Schrödinger's CRCs

(Fast Abstract)[1]

Lee Pike

leepike@galois.com

Galois Inc.

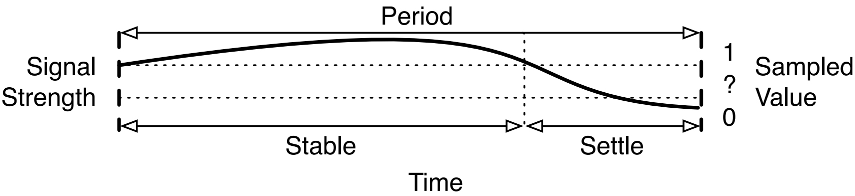
June 29, 2010

[1]Supported in part by NASA Aviation Safety Program Office Contract NNL08AD13T.

Talk Goals

- New metrics for analyzing the fault-tolerance of CRCs.
- Motivated by sources of Byzantine faults.
- Initial idea (and catchy title) originally developed in *Byzantine Fault Tolerance, from Theory to Reality*, by K. Driscoll, B. Hall, Håkan Sivencrona, and P. Zumsteg, SAFECOMP 2003.

Relevant Faults



- Frequent faults causing a receiver to misinterpret a signal.
- Could be due to faults in the sender, receiver, or interconnect.
  - "Slightly-out-of-spec" timing faults.
  - Stuck-at-$\frac{1}{2}$ faults.

Schrödinger bit errors

Schrödinger bit errors: for a fixed transmitter and receiver, bit errors that are exclusively one of

- 0s are randomly misinterpreted as 1s.
- 1s are randomly misinterpreted as 0s.

A subset of random transient faults.

Why it Matters

- Permanent faults may appear to be transient if they lead to Schrödinger bit errors.
- Upon component failure, the probability of Schrödinger bit errors may be much higher than random transient faults, causing a bit-error rate that frequently violates the Hamming distance.
- More empirical data is needed on fault-arrival rates for Schrödinger bit errors.

New Metrics

Fix a data-word width w, a CRC polynomial, and a number of bit errors e.

- **Schrödinger-Hamming weight (SHW)**: The total number of possible undetected corruptions of data-words of width w and their FCSs together resulting from e Schrödinger bit errors.
- **The Schrödinger-Hamming distance (SHD)**: The smallest number of Schrödinger bit errors resulting in a non-zero SHW.

Open Question: Does there exist a CRC and data-word size such that SHD $>$ Hamming distance?

Final Observations

- Observation: a *Manchester encoding* detects *all* Schrödinger bit errors by encoding a ‘0’ as ‘01’ and ‘1’ as ‘10’.
- Should use a Manchester encoding when expecting Schrödinger bit errors.
- Read the (short) paper and Driscoll *et al.*’s original paper!