TELETRAFFIC AND DATATRAFFIC
in a Period of Change, ITC-13
A. Jensen and V.B. Iversen (Editors)
Elsevier Science Publishers B.V. (North-Holland)
IAC, 1991

DESIGN AND ANALYSIS OF A HIGHLY RELIABLE TRANSMISSION NETWORK

Peter Key and Anne Elvidge

British Telecom Research Laboratories, Martlesham Heath, Ipswich, IP5 7RE.

Modern transmission networks have to be flexible and reliable. The use of fibre optics creates networks that are more reliable, and the introduction of digital hierarchies and digital cross-connects allows complex control and protection strategies. Such protection strategies, which permit rerouting of demands under failure, are difficult to model. Although in the initial stages of network design, simple approximations of availabilities will suffice, in the later stages we require accurate answers. In this paper we comment on existing methods of calculating network availability measures, and present a new analytic technique which can model rerouting strategies, as well as the present link-based protection techniques.

Main contribution statement: We present an approximate analytic technique for evaluating availabilities in a network with protection systems and rerouting.

1. Introduction

In the modern telecommunication environment, network providers and operators are facing increasing pressure to provide new services rapidly to a high quality. The transmission network forms an essential part in any telecommunications network, and has to have increasing *flexibility* and *resilience*. The former reflects the need to react quickly to new requirements, such as to provide a novel type of service. The latter means that networks must be robust to uncertainties in growth or demand forecasts, and also to withstand failures of individual items of equipment.

An important measure of quality for transmission networks is *availability* and associated measures, since this directly affects the customer, and can even figure in contracts. The mean availability of a demand is the proportion of time the demand can be met. Related measures are the mean down time, and the failure rate (it can be important to distinguish between 60 failures of 1 minute and a single failure lasting an hour). Reliability can be integrated with performance (such as loss in a circuit-switched network, or delay in a packet network) via *performability*, which essentially takes expectations with respect to availability [1,2].

The challenge to the modeller is to model the availability of networks. This might be done first to design a network, and secondly to accurately assess the performance. These are the issues we address in this paper. In Section 2 we introduce the concept of Synchronous Digital Networks, which lead to more manageable and robust networks, and provides the motivation for this paper. Section 3 comments on the relationship between modelling and network design. The main part of the paper in Section 4 looks at availability modelling; current techniques are mentioned, and a new method is given for calculating the reliability of networks which can re-route under failure conditions. Preliminary results are given in Section 5 and finally some conclusions are drawn in Section 6.

2. Synchronous Digital Networks

International standards, such as SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy), reflect the move towards national digital transmission and switching networks. The fibre optic equipment is intrinsically more reliable than previous technologies, and these networks can include "built-in" protection strategies, thus allowing very high end-to-end availabilities. In particular, High-Order Automatic Cross-connect Equipment (HACE) under software control opens up the possibility of sophisticated protection strategies [3].

Protection strategies can range from simple redundancy, through *N+1* link protection via a standby link (1 standby link for every *N* working links), through to complex network rerouting strategies, which can be decentralised or centralised under the control of a network management centre. There is an obvious trade-off to be made between effectiveness and cost, which is often dictated by the complexity of the scheme. For instance simple *N+m* systems (in general) are straightforward to automate and are essentially hardware solutions. More complicated schemes, such as rerouting around failed links, require software control, which is expensive. However it is possible to implement simple network-level protection on a distributed basis — for example we might allow failed links to search for spare capacity by hunting through a small number of pre-programmed paths.

3. Network design and availability modelling

For initial network design, cost information is important, while availability information is needed for differentiating between competing structures. Issues such as switch location and size (for managed transmission networks) are important, and questions of cost and practicality can dominate reliability considerations. At this stage, upper and lower *bounds* for network reliability are more important than precisely determining exact figures, particularly if the bounds can be produced in an efficient computational manner.

The use of good heuristics in design, for example providing dual access to the next level in a hierarchical network, and the use of diverse routing is a way of building reliability into a network, and there are more sophisticated optimization approaches that can be adopted [4,5]. In addition we need to account for network growth, and see that the network structure is capable of growing as the traffic demand grows.

As the basic design structure firms up, more accurate measures of availability are required to ensure the network meets given availability targets. These are needed to determine the level of protection needed on each link, and rerouting strategies.

4. Availability modelling

4.1. Framework

A general network, where there are different types of equipment (such as ducts, cables, transmission nodes etc.) which can fail and be repaired at different rates, and where there are "worker" and "standby" or "protection" systems, can be represented by a graph, $G = (V, E)$, where V is the set of vertices, and E the set of arcs (directed) or edges joining vertices. In general, this graph representation will contain more vertices and edges than the actual "physical" network: for example if there is a duct joining actual physical nodes A and B with a number of cables in it, then duct failure will cause all the cables to be lost, whereas the cables could fail independently; this could be represented by adding an additional node, C, with an edge between A and C representing the duct, and a number of edges between C and B representing the cables. If necessary, we can further reduce the graph to a directed graph in which the nodes are perfectly reliable and only the arcs fail, so that from now on we shall assume that the nodes do not fail.

In general, edges will fail at certain rates λ, ($=1/MTBF$), and be repaired at rates μ ($=1/MTTR$), which we assume to be independent of time, where the *MTBF* is the Mean Time Between Failures of the system, and the *MTTR* is the Mean Time To Restore the system. Thus the unavailability of a certain piece of equipment is

$$q = \frac{\lambda}{\lambda + \mu} \approx \frac{\lambda}{\mu}$$

which represents the proportion of time that the equipment is unavailable. If we assume that inter-event times for failure and repair are negative exponential, we have a Markov system, and strictly speaking our availabilities are steady-state quantities, which can also be interpreted as the probability that the system is available at an arbitrary point of time. We can also model different repair strategies: if the same piece of equipment is subject to multiple failures with independent repair of failures then $q = 1 - \exp(-\lambda/\mu)$.

Therefore we can represent our network by a probabilistic graph, $G = (V, E)$, where there are failure probabilities (the q's) associated with arcs.

In addition we have demands for capacity between node-pairs in this network, and a routing strategy for each demand, which says how the demand is routed across the network, and what happens in the event of failure. We shall assume for simplicity that all demands use one unit of capacity on any edge, (which might represent say a 140Mbit/s block), and that any demand has the potential to access any of the working and protection systems between two nodes. We term this collection of working and protection systems the "link" joining the nodes. A routing strategy for each demand can be described by a directed *Routing Tree* with the following properties:

- Each node of the tree represents a route the demand can take, where a route is an ordered collection of links; the nodes need not be distinct.
- Arcs between nodes are labelled with a set of links; an arc from route r to route s means that r is attempted first, and if any of the links on r are blocked and these appear as part of the label of the arc from r to s then route s is attempted.
- The routing rule is described by a depth-first search strategy conducted from left to right.

In addition we place the following additional restriction on the routing trees, for ease of analysis.

- Any link labels (blocked links) must appear in all lower branches to the right as part of a route — this ensures that this link is free if we go down a rightward branch.

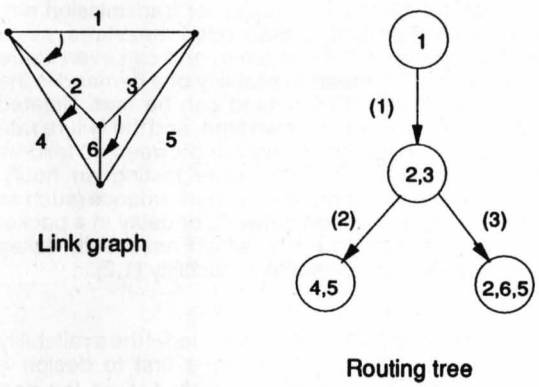

Figure 1. Routing tree description.

With this restriction, these types of trees can describe all automatic alternative routing (AAR) or step-by-step strategies in circuit-switched networks, and certain "crank-back" rules. An example is depicted in Fig. 1, where the routing rule is that we first try link 1, if this is blocked we try links 2 and 3; if 3 is blocked we try route (2,6,5) and if 2 is blocked we try route (4,5).

4.2. Exact availability modelling

For network performance analysis, one is primarily interested in accurate availability predictions (given the accuracy of the data). This becomes of increasing interest as the design of the network becomes more concrete. The complicating factor here is network protection. One can either use simulation, discrete-event ("roulette") or time-true, or attempt to use an approximate analytic model. If we restrict information just to the probabilistic graph with failure probabilities q, then we can also use Monte-Carlo techniques to randomly fail edges [6,7].

In a simulation, we can model the rerouting strategy explicitly, and also account for rerouting and switching times, which are difficult to account for in an analytic model. We can also get information on the transient behaviour of the system, and on the distribution of outages. The disadvantage is the time the simulation takes to run and the memory it requires, which can be impossibly large for realistic networks of say 400 nodes or more. A further disadvantage is the difficulty of using simulation for designing a system.

4.3. Connectedness and bounds on availability

The "two-terminal" reliability is the probability that two given nodes in our probabilistic graph, $G = (V, E)$, say s and t, are "connected". This is the probability that there is a path between them, although if we interpret our failure probabilities q as being unavailabilities in a repairable system, then strictly speaking we should talk about two-terminal availability. Calculating such quantities for a general network is known to be *NP*-hard [8], and moreover, does not necessarily model what we are interested in. This is because first, connectedness allows all possible paths rather than those allowed under the routing strategy. Secondly, connectedness ignores the contention for resources. If we use the whole network with the given probabilities q unaltered, connectedness will give an *upper bound* on availabilities, and hence is useful for network design. Although *NP*-hard, good approximate calculation is possible by not evaluating the full state-space. Recent evidence [9] suggests that the method of Dotson [10] is a relatively efficient way of evaluating connectedness.

One way of improving the method's accuracy is to construct a subgraph for each s-t pair, $G^* \subseteq G$, which only includes edges that an s-t demand can access, then produce revised probabilities q^* which are the probabilities that an s-t demand can access that edge/vertex in G^*, and then calculate the two-terminal reliability for this revised probabilistic graph. An upper bound on the availability can be found by ignoring contention on the links when calculating the q^*. A lower bound (for the routing scheme) can be found by defining the link to be available (for s-t) if it is working and if no other demand which could use this link has failed on its first-choice link.

4.4. A fixed-point approximation

We now describe a fixed-point approximation which gives point-to-point availabilities. The method is based on a decomposition which determines link "blocking probabilities", which are themselves dependent on other link blocking probabilities. Thus these form a set of fixed-point equations which can be solved recursively, and from which the availabilities can be easily found. The method has affinities with the Erlang-fixed point or reduced load approximation of calculating blocking probabilities in circuit-switched networks [11, 12] and with certain recursive reliability methods [13]. The advantage of such a method is that large networks can be analysed by such means, and moreover it is possible to extract derivative information in an equally simple form (adapting the ideas in [14]), which facilitates design and sensitivity studies.

Assumptions:

- Individual components fail independently.
- A rerouting strategy is in operation which can be described by a routing tree (see above).
- "Blockings" on protection systems are independent from link to link. These blocking probabilities are the proportion of time the demand cannot use the protection capacity given the demand has failed, and therefore are conditional time-congestions.

Notation:

Now let us introduce some notation.

i	index of demand number
$U(i)$	the unavailability of demand i
$B_j(i)$	probability that demand i cannot be carried on link j
$B_j^p(i)$	probability that demand i cannot be carried on the protection system of link j
q_j^p	failure probability of protection (standby) on link j
q_j^w	failure probability of worker system on link j
$r_k(i)$	kth route choice for demand i, comprising a set of links
$C_k(i)$	the probability that demand i is carried on route k, which is also the proportion of time or contribution to the availability of i on route k
$off(r_k(i))$	the probability that demand i is "offered" to route k (defined via Eqn. (1))
$Q_j(i)$	the probability that demand i is offered to the protection system on link j, where strictly this is only defined if $j \in r_k(i)$ for some k.

A demand offered to its first choice route is offered to a worker system, and standby systems provide link protection (one system being capable of carrying one demand) if the worker fails. If the first choice route fails, the demand is offered to the protection systems of links in the alternative routes. In calculating the probability that a demand is offered to a link on a route, we have to take into account the "thinning" and "baulking" probabilities caused by the probabilities that the demand is blocked on links before and after the link in question. Considering the first choice route, then $off(r_1(i)) = 1$, and the general formulae

$$P\{\text{demand } i \text{ is offered to link } j \text{ on route } k\} = off(r_k(i)) \prod_{\substack{h \in r_k(i) \\ h \neq j}} (1 - B_h(i)) \quad (1)$$

$$C_k(i) = off(r_k(i)) \prod_{j \in r_k(i)} (1 - B_j(i)) \quad (2)$$

hold true with $k=1$. Looking specifically at a first-choice route, then $P\{$demand i is offered to protection system on link j on route $k\}$, $Q_j(i)$, is given by

$$Q_j(i) = q_j \prod_{\substack{h \in r_1(i) \\ h \neq j}} (1 - B_h(i)). \quad (3)$$

Calculating the probability that demand i is offered to subsequent route choices is in general complicated by the fact that routes can have links in common, and we have to avoid double-counting probabilities (for ways to do this see for example [9, 11]). However with the restriction we placed on our routing trees, this problem is avoided: If we define

$P(k(i))$ the parent of route choice k in the routing tree

$L(r_k(i))$ the set of links joining $P(r_k)$ to r_k in the routing tree

then route r is used only if at least one of the links in the set $L(r)$ is blocked, and so

$$off(r_k(i)) = off(r_{P\{k(i)\}}) \times \left\{1 - \prod_{j \in L_k(i)} (1 - B_j(i))\right\} \quad (4)$$

Now the general formulae of Eqns. (1) and (2) give the probabilities that the demands are offered to links, however for all route-choices other than the first we have

$$Q_j(i) = off(r_k(i)) \prod_{\substack{h \in r_k(i) \\ h \neq j}} (1 - B_h(i)) \quad (5)$$

as in Eqn (1). rather than (3). The other difference between route 1 and the others is that

$$B_j(i) = q_j^w B_j^p(i) \quad \text{if} \quad j \in r_1(i) \quad (6)$$

since demands are first offered to a worker system, whereas

$$B_j(i) = B_j^p(i) \quad \text{if} \quad j \notin r_1(i) \quad (7)$$

because the demand is offered directly to the standby. The unavailability for demand i is given by

$$U(i) = 1 - \sum_k C_k(i) = 1 - \sum_k off(r_k(i)) \prod_{j \in r_k(i)} (1 - B_j(i)) \quad (8)$$

Thus to solve the equations we need to be able to calculate the $B_j(i)$.

Link-based models

In what follows we restrict our attention to $n+1$ protection systems — the extension to $n+m$ is straightforward.

In general, a link will comprise a number of worker systems (n) and also be offered demands which have overflowed from their first-choice route. Consider the case of a single link j with one protection system (failure probability q_j^p) which is offered d demands, a mix of fresh and overflow demands, where demand i has a probability $Q_j(i)$ of being offered to the protection system. Immediately we are faced with the problem of contention: we could consider "priority" working, in which a fresh demand always has access to the protection system if it has not failed, with the ability to pre-empt overflow demands. It is easier to implement a first-come first-served policy, in which any demand which fails can access the protection system with no pre-emption allowed, and each demand has an equal probability of accessing the resource. The probability that demand i cannot be carried on the protection system is then given by the following function F

$$B_j^p(i) = F_i(q_j^p, Q_j(1) \ldots Q_j(d)) = 1 - (1 - q_j^p) \times \mathrm{E}\left[\frac{1}{1 + \sum_{k \in \{1 \ldots d\} \setminus i} z_k}\right] \quad (9)$$

where the z_k are Bernoulli random variables taking the values 1 and 0 with probabilities $Q_j(k)$ and $(1-Q_j(k))$, and where the expectation (E) is taken with respect to these quantities.

Thus we now have the final piece of the jigsaw — the B_j are calculated from the above equation, where the Q are just the probabilities of Eqns. (3) and (5).

By altering the way the Bs are calculated, we can derive other approximations. For example if instead of Eqn. (9) we put

$$B_k^p = q_k^p \quad (10)$$

then we obtain an upper bound on the availabilities, where the demand in question takes priority over all the other demands which have access to the protection system.

4.5. Examples

Example 1: A three-node network

Consider a three-node triangle network with three demands where each link has *1+1* protection, and the routing tree for each of the demands comprises the direct link followed by the two-link alternative to be used if the direct link cannot be used. Suppose in this case that $q_i^w = q_i^s = q$, then by symmetry there are only two of the Qs which differ, say Q_f and Q_o, and only two of the Bs are different, say B_f and B_o where *f* represents first-choice traffic and *o* overflow.

Example 2: A larger network.

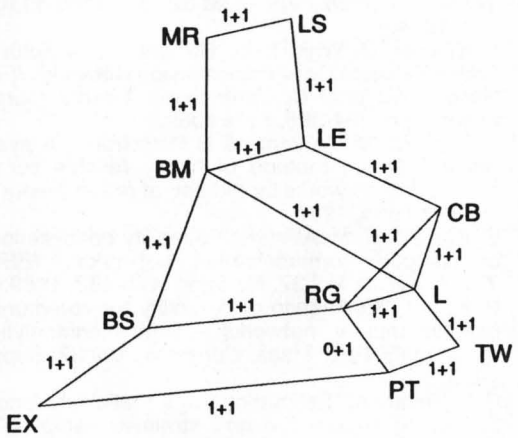

Figure 2. Simple example network.

	Route 1	Route 2	Route 3
1	BM-MR	BM-LE-LS-MR	
2	L-CB	L-RG-CB	
3	L-BM	L-RG-BS-BM	
4	L-TW	L-RG-PT-TW	L-RG-BS-EX-PT-TW
5	TW-PT		
6	EX-PT		
7	EX-BS		
8	BS-RG		
9	RG-L		
10	BS-BM		
11	MR-LS		
12	LS-LE		
13	LE-CB		
14	LE-BM		
15	RG-CB		

Table 1. Routing table for Example 2.

Consider now a more realistic network based on the BT inland trunk transmission network (Fig. 2). For clarity in this example, we have specified that all the links have one working and one protection system (except for RG-PT which is simply protection capacity). The 15 point-to-point demands chosen for this network are listed in Table 1, and were selected to show the effects of link and networking protection, including contention of various degrees.

5. Results

Consider first the triangle network of Example 1 with *1+1* protection, where all worker and protection unavailabilities are *q*. We can then solve the fixed-point equations, which are presented in Table 2, where the lower bound on the unavailability was found using equation (10) whereas the upper bound was produced by considering the state-space, picking a demand (say demand 1) and assuming that the demand could not be carried whenever there was contention.

Protection strategy	Analysis method	Unavailability
None		q
1+1 link		q^2
1+1 with networking	lower bound	$2q^3 - q^4$
	Fixed-point approx.	$3q^3 + \frac{3}{4}q^4 - \frac{107}{12}q^5 + O(q^6)$
	upper bound	$6q^3 - 10q^4 + 6q^5 - q^6$

Table 2. Protection methods and analysis techniques for Example 1 (with 1+1 protection).

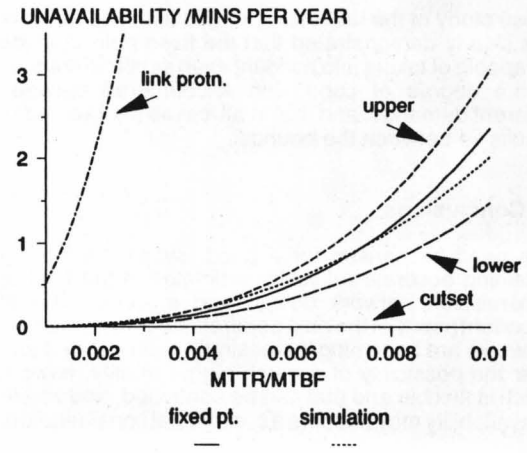

Figure 3. Demand 1 Unavailability.

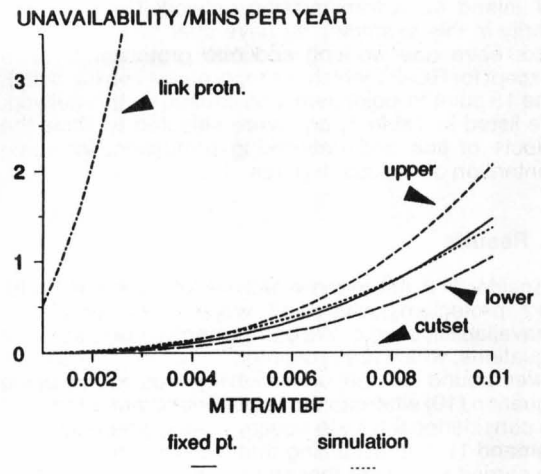

Figure 4. Demand 2 Unavailability.

Looking now at the more realistic network, Figures 3 and 4 plot the end-to-end unavailability of the first two demands (which have networking protection) obtained using the fixed point method and simulation, for the case where all system failure rates q are equal, and assuming independent repairs, over a range of system MTTR/MTBF. Also shown are upper and lower bounds calculated as above by isolating the routing sub-graph from the network and assuming no contention on the protection systems of the alternative routes (lower bound), or that access to the protection system is only possible if the working systems on the alternative routes are in service (lower bound). In addition, we show the unavailability derived from just considering connectivity (as in section 4.3) found by the use of a cutset method [15]; it is clear that it is possible to improve substantially on this technique. The unavailability for link-protection only is shown for comparison.

Close study of the full results for this example network has clearly demonstrated that the fixed point method is capable of taking into account even small differences in the degree of contention encountered between different demands, and that in all cases the fixed point results lie between the bounds.

6. Conclusions

The need has arisen for a good, simple method of obtaining accurate reliability estimates in the field of transmission network design and analysis. This is important now that the next generations of transmission networks are becoming increasingly sophisticated and offer the possibility of a much higher quality network which is flexible and that can be controlled, and where unavailability may become a contractual consideration.

The fixed-point method of calculating unavailabilities makes use of the explicit set of possible routes assigned to each end-to-end demand in a transmission network, takes account of contention between demands offered to protection systems following failures, and gives results which are substantiated by a variety of more approximate methods giving bounds on the unavailabilities. The fixed point method is simple to implement and can cope with all step-by-step alternative routing schemes, and also some forms of crank-back.

The method is capable of extension to cover more general routing strategies, including those where demands can have different priorities on different links.

References

[1] J.F. Meyer, "Performability Evaluation of Telecommunication Networks", *ITC 12*, Turin, 1988.

[2] V.O.K. Li & J.A. Silvester, "Performance analysis of networks with unreliable components", *IEEE Trans. Commun.*, Vol COM-32, pp. 1105-1110, Oct. 1984.

[3] I. Hawker, S. Whitt & G. Bennett, "The Future British Telecom Core Transmission Network", *IEE Second National Conference on Telecommunications*, pp. 364-368, April 1989.

[4] Y. Tanaka, M. Akiyama & B Wallstrom, "A systematic design method of highly reliable communication networks by the use of graph theory", *ITC 12*, Turin, 1988.

[5] S. Kiu & D.F. McAllister, "Reliability optimization of computer-communication networks", *IEEE Trans. Reliab.* Vol 37, No 5, pp. 475-483, 1989.

[6] P. Kubat, "Estimation of reliability for communication/computer networks - simulation/analytic approach", *IEEE Trans. Commun.*, Vol 37, Sept. 1989.

[7] G.S. Fishman, "Estimating the *s-t* reliability function using importance and stratified sampling", *Operations Research*, Vol 37, No 3., 1989.

[8] L.G. Valiant, "The complexity of enumeration and reliability problems " *SIAM J. Comp.* vol 8, pp 410-421, 1979.

[9] Y.B. Yoo & Narsingh Deo, "A comparison of algorithms for terminal-pair reliability", *IEEE Trans. Reliab.*, Vol. 37, pp. 210-215, 1988.

[10] W.P. Dotson, J.O. Gobien, "A new analysis technique for probabilistic graphs" *IEEE Trans. Circuits and Systems*, vol 26, pp. 855-865, 1979.

[11] P.M. Lin, B.J. Leon & C.R. Stewart, "Analysis of circuit-switched networks employing originating-office control with spill-forward", *IEEE Trans. Commun.*, Vol 26, pp. 754-765, 1978.

[12] F.P. Kelly, "Blocking probabilities in large circuit-switched networks", *Adv. Appl. Prob.*, Vol. 18, pp. 473-505, 1986.

[13] S. Rai & A. Kumar, "Recursive technique for computing system reliability", *IEEE Trans. Reliab.*, Vol. 36, pp. 38-44, 1987.

[14] F.P. Kelly, "Routing and capacity allocation in networks with trunk reservation," *Math. Oper. Res.*, Vol. 15, 1990.

[15] J.D. Esary & F. Proschan, "The reliability of coherent systems", *Redundancy Techniques for Computing Systems*, Washington D.C.: Spartan, pp. 47-61, 1962.