SAND REPORT

SAND2003-4439
Unlimited Release
Printed December 2003

Unique Signal Mathematical Analysis Task Group FY03 Status Report

Arlin Cooper, Anna Johnston, Roy Baty, Elizabeth Hart, and Allan White

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of
Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2003-4439
Unlimited Release
Printed December 2003

Unique Signal Mathematical Analysis Task Group FY03 Status Report

Arlin Cooper
Airworthiness Assurance Department

Anna Johnston
Discrete Algorithms and Math Department

Sandia National Laboratories
P.O. Box 8500
Albuquerque, NM 87185-0490

Roy Baty
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545

Elizabeth Hart
Utah State University
Logan, UT 84322

Allan White
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681

Key words: unique signal, mathematics, safety analysis

Abstract

The Unique Signal is a key constituent of Enhanced Nuclear Detonation Safety (ENDS). Although the Unique Signal approach is well prescribed and mathematically assured, there are numerous unsolved mathematical problems that could help assess the risk of deviations from the ideal approach. Some of the mathematics-based results shown in this report are:

1. The risk that two patterns with poor characteristics (easily generated by inadvertent processes) could be combined through exclusive-or mixing to generate an actual Unique Signal pattern has been investigated and found to be minimal (not significant when compared to the incompatibility metric of actual Unique Signal patterns used in nuclear weapons).
2. The risk of generating actual Unique Signal patterns with linear feedback shift registers is minimal, but the patterns in use are not as invulnerable to inadvertent generation by dependent processes as previously thought.
3. New methods of testing pair-wise incompatibility threats have resulted in no significant problems found for the set of Unique Signal patterns currently used. Any new patterns introduced would have to be carefully assessed for compatibility with existing patterns, since some new patterns under consideration were found to be deficient when associated with other patterns in use.
4. Markov models were shown to correspond to some of the engineered properties of Unique Signal sequences. This gives new support for the original design objectives.
5. Potential dependence among events (caused by a variety of communication protocols) has been studied. New evidence has been derived of the risk associated with combined communication of multiple events, and of the improvement in abnormal-environment safety that can be achieved through separate-event communication.

Acknowledgment

The work documented in this report was supported by Todd Jones, Brian Damkroger, and Dick Perry, all of Sandia National Laboratories, as well as by NASA Langley. The mathematically oriented exchanges during meetings of the core group of researchers had a synergistic benefit. Assisting the authors of this report in the meetings and in private consultation were Todd, John DeLaurentis, Lisa Brown, Ron Pedersen, Susan Camp, and John Covan, all of Sandia National Laboratories, Stan Spray, retired Sandian now consulting, Curtis Mueller (retired Sandian) and Ken Griego (Sandian, now deceased). Roy Baty is now at Los Alamos National Laboratory, but was with Sandia National Laboratories when this work was done. Elizabeth Hart, a Utah State University senior, was a Sandia National Laboratories employee during the summer of 2003.

Contents

List of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

List of Tables

Chapter 1

Preface

The function of the Unique Signal is to provide an extremely high level of resistance to inadvertent pre-arming, even in abnormal environments[1], while reliably providing an unambiguous enabling stimulus (pre-arm) to a nuclear weapon. The details of and reasons for the UQS methodology are given in SAND91-1269.

There have been a large number of contributors to mathematical assessment of Unique Signal performance, including Stan Spray, Bill Stevens, Wally Crammond, Jay Grear, Curtis Mueller, and Gene Church. Since I am the only person still working on Unique Signals as a mainstream activity, and since there are a number of important unsolved mathematical problems that could assist in Unique Signal assessment, Todd Jones proposed a study group that would both provide the opportunity to address significant mathematical problems and would create a wider base of Sandia National Laboratories Unique Signal expertise.

This report contains five chapters that represent a significant portion of the study group's work that took place during FY03. The first chapter addresses how difficult it is for unintended inputs to be accidentally generated such that they could be combined in an exclusive-or operation to inadvertently yield a Unique Signal pattern. In this work, the entire range of possible exclusive-or inputs that could result in the seven 24-event Unique Signal patterns currently used in nuclear weapons designs was examined. The second chapter documents an analysis of linear feedback shift register (LFSR) structures that can produce Unique Signal patterns, and tests some of the metrics used to guide generation of patterns against the properties of the patterns in actual use. We now know the LFSR complexity required for all Unique Signal patterns in use, and we also know how close each comes to meeting a significant number of its design goals. The third chapter tests pair-wise compatibility for members of the set of patterns currently used, as well as for some patterns that have been considered candidates for future use. This has provided the first comprehensive attempt at a pair-wise compatibility test for Unique Signal patterns. The fourth chapter utilizes Markov process state analysis to demonstrate how dependent correlation reduces with time, a property that is shown to be enhanced through separate-event communication, and addresses the determination of maximum threat levels for Markov processes. The fifth chapter demonstrates new evidence of dependence threats and indicates how threats due to all known classes of dependence can be reduced through separate-event communication.

Arlin Cooper
October 23, 2003

[1] Abnormal environments transcend normal operating environments, including all degrees of severity.

Chapter 1. Unique Signal Exclusive-Or Mixing Study

Roy Baty and Arlin Cooper

Problem Description and Results Summary

A significant number of nuclear weapon system designs incorporate "exclusive-or" mixing of two or more unique signal patterns as operands to obtain a resultant Unique Signal pattern that drives a stronglink switch. There is significant confidence in the safety robustness of this approach for many reasons (summarized in the body of this chapter). However, the question of how easily unintended inputs could be accidentally generated such that they could be combined in an exclusive-or operation to inadvertently yield a Unique Signal pattern has never been addressed for the entire population. In this project, the entire range of possible exclusive-or inputs that could result in the seven 24-event Unique Signal patterns currently used in nuclear weapons designs was examined using trial vulnerability metrics. No significant safety problems have yet been found.

Background

The modern quantitative parameters for the Unique Signal (24 bi-valued "events") had their genesis in the jointly (DoD, DOE, and Sandia) agreed-on abnormal-environment requirement that is part of the "Walske letter"[2] of 1968. The abnormal-environment requirement is that "The probability of a premature nuclear detonation … shall not exceed 1 in 10^6 per … exposure or accident." This requirement places a very high demand on weapons systems, which must respond safely, even given an exposure or accident[3].

Sandia systems personnel (in consultation with safety personnel) decided that it was necessary to use two abnormal-environment safety subsystems in the ENDS (Enhanced Nuclear Detonation Safety) approach, with the aim of making each significantly better than 10^{-3} per exposure, and engineering a high degree of independence[4] between the two subsystems. This (along with requirements for complete human intent) meant that there would be a separate Unique Signal for each abnormal-environment safety subsystem. Each Unique Signal was to be applied to its own "stronglink switch." The safety burden for the two abnormal-environment safety subsystems (significantly better than 10^{-3} per exposure) rests mainly on the information incompatibility of each Unique Signal, because the probabilistic isolation/inoperability protection of the exclusion regions and stronglink switches is much more difficult to assure.

The SNL goal is to implement two human-initiated Unique Signal event sequences (each having a different and unrelated pattern of events), one for each abnormal-environment

[2] Carl Walske was then the DoD Military Liaison Chairman and Assistant to the Secretary of Energy.

[3] There is also a normal-environment requirement (one in 10^9 over weapon lifetime), so a third safety subsystem is required, but it does not require a unique signal.

[4] The relation $10^{-3} \times 10^{-3} = 10^{-6}$ is not defensible unless the two subsystems are independent.

safety subsystem (double intent). Without any human intent, the generation of trajectory unique signals is difficult to distinguish from some accident environments. A Unique Signal for human intent for the early trajectory safety subsystems was not available from the DoD. Therefore a constrained strategy was necessary, using the only intent signal available from the DoD for both safety subsystems. This design, called "intent enablement," was first introduced in the B77/B83 development in the late 1970s. It consisted of using the intent signal both to drive the intent stronglink and to combine with a trajectory-generated signal to drive the trajectory stronglink. Double intent (with trajectory enhancement) was the ideal solution to the problem.

The double-intent trajectory-enhanced architecture requires combination of the second intent Unique Signal with a trajectory-derived signal. For example, a human intent Unique Signal pattern can be combined with a trajectory-generated unique signal pattern in an exclusive-or mixing operation[5] to drive a trajectory stronglink, as shown in Fig. 1.

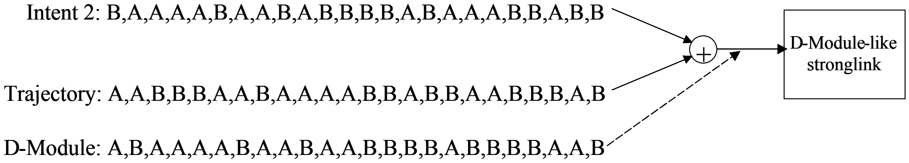

Intent 2: B,A,A,A,A,B,A,A,B,A,B,B,B,B,A,B,A,A,A,B,B,A,B,B
Trajectory: A,A,B,B,B,A,A,B,A,A,A,A,B,B,A,B,B,A,A,B,B,B,A,B
D-Module: A,B,A,A,A,A,B,A,A,B,A,A,B,B,B,B,A,B,B,B,B,A,A,B
+
D-Module-like stronglink

Figure 1. Example of Exclusive-Or Mixing

This example is the implementation specified in the Unique Signal System Design Guide [Ref. 1]. However, other designs have been produced, so the scope of this project was to allow for the possibility that exclusive-or mixing might be implemented for any of the currently used 24-event Unique Signal patterns. All Unique Signal patterns used in this manner are carefully engineered for abnormal-environment safety, meaning that they are intended to be extremely unlikely to be inadvertently generated by almost all processes. For example, they have equal numbers of As and Bs, and the numbers of transition pairs (A followed by A, etc.) are as closely balanced as possible. In addition to a significant number of mathematical constraints, human expert engineering judgment is used to assure Unique Signal patterns are qualitatively extremely good, and these two factors combine to result in only a few acceptable Unique Signal patterns.

A question that has been addressed in various ways, but never comprehensively, is whether or not two "bad" patterns could be combined in an exclusive-or operation to yield an "extremely good" pattern (i.e., whether inadvertent generation of a pattern like the D-Module pattern would be more likely through the exclusive-or inputs, rather than directly). Since for any chosen 24-event Unique Signal pattern, there are 8,388,608 pattern pairs[6] that will combine to give an engineered Unique Signal pattern, it is certain

[5] System designers have usually chosen to represent an "A" as logical "one," and a "B" as logical "0."

[6] This number can be derived by noting that each resultant event can be generated in 2 ways, giving 2^{24} ways to generate a 24-event pattern. However, each pattern appears twice, once as the first operand and once as the second operand, yielding 2^{23} = 8,388,608 pairs.

that not very many of these will have even one extremely good member. The safety concern would be if neither member met even minimal safety criteria.
Considerable effort has been applied in examination of potential pattern pairs that yield a Unique Signal pattern without finding any pairs that were considered safety risks. There is also a mathematical indication that the exclusive-or operation is resistant to input risk, and in fact it is the only known mixing operation that is consistent with abnormal-environment safety [Ref. 2]. In brief summary, consider two inputs, *a* and *b*, that are exclusive-or mixed to yield an output, *c*. If the occurrence of the inputs can be treated probabilistically, the probability that *c* is correct depends on the probabilities that *a* and *b* are correct, as follows:

$$P(c) = P(a)P(b) + [1 - P(a)] \times [1 - P(b)] \qquad (1)$$

If *a* and *b* are represented as deviating from random by an amount α and β, respectively (where α and β are bounded by zero and ± ½) the result becomes:

$$P(c) = (\frac{1}{2} + \alpha)(\frac{1}{2} + \beta) + (\frac{1}{2} - \alpha) \times (\frac{1}{2} - \beta) = \frac{1}{2} + 2\alpha\beta \qquad (2)$$

This indicates that the output tends to be at least as "random" (used here to mean equally likely and independent) as either input. For example, if either input is completely random (α or β equal to zero), the output is random. For non-probabilistic inputs, specific examination of all possible pairs leading to all possible unique signal patterns is apparently required. However, the population previously examined represents a very small portion of the total 8,388,608 pairs. In this project, all pairs were examined.

Project Description

This project was carried out by Roy Baty with guidance from Arlin Cooper. The first goal was to seek any underlying mathematical structure that would make the quality of the results objective rather than subjective. Contributing to the possibility that such a structure could be found was the linear mathematical nature of the exclusive-or function (identical to a Galois Field addition of a two-element field). Working against finding a mathematical structure was the qualitative nature of assessing unique signal patterns. This latter consideration overwhelmed the former, and no useable structure was identified. Although such a structure may be present, it appears very unlikely based on current knowledge, so no further effort on this will be expended as part of the current project.

It was recognized that if a quantitative metric for pattern quality were developed, the operand space of 8,388,608 could be exhaustively searched. The second goal was therefore to develop a trial metric, recognizing that it would probably evolve with time as more is learned about this type of pattern assessment. Considerable effort was expended in development of the metric reported here, but it is not considered "final."

The third goal was to generate a discrete probability density space for the minimum-metric pattern and for the maximum-metric pattern of each operand pair. This was done by artificially constraining the operand patterns' likelihoods to be equal. Since this constraint does not meet the spirit of the abnormal-environment Walske safety criterion (to be met under the extreme condition resulting from any credible accident), a fourth goal was to identify the minimum metric of the maxima for all pairs.

Trial Metric for Unique Signal Pattern Quality

The trial metric used for 24-event unique signal patterns was to equally value four attributes, 1) balanced numbers of each event type, 2) balanced transition pairs, 3) "ideal" (12) number of "runs" of the same event type, and 4) number of run patterns and dissimilarity of run patterns for each event type. The quantitative construction of the metric is specified in Eq. 3[7]:

$$\begin{aligned} M(UQS) &= 0.25(25-\frac{25n}{12})+0.25(\frac{25t_1t_2t_3t_4}{1080})+0.25(25-\frac{25\times|12-r|}{12}) \\ &+0.25\{(\frac{25}{26})[40.1-\sum_{i=1}^{2}\sum_{j=1}^{24}(|r_{ij}-\frac{3}{j}|)]-2[number(r_{1j}=r_{2j})and(r_{1j}\neq 0)]\} \end{aligned} \tag{3}$$

where n is the deviation from 12 of numbers of each event type, t_1, t_2, t_3, and t_4 represent the numbers of each type of transition pair (e.g., AAs, ABs, BAs, BBs), r represents the number of runs, r_{ij} represents the runs of length j for event type i, and the numeric count is the number of non-zero runs of each length that are equal for each type. Each of the four parts to Eq. 3 can range from about zero to 25; the overall metric can range from about 18 to 100 (the "best" score for the metric).

A list of the metrics for a selection of important 24-event Unique Signal patterns[8] is given in Table 1.

Table 1. Metrics for Seven Unique Signal Patterns

UQS ID	C	D	Intent 2	Trajectory	TUQS2	Intent 2*	Trajectory*
Metric	100	96	94	95	94	96	95

[Note: The "*" notation indicates patterns that replaced earlier designs.]

Probability Density Space for Minima and Maxima

The percentage of patterns having a metric score in each range of 0.05 are plotted in Fig. 2, giving the maxima and the minima of the pairs of exclusive-or operands that generate

[7] This metric covers only a very small portion of the considerations that go into selecting unique signal patterns, and does not lend itself to a "percentile" score.

[8] These are the C-Module pattern, the D-Module pattern, the original System 2 Intent 2 and trajectory patterns, the W76-1 trajectory stronglink pattern, and the current System 2 Intent 2 and trajectory patterns, respectively (see Appendix for explicit patterns).

the C-Module pattern. The value of most safety interest is the minimum of the maxima, which is 48.

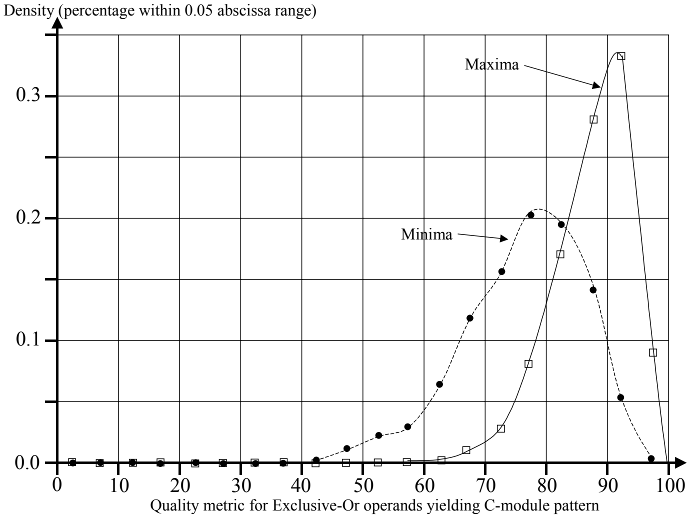


Figure 2. Density Plots for C-Module Metric Minima and Maxima

The percentage of patterns having a metric score in each range of 0.05 are plotted in Figs. 3−8 for the maximum and the minimum for each pair of exclusive-or operands that generate the other six Unique Signal patterns that were examined. The similarity of the plots in Figs. 2−8 hints at an undiscovered mathematical structure. Although some of the functions appear nearly identical on the display scale used for the figures, there was a few percent variation in the exact ordinate values.

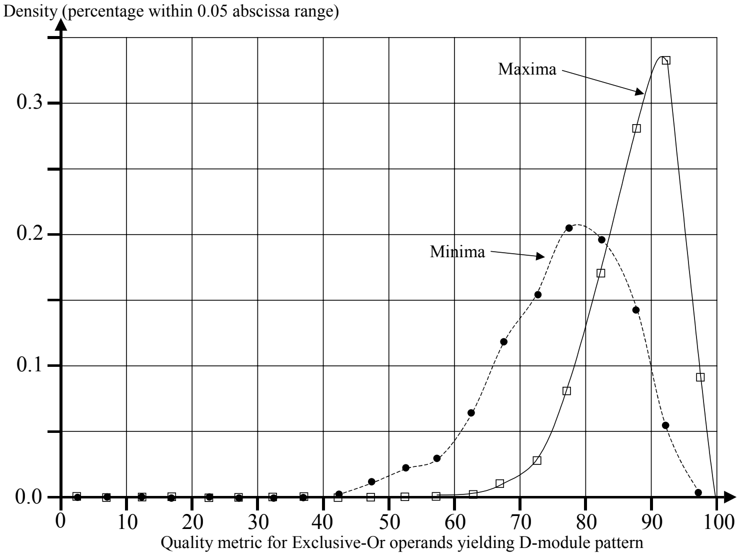


Figure 3. Density Plots for D-Module Metric Minima and Maxima

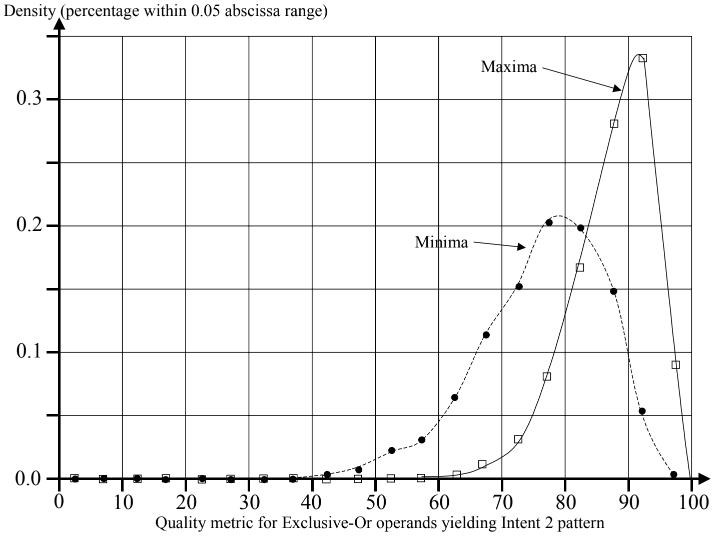


Figure 4. Density Plots for Intent 2 Metric Minima and Maxima

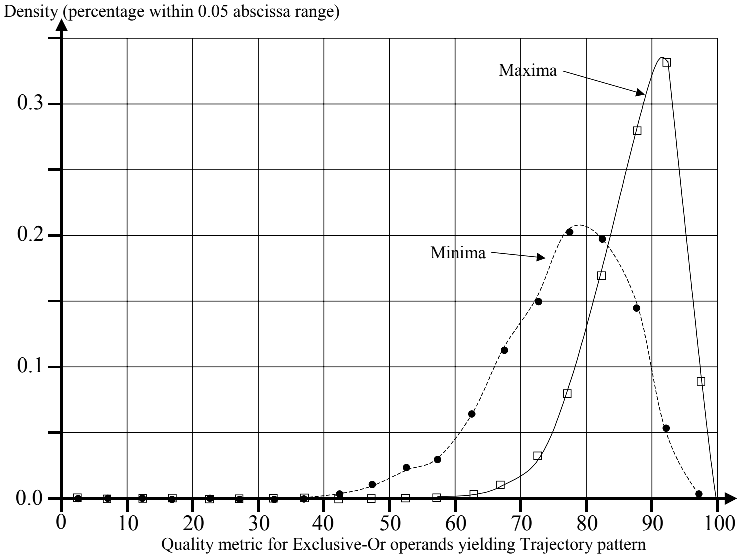


Figure 5. Density Plots for Trajectory Metric Minima and Maxima

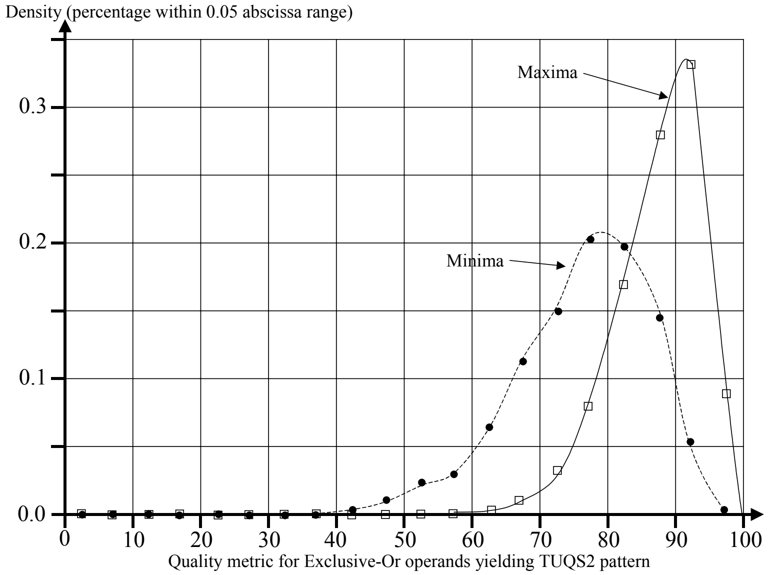


Figure 6. Density Plots for TUQS2 Metric Minima and Maxima

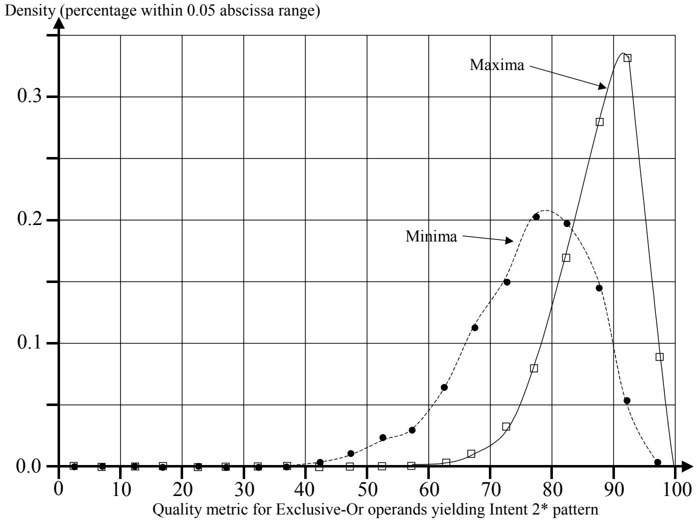


Figure 7. Density Plots for Intent 2* Metric Minima and Maxima

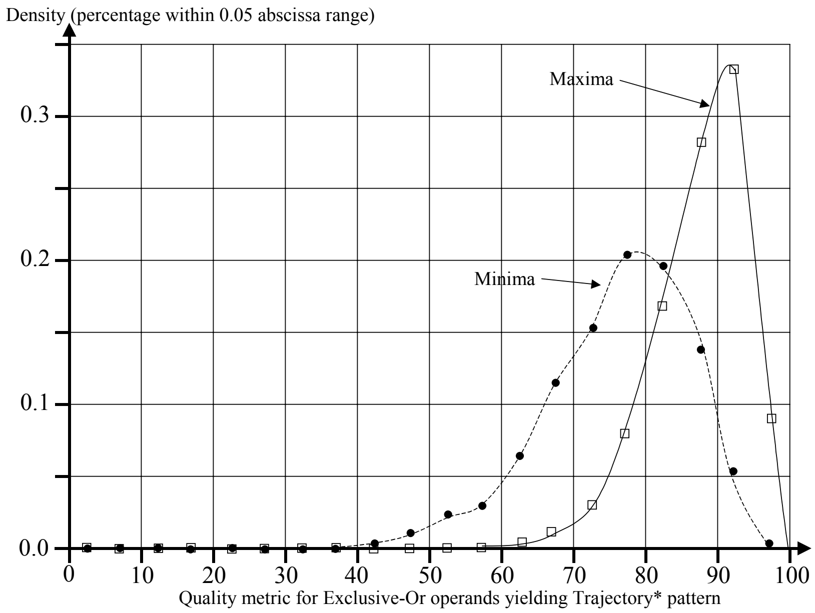


Figure 8. Density Plots for Trajectory* Metric Minima and Maxima

Minimum of the Maxima Operands for 24-Event Unique Signal Patterns

The minimum of the maxima of the potential exclusive-or operands are tabulated in Table 2 for a selection of important Unique Signal patterns.

Table 2. Minimum of Maxima Exclusive-Or Operand Metrics for Unique Signal Patterns

UQS ID	C	D	Intent 2	Trajectory	TUQS2	Intent 2*	Trajectory*
Metric	48	48	47	46	47	47	47

Conclusions

The metrics in Table 2 are not commensurate with ideal Unique Signal patterns, but they are well above the range that we know to be associated with safety-deficiency. In addition, it should be noted that although the safety burden is on the “best” input to the exclusive or function, both inputs must be compromised in order to obtain the inadvertently correct output. One more informative indicator can be derived from the density functions. Although the Walske criterion implies consideration of extremes rather than the range of probabilistic density functions, these plots indicate that scores below 60 for the minimum of the maxima are relatively rare. Based on all of these results, there is no obvious safety concern over the use of exclusive-or mixing. These conclusions depend on the robustness of the chosen trial metric, which has not been fully validated.

References

1. DG10276/A – Implementation of Unique Signal and Related Components, June 24, 2003.
2. Cooper, J. A., "An Assessment of Mixing Multiple-Source Unique Signals," Sandia National Laboratories Report SAND89-2910, June 1990.

Appendix: List of Unique Signal Patterns Examined

(C) C-Module:A,B,B,B,B,A,A,A,B,A,A,A,B,B,A,A,B,B,B,A,B,A,A,B
(D) D-Module:A,B,A,A,A,A,B,A,A,B,A,A,B,B,B,B,A,B,B,B,B,A,A,B
Intent 2: A,A,A,A,B,B,B,A,A,B,B,A,B,B,A,B,A,B,A,A,B,A,B,B
Trajectory: A,B,B,B,A,B,B,A,B,B,B,A,A,A,A,B,B,A,B,A,A,A,B,A
TUQS2: A,B,B,B,A,B,B,A,A,A,A,B,B,A,B,A,B,A,A,B,B,B,A,A
Intent 2*: B,A,A,A,A,B,A,A,B,A,B,B,B,B,A,B,A,A,A,B,B,A,B,B
Trajectory*: B,B,A,A,A,B,B,A,B,B,B,B,A,A,B,A,A,B,B,A,A,A,B,A

Chapter 2. Shift-Register Analysis and Enumeration of 24-Long Bi-Valued Patterns

Anna M. Johnston

1 The Problem

Unique signals (UQS) are used in nuclear weapons to protect against accidental pre-arming of the weapon. A 24-event pattern, where an event comes from a binary set, protects the weapon against abnormal-environments, such as natural phenomena, accidents, equipment malfunctions, etc., which might otherwise cause the pre-arm signal. Although the chances of a natural or accidental event pre-arming the weapon are remote, remote is not good enough for nuclear safety. The 24-event pattern protects against this by creating a sequence most unlikely to appear inadvertently.

Although the events are not true bits, the sequence will be referred to as a binary stream. This simplifies the analysis and facilitates a better understanding of the sequences.

2 The Constraints

The goals placed on the UQS streams are as follows:

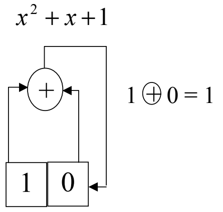
1. 24-long event pattern, represented by **A** and **B** in the final sequence but for simplicity, as binary elements (**0**,**1**) here;
2. Exactly half 0, half 1's;
3. As equal as possible number of digraphs (pairs);
4. At least one each isolated 1 and 0;
5. No 6 long or greater duplicated or complemented substring;
6. No 8 long or greater mirror or complemented mirror substring;
7. No 5 or greater runs;
8. $\Pr(1|0) \approx \Pr(0|0) \approx \Pr(1|1) \approx \Pr(0|1) \approx 0{:}5$.

3 Why not Linear Feedback Shift Registers?

A linear feedback shift register, or LFSR, generates a well behaved, well understood stream of bits. The streams appear random and can be created to match many of the requirements above. Any binary stream of length *n* can be represented by a LFSR of degree less than *n*. The problem with **low** degree LFSR's, or combinations (exclusive-or) of low degree LFSR's is that they can be imitated by nature. For this reason, streams generated by low degree LFSR's should be avoided.

A LFSR uses a driving polynomial of degree *n* and an initial register fill of *n* bits. If the polynomial is $\sum_{i=0}^{n} a_i x^i$, with $a_n = 1$, $a_i \in \{0,1\}$ and an initial fill of $s_0 s_1 \ldots s_{n-1}$ then the *n*-th bit is $s_n = \oplus_{i=0}^{n-1} (a_i \otimes s_i)$ and the (*n* + *t*) bit is $s_{n+t} = \oplus_{i=0}^{n-1} (a_i \otimes s_{i+t})$ [9].

Linear Feedback Shift Register



[9] $\oplus$ and $\otimes$ are GF(2) operators.

For example, the polynomial $x^2 + x + 1$ with initial register of 10 generates the pattern:

1 0 1 1 0 1 1 0 . . .

This polynomial is primitive — that is it generates a $2^n - 1$ long stream (the longest possible) before it repeats. With $n = 2$, the stream repeats every three bits.

A driving polynomial can be either primitive (generating all possible non-zero n-long streams), irreducible (i.e., the driving polynomial can not be factored into smaller degree polynomials), or composite. If the driving polynomial is primitive it will generate the longest bit stream ($2^n - 1$ bits) before repeating. If it is irreducible (primitive polynomials are also irreducible) then it cannot be factored into smaller degree polynomials. If it is composite, the polynomial can be factored into smaller degree polynomials. Streams generated by composite polynomials can also be obtained by adding (exclusive-or) streams generated by its polynomial factors.

For these reasons an important portion of the analysis is to determine the driving polynomial and its factorization.

4 Mapping a Binary Stream to a Driving Polynomial

Given a d-long binary stream, $S_d = s_0 s_1 \ldots s_{d-1}$, the lowest degree polynomial generating it can be determined with the Berlekamp-Massey algorithm (see [2], page 200). The algorithm begins with only a few bits of the stream, finding a polynomial which fits it. It then checks the next bit of the stream to see if it fits the current polynomial. If it does, great! No changes are needed (yet). If it doesn't fit the current polynomial, then the polynomial is modified, possibly increasing the degree, so that it does fit the all bits up to this point.

The Berlekamp-Massey algorithm generates the reciprocal of the driving polynomial. The reciprocal of a polynomial $P(x) = \sum_{i=0}^{n} a_i x^i$ is:

$$R(x) = x^n P(x^{-1}) \sum_{i=o}^{n} a_{n-1} x^i = \sum_{i=0}^{n} r_i x^i$$

Converting the reciprocal, $R(x)$, back to the polynomial, $P(x)$, follows the exact same process:

$$P(x) = x^n R(x^{-1})$$

However, since a_0 may be zero and $r_n = a_0$, there is a chance that the actual degree of R is less than n. Because R represents P, the degree of R will still be considered n even if $r_n = 0$.

Recall that $P(x)$ satisfies the stream $S_t = s_0 s_1 \ldots s_{t-1}$ if:

$$P(S_{(k+n+1)}) = \sum_{i=0}^{n} a_i s_{i+k} = 0$$

for all $0 \le k < t - n$. Letting

$$R(x)|_{s_j} = \sum_{i=0}^{n} r_i s_{(j-1)-i}$$

then $R(x)|s_j = P(S_j)$. The reciprocal (and thus the polynomial) satisfies the stream S_t if $R(x) \mid S_j = 0$ for all $n < j \leq t$. In Berlekamp-Massey, $R_i(x)$ will be the reciprocal polynomial, of degree n_i, which satisfies the sub-stream S_i. If $u < t$ with $R_t(x)|S_{t+1} \neq 0$ and $R_u(x)\ |S_{u+1} \neq 0$, then we know that the polynomial $R_t(x) + x^{t-u}R_u(x)$ has the following properties:

- $x^{t-u} R_u(x)|_{s_{t+1}} = R_u(x)|_{s_{u+1}}$;
- $[R_t(x) + x^{t+u} R_u(x)]|_{s_{t+1}} = [R_t(x)]|_{s_{t+1}} + [x^{t-u} R_u(x)]|_{s_{t+1}} = 0$
- $[R_t(x)]|_{s_j} = [x^{t-u} R_u(x)]|_{s_j} = 0$ for $\max(n_t, t - u + n_u) < j \leq t$.

The polynomial $R_t(x)+x^{t-u}R_u(x)$ satisfies the sub-stream S_{t+1} but it may not have minimal degree. The degree of this polynomial is $\max(n_t, (t - u) + n_u)$. To insure the minimal degree we need to start with a minimal initial n_t, n_u and only update u when it keeps the degree minimal.

Initial minimal R_t, R_u polynomials can be easily derived by noticing that if s_i, s_j with $i < j$ are the first two non-zero bits, then:

1. for S_k with $0 \leq k \leq i$, the stream is all zeros and the minimal polynomial is $R_k(x) = 1$ with degree $n_k = 0$;
2. for S_k for $i < k \leq j$ is $R_k(x) = 1$ with degree $n_k = (i+1)$ (i.e., ignore the first $(i + 1)$ bits).
3. for S_{j+1} the minimal polynomial is $R_{j+1}(x) = 1 + x^{(j-i)}$ with degree $n_{j+1} = \max(i + 1; j - i)$.

The value of t will be $j + 1$ while the value of u will be between zero and j such that $u - n_u$ is minimal. For $0 \leq k \leq i$ the maximal values are $u = i$ with $n_u = 0$. For $i < k \leq j$ the maximal values are $u = j$ with $n_u = i + 1$. Thus if $i - 0 < j - i - 1$, which implies $i + 1 < j - i$, then let $u = j$, $n_u = i + 1$. Otherwise let $u = i$ and $n_u = 0$. Notice that these minimal initial polynomials also have the property that $n_t - 1 = u - n_u$.

With these minimal polynomials to start with, the algorithm next checks to see that $R_t\ |S_{t+1} = 0$. If it is then $R_{t+1} = R_t$ and $n_{t+1} = n_t$ and u remains the same. If $R_t\ |S_{t+1}$ is not zero then R_{t+1} is the updated polynomial:

$$R_{t+1}(x) = R_t(x) + x^{t-u}R_u(x).$$

The u value is changed to t only if $t - n_t > u - n_u$ (notice that this occurs if and only if $t - u + n_u > n_t$, or $n_{t+1} > n_t$). Furthermore the initial relationship of $n_t - 1 = u - n_u$ will be retained by this update:

$$\begin{aligned} n_{t+1} - 1 &= (t - u + n_u) - 1 \\ &= (t - n_t + 1) - 1 \\ &= t - n_t \end{aligned}$$

Since the value of u becomes t, n_u becomes n_t, and t becomes $t + 1$, the relationship remains[1].

Berlekamp-Massey

1. Initial polynomials:
    - Find the first two non-zero bits, s_j , s_k with $j < k$.
    - If $j + 1 < k - j$, then let $u = k$, $n_u = j + 1$; otherwise u = j and $n_u = 0$.
    - Let $t = k + 1$ and $R_t(x) = x^0 + x^{k-j}$ with $n_{k+1} = \max(j + 1; k - j)$.
2. While $t < n$:

[1] This relationship is used in [2] to convert the update condition to $n_t \leq t/2$

```
(a) Compute $d = R_t(x) |_{S_{t+1}}$.
(b) If $d = 1$ then $R_t$ does not fit $S_{t+1}$:
    i. $R_{t+1} = R_t(x) + x^{t-u}R_u(x)$;
    ii. If $t + n_t > u + n_u$, then
            A. $n_{t+1} = t - u + n_u$
            B. $u = t$;
            otherwise $n_{t+1} = n_t$
(c) If $d = 0$ then $R_{t+1} = R_t$ and $n_{t+1} = n_t$.
(d) $t = t + 1$.
```

5 Factoring Polynomials

Once we have the driving polynomial we need to determine its factorization. If the driving polynomial is composite then the stream is actually constructed from the streams generated by its factors. So even if the driving polynomial has a very high degree, its stream may be generated by combining several short repeating streams. For this reason it is important to know the factorization of the driving polynomial.

Berlekamp has another algorithm for factoring polynomials over small fields. The algorithm first reduces the polynomial so that it has no repeated factors (all repeated factors of $f(x)$ are in *gcd* ($f(x)$, $f'(x)$)), then factors the remaining polynomial by using the following theorem (contained in [1], 4.2) :

Theorem 1 *Let f(x) be a monic polynomial over the finite field F_q and $h \in F_q[x]$ is such that $h^q \equiv h$* mod *f(x) then*:

$$f(x) = \prod_{c \in F_q} \gcd(f(x), h(x) - c)$$

For our purposes, we need to find a polynomial over $F_q = GF(2)$ (i.e., whose coefficients are modulo 2), $h(x)$, such that $h(x)^2 \equiv h(x) \bmod f(x)$. Let d be the degree of $f(x)$. Any polynomial modulo $f(x)$ will be a linear combination of the exponents x^k for $k = 0, 1, \ . \ . \ . \ d - 1$. Because h is a polynomial over $GF(2)$, if $h(x) = \sum_{i=0}^{d-1} a_i x^i$ then $h(x)^2 =. \sum_{i=0}^{d-1} a_i x^{2i}$. All other internal coefficients will be multiples of two, and therefore zero modulo two, and $a_i^2 \equiv a_i$ for all $a_i \in GF$ (2). So $h(x)^2 - \text{h(x)} \equiv 0 \bmod f(x)$, implies that the sum $\sum_{i=0}^{d-1} a_i (x^{2i} - x^i) \equiv 0 \bmod f(x)$. We can find such a polynomial h by creating a matrix with column j representing the coefficient of x^j and row i containing $x^{2i} - x^i \bmod f(x)$. Solving for this matrix's null-space will give us the coefficients of $h(x)$. The size of the null space gives us the number of factors of f. There will be at least one factor, more than one if f is composite.

6 A Small Example

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1

Analyzing the polynomial structure of this sample stream has three parts: First, find the generating polynomial using Berlekamp-Massey. Second, factor the polynomial. Finally, determine what streams generated by the factors of the polynomial were used to generate the stream.

6.1 Finding the Minimal Polynomial

Using Berlekamp-Massey on this stream begins with an initial polynomial of $R_2(x)$ = 1 + x, with degree one at step t = 2 and previous polynomial of $R_0(x)$ = 1 with degree zero (u = 0).

t	n_t	R_t		u	n_u	R_u		$R_t \|_{s_{t+1}}$
2	1	[0,1]		0	0	[0]		1
3	2	[0,1,2]		2	1	[0,1]		1
4	2	[0]		2	1	[0,1]		0
5	2	[0]		2	1	[0,1]		0
6	2	[0]		2	1	[0,1]		0
7	2	[0]		2	1	[0,1]		0
8	2	[0]		2	1	[0,1]		0
9	2	[0]		2	1	[0,1]		1
10	8	[0,7,8]		9	2	[0]		1
11	8	[0,1,7,8]		9	2	[0]		0
12	8	[0,1,7,8]		9	2	[0]		0
13	8	[0,1,7,8]		9	2	[0]		0
14	8	[0,1,7,8]		9	2	[0]		0
15	8	[0,1,7,8]		9	2	[0]		0

$$R_{16}(x) = 1 + x^1 + x^7 + x^8 \qquad P(x) = 1 + x^1 + x^7 + x^8$$

The reciprocal polynomial obtained from the Berlekamp-Massey algorithm in this case is the same as the actual polynomial.

6.2 Factoring $P(x)$

The next step in analyzing the stream is to factor $P(x)$. Factoring polynomials over $GF(2)$ is a two step process. The first step is to compute the greatest common divisor of $P(x)$ with its derivative:

$$gcd\ (1 + x + x^7 + x^8,\ 1 + x^6) = (1 + x^2):$$

The greatest common divisor of $P(x)$ is $g(x)$ = $(1+x)^2$ and $P(x)/g(x)$ has no repeated factors. Let $P_1(x)$ = $P(x)/g(x)$ = $x^6+x^5+x^4+x^3+x^2+x+1$, and finish the factoring by finding $r(x)$ mod $P_1(x)$ such that $r(x)^2 \equiv r(x)$ mod $P_1(x)$, and compute gcd ($P_1(x)$, $r(x)$), gcd ($P_1(x)$, $r(x)$ + 1).

Compute $r(x)$ by letting $r(x)$ = $\sum_{i=0}^{n} a_i x^i$ and recalling that $r(x)^2 - r(x) =$ $\sum_{i=0}^{n} a_i (x^{2i} + x^i)$ modulo two. The values for $x^{2i} + x^i$ modulo $P_1(x)$ are as follows:

i	$x^{2i} + x^i \bmod P_1(x)$
1	$x + x^2$
2	$x^2 + x^4$
3	$1 + x^1 + x^2 + x^4 + x^5$
4	$x^1 + x^4$
5	$x^3 + x^5$

Solving the following system produces *r*(*x*):

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

The null space has dimension two (two factors) and is defined by

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The non-trivial polynomial *r*(*x*) is *r*(*x*) = $x^1 + x^2 + x^4$. Computing the greatest common divisors:

$$gcd\,(1 + x + x^2 + x^3 + x^4 + x^5 + x^6;\ x^1 + x^2 + x^4) = 1 + x + x^3$$
$$gcd\,(1 + x + x^2 + x^3 + x^4 + x^5 + x^6;\ 1 + x^1 + x^2 + x^4) = 1 + x^2 + x^3$$

gives the factorization.

6.3 Substream Formation

The initial stream:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1

can be broken into several parts, determined by its generating polynomial's factorization, all exclusive-or'ed together. This is done by solving a simple system of linear equations based on the stream and the generating polynomials.

Let $S^0 = s_0^0 s_1^0 \ldots$ be the stream generated by $(1 + x)^2$, $S^1 = s_0^1 s_1^1 \ldots$ be the stream generated by $1 + x^2 + x^4$, $S^2 = s_0^2 s_1^2 \ldots$ be the stream generated by $1 + x + x^3$, and $S = (s_0^0 \oplus s_0^1 \oplus s_0^2)(s_1^0 \oplus s_1^1 \oplus s_1^2)$ be the full stream. S^0 is uniquely determined by s_0^0, s_1^0, S^1 is uniquely determined by s_0^1, s_1^1, s_2^1, S^2 is uniquely determined by s_0^2, s_1^2, s_2^2, and *S* = 1100000001111111 is known. This gives the following set of equations:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} s_0^0 \\ s_1^0 \\ s_0^1 \\ s_1^1 \\ s_2^1 \\ s_0^2 \\ s_1^2 \\ s_2^2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Solving this system gives:

$$[s_0^0 \quad s_1^0 \quad s_0^1 \quad s_1^1 \quad s_2^1 \quad s_0^2 \quad s_1^2 \quad s_2^2] = [1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$$

which generates the streams:

$(1+x)^2$	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
$1+x+x^3$	1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0
$1+x^2+x^3$	1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1
	1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1

Other forms of inadvertent generation will be investigated in the near future.

7 Partial Enumeration

The 8 conditions required for the streams create a complex enumeration problem. Hard formulas which took in the length of the stream and parameters of the constraints (such as the maximum duplicate sub-stream allowable) may be possible but will be very difficult to find. However, formulas for upper bounds based on one or more of the constraints can be found.

For example, the condition that all the bits are evenly distributed between events gives an upper bound of $\binom{n}{n/2}$. This is the number of *n*-long streams that have equal numbers of both types of events.

Other insights which may tighten bounds:

- All the conditions are independent of event. So if a stream passes all the conditions then so does its complement, its mirror, and its mirror complement.
- An alternative representation (but not an allowed mode of generation!) for the streams is a run listing. For example, the stream 100010100111 could be represented as 1311123. Some of the conditions, such as even bit and digraph counts, are easier to count with this representation. The sum of alternating digits must be the same to have the same number of zeros and ones. In the example above 1 + 1 + 1 + 3 = 3 + 1 + 2. Digraph counts are also easy to compute or create with this format. If there are *k* digits in the run-count representation there are (*k* –1) transition digraphs (i.e., 01 or 10) and (*k* –1)/2 each of 01 and 10 (minor adjustments need to be made if *k* is even): for the example *k* = 7 so there are (7 –1)/2 = 3 each of 01 and 10. For the 00 and 11 digraphs is again the sum of alternating digits, but this time subtracting one from each digit: for the example (1–1) + (1–1) + (1–1) + (3–1) = 2 of the first type and (3 – 1) + (1 – 1) + (2 – 1) = 3 of the second type.

8 Enumeration By Exhaustion

Even though a formula has not yet been derived, the relatively short length of the streams means exhaustion is possible. I wrote code[10] which allows the user to input the various conditions on the streams then intelligently exhausts, outputting the passing streams and statistics on the generating polynomials for these streams.

The code ran with the following restrictions on the streams:

1. 24-long streams;

[10] A similar VAX program was written by Curtis Mueller about 15 years ago.

2. Equal number of ones and zeros;

3. As evenly as possible split of the digraphs (00,11,01,10);

4. The maximum duplicated or duplicated complement substream has length less than 6;

5. The maximum mirror duplicated or mirror complement substream has length less than 8;

6. The maximum run (i.e., adjacent zeros or adjacent ones) length less than 5.

With these restrictions the total number of streams was 356. The degrees of the largest factor of the generating polynomials for these streams were distributed as follows: Total polynomial count:

degree	# of polys.
4	3
5	28
6	47
7	46
8	27
9	36
10	41
11	40
12	83
13	5

Below are a few of the streams generated by the exhaustion. These streams where chosen for examples because they had the highest degree generating polynomials (degree 13).

010010111001101111000100
111000100101000110111100
110111100010010100011001
110101100111000010001011
110100110001001010001111

9 Reports for some chosen streams

Below are some of the UQS streams of some interest:

number	name	stream
1	C-Module	100001110111001100010110
2	D-Module	101111011011000010000110
3	Intent-2	111100011001001010110100
4	Trajectory	100010010001111001011101
5	TUQS2	100010011110010101100011
6	Intent 2*	011110110100001011100100
7	Trajectory*	001110010000110110011101

None of these streams passed all the initial conditions. The following chart describes which stream passes which test:

test	C-mod	D-mod	Int	Traj	TUQS
bit count	✓	✓	✓	✓	✓
equal digraphs	✓	✓	X	✓	✓
isolated 0/1	✓	✓	✓	✓	✓
Substring Equivalent Tests					
Max. < 6	✓	X(6)	✓	✓	✓
Max. comp < 6	X(7)	X(8)	X(7)	X(6)	X(7)

Max. mirror < 8	X(11)	X(15)	X(8)	X(11)	X(12)
Max. mirror comp. < 8	X(14)	X(8)	X(12)	✓	X(14)
Max. run length < 5	✓	✓	✓	✓	✓
Max. degree poly. factor	12	8	6	10	9

9.1 A Few Other Examples

A few other streams which needed to be analyzed are below. These were chosen as examples of bad sequences. Analysis of four of the bad sequences follow:

Stream #	stream
1	111011011010110110111011
2	100101010010000101010010
3	110101101101101111011011
4	100101001001010010100010

None passed the bit count, digraph, or equivalent substring tests, but all passed the isolated 0/1 test, the maximum run length test and the maximum equivalent mirror complement test.

test	1	2	3	4
bit count 0/1	X 7/17	X 15/9	X 7/17	X 15/9
equal digraphs 00/01/10/11	X 0/7/7/9	X 6/8/9/0	X 0/7/7/9	X 6/8/9/0
Isolated 0/1	✓	✓	✓	✓

Substring Equivalent Tests

Max. < 6	X(9)	X(11)	X(10)	X(10)
Max. comp. < 6	✓	X(6)	✓	✓
Max. mirror < 8	X(20)	X(10)	X(16)	X(16)
Max. mirror comp. < 8	✓	✓	✓	✓
Max. run length < 5	✓	✓	✓	✓
Max. degree poly factor	6	8	11	12

10 Summary

Unique Signal event streams are used to prevent natural or accident events from inadvertently pre-arming a weapon. Requirements for the streams were designed to minimize this risk. This analysis was done by a mathematician who does not fully understand all the reasons behind the goals. The analysis done on the given streams did not meet all the goals, which means that either better event sequences exist or that the goals may be improved.

Several programs were written to perform the analysis. An exhaustive search program enables a user to input the length of the stream (less than 32 events) and which of the requirements to place on the stream. The output will be all the streams which pass the requirements, the count of the passing streams, and a statistical summary of the maximal degrees of the factors of the generating polynomials.

Another program generates individual reports for a given stream or checks the chosen requirements. The information in a streams report is:

- the ones and zeros counts;
- the digraph counts;
- the trigraph counts;

- the length of the maximum equivalent substream, equivalent complement, equivalent mirror and equivalent complement mirror substreams;
- the maximum run length (of either ones and zeros);
- it there was an isolated 0/1 event;
- the minimal generating polynomial and its factorization.

The final two pieces of code do the individual tasks of reading in a stream and finding its generating polynomial (and factoring), or reads in a polynomial and finds its factors. This code is available upon request.

References

[1] R. Lild and H. Niederreiter, Finite Fields, Cambridge University Press, second ed., 1997.
[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

Chapter 3. Investigating the Incompatibility between Unique Signal Patterns

Elizabeth Hart

Project Description

Because nuclear weapons systems employ two stronglinks and therefore two unique signals (UQS), there is a concern for assuring that delivery of one UQS does not affect the probability that another UQS could be inadvertently generated. While some work has been done looking at pairs of patterns, there has been no extensive evaluation specific to this question. Under direction from Arlin Cooper, my goal was to write a program that looks for certain similarities between patterns and calculates a "grade" for each pattern from the results of these metrics that might help in judging a pattern's uniqueness in respect to other patterns.

Constraints

This study was limited to an analysis of patterns specified for this study. These are the seven currently used patterns and five additional patterns proposed by Anna Johnston that might be considered for future use. Other patterns that were previously identified as possible candidates were omitted from this study due to lack of time.

The Metrics

Nine metrics were used in evaluating each possible pair of patterns. These metrics are measures of similarities between patterns that ought to be kept to a minimum.

The first metric (M1) looks at how many relative positions in the two patterns contain the same event type and how many contain complement event types. We want this to be a balanced ratio of 12/12 and so for our purposes, 10/14 is the same as 14/10 and so all ratios are expressed with the higher number first. The greatest difference goal is 15/9.

The rest of the metrics are looking for the length of the longest string contained in both patterns of a pair. Four metrics (M1, M2, M6, M7) are looking for strings that are in the same relative position in both patterns. The other four metrics (M3, M4, M8, M9) are looking for strings that are contained anywhere along the length of the patterns. To find this, one pattern is slid along the length of the other and the substrings that line up are examined. Although it is not initially obvious, I discovered that both patterns must slide (or the initial alignment must be offset) in order to locate the longest string. The diagram below is an example that demonstrates this by highlighting the longest similar string found by sliding each pattern.

```
                    C: ABBBBAAABAAABBAABBBABAAB
                       D: ABAAAABAABAABBBBABBBBAAB→
                                   6
                                 versus

                              C: ABBBBAAABAAABBAABBBABAAB→
       D: ABAAAABAABAABBBBABBBBAAB
                                        7
```

The desired maximum for the length of aligned strings is 5 and the goal for maximum length of common strings is 9. There are four types of strings that are looked for: similar strings, as seen above; complement strings, such as ABBA and BAAB; mirrored similar strings (ABBB and BBBA); and mirrored complement strings (BABB and AABA).

Scoring

The problem with combining the results of the metrics into one grade is that we are decided to minimize the result of each individual metric, but maximize the final grade. In order to solve this problem, an inverse relationship based on the smallest possible result for each metric was established. For each metric, the result is turned into a score between 1 and 0, 1 being the best. The general equation used to curve the results is

$$score = \frac{-(x-c)}{24-c} + 1$$

where x is the result for the current pair and c is the "ideal" result for the metric.

The ideal for M1 as stated earlier is a balance of 12/12. The reason behind the ideal of 12/12 is the same as the reason behind the balancing of 12 of each event type. For scoring purposes, the largest number in the ratio is used. For example, a pair that has a ratio of 14/10 event types would be scored off of the 14.

The ideals for the rest of the metrics are based off of the observed results. Metrics were grouped by whether they found aligned sub-strings or any common sub-strings as well as by whether the string was mirrored or not. Looking at the results from all 66 pairs derived from the current selection of 12 patterns, the ideal for each metric group was set at one less than the lowest result found for that group. Specifically, the smallest common string found is of length 5, so c for M4 (similar string) and M5 (inverse string) is set at 4. M8 and M9 use 5, M2 and M3 use 0, and M6 and M7 use 2 as ideals. There is room here for more research in what is truly possible.

Grade

The score from each metric is added to a corresponding subtotal for the patterns in the pair. After all the pairs have been evaluated by all the metrics, the 9 subtotals for each pattern are averaged, weighted and added together to get the "grade" of the pattern. The weights were given to me by Arlin Cooper and are being used on a trial basis. The general formula for this calculation is

$$grade^{p} = \frac{s_1^P}{n-1} * .4 + \frac{s_2^P}{n-1} * .16 + \frac{s_3^P}{n-1} * .16 + \frac{s_4^P}{n-1} * .08 + \frac{s_5^P}{n-1} * .08 + \frac{s_6^P}{n-1} * .04 + \frac{s_7^P}{n-1} * .04 + \frac{s_8^P}{n-1} * .02 + \frac{s_9^P}{n-1} * .02$$

where s_n^p is the subtotal of pattern P for metric n. All grades are between 0 and 1.

Sample Calculations

These are some sample calculations for pattern L.

$$M4_{KL} = 7 \qquad score = \frac{-(7-4)}{24-4} + 1 = 0.85$$

$$s_4^K + = 0.85 \qquad s_4^L + = 0.85$$

$$grade^L = \frac{9.33}{12-1}*.4 + \frac{8.70}{12-1}*.16 + \frac{9.08}{12-1}*.16 + \frac{9.05}{12-1}*.08 + \frac{9.00}{12-1}*.08 + \frac{9.63}{12-1}*.04 + \frac{9.31}{12-1}*.04 + \frac{9.36}{12-1}*.02 + \frac{9.26}{12-1}*.02 = 0.8322$$

Graphs

A graph for each metric is created that displays the results for all pairs. These are useful both as a quick overview of the typical result for a metric as well as a place to look up the results of a specific pair. The graphs indicate the desired maximum by a horizontal line and the results of each pair in a vertical line with the labels of the patterns in the pair underneath. Below are two examples.

```
M2
Determines the length of the longest identical string in the same
relative
position in the two patterns.
```

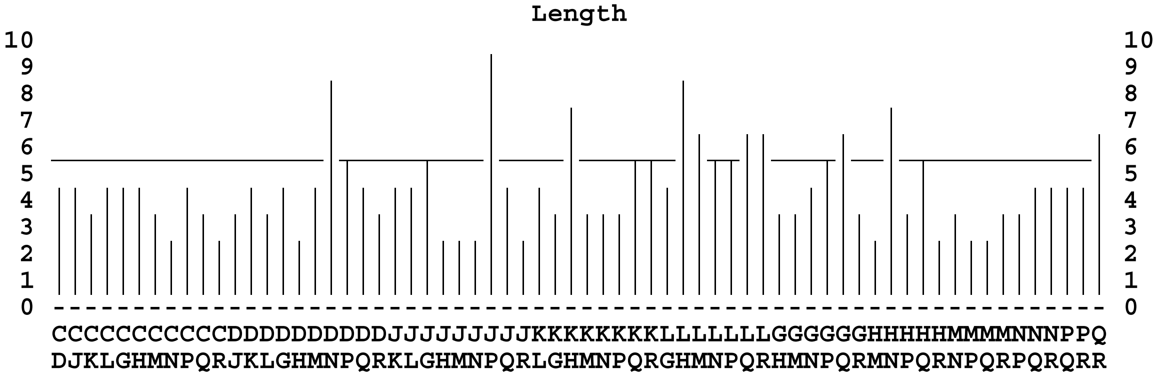


Figure 1. Graph of the M2 Metric

```
                                   M4
Determines the length of the longest identical string in the two
patterns.
```

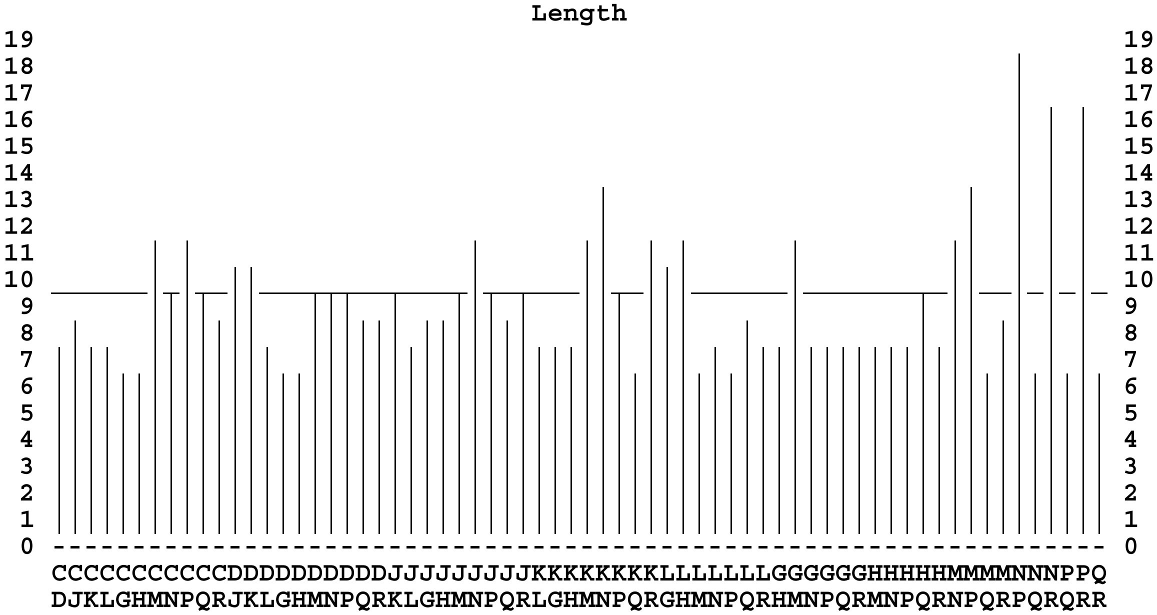


Figure 2. Graph of the M4 Metric

Results

Below are the grades for notable subsets of the population of patterns included in this study. They have been sorted by grade to illustrate the impact that the set has on each pattern's grade.

In Use	
D	0.878703
L	0.865251
J	0.861097
C	0.835089
K	0.829426

In Use and Designed	
C	0.859314
D	0.85928
H	0.85417
J	0.844392
L	0.844208
G	0.839806
K	0.827209

All Studied Patterns	
C	0.854725
D	0.845871
H	0.843968
K	0.841289
M	0.836621
N	0.835738
L	0.832256
P	0.829104
J	0.82869
R	0.816278
G	0.814262
Q	0.796092

In addition to the grades, it is enlightening to look at the results of all the pairs. Only 9 pairs did not violate at least one desired maximum set for the metrics. They are CL, CN, DR, JQ, JR, LQ, GM, NP and NQ. All these pairs include at least one pattern that was discovered by Anna Johnston.

Summary and Future Work

The program allows the user to input the number of patterns desired to be read in from a file and creates a file that lists the patterns evaluated, their corresponding grades and also includes graphs of results for all nine metrics. The code can be requested from Arlin Cooper.

This project is a complement to other work done on UQS patterns. It looked for trends similar to the trends found in individual patterns. The next step in the process of evaluating unique signal patterns is to find a way of combining the many different studies done to grade patterns into a single quantitative analysis.

Patterns Used in Study

C (C-Module): A,B,B,B,B,A,A,A,B,A,A,A,B,B,A,A,B,B,B,A,B,A,A,B
D (D-Module): A,B,A,A,A,A,B,A,A,B,A,A,B,B,B,B,A,B,B,B,B,A,A,B
G (Intent 2): A,A,A,A,B,B,B,A,A,B,B,A,B,B,A,B,A,B,A,A,B,A,B,B
H (Trajectory): A,B,B,B,A,B,B,A,B,B,B,A,A,A,A,B,B,A,B,A,A,A,B,A
J (Intent 2*): B,A,A,A,A,B,A,A,B,A,B,B,B,B,A,B,A,A,A,B,B,A,B,B
K (Trajectory*): B,B,A,A,A,B,B,A,B,B,B,B,A,A,B,A,A,B,B,A,A,A,B,A
L (TUQS2): A,B,B,B,A,B,B,A,A,A,A,B,B,A,B,A,B,A,A,B,B,B,A,A
M: A,B,A,A,B,A,B,B,B,A,A,B,B,A,B,B,B,B,A,A,A,B,A,A
N: B,B,B,A,A,A,B,A,A,B,A,B,A,A,A,B,B,A,B,B,B,B,A,A
P: B,B,A,B,B,B,B,A,A,A,B,A,A,B,A,B,A,A,A,B,B,A,A,B
Q: B,B,A,B,A,B,B,A,A,B,B,B,A,A,A,A,B,A,A,A,B,A,B,B
R: B,B,A,B,A,A,B,B,A,A,A,B,A,A,B,A,B,A,A,A,B,B,B,B

Chapter 4. Toward a Theory of Secure[1] Communications in a Non-Random Environment

Allan L. White, NASA Langley, Hampton, Virginia

Keywords: secure communication, nonrandom noise, Markov models

Abstract

An open problem is to quantify the probability of receiving a given signal from a noisy environment when little is known about the environment's signal generating properties. The signals may have a mix of random, correlated, and deterministic elements. Because of the engineered design of unique signal patterns, inadvertent generation of the patterns requires complex unlikely generators. This paper considers a class of models that can reproduce a mix of random, correlated, and deterministic signals depending on the value of the model's parameters. The approach is to find the parameters that yield the maximum probability of generating a given signal. This maximum probability, because it uses the optimum parameters, is larger than the probability of generating the signal from most noisy environments.

Introduction

At the 20th International System Safety Conference, a representative from Sandia National Laboratories posed a problem (ref. 1) in secure[1] communication in the presence of noise that is neither random nor deterministic (ref. 2). The problem is to devise a signal that is unlikely to be generated by an "accident-induced-structure" when the signal generating properties of the "accident-induced-structure" are ill-defined. Subsequent conversations revealed that the "accident-induced structure" and the signal it generates are likely to have the properties that are listed in a section that describes the noise environment.

This paper discusses the problem from the point of view of discrete Markov models. It is shown that discrete Markov models can generate signals that are "random", that are "deterministic", and that are neither. The memory properties of these models are presented, and an example is given of correlation decreasing with time. After these introductory topics, the paper formulates the general problem in terms of Markov models: for a given signal, find the transition probabilities that maximize the probability of generating the signal.

The combinatorial and probability parts of this problem have been solved, and the matter reduced to an exercise in numerical methods. Unfortunately, it is a difficult problem in numerical methods. It is a search for the maximum value of a function in a very high dimensional space where there are constraints on the domain. For this reason another approach is presented. It attempts to design a signal that forces the optimum jump probabilities to assume certain values.

[1] Editorial note: The author uses "secure" in this material to denote "assured;" there is no security implication.

This work is in an early stage, and it is still contending with the large model problem.

Disclaimer

This work was inspired by and it is hoped it is a contribution to a problem presented by Sandia National Laboratories, but that does not imply that Sandia National Laboratories agrees with or endorses any of the ideas or results in this paper.

Description of the Noise Environment

Signals (arising from noise) are often considered “deterministic” or “random” where “random” implies the outcome is equally likely and is independent of previous outcomes. Given these definitions, we assume the following properties about signals, where a signal is a sequence of A’s and B’s.

1. The more complicated the system needed to produce the signal with a high probability, the less likely the signal.

2. The signals can be a mix of random and deterministic elements.

3. The system can have some memory (which is seen as correlation in the generated signal).

4. Correlation in the signal tends to decrease with time. This is relevant if the signal is high frequency noise, and the detector samples at a low rate. In this case, noise will appear more random.

The original version of property 2 was

> 2b. Deterministic signals are likely. Deterministic signals with a little perturbation are likely. Random signals are likely. Random signals with a little determinism are likely. Signals with an equal mix of determinism and randomness are unlikely.

As shown below, Markov models can handle all five of the conditions mentioned in property 2b by adjusting the jump probabilities. Since our approach to the problem lets the jump probabilities take on arbitrary values, there is no need to distinguish between what is likely and unlikely. It is necessary, however, to demonstrate first that Markov models can handle all of the five conditions, and this is done in the section below.

The Noise Environment and Markov Models

We’ll illustrate modeling the four properties above with discrete Markov chains, which are general random models. “Random” here does not mean equally likely and independent of previous outcomes. In fact, from this point of view, deterministic functions are random variables (with zero variance).

Property 1: The simplest system of interest is a two state model.

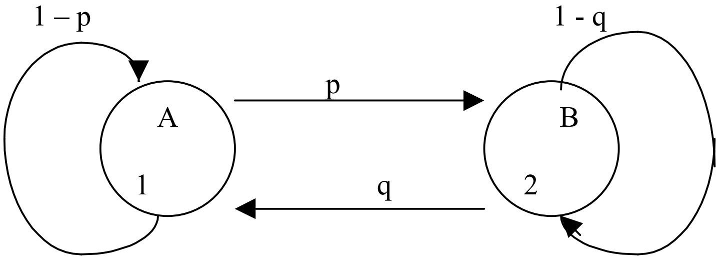


Figure 1 – A Two State, Noise Generating, Markov Model

The states are labeled "1" and "2".

The probability of going from 1 to 2 is p
The probability of going from 1 to 1 is 1-p
The probability of going from 2 to 1 is q
The probability of going from 2 to 2 is 1-q

When the system makes a jump into state 1 (even if the jump is from state 1), the system emits the signal A. When the system makes a jump into state 2, the system emits the signal B.

Property 2: We show that Markov models can handle all the conditions in property 2b. The system in Figure 1 is "deterministic" (for that model) if both p and q are equal to zero or one. The four cases are

p=1; q=1
p=1; q=0
p=0; q=1;
p=0; q=0

The system is "deterministic with a little perturbation" if p and q are close to zero or one.

The system is "random" if p = q = ½. The signal is "random with a little determinism" if p and q are close to ½.

The signal has "an equal mix of randomness and determinism" if p = ½ and q = 0 or 1 (or vice versa).

Property 3: An important property is the amount of memory a system has. An example of a "system" with zero-step memory is flipping a coin. The appearance of H or T does not depend on the outcome of the last (or any) previous flip. A discrete Markov model has one-step memory. The probabilities of the next outcome depend on the current state.

It's possible to embed multi-step memory into a Markov model. Suppose the system always emits precisely BBB, never just a B or BB and never more than three B's in a row. Two methods of accomplishing this are

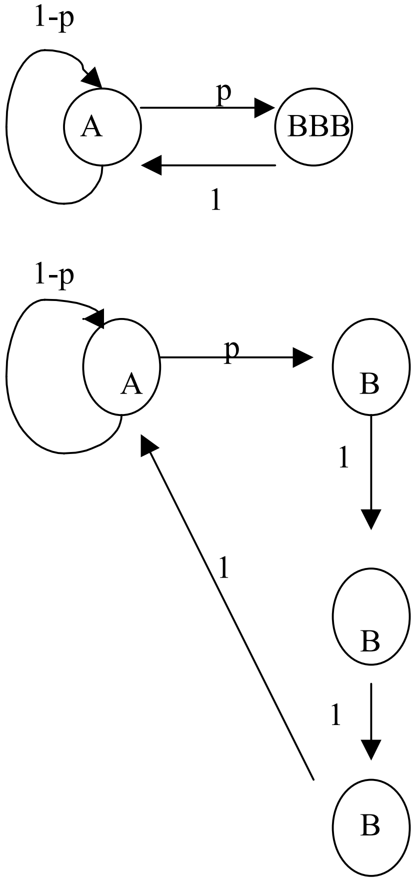


Figure 2 – Two Models That Generate BBB

<u>Property 4</u>: Arrange the transitions in Figure 1 as a matrix. Let $s_i(k)$ be the probability of being in state s_i at time k.

$$\begin{bmatrix} s_1(k+1) \\ s_2(k+1) \end{bmatrix} = \begin{bmatrix} 1-p & q \\ p & 1-q \end{bmatrix} \begin{bmatrix} s_1(k) \\ s_2(k) \end{bmatrix} \tag{1}$$

If $p = q = 0.1$, the system is highly correlated—the system will tend to remain in its current state. Note, however,

$$M = \begin{bmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{bmatrix}$$
$$M^{20} = \begin{bmatrix} 0.51 & 0.49 \\ 0.49 & 0.51 \end{bmatrix} \qquad (2)$$

That is, if the signal is sampled once every twenty times, it will appear nearly "random."

<u>Probability and Model Size</u>: Given a sufficiently large Markov model, any signal can be generated with probability one. Suppose the signal is $Q_1 Q_2 \ldots Q_n$. Consider the model in Figure 3.

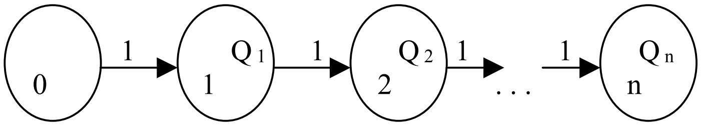


Figure 3 – A Model to Generate a Given Signal with Probability One

Statement of the Problem

The previous section has shown that Markov models can depict all the characteristics listed in the section about the properties of the noise environment. Hence, they are a natural domain for this investigation. Since a sufficiently large model can generate any given signal with probability one, a restriction on size is necessary for there to be any problem at all. By setting transitions equal to zero, a model includes all smaller models

With the above in mind the general problem becomes

> Suppose noise is generated by a Markov model with less than or equal to N states. Suppose the transition probabilities can be any value (between and including zero and one). Find a signal whose probability of being generated is less than some given quantity.

A disadvantage of this formulation is that there can be no correlation between the size of the physical system producing the noise and the size of the Markov model needed to generate the noise with high probability.

The Class of Symmetric Models

We work with a class of symmetric models. They have an even number of states where half of them emit an A when entered and half emit a B when entered. A four state example is given in Figure 4. To avoid clutter, the jumps between states are not labeled.

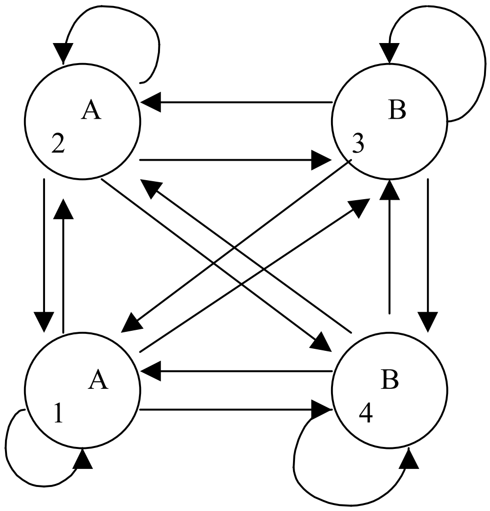


Figure 4 – A Four State Symmetric Model

The notation for jump probabilities is as follows. If the system is in state i at time n then the probability of being in state j at time n+1 is p_{ij}.

We need a method for writing the probability of a string of A's and B's. To this end, let
BK(i,j) = probability of K B's given the system begins in state i and ends in state j. Similarly for AK(i,j).

As an example, for the four state model in Figure 4,

$$B3(2,4) = p_{23}\,p_{33}\,p_{34} + p_{23}\,p_{34}\,p_{44} + p_{24}\,p_{43}\,p_{34} + p_{24}\,p_{44}\,p_{44} \qquad (3)$$

Given the system begins in state 1, the probability of the string AAABBB is

$$A3(1,1)B3(1,3) + A3(1,1)B3(1,4) + A3(1,2)B3(2,3) + A3(1,2)B3(2,4) \qquad (4)$$

Computing the Maximum Probability of Generating a Signal

The method currently being used to find the maximum probability of generating a signal is as follows:

> Given a symmetric model and an initial state,
> write the probability of generating the expression.
> (For instance, equations (3) and (4) above.)
>
> Search for the transition probabilities that maximize the probability.

The search has the constraint that the transitions out of any state must sum to one.

As an example, consider the signal AAABBB and the four state symmetric model with the initial state being state 1. The search found the maximum probability

$$P = 0.23 \tag{5}$$

with the transition values given by the matrix

$$\begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0 \\ 0 & 0.5 & 0.55 & 0.05 \\ 0 & 0 & 0.45 & 0.95 \end{bmatrix} \tag{6}$$

The general problem is a search for the maximum value of a function in a very high dimensional space. For larger models there appear to be plateaus and numerous local maxima.

The Equi-Probable Transition Approach

Finding the optimum parameters for an arbitrary signal becomes arduous for large models. This approach attempts constructing a signal that has a convenient set of optimum transition probabilities. Perhaps the most convenient set is where all transitions have the same probability. An example follows.

Consider the two state model in Figure 1. Suppose the system begins in state 1 and consider the sequence

AB BA AB BA AB BA

We will show that for any values for p and q there is less than one chance in a thousand of this model generating the sequence. This is done by showing that the values that maximize the probability of getting this sequence are $p = q = ½$.

If the system is in state 1, the probability of getting an AB is $p(1-p)$. After generating AB the system is in state 2. If the system is in state 2, the probability of getting a BA is $(1-q)q$. After generating BA the system is in state 1. etc.

Using the derivative to find the value for p that maximizes this probability of AB yields $p = ½$.. A similar argument gives $q = ½$.

This method has not been generalized to larger models.

Summary

A proposed test for signals intended to be generated as “noise” where the noise can be a mix of random, correlated, and deterministic elements was sought. It was shown that discrete Markov models were a productive area for study, because they can generate signals with all of these characteristics. It was also shown that a sufficiently large

Markov model can generate a given signal with probability one, but this property is true of many generator models. Hence, the problem becomes: given a restriction on the size of the Markov model test existing signal patterns and/or produce new signal patterns that can be generated with only a small probability. Two approaches are being considered. The first is based on numerical methods and searches for the jump probabilities that give the maximum probability of generating a specified signal. The second approach attempts to design a signal that forces the optimum jump probabilities to assume certain values. This work is in an initial stage. To date both approaches have been applied to only small models.

References

1. J. A. Cooper, Unique Signal Methodology for Random Response to Non-random Threats, *Proceedings of ISSC 20*, 2002.

2. P. G. Hoel, S. C. Port, and C. J. Stone, Introduction to Stochastic Processes, Houghton Mifflin, Boston, 1972.

Chapter 5. Dependence Threats and Protective Measures

Arlin Cooper

Introduction

The ideal "incompatibility" inherent in the Unique Signal approach assures that inadvertent generation of a Unique Signal is as unlikely as it can be made for a particular number of events and that the assurance can be supported by analysis, since the likelihood can be made to approach that of random inputs [Ref. 1]. This analytically supported incompatibility requires separate-event communication of a carefully engineered pattern. If either the pattern used or the communication technique is compromised, the assurance possible is also compromised. The main reasons for this are that any dependence that is allowed to appear in the pattern or in the communication technique can make the pattern easier to inadvertently generate, and at the same time, weaken the analytical support of the incompatibility metric.

This concept and its importance to abnormal-environment safety has proven difficult to persuasively portray. Part of the reason is that high consequence safety forces attention on the extremes of how bad things can get and part is because scenarios that are constructed to demonstrate the problems cannot be comprehensively general. The protection against "extremes" rather than (or in addition to) "averages" is considered good safety practice. The scenario sensitivity is especially pronounced for abnormal environments, which is the reason that dependence on scenarios has never been part of the Unique Signal concept.

This chapter addresses the relation of dependence to ease of inadvertent generation, and the contribution of separate-event communication to independence and the resultant protection afforded.

Making Unique Signal Patterns Difficult to Inadvertently Generate

The engineered design features in Unique Signal patterns are to introduce "uncertainty" about what next event in a sequence of events might be required to match the pattern. This is analogous to assuring that prescribed generators (that might be designed into a system or inadvertently caused by an abnormal environment) are unable to easily produce the correct sequence, which is otherwise unavailable to the system. For example, oscillations are minimized in Unique Signal patterns, because sources of oscillation are expected to be present in systems or generated in accidents. Linear feedback shift register (LFSR) characteristics are also minimized, because LFSRs are commonly used and relatively easy to generate accidentally. The LFSR property was tested by Anna Johnston's work described in Chapter 2. The ability to produce combinations of patterns that result in a Unique Signal pattern is also minimized. Roy Baty's work described in Chapter 1 was a test of this property. Elizabeth Hart's work described in Chapter 3 also demonstrated constraints that are necessary for groups of patterns in a set. The "ease of generation" property does not correspond comprehensively to mathematical tests, although first-order dependence effects are mathematically precluded by balancing the appearance of pairs. This type of dependence was a key to the Markov state models described by Allan White in Chapter 4. He also clearly demonstrated how dependence effects can be suppressed as communication time increases. This is a key to the protective effects of separate-event communication described later in this chapter. Ease of generation can be further associated with the "dependence" property, as addressed in the next section.

Effects of Dependence in the Absence of Separate-Event Communication

Dependence effects can be a threat to safety, and the threat is especially pronounced where separate-event communication is not implemented. One of the most fundamental illustrations of the effect of dependence is to consider complete pair-wise dependence (duplication) compared to an independent reference condition (e.g., a number of equally likely bi-valued events (*n*), chosen from a binomial distribution). The choices from a binomial distribution are independent. Because of the importance of extremes, the following example emphasizes threats in the vicinity of an inadvertent pattern match. For the binomial distribution, the probability of inadvertently duplicating any particular pattern would be $\frac{1}{2^n}$. The probability of matching all or all but one position would be $\frac{n+1}{2^n}$. The probability of matching all or all but one or all but two positions would be $\frac{n^2+n+2}{2^{n+1}}$, etc.

Consider introducing a dependence of disjoint pairs of events, such as specified below in Eq. 1, where *e*(*n*) signifies event *n*.

$$e(n+1) = e(n) \text{ for odd } n \qquad (1)$$

Here, there are only 12 unconstrained choices, so there are $2^{n/2}$ possible patterns that could be inadvertently generated. If the "unique signal" pattern were one of these, the probability of inadvertently generating it would be $\frac{1}{2^{n/2}}$. The probability of matching all or all but one position would also be $\frac{1}{2^{n/2}}$. The probability of matching all or all but one or all but two positions would be $\frac{\frac{n}{2}+1}{2^{n/2}}$, etc. These results are graphed in Fig. 1 for $n = 24$. The abscissa is plotted logarithmically because the differences are quite large.

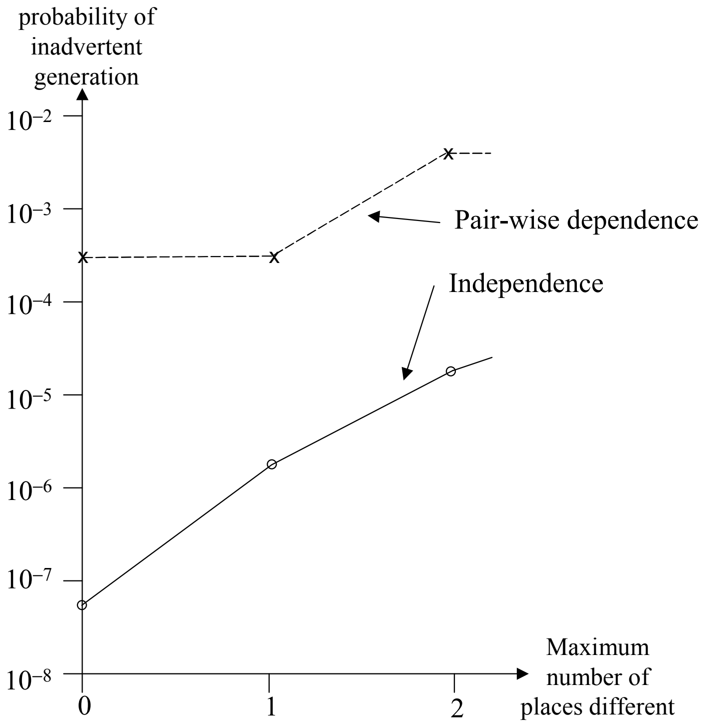


Figure 1. Effect of Pair-Wise Dependence

Although this form of dependence is avoidable through pattern design, it is possible to construct similar examples for any pattern no matter how carefully engineered. As an example, the "D-module" Unique Signal pattern can be generated by a combination of three oscillatory patterns [Ref. 2]. This is described in Eq. 2, below.

$$y = \sin(2.28x - \frac{\Pi}{11}) + 0.855\sin(0.254x - \frac{7\Pi}{9}) + 0.26\sin(1.1x - \frac{\Pi}{8}) \qquad (2)$$

where samples are taken at $x = 0, 1, 2, \ldots$ and A results from $y < 0$ and B results from $y \geq 0$.

It is also possible to prescribe a dependence relation (shown in Eq. 3) that reduces the designed effectiveness of the D-module pattern.

$$e(3n + 3) = e(3n) \qquad [n \text{ odd}] \qquad (3)$$

This relation generates four events in a recursion corresponding to the D-module pattern. Therefore, under this type of dependence, only 20 inadvertent events have to be generated independently in order to generate the 24-event D-module pattern. In summary, engineered pattern design is necessary, but not sufficient, unless separate-event communication is implemented.

Another revealing example is the "random coin-engraving" problem. Consider a coin that is to be engraved with a random choice of "heads" or "tails" on one side and another random choice on the other side. Perhaps counter-intuitively, the probability of particular patterns of *r* outcomes from *r* random coin throws is *not* 2^{-r}. For example, the probability of two heads from two random tosses is 3/8. Figure 2 depicts the re-selection of such coins after *r* tosses until 24 tosses are achieved. The chosen *r* were those that divide 24.

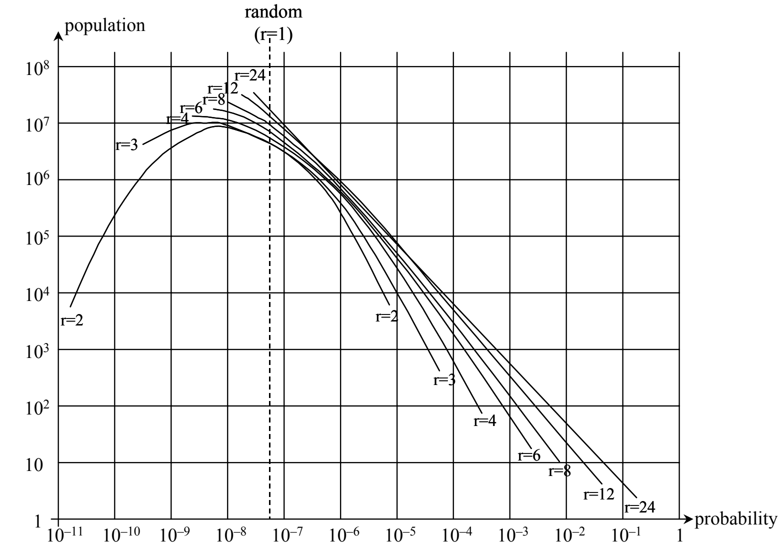


Figure 2. Population Density for Random Coin-Engraving Problem

The results show that "re-setting" the process infrequently (e.g., *r* large) causes distinctly non-random results due to dependence. Frequent re-setting (e.g., *r* small) causes the results to approach random. Separate-Event Communication is intended to cause re-setting between each event ($r = 1$).

Another informative dependence model is to consider a cube with three As and three Bs, such that there is only a single boundary shared between each of the events of each type. The structure is diagrammed in Fig. 3. Topology-wise, there are two arrangements that are possible, but the above definition assures that there is a pair of *B*s on opposite sides of the cube and a pair of *A*s on opposite sides of the cube.

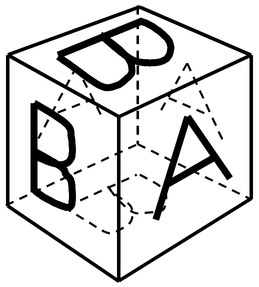


Figure 3. A Cube with Three *A*s and Three *B*s

The example event generation is to give the cube a random throw for a starting position, and then to turn it one position in a randomly chosen direction. The probability of an *A* followed by a *B* is 1/3, which demonstrates the non-random nature of the dependence.

Now consider turning two positions in randomly chosen directions prior to "reading." The probability of an *A* followed by a *B* is 5/24. For three random turns before reading, the probability of an *A* followed by a *B* is 13/48, etc. The actual general result is:

$$P(A,B) = \frac{3\times 2^{s-1} + (-1)^{s-1}}{12\times 2^{s-1}} \tag{4}$$

The result approaches the random expected value (1/4) asymptotically as the number of turns is increased. In other words, the enforcement of letting communication periods pass in between reads has a randomizing effect.

The Effect of Separate-Event Communication on Dependence

The type of dependence illustrated in Eq. 1 can be rendered harmless by a communication capability that could only receive every other event (or only odd events or only even events). This advantage would not be obtained for receiving, for example, every (*n* + 1)th event. From a more practical viewpoint, communication at separate and unrelated times would be sufficient to assure that the dependent pairs of events specified in Eqs. 1-4 would be statistically independent. This is actually true of all types of dependence that have been identified. However, statistically independent time intervals are not easily assured. Adding to this consideration, in the spirit of the Walske requirement, engineered pattern design is also necessary.

References

1. Cooper, J. A., "Mathematical Aspects of Unique Signal Assessment," Sandia National Laboratories Report SAND2002-1306, May 2002.
2. Cooper, J. A., "Dependence Effects in Unique Signal Transmission," Sandia National Laboratories Report SAND88-0394, April 1988.

Prognosis

Although there have been a large number of results obtained by the Unique Signal Mathematics Study Group, a number of interesting challenges remain for assessing deviation from Unique Signal principles. For example, stronglink switches that can have multi-position responses to single event inputs combined with certain environments are known to be capable of producing what appear to be correct unique signal responses with greater than random probability. Exactly how bad the effects are requires solving for the maximum value or values on a multidimensional hyper-surface. There has been considerable work done on this problem without a satisfactory solution. A similar surface maximum problem was cited by Allan White in Chapter 4, in association with the maximum probability of achieving a particular response by a symmetric Markov state model. As another example, Anna Johnston produced an elegant solution for the difficulty of LFSRs producing Unique Signal patterns, but little work has been done on nonlinear generators. One other problem was made more apparent by Elizabeth Hart's work. The assessment of which Unique Signal patterns work well with other patterns obviously depends on the set chosen. The definition of the set of interest is elusive, which makes specification of any potential new patterns difficult. In addition to the set definition problem, the metric determination for rating unique signal patterns as standalone entities and as members of a set is still in an incomplete stage.

Work on these mathematically challenging problems should assure an interesting future.

DISTRIBUTION:

Roy S. Baty
ESA-WSE, MS C936
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545 (3 copies)

Allan White
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681

Carlson, David D.	12300	MS 0428
Johnson, Victor J.	12301	MS 0428
Spray, Stanley D.	12300	MS 0428
Stevens, William L.	12300	MS 0428
Sjulin, Janet M.	12323	MS 0829
Spencer, Floyd W.	12323	MS 0829
Olson, David R.	02912	MS 0647
Chen, Kenneth C.	12332	MS 0492
Cincotta, Harry L.	12332	MS 0492
Dvorack, Michael A.	12335	MS 0830
Mahn, Jeffrey A.	12332	MS 0492
Maloney, Kevin J.	12332	MS 0492
Summers, Daniel A.	12332	MS 0492
Wolcott, James F.	12332	MS 0492
Jones, Todd R.	12333	MS 0405
Anderson, Katherine	12333	MS 0405
Brown, Thomas D.	12333	MS 0405
Camp, Susan E.	12333	MS 0405
Fuentes, Martin K.	12333	MS 0405
Lin, Yau Tang	12333	MS 0405
Pedersen, Ronald D.	12333	MS 0405
Sobolik, Keri B.	12333	MS 0405
Diegert, Kathleen V.	12335	MS 0830
Hoffman, John P. Jr.	12345	MS 0491
Stichman, John H.	2000	MS 0457
Novotny, George C.	2001	MS 0457
Rottler, Stephen J.	2100	MS 0429
Hartwig, Ronald C.	2100	MS 0427
Lucy, Tana B.	2102	MS 0435
Sanders, Gary A.	2103	MS 0453
Harrison, James O.	2111	MS 0447
Hoover, Phil D.	2111	MS 0447
Hillhouse, Aaron L.	2112	MS 0483
Caldwell, Michele	1643	MS 1152

Rosenthal, Mark A.	2114	MS 0481	
Thomas, Danny L.	2114	MS 0481	
Meeks, Kent D.	2131	MS 0482	
Ortiz, Keith	2131	MS 0482	
Callahan, Michael W.	2300	MS 0509	
Plummer, David W.	2330	MS 0503	
Molley, Perry A.	2331	MS 0537	
Brandt, Dale J.	2331	MS 0537	
Laguna, George R.	2333	MS 0533	
Weiss, Douglas R.	2333	MS 0533	
Eilers, Dennis L.	2339	MS 0503	
Cooper, Harold L.	2339	MS 0503	
Deming, Douglas M.	2339	MS 0503	
Kreutzfeld, Richard E.	2613	MS 0319	
Eras, Kenneth.	2613	MS 0319	
Greenwood, William H.	2613	MS 0319	
Randall, Gary T.	2613	MS 0319	
Robinson, Jeffrey A.	12326	MS 0KCP	
Vanecek, Charles W.	2613	MS 0319	
Nicolaysen, Scott D.	2613	MS 0319	
Brown, Jimmy	2613	MS 0319	
Peter, Frank J.	2614	MS 0329	
Murphy, Melissa J.	2900	MS 0469	
Shaw, John D.	2911	MS 0631	
Rogulich, Andrew J.	12326	MS 0638	
D’Antonio, Perry E.	9713	MS 0145	
Tatro, Marjorie L.	6200	MS 0741	
Robinett III, Rush D.	6200	MS 0741	
Kelley, J. Bruce	6245	MS 0734	
Hoover, Eddie R.	6211	MS 1033	
Horschel, Daniel S.	6233	MS 0755	
Perry, Richard L.	6252	MS 0615	
Cooper, J. Arlin	6252	MS 0490	(20)
Covan, John M.	6252	MS 0490	
Ekman, Mark E.	6252	MS 0490	
Kuswa, Glen W.	2954	MS 0635	
Dalton, Larry J.	2662	MS 0860	
McCaughey, Kathleen G.	14400	MS 0868	
Cranwell, Robert M.	15312	MS 1176	
Robinson, David G.	6413	MS 0748	
Camp, Allen L.	6410	MS 0747	
Wyss, Gregory D.	6410	MS 0747	
Trucano, Timothy G.	9211	MS 0819	
Johnston, Anna M.	9215	MS 1110	
DeLaurentis, John M.	9214	MS 1110	
Hendrickson, Bruce	9215	MS 1111	

Ringland, James T.	8112	MS 9201
Henson, Douglas R.	8200	MS 9007
Damkroger, Brian K.	8240	MS 9005
Miller, Russell G.	2820	MS 9005
Van Cleave, Randall A.	8221	MS 9034
Talbot, Edward B.	8222	MS 9036
Hinckley, C. Martin	8231	MS 9007
Brown, Lisa M.	8222	MS 9036
DeVay, Michael	8221	MS 9034
Fonte, Daniel J.	8222	MS 9036
Wichman, Elizabeth C.	8222	MS 9036
Gehmlich, Douglas L.	8241	MS 9014
Johnson, Alice J.	8241	MS 9014
Monson, Robert D.	8243	MS 9108
Molle, Raphael M.	8241	MS 9014
Cashen, Jerry J.	8205	MS 9202
Schroeder, Donald H.	9630	MS 0630
Central Technical Files	8945-1	MS 9018
Technical Library	9616	MS 0899 (2)