Evaluating system reliability with polynomials

Background

Combinatorial vs. State-Space based analytical and simulation methods

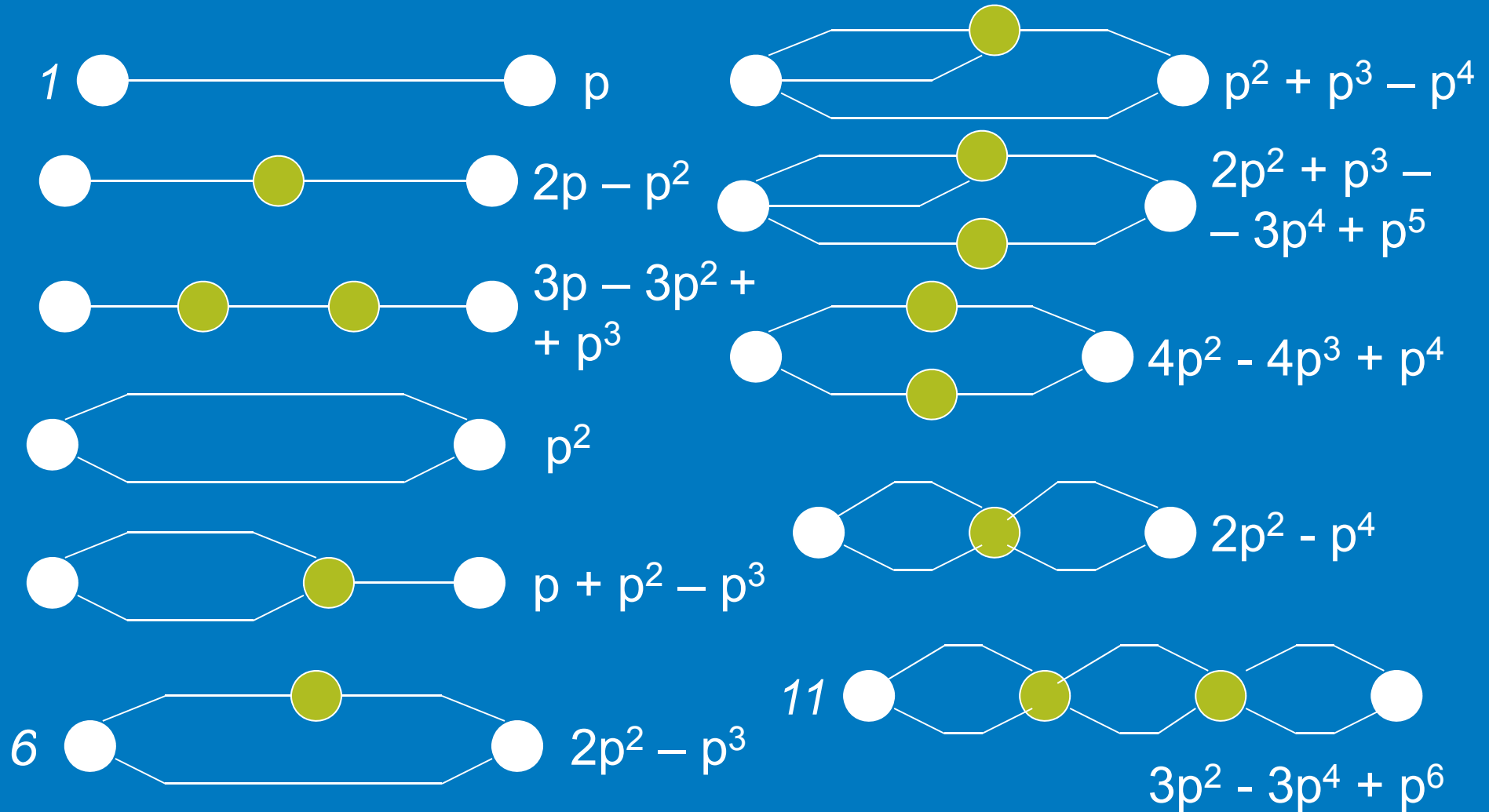**Absence of dependable input data for simulation**

Simplified technique from other domain (analysis of the blocking properties of telephonic switches)
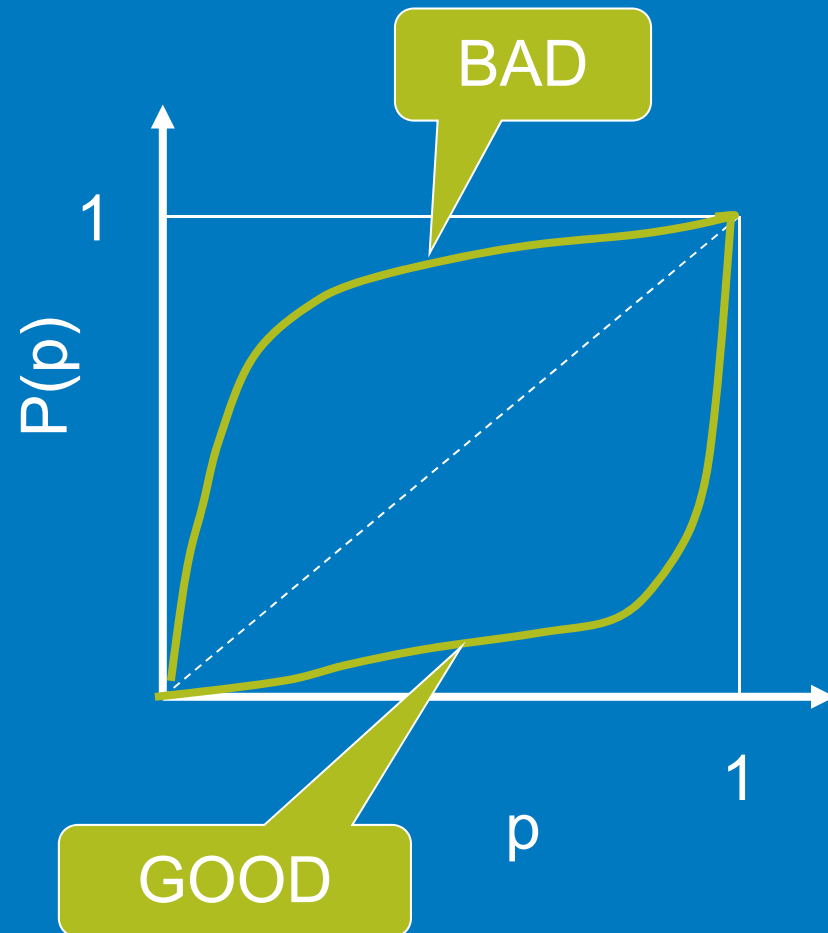
Analogy with forensics

The 'blocking polynomial" to calculate the blocking probability of a switching network with reduced number of crosspoints

MOTOROLA

Simple graphs and corresponding polynomials

1 p

$2p - p^2$

$3p - 3p^2 + p^3$

p^2

$p + p^2 - p^3$

6 $2p^2 - p^3$

$p^2 + p^3 - p^4$

$2p^2 + p^3 - 3p^4 + p^5$

$4p^2 - 4p^3 + p^4$

$2p^2 - p^4$

11 $3p^2 - 3p^4 + p^6$

MOTOROLA

Polynomial Trajectory Space & Figure of Merit

BAD

GOOD

1

P(p)

p

1

p – the blocking or failure probability of the individual links in the graphs

P(p) – the probability of blocking or failure of the overall system

$$F = \int_0^1 P(p)dp$$

$F_1=0.5$
$F_6=0.42$
$F_{11}=0.24$

4

MOTOROLA

Theorems and corollaries

Th 1: The Trajectory Must intersect 0,0 and 1,1

    COROLLARY 1a: The algebraic sum of the coefficients must be Unity

    COROLLARY 1b: p must be a factor

Th 2: The Trajectory Must be Monotonic in Real Bounds

    COROLLARY 2a: There can be no Roots for $0 < p \leq 1$

    COROLLARY 2b: The first derivative must have no roots for $0 < p < 1$

    CORROLARY 2c: The coefficient of the low-order term must be positive

Th 3: The Order of the Polynomial Must be equal to the Number of Links

Th 4: The Number of Sign Changes Must be $\geq$ the Number of Internal Nodes

Th 5: The Order of the Low-Order Term is equal to the Minimum Cross-Section

Th 6: The Coefficient of the Low-Order Term equals the Number of Cutsets of the Minimum Cross-Section.

MOTOROLA

Interpretation w.r.t. reliability

$$a_0p^0 + a_1p^1 + a_2p^2 + \dots + a_np^n$$

Term cannot exist

a_i is the number of Single Points of Failure in the System (and also the slope at the origin)

n is the total number of elements (and roots)
a_n must be ± 1

No. of sign changes is $\geq$ the no. of internal nodes

$\sum a_i = 1$

$F = \int P(p)\, dp$ is the Figure of Merit; best $F \leq \frac{1}{2}$

- The presence of a low-order term of order one indicates that there are single points of failure
- The coefficient of an order one term indicates the number of single points of failure.
- The integral of the polynomial over p indicates the merit of the system with regard to how vulnerable it is to system failure relative to the reliability of its constituents
- The order of the polynomial indicates the total number of significant elements in the system

MOTOROLA

Example 1

System 1 – a switch structure manufactured by a well-known telecommunications equipment manufacturer:

$P(p) = 65536p^{7680} - 524288p^{8160} + 1966080p^{8640} - 4587520p^{9120} + 7454720p^{9600} - 8945664p^{10080} + 8200192p^{10560} - 5857280p^{11040} + 3294720p^{11520} - 1464320p^{12000} + 512512p^{12480} - 139776p^{12960} + 29120p^{13440} - 4480p^{13920} + 480p^{14400} - 32p^{14480} + p^{15360}$

The Figure of Merit of this system is less than 0.0005, meaning that it approaches the ideal in its trajectory

Certain symmetries in this expression are of some interest: note for example that the order of the polynomial (representing the number of elements in the system) is exactly twice the order of the lowest order term (representing the size of the minimum cut set).

MOTOROLA

Example 2

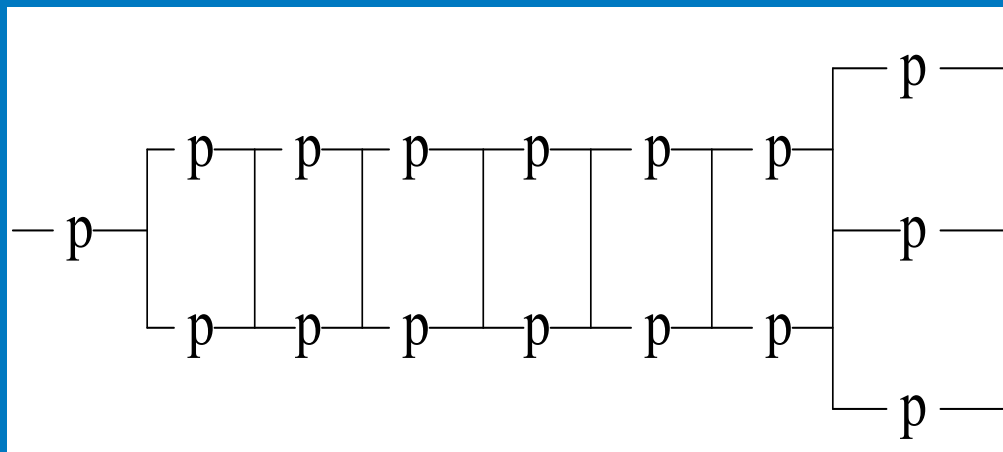**System 2 is a similarly large system deployed in the London Underground.**

$$P(p) = 10p + 2p^2 - 128p^3 + \ldots + 32p^{40} - p^{41}$$

Note that this system has 10 occurrences of single points of failure. It also clearly has 41 elements, and its Figure of Merit is unfortunately significantly above ½.

Example 3

System 3 is a wireless system that was in production for a number of years.


$$P(p) = p + 6p^2 - 5p^3 - 16p^4 + 9p^5 + 26p^6 - 5p^7 - 30p^8 - 5p^9 + 26p^{10} + 9p^{11} - 16p^{12} - 5p^{13} + 6p^{14} + p^{15} - p^{16}$$

There are 16 elements, and 7 internal nodes. It also indicates one single-point-of-failure. F=0.73, significantly above ½.

MOTOROLA

Example 4

System 4 is a design proposed for a wireless system

$P(p) = 2p + 4p^2 - 6p^3 - 13p^4 + 4p^5 + 34p^6 + 12p^7 - 51p^8 - 46p^9 + 38p^{10} + 82p^{11} - 82p^{13} - 38p^{14} + 46p^{15} + 51p^{16} - 12p^{17} - 34p^{18} - 4p^{19} + 13p^{20} + 6p^{21} - 4p^{22} - 2p^{23} + p^{24}$

The number of elements is clear from the polynomial, and the first term picks out the two single points of failure. F=0.78

MOTOROLA

Example 5

Cisco's Catalyst 8540 Switch/Router nominally employed as a multi-service switch that provides Layer 3 and ATM interfaces
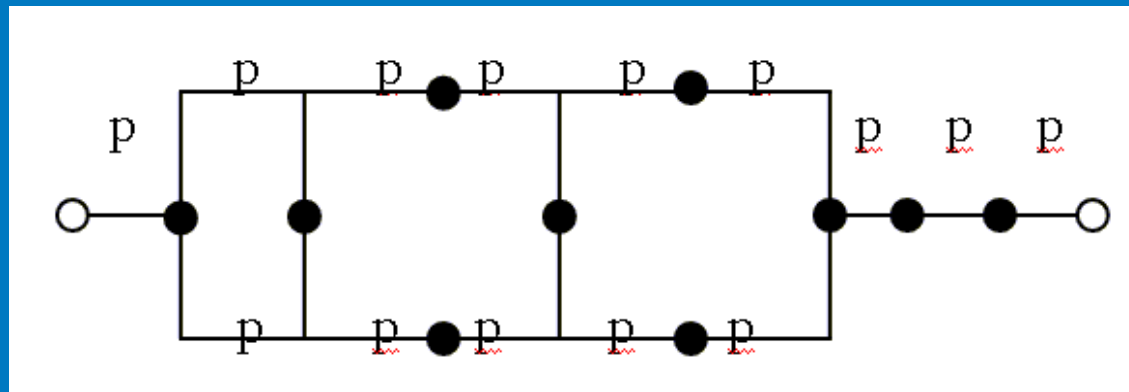
$$P(p) = 4p + 3p^2 - 40p^3 + 63p^4 + 44p^5 - 261p^6 + 336p^7 - 123p^8 - 164p^9 + 257p^{10} - 168p^{11} + 61p^{12} - 12p^{13} + p^{14}$$

The 4 single points of failure are in evidence in the low order term, and F=0.85 (not an attractive number).

MOTOROLA

Reverse problem:
synthesizing a graph from a polynomial

Can we reverse the process by synthesizing a graph from its polynomial?

If it is feasible, it offers the possibility of manipulating the structure of a system in the mathematical domain and synthesizing a better design.

- **Synthesis by Inspection – for gaining insight**
- **Synthesis via Mathematical Manipulation – for complex systems if the manipulation can be done in accordance with a programmable algorithm**

MOTOROLA
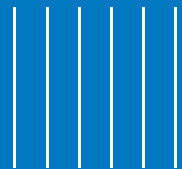
Synthesis via inspection

2 is the number of cuts with min cross-section

3 is the minimal cross-section

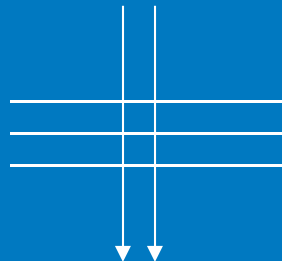7 is the number of elements
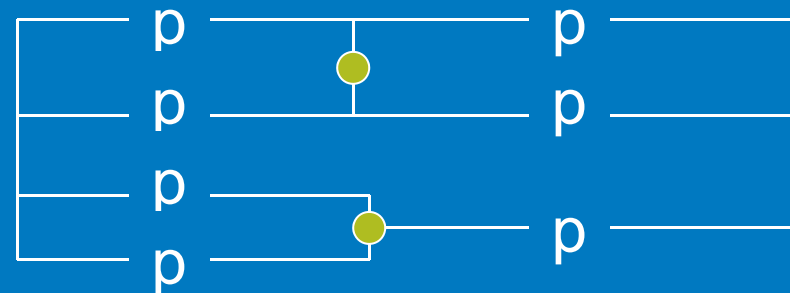
$$2p^3 + 2p^4 - 3p^5 - p^6 + p^7$$

2 – the number of sign changes – is the number of internal nodes

internal nodes

elements

minimal cross-section

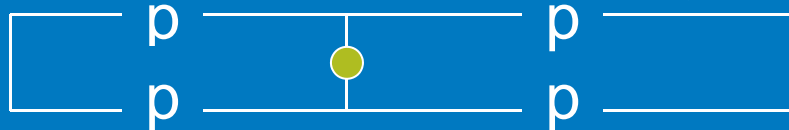cut sets

synthesized graph

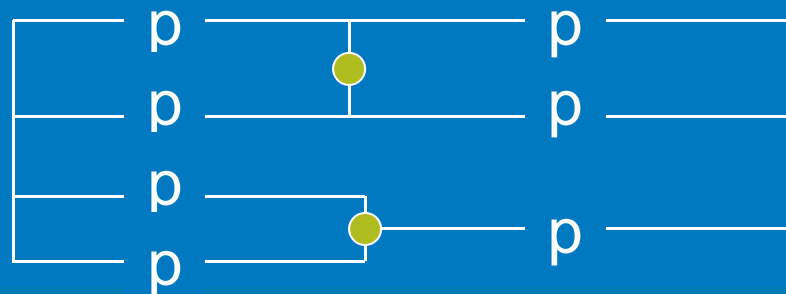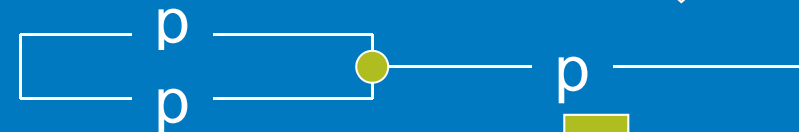**MOTOROLA**

Synthesis via math manipulation

$2p^3 + 2p^4 - 3p^5 - p^6 + p^7 =$

$(2p^2 - p^4)(p + p^2 - p^3)$

2 factors are parallel elements in the graph, each obeying the requirements for realizability; therefore p^2 is not factored out

$2p^2 - p^4 = 1\text{-}1 + 2p^2 - p^4 =$

$1 - (1 - p^2)(1 - p^2)$

$p + p^2 - p^3 = 1\text{-}1 + p + p^2 - p^3 =$

$1 - (1 - p)(1 - p^2)$

MOTOROLA

Exercise for synthesis
(two examples from Trivedi "Redbook" [4])

$$3p - 2p^2 - p^3 + p^5 + 2p^6 - 3p^7 + p^8$$

$$2p^2 + p^3 - 3p^5 - 2p^6 + 3p^7 + 2p^9 - 3p^{10} + p^{11}$$

MOTOROLA

DNA analogy

$$2p^3 + 2p^4 - 3p^5 - p^6 + p^7$$

Representing a polynomial with its vector of coefficients

0   0   0   2   2   -3   -1   1

All the properties of the polynomial are represented by this vector, which can be viewed as being analogous to a DNA strand because it uniquely represents a dependency graph of a system.

Simple manipulations of such vectors can be readily interpreted: e.g., shifting one place to the right (DNA tampering) creates a new graph with a single element in parallel with the entire former graph

MOTOROLA

Genome analogy

Would it be possible (and useful) to enumerate all (within bounds) DNA analogy strands?

1) **This does not mean identifying all polynomials of order less than or equal to a given value (reliability polynomials make up a relatively tiny subset of these).**

2) **Having the DNA strands of all reliability polynomials of, say, order 64 or less, would capture the structures of essentially all existing and foreseeable systems. It would be relatively easy to catalog the characteristics of each (e.g., the number of elements, the number of single-points-of-failure, the Figure of Merit, etc.) for selection.**

MOTOROLA

Metamorphosis under failure
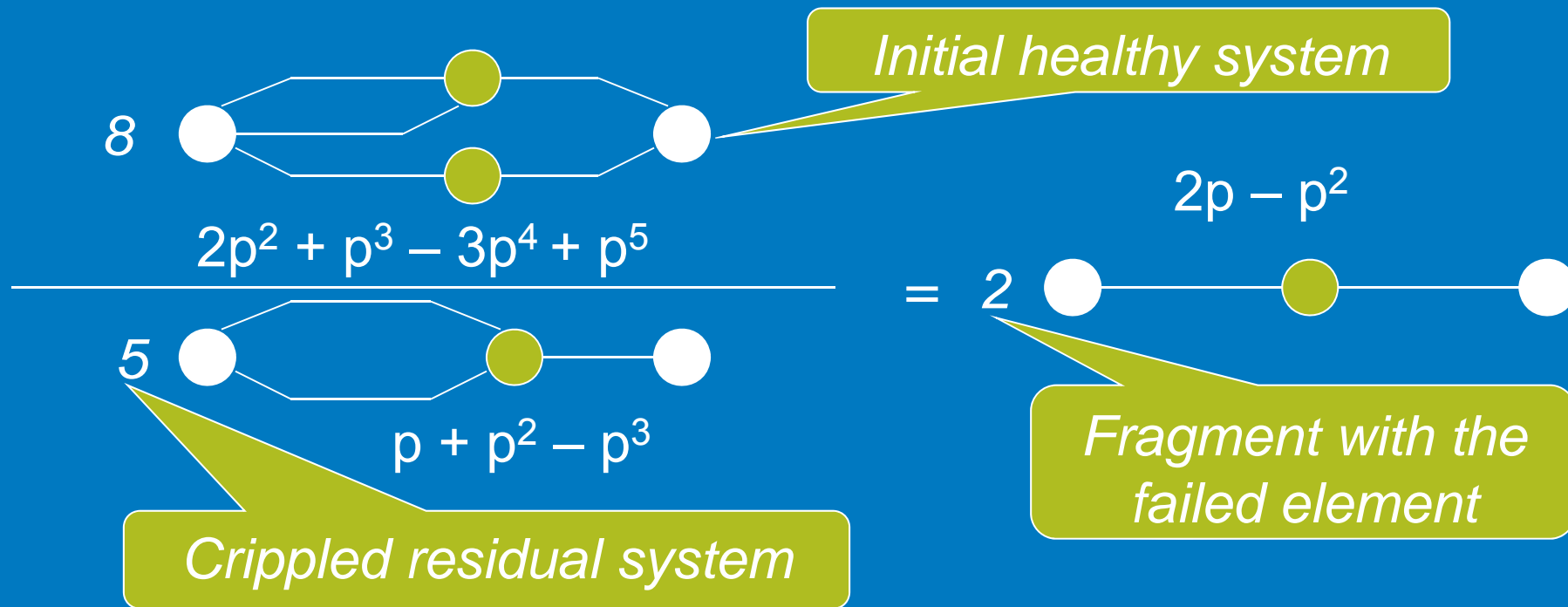

Multiple failure

MOTOROLA
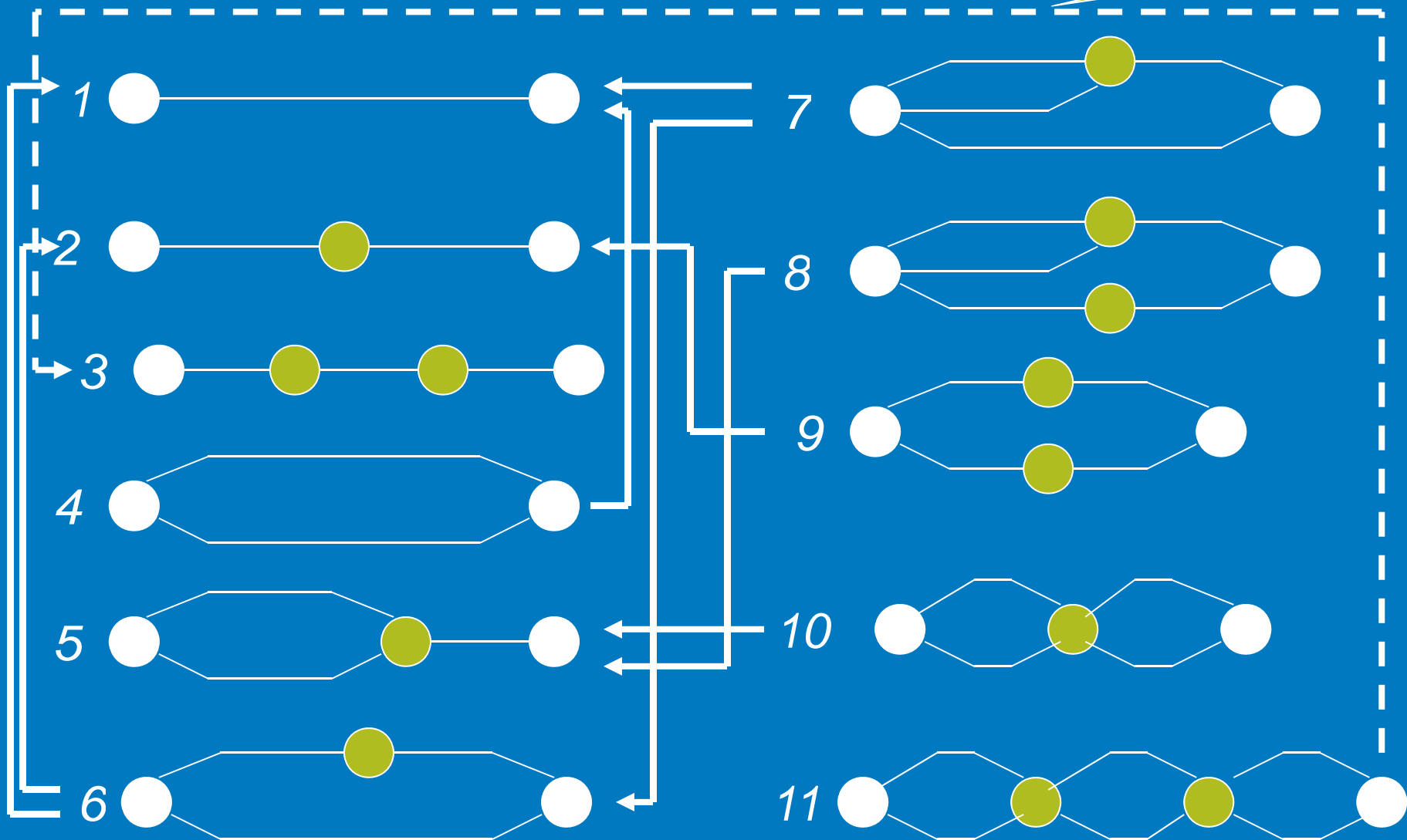
Real failure probability numbers

Eventually, as a design takes shape, there is interest in putting flesh upon the bones (as firm reliability numbers for system elements become available). There is no problem in substituting real numbers in the calculations at some point, after the strength of the skeleton has been tested.

Alternatively, all element failure probabilities can be parameterized as individual variables, and multivariate algebraic systems can be employed for further analysis.

MOTOROLA

Potential diagnostic capability

Initial healthy system

8

$$\frac{2p^2 + p^3 - 3p^4 + p^5}{p + p^2 - p^3} = 2 \cdot (2p - p^2)$$

5

Crippled residual system

Fragment with the failed element

It is often true that the crippled system's reliability polynomial is a factor of the reliability polynomial of the healthy system that spawned it, so that division of the healthy system's polynomial by the crippled system's polynomial will yield the polynomial of the system fragment containing the failed element.

MOTOROLA

Conclusions

This is a tool for gaining insight into the merits of a system from the point of view of reliability. It looks at a mathematical representation of system structure that identified weaknesses and strengths, and explored the possibilities of manipulation in the mathematical domain and subsequent synthesis of improved systems.

It is possible, using the tools described, to gain considerable insight into the merit of a system design relative to the probability of failure and its resilience in the face of element reliability variation.

The technique can be of particular value early in the design process, when individual element reliabilities are unknown: if a design proves inadequate under this analysis technique, it has little hope of proving adequate under more sophisticated, state-space analysis. In that sense, it could serve as a gating technique towards the use of more refined analytical methods.

It is also in the realm of possibility to determine improvements that can be made to a design, and synthesize the corresponding improved design.

Identifying system structures by their DNA holds merit, as does classification of structures within a finite Genome of structures.

MOTOROLA

Next steps

It is intended that these techniques be applied to a number of system architectures early in their design phase.

Application of multivariate algebras to the generalized case of individual element parameters is also envisioned.

Formulating a generalized approach to decomposition of non-series-parallel structures for analytical purposes is another goal.

These analytical techniques may be crystallized into a software tool for system architects.

Pursuit of the System Structure Genome will be aided by this tool.

MOTOROLA

References

[1] Bruce Briley, "A New Approach to Switching Network Synthesis," *International Conference on Communications Technology*, Shanghai, PRC, 1994.

[2] Manoj Chari and Charles Colbourn, "Reliability Polynomials: A Survey*," Journal of Combinatorics, Information & System Sciences*, Vol. 22, Nos. 3-4, 1997, pp. 177-193.

[3] Chris Oggerino, *High Availability Network Fundamentals*, Cisco Press, 200a, ISBN 1-58713-017-3, p. 126.

[4] R. Sahner, K.S. Trivedi, A. Puliafito, *Performance and Reliability Analysis of Computer Systems*, Kluwer, 1996, ISBN 0-7923-9650-2.

[5] X-by-Wire Consortium Team, "X-by-Wire, Safety Related Fault-Tolerant Systems in Vehicles," Project No. BE95/1359, 1998.

[6] Patrick D.T. O'Connor, "Commentary: Reliability – Past, Present and Future," *IEEE Transactions on Reliability*, Vol. 49, No. 4, Dec., 2000, pp. 335-341.

MOTOROLA