Surrogate Oracles, Generalized Dependency and Simpler Models

Larry Wilson
Old Dominion University
Supported by NAG-1-750

Abstract

Software reliability models require the sequence of interfailure times from the debugging process as input. We have previously illustrated that using data from replicated debugging could greatly improve reliability predictions. However, inexpensive replication of the debugging process requires the existence of a cheap, fast error detector. We can design laboratory experiments around a gold version which is used as an oracle or around an n-version error detector. Unfortunately, we can not expect software developers to have an oracle or to bear the expense of n-versions. We are investigating a generic technique for approximating replicated data by using the partially debugged software as a difference detector.

We believe that the failure rate of each fault has significant dependence on the presence or absence of other faults. Thus, in order to discuss a failure rate for a known fault, we need to specify the presence or absence of each of the other known faults.

Also, we are interested in simpler models which use shorter input sequences without sacrificing accuracy. In fact we, conjecture a possible gain in performance.

To investigate these propositions, we are using NASA computers running LIC (RTI) versions to generate data. This data will be used to label the debugging graph associated with each version. These labeled graphs will be used to test the utility of a surrogate oracle, to analyze the dependent nature of fault failure rates and to explore the feasibility of reliability models which use the data of only the most recent failures.
VALUE OF PDG

DATA <

USEFUL

OBTAINABLE

SURROGATE ORACLE
DATA DEPENDENCE
NEW MODELS


guides intuition
in Reliability Prediction

when replicated

Real World

with surrogate
oracle

ORIGINAL PAGE IS
OF POOR QUALITY
Normal Debugging

\[
\begin{align*}
\text{0} & \quad T_1 & \quad T_2 & \quad \ldots & \quad T_n \\
\text{P} & \quad P_1 & \quad P_2 & \quad \ldots & \quad P_n \\
\end{align*}
\]

\[ t_i = T_i - T_{i-1} \quad \text{interfailure times} \]

Models take as input \((t_1, t_2, \ldots, t_n)\) and produce estimates of \(\lambda\)

INPUT DISTRIBUTION / RANDOM INPUTS
ERROR DETECTOR
• Conclusion 1: These SR models should never be used to predict software reliability if we only use normal debugging process.

• Conclusion 2: The models are stable after the randomness is removed by replicated debugging. With replication, conceivable to use models.

• Future:

1. GCS
2. Front end for repliability models.
3. Estimate and control the cost of replication.
4. Analyze debug graph to get better models.
Debug Graph

\[ V \]

\[ V_1 \]
\[ V_{12} \quad V_{13} \quad V_{1N} \quad V_{23} \quad V_{2N} \]

\[ \cdots \]

\[ V_{N} \]
\[ V_{N-1N} \]

\[ \cdots \]
\[ \vdots \]
\[ \vdots \]

\[ \vdots \]

\[ V_{12 \ldots N} \]
EMBEDDED PARTIAL DEBUG GRAPH
Partial Debug Graph

\[ V \]

\[ V_1 \quad \ldots \quad V_{2n} \quad V_{n-1,n} \]

\[ V_{12} \quad V_{13} \quad \ldots \quad V_{1n} \quad V_{23} \quad \ldots \quad V_{2n} \]

\[ V_{12 \ldots n} \]

\[ \vdots \]

\[ \vdots \]

\[ \vdots \]
RPDG1

V  42.344%

V1 94.27
V2 43.80
V3 42.50
V4 42.90
V5 42.88
V6 42.72
V7 42.70
V8 42.40
V9 42.40
V10 42.4
RPDG 9

V_1   V_2   V_3   V_4   V_5   V_6   V_7   V_8   V_9   V_10

V1..10  99.999%
\( \Delta \text{RPDG9} \)

- V-1: 45.729
- V-2: 97.254
- V-3: 99.797
- V-4: 98.618
- V-5: 98.984
- V-6: 99.847
- V-7: 99.967
- V-8: 99.998
- V-9: 99.998
- V-10: 99.999%

Branches:
- V-2: 0.15%
- V-3: 0.2%
- V-4: 1.4%
- V-5: 0.0%
- V-6: 0.03%
- V-7: 0.002%
- V-8: 0.002%
- V-9: 0.001%
- V-10: 0.03%
- V-1: 0.5%
ΔPDG1

V

V1 V2 V3 V4 V5 V6 V7 V8 V9 V10

53.57% 2.80% ?? 0.19% 0.96%
1. ANALYZE BUG DEPENDENCY
   FILL IN ΔRPDG

2. NEW MODELS
   FILL IN ROWS 8 AND 9 ΔSRPDG
   ANALYZE

3. REPEAT FOR LIC 3.C

4. CONTINUE WITH GCS DATA