Squeeziness

A metric for avoiding fault masking in software testing
• Joint work with

• Rob Hierons

• Haito Dan

• Matt Moroz

• with help from Sebastian Hunt and Laurie Tratt
software fault masking

- also called **error masking**
- reduces test set effectiveness
- Error masking condition:

\[
\exists x, s, s', y . \text{PRE}(x) \land A_{SC}(x, s) \land \text{PRE}_C(s) \\
\land \neg \text{POST}_C(s, s') \land \text{wp}(G(E_C, E), \text{POST})(x, s') \\
\land \text{POST}(x, y)
\]

Laski et al. ’95
\text{PRE}(x)

\text{PRE}_C(s)

\text{AS}_C(x, s)

\text{wp}(G(E_C, E), \text{POST})(x, s')

\neg \text{POST}_C(s, s')

\text{POST}(x, y)

G(E_C, E)
example

**Intended**

```plaintext
x = x + 2;
if (x > 0)
    x = x % 4;
else
    x = x;
```

**Output**

- t1: x == 1
- t2: x == -3

**Unintended**

```plaintext
x = 3 * x;
if (x > 0)
    x = x % 4;
else
    x = x;
```

**Input**

- t1: x == 3
- t2: x == -5

**Output**

- t1: x == 1
- t2: x == -15
collisions and state abstraction

- \((x>0)== true; x \% 4\): collisions
- **also:** oracle may examine only part of the state
- execution path plus oracle identify good and bad states
Domain to Range Ratio

- collisions *necessary*, not *sufficient*, for fault masking
- [Woodward and al-Khanjari (2000)] observed fault masking associated with domain to range ratio
- “loss of information measure” $\frac{|D|}{|R|}$
Treat the input space and the output space for a program as random variables: I and O

Information in a random variable

$$H(X) = - \sum_{x \in X} p(x) \log_2 p(x)$$
Loss of information from running program $P$

$$H(I) - H(O)$$

where \([P]I = O\)

We call this quantity **Squeeziness**.

$$Sq(f) = H(I) - H(O) = \sum_{o \in O} p(o) H(f^{-1}o)$$

via the partition property
\[ \mathcal{H}(f^{-1}o) \]

\[ f^{-1}o \]

\[ f \]

\[ p(o) \]
it’s not DRR

- Squeeziness is not a refinement of DRR (and vice versa).
- DRR is a cruder measure than Squeeziness and makes fewer distinctions.
- Orderings they produce on \((f, I)\) pairs are inconsistent.
the likelihood of collisions

assume uniform distribution on I

\[ PColl(f) = \sum_{i=1}^{n} \frac{m_i \ast (m_i - 1)}{d \ast (d - 1)} \]

Relationship between Squeeziness and PColl not monotonic
<table>
<thead>
<tr>
<th>Domain size</th>
<th>Max sub</th>
<th>Corr with Sq</th>
<th>Corr with DRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00E+05</td>
<td>200</td>
<td>0.981</td>
<td>0.849</td>
</tr>
<tr>
<td>1.00E+05</td>
<td>200</td>
<td>0.986</td>
<td>0.889</td>
</tr>
<tr>
<td>1.00E+05</td>
<td>2000</td>
<td>0.981</td>
<td>0.849</td>
</tr>
<tr>
<td>1.00E+05</td>
<td>2000</td>
<td>0.986</td>
<td>0.889</td>
</tr>
<tr>
<td>1.00E+06</td>
<td>200</td>
<td>0.971</td>
<td>0.748</td>
</tr>
<tr>
<td>1.00E+06</td>
<td>200</td>
<td>0.964</td>
<td>0.686</td>
</tr>
<tr>
<td>1.00E+07</td>
<td>200</td>
<td>0.968</td>
<td>0.645</td>
</tr>
<tr>
<td>1.00E+07</td>
<td>200</td>
<td>0.975</td>
<td>0.606</td>
</tr>
<tr>
<td>1.00E+08</td>
<td>200</td>
<td>0.978</td>
<td>0.584</td>
</tr>
<tr>
<td>1.00E+08</td>
<td>200</td>
<td>0.975</td>
<td>0.668</td>
</tr>
</tbody>
</table>
what can we do with Squeeziness?

• (1) Measure how much Software Under Test is inclined to fault masking (not so helpful . . . )

• (2) Improve test set selection?
test suite selection

- current “standard” for white box testing is structural coverage: statements, branches, etc.
- limited relationship between coverage and test suite effectiveness, e.g. [Cai and Lyu. A-MOST 2005] plus other papers
Use covering paths to generate tests

Pick a less Squeezy path

Reduce possible fault masking
How can developers know the random variable in inputs?

(1) Maximum Entropy Principle (= Uniform distribution)

\[ Sq(f) = \frac{1}{|I|} \sum_{o \in O} |f^{-1}o| \log_2(|f^{-1}o|) \]

(2) Maximum Squeeziness:

\[ Sq(f) = \log_2|f^{-1}o'| \]

(3) WesWeimar: estimating path execution frequency statically
current research

- experimental validation of post structural element path selection using a mutation testing approach
- theory of probabilistic testing
- program analyses to estimate Squeeziness
- relationship to mutation testing, SBT

- position paper: Clark and Hierons. Squeeziness: An Information Theoretic Measure for Avoiding Fault Masking. Accepted for publication in Information Processing Letters
Questions?