Diss. ETH No. 11272

A Reliability Growth Model for Protocol Validation and Testing by Random State Exploration

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH

for the degree of

Doctor of Technical Sciences

presented by

Angelo Einar Tosi

Laureato in Ingegneria Elettronica, Politecnico di Milano, Italy

born on May 1, 1961

citizen of Italy

accepted on the recommendation of

Prof. Dr. Bernhard Plattner, examiner

Prof. Dr. Alessandro Birolini, co-examiner

Dr. Colin H. West, co-examiner

1995

Kurzfassung

Die Random-State-Explorations-Methode - oder Random-Walk-Technik - wurde zuerst zur Validierung komplexer Kommunikationsprotokolle eingesetzt, deren Zustandsraum zu gross ist, um ausführlich untersucht zu werden. Die Methode basiert auf einem zufällig erzeugten Besuch der Menge derjenigen Zustände, die von einem Anfangszustand, gewöhnlich dem Initialisierungszustand des Protokolls, auserreichbar sind. Der Algorithmus registriert nicht, welche Zustände schon untersucht worden sind; ein Zustand kann deswegen immer wieder besucht werden. Die Technik ist erfolgreich zur Validierung sowie zum Testen von Kommunikationsprotokollen eingesetzt worden, und hat Defekte in Protokollspezifikationen sowie -implementationen offenbart, die bereits sorgfältigeren Kontrollen unterzogen worden waren. Die Methode ist grundsätzlich empirisch, und ihre konzeptionellen Fundamente blieben weitgehend unerforscht.

Diese Dissertation bietet einen neuen Einblick in die Mechanismen der Random-Walk-Technik und trägt dazu bei, die Gründe ihres Erfolgs besser zu erläutern. Sie befasst sich mit einem Muster, das in sämtlichen Anwendungen der Technik auftritt: die Anzahl der entdeckten Ausfälle scheint linear mit dem Logarithmus der Anzahl der Schritte im Zustandsraum anzusteigen. Ich schlage ein neues Modell für die Random-Walk-Technik vor, welches auf der Theorie der regenerativen Prozesse basiert. Die meisten Protokollzustände können als seltene Ereignisse betrachtet werden, und die Random-Walk-Technik kann mit einem zufälligen Stichprobenverfahren aus dem Zustandsraum approximiert werden. Die erwartete Anzahl der verschiedenen besuchten Zustände wird als eine Funktion der gesamten Anzahl der ausgeführten Protokollprimitiven formuliert. Weiter zeige ich, dass die Kurve der erwarteten Zustandsdeckung eine lineare Funktion des Logarithmus der gesamten Anzahl der ausgeführten Schritte ist, wenn die nach Grösse geordneten Wahrscheinlichkeiten des ersten Besuches der Protokollzustände geometrisch abnehmen. Das Modell wird anhand von experimentellen Daten verifiziert, die im Rahmen eines Random-Walk-Testprojektes am IBM Forschungslaboratorium Zürich gesammelt worden sind.

Ausgehend von der Hypothese, dass Ausfälle auf Systemebene zufälligerweise im Zustandsraum auftreten, leite ich aus der erwarteten Zustandsdeckung ein Modell für den Defektentdeckungsprozess her und behandle die Methoden zu der Parameterschätzung

und dem Anpassungstest. Dieses Modell kann als Zuverlässigkeitswachstumsmodell zur Planung und Kontrolle der Random-Walk-Technik eingesetzt werden.

Schliesslich verifiziere ich das Modell anhand der experimentellen, aus zwei umfangreichen Random-Walk-Validierungsprojekten stammenden Daten, die Colin H. West in den letzten Jahren am IBM Forschungslaboratorium Zürich durchführte. In beiden Fällen stimmt das vorgeschlagene Modell mit den experimentellen Stichproben gut überein.

Abstract

The random state exploration method - or random walk technique - was proposed to validate complex communications protocols, whose state space is too large to be validated by an exhaustive search. It entails the random exploration of the set of all states reachable from an initial state, i.e. the initialization or idle state of the protocol. The algorithm does not keep track of the states already explored, thus the same state may be visited any number of times. The technique has been applied in validation as well as testing projects, always with considerable success, detecting defects in protocol specifications and implementations that had already passed careful reviews and controls. The method is essentially empirical, and its conceptual foundations remain widely unexplored.

This thesis provides new insight into the nature of the random walk technique, and sheds light on the mechanisms that contribute to its apparent success. Attention is focused on a trend shown by all applications of the technique, according to which the number of distinct failures observed increases approximately logarithmically with the total number of steps executed. We propose a novel model for the random walk technique based on the theory of regenerative processes. Most protocol states may be treated as rare events, and the random walk technique may be approximated with a random sampling of the protocol state space. An expression is derived for the expected number of distinct states covered as a function of the total number of protocol primitives executed. We also show that the expected state coverage curve is a linear function of the logarithm of the total number of steps executed under the hypothesis that the probabilities of first hitting time of the protocol states, ordered by magnitude, decrease geometrically. The model is verified with the experimental coverage data collected while participating in a random walk testing project at the IBM Zurich Research Laboratory.

Based on the assumption that systematic failures in a mature specification or implementation are randomly distributed in the protocol state space, a model is derived for the defect detection process based on that for the expected state coverage, and the procedures for parameter estimation and goodness-of-fit testing are discussed. This model may be applied as a reliability growth model to plan and manage the application of the random walk technique to protocol validation and testing.

Finally, this model is verified with the experimental data originating from two major

random walk validation projects conducted by Colin H. West at the IBM Zurich Research Laboratory in recent years. In both cases, the present model provides a good fit to the experimental samples.