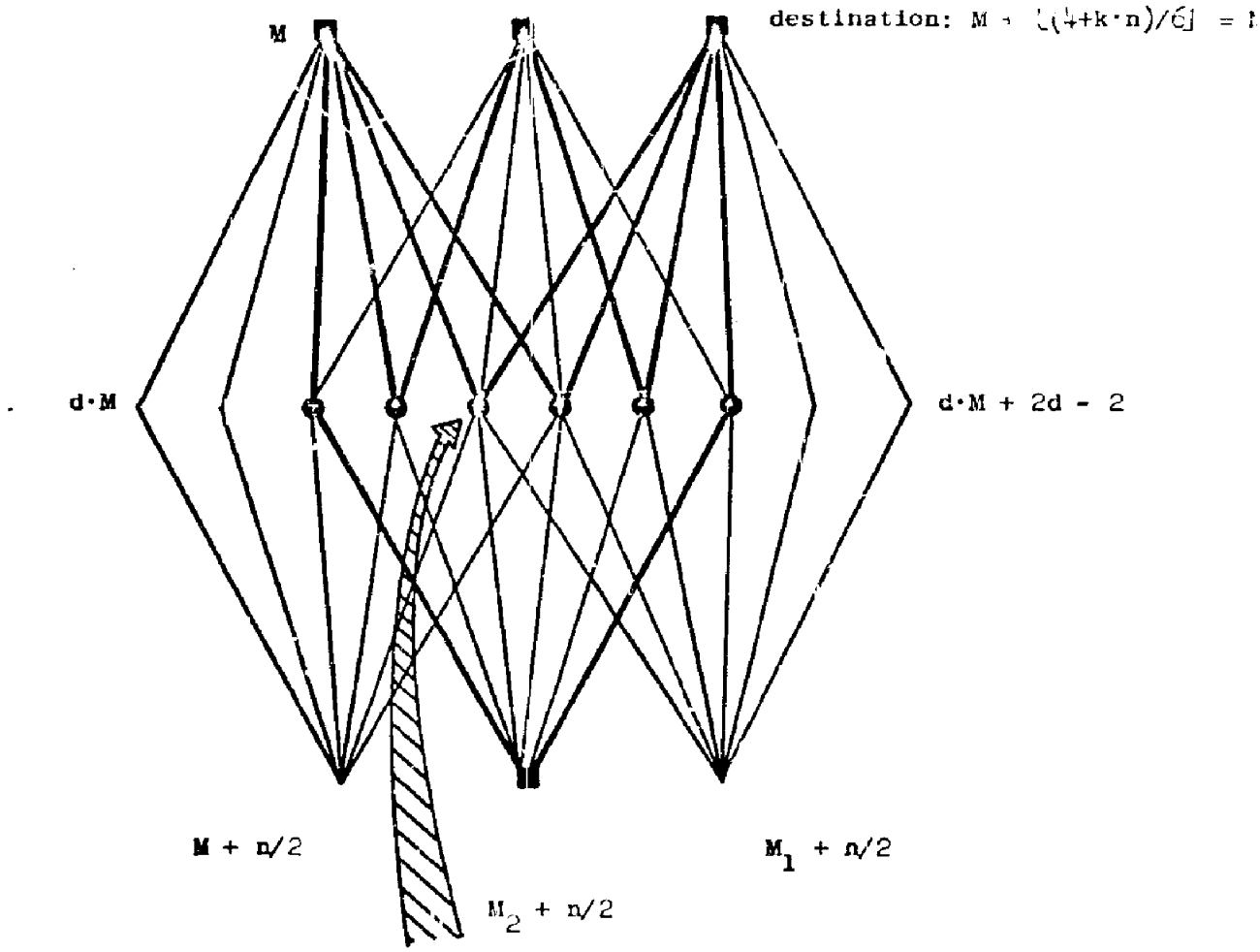
Another restriction appears when (in Fig. 2-1) M_2 is between $d\cdot M + e$ and $d\cdot M + d-1$ (one of the intermediate nodes on the "direct" 2-steps path). Fewer independent paths exist. We show later that for n large enough, at most one node in 2·d nodes with consecutive addresses can be like that. This restricts the minimum number of node-independent paths to d-g-1.

This finishes the discussion of the first scheme. The second one gives g-1 new independent paths and is four or six steps long. Figure 2-3 shows such a detour in the same case as Figure 2-1. The steps are shown in Table 2-10.

Figure 2-4: Possible connections for the paths of Theorem 2-3.

d=6, g=2 .

$M + \lfloor (2+h \cdot n)/6 \rfloor = M_2$



The edges used by the paths are dark lines.

There are three cases where those paths are not node-independent, when the paths of the first detour are included.

The first case of dependence is when a node of address $M+h+q \cdot n/g$ is between $d \cdot M+e$ and $d \cdot M+e+d-1$. There is at most one such node, for n large enough, as these nodes are n/g apart.

The second case of dependence is when an ancestor to a node with address $M+h+q \cdot n/g$ is the same as an ancestor to one of the nodes of addresses between $d \cdot M+e$ and $d \cdot M+e+d-1$ already used in some path. This is included in the first case.

The last case of dependence is when one of those ancestors to a node with address $M+h+q \cdot n/g$ is the same as one of the nodes of addresses between $d \cdot M + e$ and $d \cdot M + e + d-1$ already used in some path. Such a node can always be avoided as there are d-g possible such nodes per path, and their addresses are of the order of n/d apart. Q.E.D.

Theorem 2-4:

There exist at least d node-independent paths of two steps or less between two nodes with the same descendants in a network where n is a multiple of d.

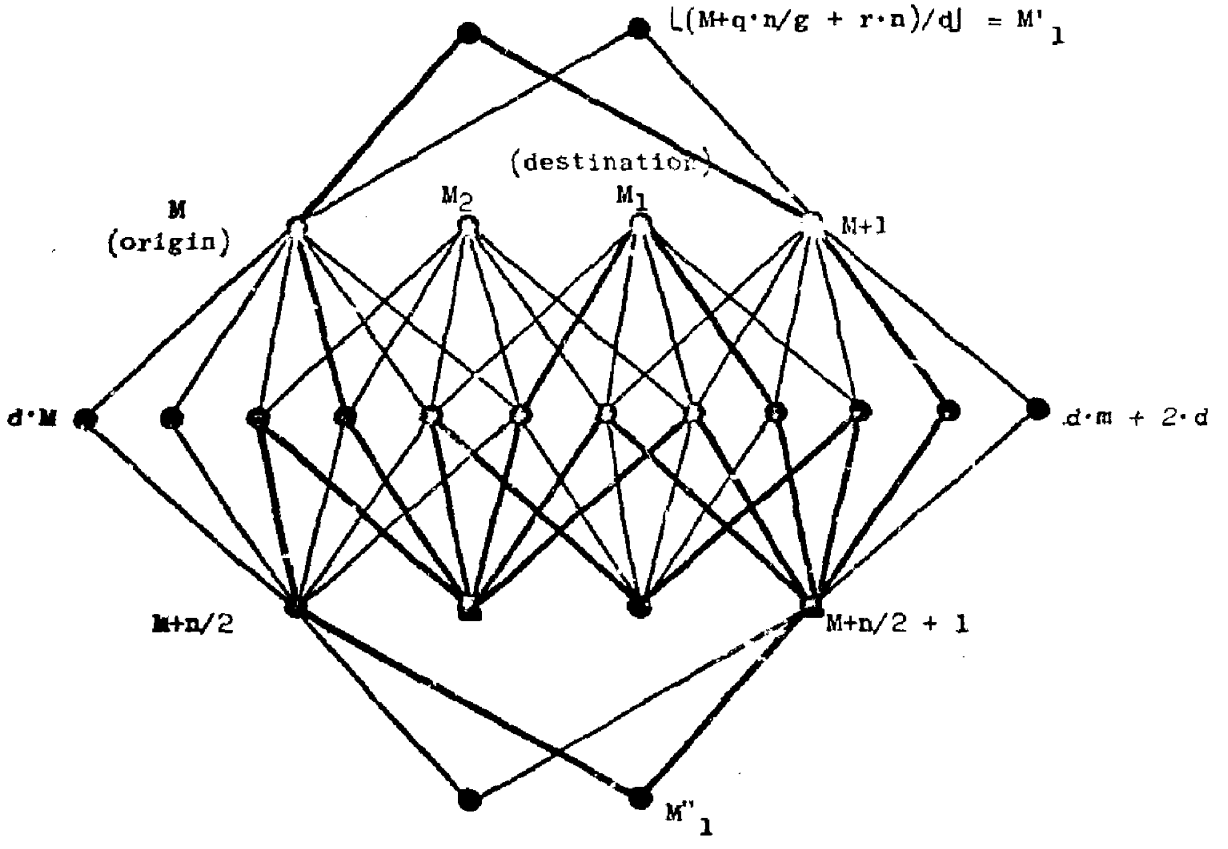
Proof:

The two nodes have d descendants in common, this gives d node-independent paths. Q.E.D.

In summary, we have shown the existence of at least d-1 node-independent detours around a faulty node, when $n \neq k \cdot d^2$, and d node-independent detours when $n = k \cdot d^2$. Similarly we have shown the existence

Figure 3-2: Possible connections for the theorem of 2-3, when the two types of paths are used.

d=6, g=2 .



The edges used by the paths are dark lines.

of d-1 or d node-independent paths between two nodes with common descendants, depending on the divisibility of n by d^2.

We have shown a six-step by-pass mechanism that allows a message to avoid an inoperative node. This does not change the locality of the controls of the network, but requires a stack, when the network is used in an oriented manner, in order to handle possible bad nodes encountered during the detour. This stack could be incorporated in the control part of the message. If too many nodes are inoperative, or if the degree of the network is four, the detour mechanism might fail. This leads us to study the conditions under which communications are possible between two nodes in the network, and the number of nodes that can become inoperative without impairing the communications within the rest of the system.

III. Vulnerability of a de Bruijn network

This section studies in which ways portions of the system can become inoperative without impairing the rest of the system. We discuss the sensitivity of the network to the destruction of a given number of nodes or edges. By counting the number of distinct neighbors a node has, we show that the number of nodes with less than $2 \cdot d$ distinct neighbors, where d is the out-degree of the network, is independent of the size of the network. We then study cycles and show the existence of oriented cycles of various lengths. The existence of such cycles is useful in studying how to isolate a group of nodes from the rest of the network. Finally a study of node-independent paths shows that there are at least $d-1$ node independent paths in an oriented de Bruijn network with d^k nodes and out-degree d.

The connectivity of a network is the smallest number of nodes that must be removed from the network, for the network to be disconnected. Similarly, the cohesion of a network is the smallest number of edges needed to disconnect the network. As we have allowed self-loops and parallel edges, the degree of a node does not indicate the number of independent neighbors a node has. The node and edge vulnerability of a node are the minimum number of nodes and edges, respectively, that must be removed in order to disconnect that node from the rest of the network. The node and edge vulnerability of a network are the minimum, respectively, of the node and edge vulnerability of individual nodes.

We look for bounds on the connectivity and conesion of de Bruijn

networks of degree 2·d. The detour mechanisms outlined in the previous sections give a lower bound on the connectivity of the network. This lower bound is d-1 if n is not divisible by d^2, and d if n is divisible by d^2. The node and edge vulnerability in such networks give an upper bound on the cohesion and vulnerability of d-1 or 2·d-2 in oriented or unoriented networks, respectively.

Denoting the connectivity of a network as Cn, and the cohsion as Ch, Boesch and Thomas [Boe70] derived the following relation in an unoriented network with n nodes and e edges:

$$Cn \leq Ch \leq 2 \cdot e/n \ .$$

Thus, in order to find a lower bound for both the connectivity and the cohesion, we only have to find one for the connectivity.

Lemma 3-1:

The connectivity of an unoriented de Bruijn network is at least k+1 when there are at least k independent detours between two nodes separated by a bad node.

Proof:

The connectivity of the network is equal to the least number of nodes needed to disconnect the network.

The theorems of the previous section show how many node-independent detours exist between two nodes separated by one bad node. When there are k such detours at each node, we use a proof by induction to show that the connectivity is at least k+1.

Suppose k=0. As we are in a network, the connectivity is one. Now suppose that there are k ≥ 1 detours, the connectivity is at least k. In order to cut a node from another, at least k nodes must fail. If only k nodes fail, there still exists a path connecting any two nodes, as there still is one detour among the k node-independent detours, that does not fail around any of the bad nodes, as there only are k-1 other bad nodes. The connectivity of the network is at least k+1. Q.E.D.

Theorem 3-1:

Let 2·d be the degree of an unoriented de Bruijn network. The connectivity of this network is at least:

d, when the number of nodes in the network is a multiple of d^2,

d-1, otherwise.

Proof:

The proof follows immediately from Theorems 2-1 and 2-2 and Lemma 3-1. Q.E.D.

We now look for an upper bound on the connectivity and cohesion of the network. The node and edge vulnerability is such a bound, because if all the independent neighbors to a node fail, there is not path left between that node and the rest of the network.

An immediate upper bound for the node and edge vulnerability is the degree of the network, as all nodes have the same degree. In some

cases, a node may have a lower node or edge vulnerability. We look at those cases and count the number of loops there are in some networks.

Theorem 3-2:

In a network where d is the out-degree, n the number of nodes and g the gcd(n,d-1), the number of self-loops is equal to d+g-1, when n is larger than d-1.

Proof:

In general a node with address M has as descendants the nodes with addresses:

$$d \cdot M + j \mod n,$$

where j is between 0 and d-1, and n is the number of nodes in the network. The addresses of the nodes that have themselves as descendants satisfy:

$$M = d \cdot M + j \mod n.$$

We can rewrite this as:

$M = (k \cdot n - j)/(d-1)$, where $0 \leq k < d$, and k is an integer that corresponds to the "mod n" in the above equation.

Let $g = \gcd(n,d-1)$. The possible values of M are:

$$M_1 = \lfloor (k \cdot n)/(d-1) \rfloor \text{ , with } k=0,\ldots,d-2 \text{ ,}$$

and

$$M_2 = k \cdot n/(d-1) - 1, \text{ when this is a positive integer.}$$

This also is:

$$M_2 = q \cdot n/g - 1, \text{ with } q=1,\ldots,g$$

There are d-1 independent M_1's, and g independent M_2's. A repetition might occur between an M_1 and an M_2 if two M_1's are only one apart, as all M_2's are one away from a given M_1. This gives for the repetitions:

$$(k \cdot n - j)/(d-1) = (k \cdot n + n - d+1)/(d-1) .$$

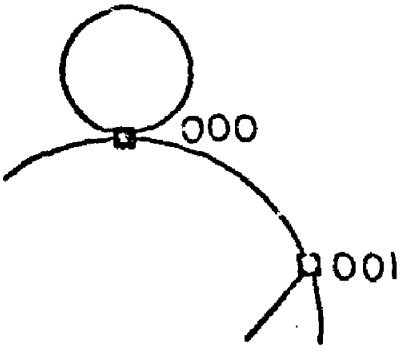
or

$$n = d-1-j .$$

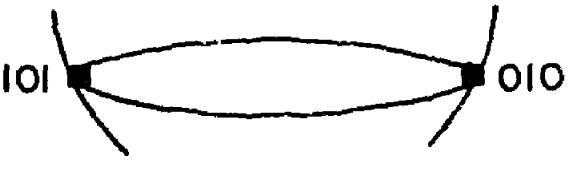
This is possible only if $n < d$. This gives us, for $n \geq d$, a total of d+g-1 independent nodes with a self-loop. Q.E.D.

The nodes with self-loops, in an oriented network, have a node and edge vulnerability of d-1. If n is smaller than d, the node and edge vulnerability may be larger.

We now look at node and edge vulnerability in an unoriented network. The cases where the edge or node vulnerability are less than the degree occur when a node has a self-loop, or when two edges are parallel. Those two examples are shown in Figure 3-1. The numbering of the nodes is taken from a de Bruijn graph with 8 nodes and degree 4.



self-loop



parallel edges

Fig. 2-1: Cases where edge or node vulnerability are less than the degree of a node.

We first show that in large enough a network, there is no node with both a self-loop and parallel edges.

Lemma 3-2:

In an unoriented network with more than d^2 nodes, a node cannot have both a self-loop and parallel edges.

Proof:

If j,k,p are integers between 0 and d-1 included, the address of M of a node with both a self-loop and parallel edges satisfies the relations modulo n:

$$M = d \cdot M + j = d^2 \cdot M + d \cdot j + j ,$$

for the self-loop, and

$$M = d^2 \cdot M + d \cdot k + p, \text{ with } k \neq j, \text{ for the parallel edges.}$$

This gives, modulo n:

$$d^2 \cdot M + d \cdot j + j = d^2 \cdot M + d \cdot k + p ,$$

and:

$$d \cdot (j-k) = p-j, \text{ which is impossible, with } j \neq k, \text{ when}$$

$$n \geq d^2 . \qquad \text{Q.E.D.}$$

We already have found the occurrences of self-loops. When a node has a self-loop in an unoriented network, its edge and node vulnerability

become $2 \cdot d-2$ if the degree of the network is $2 \cdot d$. In case of parallel edges, the edge vulnerability is unchanged, but the node vulnerability goes to $2 \cdot d-1$.

Theorem 3-3:

In an unoriented de Bruijn network, where n is the number of nodes and $2 \cdot d$ the degree of the network, if n is larger than d^2, and $g = \gcd(n, d^2-1)$, the number of nodes with parallel edges is equal to d^2+g-1.

Proof:

Parallel edges happen when a node has one of its "descendants" among its ancestors, for n larger than d. This occurs for:

$$M = d^2 \cdot M + d \cdot j + i \mod n, \text{ where i and j are d-ary digits.}$$

If $g = \gcd(n, d^2-1)$, the solutions to this congruence are, including some repetitions:

$$M_1 = \lfloor (k \cdot n)/(d^2-1) \rfloor \text{ , with } k = 0,\ldots,d^2-2 \text{ ,}$$

and

$$M_2 = q \cdot n/g - 1 \text{ , with } q = 1,\ldots,g \text{ .}$$

As in Theorem 3-2 we can count the repetitions, and similarly, when n is larger than d^2, the congruence has d^2+g-1 independent solutions. Q.E.D.

Some of those "parallel edges" are actually self-loops used twice, the actual number of nodes with parallel edges that are not self-loops is then:

$$d^2-d+\gcd(n,d^2-1)-\gcd(n,d-1) \ .$$

We can now find the node and edge vulnerability of an unoriented de Bruijn network with more than d^2 nodes.

Theorem 3-4:

The node and edge vulnerability of an unoriented de Bruijn network with more than d^2 nodes is $2 \cdot d-2$, where $2 \cdot d$ is the degree of the network.

Proof:

When the number of nodes is larger than d^2, there is not overlap between self-loops and parallel edges: all self-loops are considered as parallel edges, and there is at most one self-loop per node.

The node and edge vulnerability of the network is then that of the nodes with self-loops, $2 \cdot d-2$. Q.E.D.

We study now the node and edge vulnerability of an oriented network, then count the number of cycles of various lengths that exist in those networks.

Theorem 3-5:

Let d be the out-degree of an oriented de Bruijn network. The node and edge vulnerability of such a network is d-1, when the number of nodes in the network is larger than d.

Proof:

When the number of nodes in the network is larger than d, no two descendants of a given node can be the same. The only case where the number of distinct neighbors of a node is less than d is when one

of those descendants is the node itself. The edge and node vulnerability of such a node is d-1. This is also the node and edge vulnerability of the network. Q.E.D.

Cycles in the graph show how strongly nodes are connected, and help in defining measures of connectivity that include a group of nodes [Boe71]. We show the existence and count various cycles in the network.

Theorem 3-6:

In an oriented de Bruijn network with n nodes and out-degree d, the number of cycles of length L and no less, with $L \leq \lfloor \log_d n \rfloor$, is equal to:

$$\left(\sum_{\substack{q \\ q \mid L}} mu(q) \cdot f(L/q)\right)/L \ ,$$

where mu(q) is the Mobius function:

$$mu(q) = \begin{cases} 1 \text{ if } q=1, \\ (-1)^r \text{ if } q \text{ is the product of } r \text{ distinct primes,} \\ 0 \text{ if } q \text{ contains any repeated prime factors.} \end{cases}$$

and f(q) as:

$$f(q) = d^q + \gcd(n, d^q - 1) - 1 \ .$$

Proof:

Berlekamp [Ber68, pp. 81-85], has proven this theorem in his book, for general functions f(q). Q.E.D.

We now have upper and lower bounds for cohesion and connectivity of an unoriented de Bruijn network with n nodes and degree 2d:

If n is not divisible by d^2:

$$d-1 \leq Cn \leq Ch \leq 2 \cdot d-2 .$$

and, when n is divisible by d^2 :

$$d \leq C_n \leq Ch \leq 2 \cdot d-2 .$$

For an oriented network, we have:

$$1 \leq Cn \leq Ch \leq d-1 .$$

Another way to look at the connectivity of a graph is to look at the number of node-independent paths between any two nodes in the graph [Fra71, Ber62].

Two paths between two nodes are called "node-independent" if they have only the origin and destination nodes in common. Two paths are called edge-independent if they have no edge in common. We already know that the number of node-independent paths in a network is equal to the connectivity of that network.

This section studies the construction of node-independent paths in networks with d·n nodes, from the construction of corresponding paths in networks with n nodes. It shows in particular that there are at least d-1 node-independent paths between any two nodes in an oriented network with d^k nodes. It also shows that for unoriented networks with degree 4 and 2·n nodes, there are at least 2 node-independent paths between any two nodes.

In the rest of this section, we call a de Bruijn network with degree $2 \cdot d$ and n nodes as a (d,n) network. As usual, the definition for the integer k is:

$$d^{k-1} < n \leq d^k ,$$

an earlier report [Sch74] shows that k is an upper bound for the diameter of the network. A path is monotone if it is possible to go from one end of the path to the other end, following the orientation of the edges. A path is singular if it consists of at most two monotone subpaths.

We first extend a result that is already known for (d,d^k) networks [Gol67]: there is an isomorphism between the oriented edges of a (d,p) network and the nodes of a $(d,d \cdot p)$ network. We then prove a theorem on node-independent singular paths, constructing such paths in a $(d, d \cdot p)$ network from corresponding paths in a (d,p) network. Another theorem shows that if d node-independent monotone paths exist between any two nodes of a (d,p) network, the same is true of a $(d,d \cdot p)$ network. This theorem applied to (d,d^k) networks shows the existance of at least d-1 node-independent paths between any two nodes in such networks. This also gives a good lower bound for the connectivity of such networks.

We now show how the edges of a (d,p) network correspond to the nodes of a $(d,d \cdot p)$ network. Figure 3-2 shows possible addresses for the edges of a (3,7) network.

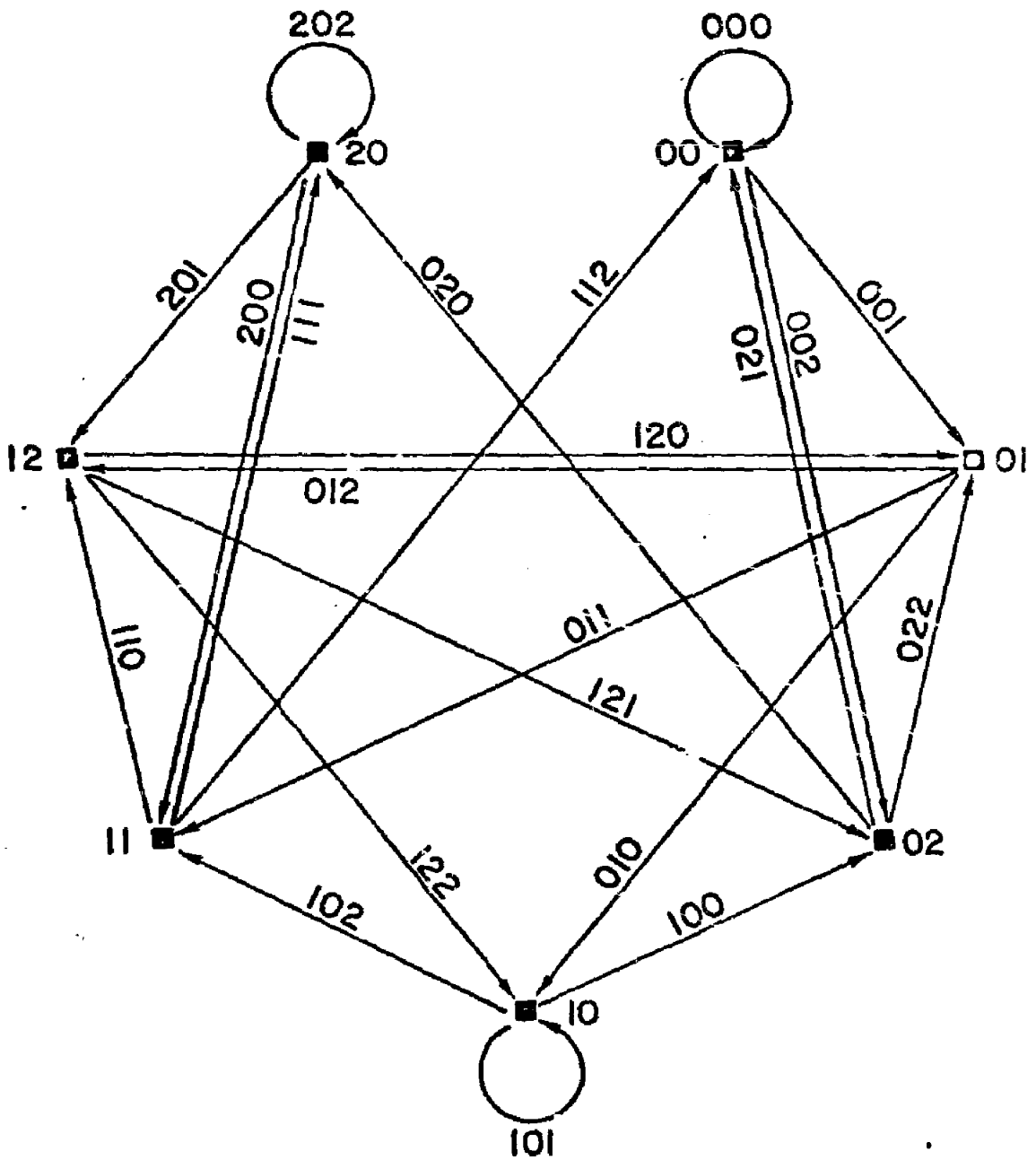


Fig. 3-2: Addresses of edges in a (3,7) network.

Lemma 3-3:

There exists an isomorphism between the edges of a (d,p) network and the nodes of a (d,d·p) network.

Proof:

To each edge in the (d,p) network, we associate a node of the (d,d·p) network in the following manner:

If the address of the origin of the edge is M, and that of the destination is d·M + j mod p, the node in the (d,d·p) network associated to that edge of the (d,p) network has an address of:

$$d \cdot M + j \mod d \cdot p \ .$$

We define the descendants of an edge as the edges leaving from the destination node of that edge. If a node associated with a given edge has address M, its descendant nodes have addresses:

$$d \cdot M + j \mod d \cdot p, \text{ with } j \text{ between } 0 \text{ and } d-1 \ .$$

These addresses are the same as those of the nodes associated with the descendant edges of the edge associated with the node of address M.

The correspondence between the nodes and edges keeps the connection patterns. To each edge in the (d,p) network, we can associate a node in the (d,d·p) network, and to each node in the (d,d·p) network, we can associate an edge in the (d,p) network: If there is a node without an associated edge, the same is true of all its descendant nodes, and we know that any node has eventually all the nodes in the network as

descendants. If there is then one node without an associated edge, there is no node with an associated edge, which is in contradiction with the possibility of associating a node with any edge. In conclusion, as there is the same number of edges and nodes, there is an isomorphism between the edges of a (d,p) network and the nodes of a (d,d·p) network. Q.E.D.

In particular an oriented path along the edges of a (d,p) network corresponds to an oriented path between nodes of a (d,d·p) network.

We can then extend to all (d,d·p) networks the known result [Gol67] that all (d,d^k) networks have an Hamiltonian circuit: it corresponds to the Eulerian circuit in the (d,p) network.

We now show how to go from a singular path in a (d,p) network a singular path in a (d,d·p) network.

Transformation 3-1:

-If the singular path is a monotone path in the (d,p) network, the transformation is immediate, the path, instead of going from edge to edge in the (d,p) network, goes from node to node in the (d,d·p) network, and those nodes are associated to the edges in the same way as in Theorem 3-3.

-If there is a change of orientation, the two monotone subpaths can be transformed as above. The resulting path is not complete, but the open ends, not the origin and destination, come from the same ancestor or go to the same descendant, as the corresponding edges join in one node in

the (d,p) network. Adding one node to the paths bridges the gap, and keeps the singularity of the resulting path, as shown in Fig. 3-3.

Definition: A forward singular path is a singular path which in an oriented network takes an edge out of at least one of its extremities.

For example a monotone path is a forward singular path, Figure 3-4 shows a path that is not forward singular.

We are now ready to prove the following theorem:

Theorem 3-7:

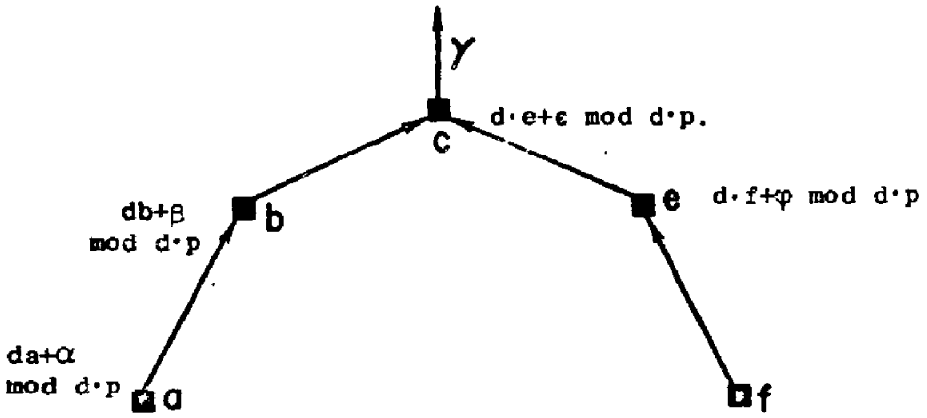
If there exist s node-independent forward singular paths between any two nodes in a (d,p) network, with $s \leq d$, then there are s node-independent forward singular paths between any two nodes in a $(d, d \cdot p)$ network. These paths are the transformed by transformation 3-1 of the forward singular paths between the destination nodes of the edges corresponding to the extremities of the paths in the $(d, d \cdot p)$ network.

Proof:

This proof shows that such paths keep their independence and forwardness in transformation 3-1.

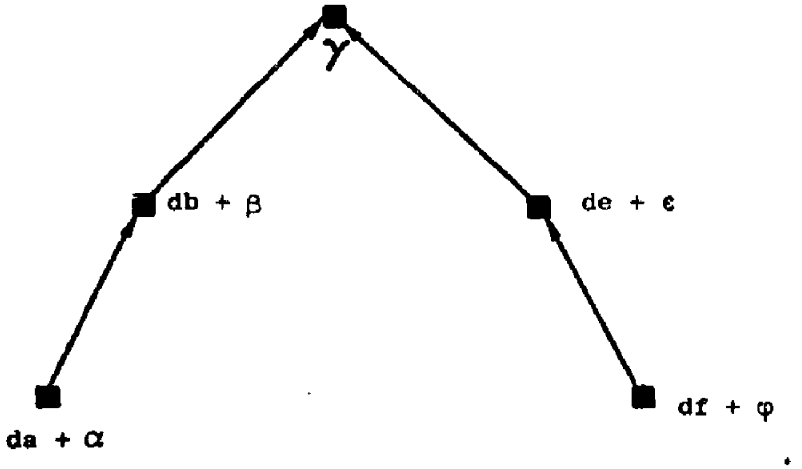
The node-independence of the paths in the (d,p) network implies the edge-independence of these paths. The transformed paths in the $(d, d \cdot p)$ network correspond to edge paths with an extra edge at the summit of the forward singular paths. As the degree of the net is $2 \cdot d$, and there is at most one self-loop per node, it is always possible to choose that

Fig. 3-3: Transforming singular paths in Transformation 4-1.



in the (d,p) network

gives



in the (d, d·p) network.

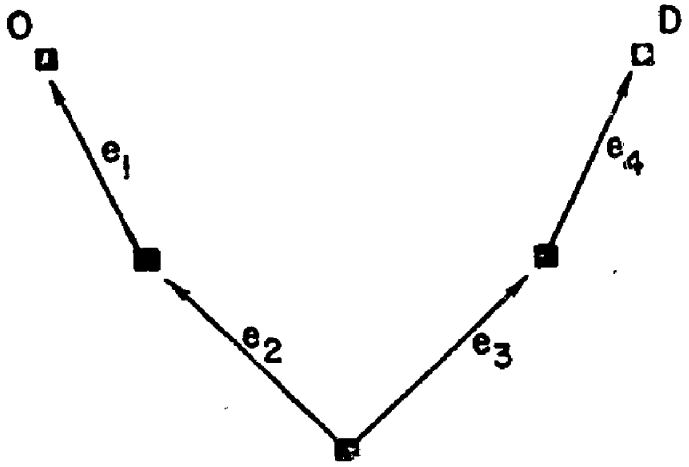


Fig. 3-4: A path that is not forward singular.

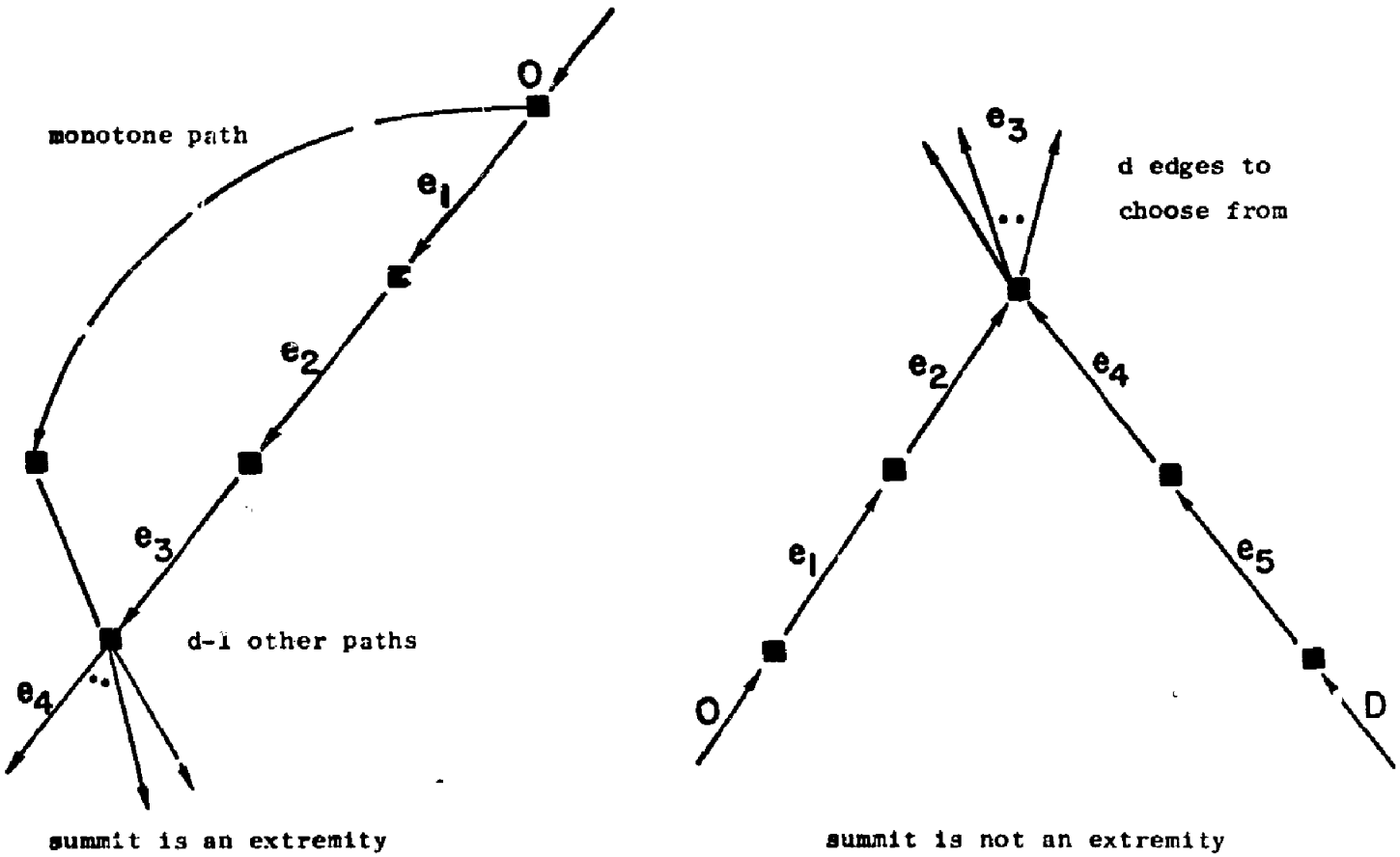


Fig. 3-5: How to choose the last node.

last edge independently from the other s-1 paths, when $s \leq d$. When the summit is not an extremity, we can choose any edge out of this summit because of the node-independence of the paths. When the summit is an extremity, the choice goes as follows: each node has at most one self-loop, hence at least $2 \cdot d-1$ independent edges (Thm 3-2). At most d-1 incoming paths use $2 \cdot d-2$ edges, as they actuall use the extremity as a summit, and the last path goes directly to the destination edge and does not need an extra edge. Q.E.D.

Figure 3-5 shows such choices.

The paths that we get may still be shortened if the extra node is linked to some other node in that path.

We now prove a similar theorem for monotone paths:

Theorem 3-8:

If there exist s node-independent monotone paths between any nodes in a (d,p) network, then there are at least s node-independent monotone paths between any nodes in a $(d,d \cdot p)$ network.

Proof:

In the (d,p) network we look for edge-independent paths between the nodes corresponding to the destination of the origin edge and the origin of the destination edge. as shown in Figure 3-6.

If those two nodes are different, there are s node-independent paths between them in the (d,p) network, which transformation 3-1 transforms into s node-independent paths in the $(d,d \cdot p)$ network. Boesch and Frisch [Boe68], have shown that this is enough for the connectivity of the path to be s, and for s node-independent paths to exist between

any two nodes. Q.E.D.

In some cases, this theorem gives a better lower bound than the general one on the number of node-independent paths between two nodes in a de Bruijn network. We look at the number of node-independent monotone paths in a (d,d) network.

Lemma 3-4:

There are at least d-1 monotone node-independent paths between two nodes in a (d,d) network.

Proof:

The connection pattern of the (d,d) network is the complete directed graph with d nodes and a loop on each node. There always are d-1 independent paths between any two nodes made of the edges from the origin node to all other nodes, and if necessary the edges to the destination node. Q.E.D.

Theorem 3-9 generalizes this result to a larger class of networks:

Theorem 3-9:

For any (d,d^k) network, with d and k being integers, there are at least d-1 monotone node-independent paths between any two nodes.

Proof:

The proof follows immediately from the above lemma and theorem. Q.E.D.

This gives a better lower bound for the connectivity of an oriented (d,d^k) network: monotone paths are paths in such a network, and the connectivity is at most d-1. This gives:

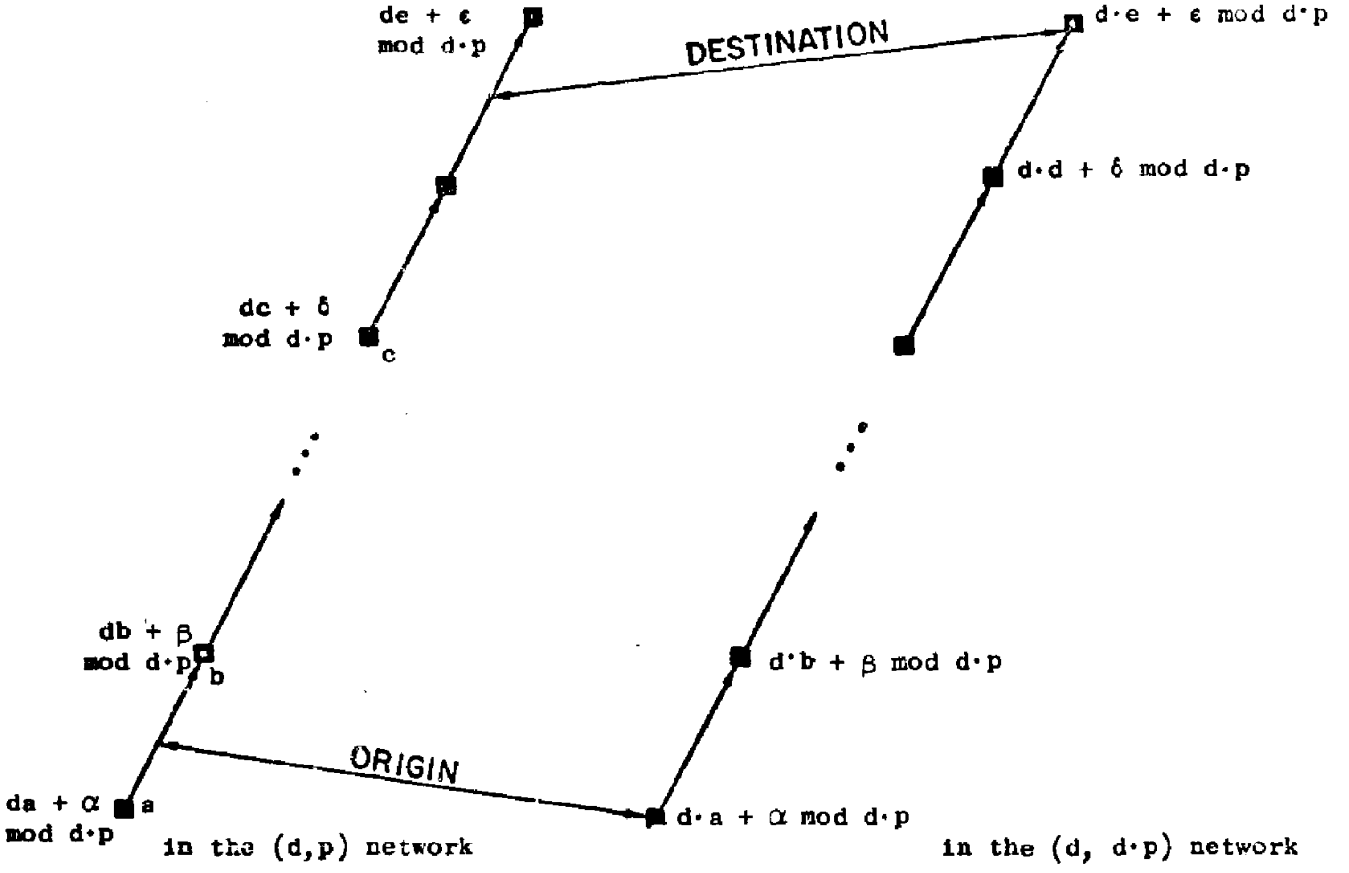


Fig. 3-6: Transforming a monotoneous path.

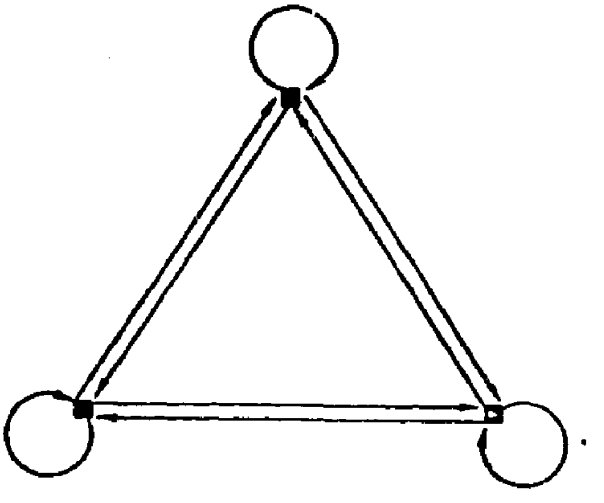


Fig. 3-7: The (3,3) network.

Theorem 3-10:

The connectivity of an oriented (d,d^k) network is d-1.

Proof:

The proof follows immediately from the above theorem. Q.E.D.

Going back to unoriented networks, we can tell a little more about the case where d=2:

Theorem 3-11:

There are at least 2 node-independent paths between any two nodes of a $(2,2 \cdot p)$ network.

Proof:

This is an immediate derivation from the existance of a Hamiltonian circuit in those networks. Q.E.D.

Vulnerability in a de Bruijn network is a function of the degree of that network. For an unoriented $(d,d \cdot p)$ network, the connectivity and cohesion increase with d. For (d,d^k) oriented networks, the connectivity is d-1, for unoriented networks it is at least d; for small values of k, the connectivity is in fact $2 \cdot d-2$.

IV. Conclusion

De Bruijn networks have interesting properties for communications networks: a small diameter with respect to the number of nodes in the network, and an easy routing and rerouting scheme. The control information for the by-pass of a bad node can easily be added to the header of the message. In case of a single bad node, it takes only an extra four steps to go around it. A limited number of nodes, independently of the size of the network are more vulnerable than the rest of the nodes in the network. The larger the network, the more "invulnerable" it is, the same is true when the degree increases.

An open problem is the statistical analysis of the message flow inside such a network. This problem is studied in a coming report.

Bibliography

Ber62 C. Berge, The Theory of Graphs and its Applications, John Wiley and Sons, New York, 1962.

Ber68 E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

Boe68 F. T. Boesch and I. T. Frisch, "On the smallest disconnecting set in a graph," IEEE Trans. Circuit Theory (Correspondence), vol. CT-15, pp. 286-288, September 1968.

Boe70 F. T. Boesch and R. Emerson Thomas, "On graphs of invulnerable communication nets," IEEE Trans. Circuit Theory, vol. CT-17, No. 2, pp. 183-192, May 1970.

Boe71 F. T. Boesch and A. P. Felzer, "On the minimum m-degree vulnerability criterion," IEEE Trans. Circuit Theory, vol. CT-18, No. 2, pp. 224-228, May 1971.

Fra71 H. Frank and I. T. Frisch, Communication, Transmission and Transportation Networks, Addison-Wesley, Reading, Mass., 1971.

Gol67 S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, Calif., 1967.

Sch74 M. L. Schlumberger, "Logarithmic communications networks," to appear.