Results in Nonlinear Analysis 3 (2020) No. 3, 160–166
Available online at www.nonlinear-analysis.com

Results in Nonlinear Analysis
ISSN 2636-7556

Peer Reviewed Scientific Journal

Application of Nonlinear Approximation Methods to Network Fault Estimation Problems

Yao Tong[1], Shigeo Akashi[1]

[a] *Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science, Japan.*

Abstract

In the contemporary communication systems based on the Internet, the problem asking how to detect where the network failures have occurred is different from the problem asking how to predict numerically how often the network failures occur, because the former problem which is called the network fault detection problem and the latter problem which is called the network fault estimation problem are investigated with the network skills based on the statistical methods and the network skills based on the mathematical methods, respectively. Since it is one thing to locate the network failures on the network segments and quite another to predict them beforehand. Therefore it is important to apply not only statistical methods but also mathematical ones to the solutions to these problems.
In this paper, we discuss the problem asking what kinds of network skills based on mathematics the network fault estimation systems should be equipped with, for the purpose of predicting the occurrence of the network failures. Exactly speaking, it is shown that application of nonlinear approximation methods to these problems enables us to estimate numerically the degree indicating how often the network failures occur without looking up in the data consisting of the SNMP traps stored in the SNMP managers.

Keywords: monotone decreasing step function, Taylor expansion, Lagrange remainder term, network fault estimation.
2010 MSC: 60C05, 60E05, 90B15, 90B25.

1. Introduction

Nowadays, it is said that the network failures have hardly occurred, because the network fault detection systems have been prevalent everywhere in our daily life, Exactly speaking, simple network management protocol, which can be abbreviated to SNMP, plays so important roles in detecting local network failures as

Email addresses: 6320519@ed.tus.ac.jp (Yao Tong), akashi@is.noda.tus.ac.jp (Shigeo Akashi)

Received July 17, 2020, Accepted: August 24, 2020, Online: August 29, 2020.

soon as they have occurred before they bring about some other global and large-scale network failures. In the network segments equipped with SNMP, several servers, which are called SNMP managers, are always monitoring many routers and switches, which are called SNMP agents. The SNMP managers and the SNMP agents are corresponding regularly with each other in the way of exchanging SNMP packets mutually. The network fault detection systems acting on a certain network segment such as the SNMP server-client systems can be classified into two types, namely the system collecting SNMP traps issued from all the SNMP agents sharing the same network segment as the SNMP managers co-exist in, and the system monitoring the sequential behavior of all the SNMP agents. Actually, the network fault detection systems cannot mathematically predict when and where the network failures are likely to occur, though these systems can statistically record which area of the network segment the network failures have occurred in and how frequently the network failures have occurred by looking up in the SNMP database consisting of the SNMP traps collected by the SNMP managers.
In this paper, we discuss the problem asking what network skills based on mathematics should be installed on the network fault estimation systems, for the purpose of predicting the occurrence of the network failures. Exactly speaking, it is shown that application of nonlinear approximation methods to these problems enables us to estimate numerically the degree of the occurrence without inquiring at the SNMP managers.
These results stated in this paper are closely related to the disguised packet transfer problem and the equal cost multipath problem, As for the network skills which is vulnerable to the modern network failures, we can refer to [4] and [5], and as for an example of the network failures caused by the disguised packet transfer, we can refer to [1] and [2].

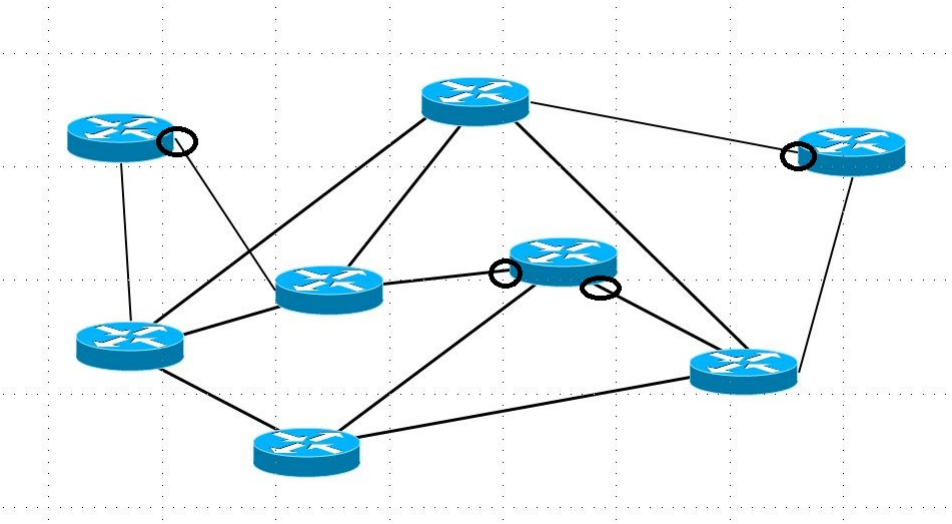
2. Classification of the alerts issued by SNMP agents

There are eight messages used in the simple network management protocols. We can arrange all of them in the order of descending priorities as the following: Emergencies, Alerts, Critical, Errors, Warning, Notification, Informational, Debugging. Actually, for the purpose of simplicity, we restrict all the messages as the following two types:

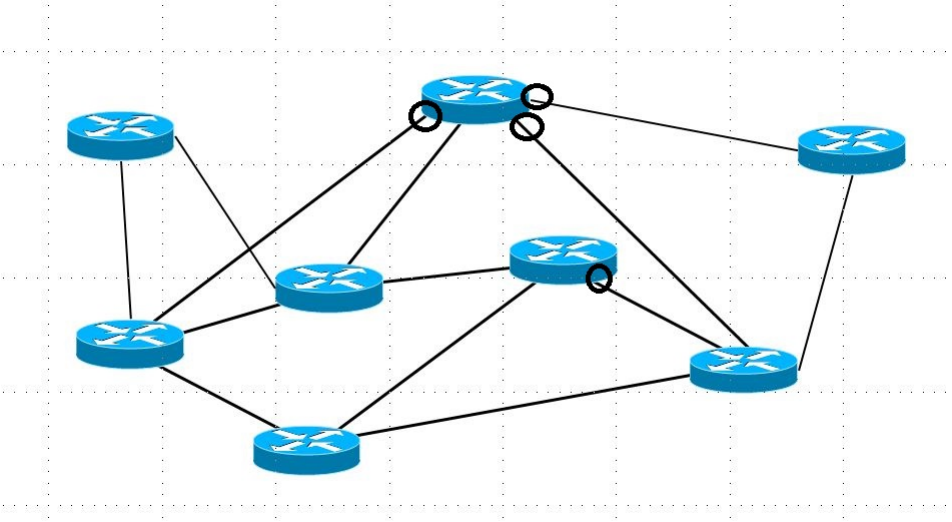
Type 1: The message informing the SNMP managers of the network failures that there exists at least one router including more than one interface having been out of order,

Type 2: The message informing the SNMP managers of the network failures that there exists either at least one router including more than two interfaces having been out of order or at least two routers, each of which includes more than one interfaces having been out of order.

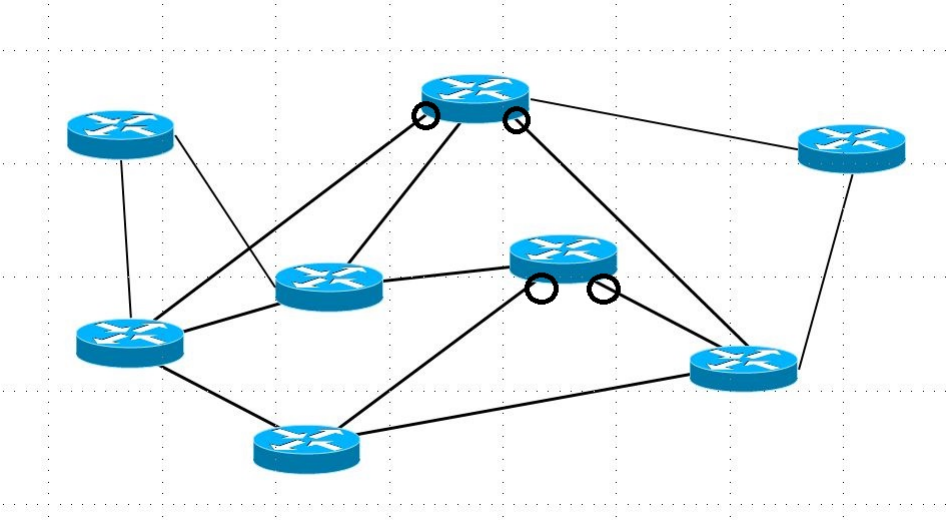
For example, a network segment where there exist four interfaces having been out of order, which is indicated by the alert based on Type 1 can be illustrated as the following figure:



where the four interfaces having been out of order are encircled in black. Moreover, two network segments where there exist four interfaces having been out of order, which is indicated by the alert based on Type 2 can be illustrated as the following two figures:



where there exist one router including three interfaces having been out of order and one router including one interface having been out of order, and



where there exist two routers, each of which includes two interfaces having been out of order. While the network failures reported in the way of sending Type 1 are regarded as slightly damaged, the network failure reported in the way of sending Type 2 are regarded as severely damaged. Therefore, it is reasonable that the alert based on Type 2 should be prior to the alert based on Type 1, because the network failures indicated by Type 2 will never occur if the network failures indicated by Type 1 do not occur previously. This implies that it is important for us to detect and to predict the network failures indicated by Type 1, for the purpose of preventing the network failures indicated by Type 2. By the way, the network failures indicated by Type 1 are strictly disjoint from such a network failure as the situation that a network segment is composed of the routers, each of which includes at most one interface having been out of order. This implies that the problem asking how often the alert based on Type 1 is issued can be attributed to the problem asking how frequently the network segments where any router includes at most one interface having been out of order occur. In the sequel, we discuss some probabilistic methods which should be installed on the network fault estimation systems. As for the mathematical aspect of the infrastructure of the contemporary networks, we can refer to [3].

3. Nonlinear approximation of discrete probability distributions

Throughout this section, we discuss the problems which are stated in the previous section. Let n and m be two positive integers, and consider a certain highly durable network including n routers equipped with m interfaces having been out of order. The assumption of the durability of this network assures that such a relation between n and m as $\frac{m}{n} \approx 0$ holds. Moreover, let $P_1(m,n)$ (resp. $P_2(m,n)$) be the probability showing how often the network failures indicated by Type 1 (resp. Type 2) occur. Then, the probability showing there does not exist any router including more than one interface having been out of order can be exactly characterized as $1 - P_1(m,n)$. This implies that

$$1 - P_1(m,n) = \prod_{k=0}^{m-1} (1 - \frac{k}{n})$$

holds. If it is assumed that n is very huge positive number, then the value of $1 - P_1(m,n)$ can be estimated from below and from above as the following:

$$\begin{aligned} \int_0^{\frac{m}{n}} \log(1-x)\,dx &< \frac{1}{n}\log\left(1 - P_1(m,n)\right). \\ &< \int_0^{\frac{m}{n}} \log(1 - x + \frac{1}{n})\,dx, \end{aligned}$$

because the logarithmic function used here is monotone decreasing. Therefore, these inequalities lead us to the following:

$$\begin{aligned} [(x-1)\log(1-x)]_0^{\frac{m}{n}} &< \frac{1}{n}\log\left(1 - P_1(m,n)\right) \\ &< [(x-1)\log(1 + \frac{1}{n} - x)]_0^{\frac{m}{n}}. \end{aligned}$$

If we assume that, for a positive integer s which is less than one, $m = [sn]$ holds, then we can obtain

$$\lim_{n\to\infty} \frac{1}{n}\log\left(1 - P_1([sn],n)\right) = \int_0^s \log(1-x)\,dx,$$

where $[\cdot]$ means Gaussian symbol. Since we can regard the left hand side term as a characteristic function of s, which indicates numerically how often network failures occur under the condition that the total number of the routers is sufficiently large, we denote this term as $C(s)$ in the sequel. These results stated above enable us to represent the asymptotic behavior of $P_1(m,n)$ as the following:

Proposition 1. Let s and t be positive numbers satisfying $0 < s < t < 1$ and n be a positive integer. Then, the next equality:

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\log(\frac{1-P_1([sn],[tn])}{1-P_1([sn],n)}) &= \frac{1}{t}\int_0^s \log(t-x)\,dx - \int_0^s \log(1-x)\,dx \\ &\quad + \frac{s}{t}\log(\frac{1}{t})\end{aligned}$$

holds.

Proof. The following equality derived from the integration by substitution:

$$\int_0^a \log(1-x)\,dx = \frac{a}{b}\int_0^b \log(\frac{b}{a}-x)\,dx + a\log\frac{a}{b},$$

where a and b are two positive integers satisfying $0 < a < b < 1$ and the next equality:

$$\lim_{n\to\infty}\frac{1}{n}\log(\frac{1-P_1([sn],[tn])}{1-P_1([sn],n)}) = \int_0^{\frac{s}{t}} \log(1-x)\,dx - \int_0^s \log(1-x)\,dx$$

conclude the proof. □

Proposition 1 implies that, for any positive integers m, n_1 and n_2 satisfying $m < n_1 < n_2$, $P_1(m,n_1)$ can be compared with $P_1(m,n_2)$ as the following equalities:

$$\begin{aligned}\log(\frac{1-P_1(m,n_1)}{1-P_1(m,n_2)}) &= \log(\prod_{k=0}^{m-1}\frac{1-\frac{k}{n_1}}{1-\frac{k}{n_2}}) \\ &= \sum_{k=0}^{m-1}\{\log(\frac{n_1}{n_2}-\frac{k}{n_2}) - \log(1-\frac{k}{n_2})\} - m\log(\frac{n_1}{n_2}).\end{aligned}$$

Therefore, roughly speaking, the above equalities assure that the following approximate equality:

$$\begin{aligned}\frac{1}{n_2}\log(\frac{1-P_1(m,n_1)}{1-P_1(m,n_2)}) &\approx \int_0^{\frac{m}{n_2}} \log(\frac{n_1}{n_2}-x)\,dx - \int_0^{\frac{m}{n_2}} \log(1-x)\,dx \\ &\quad - \frac{m}{n_2}\log(\frac{n_1}{n_2})\end{aligned}$$

holds. As for a relation between $P_2(m,n)$ and $P_1(m,n)$, we can obtain the following equality:

$$P_2(m,n) = \frac{(m-1)P_1(m-1,n)}{n}.$$

The reason why the above relation holds is the following. The network failure indicated by Type 2 can be classified into two subtypes, namely, the subtype that there exists at least one router including more than two interfaces having been out of order and the subtype that there exists at least two routers, each of which has more than one interface having been out of order. Therefore, we cannot refrain the SNMP servers from receiving the alert based on Type 2, if some of the interface having been out of order cannot be repaired without delay. This consideration assures that some of the networks where the SNMP servers receive the alert based on Type 1 are likely to change themselves to the networks where the SNMP servers receive the alert based on Type 2 in the near future. In other words, there does not exist any SNMP servers receiveing the alert based on Type 2 without receiving the alert based on Type 1 previously.

4. Asymptotic behavior of Lagrange remainder terms

Let x be a real number and $f(\cdot)$ be a real-valued infinitely differentiable function defined on the set of all real numbers. Then, Taylor expansion assures that, for any positive integer n and for any real number h, there exists a positive number $\theta_{x,n,h}$ which is less than one, satisfying the following equality:

$$\frac{f^{(n)}(x+\theta_{x,n,h}h)h^n}{n!} = f(x+h) - \sum_{k=0}^{n-1}\frac{f^{(k)}(x)h^k}{k!}.$$

Therefore, when $|h|$ is sufficiently small, the asymptotic behavior of $\theta_{x,n,h}$ can be represented as the following:

Proposition 2. Let n be a positive integer. Then, for any real number x satisfying $f^{(n+1)}(x) \neq 0$, the following equality:

$$\lim_{h\to 0}\theta_{x,n,h} = \frac{1}{n+1}$$

holds.

Proof. It is sufficient to prove the case of $h > 0$. If we compare Lagrange remainder term included in the Taylor expansion of the n-th degree with Lagrange remainder term included in the Taylor expansion of the $(n+1)$-th degree, we can obtain the following equality:

$$f^{(n)}(x+\theta_{x,n,h}h) = f^{(n)}(x) + \frac{f^{(n+1)}(x+\theta_{x,n+1,h}h)h}{n+1}.$$

Moreover, if we apply the mean value theorem to the left-hand side term of the above equality, then we can find a positive number $p_{x,n,h}$ which is less than one, satisfying the following equality:

$$f^{(n)}(x+\theta_{x,n,h}h) = f^{(n)}(x) + f^{(n+1)}(x+p_{x,n,h}\theta_{x,n,h}h)\theta_{x,n,h}h.$$

These two equalities enables $\theta_{x,n,h}$ to be characterized as the following:

$$f^{(n+1)}(x+p_{x,n,h}\theta_{x,n,h}h)\theta_{x,n,h} = \frac{f^{(n+1)}(x+\theta_{x,n+1,h}h)}{n+1}.$$

This equality allow us to characterize the asymptotic behavior of $\theta_{x,n,h}$:

$$\begin{aligned}\lim_{h\to 0}\theta_{x,n,h} &= \lim_{h\to+0}\frac{f^{(n+1)}(x+\theta_{x,n+1,h}h)}{(n+1)f^{(n+1)}(x+p_{x,n,h}\theta_{x,n,h}h)}\\ &= \frac{1}{n+1}.\end{aligned}$$

These equalities conclude the proof. □

Proposition 2 can be applied to the numerical approximation of $C(s)$ in terms of the formula without using the integration as the following:

Corollary 3. Let s be a sufficiently small positive number, then the next equality:

$$\lim_{s\to+0}\frac{C(s)}{s^2} = \frac{-1}{2}$$

holds.

Proof. Application of the mean value theorem to the definition of $C(s)$ assures that there exists a certain positive number θ_s satisfying

$$\int_0^s \log(1-x)\,dx \;=\; s\log(1-\theta_s s).$$

Moreover, for any s, there exists a positive number p_s which is less than one satisfying

$$\log(1-\theta_s s) \;=\; -\theta_s s - \frac{(p_s\theta_s s)^2}{2}.$$

These two equalities conclude the proof because $\lim_{s\to+0}\theta_s = \frac{1}{2}$ can be derived from Proposition 2. □

Application of l'Hospital theorem enables to prove Corollary 3 in another way, and this corollary shows that the probability $P_1(m,n)$ can be easily estimated approximately, if n is sufficiently large and $\frac{m}{n}$ is sufficiently small.

References

[1] S. Akashi and Y. Tong, *Classification of DHCP Spoofing and Effectiveness of DHCP Snooping*, Proceedings on 2018 International Conference on Advances in Computer Technology, Information Science and Communication, edited by Wen-Bing Horng and Yong Yue, 233-238, ISBN:978-989-758-357-5, 2019.
[2] C. Hopps, *Analysis of an Equal-Cost Multi-Path Algorithm*, RFC2992, Available: https://tools.ietf.org/html/rfc2992
[3] D. E. Knuth, *The Art of Computer Programming*, Addison-Wesley Publishing Company, Massachusetts, 2nd edition, 1973.
[4] O. Santos and J. Muniz, *CCNA Cyber Ops Secfnd 210-250*, Cisco Press, Indianapolis, 1st edition, 2017.
[5] O. Santos and J. Muniz, *CCNA Cyber Ops Secops 210-255*, Cisco Press, Indianapolis, 1st edition, 2017.