Proceedings of Symposia in Pure Mathematics
Volume 50 (1990)

Developments in "The Synthesis of Reliable Organisms from Unreliable Components"

NICHOLAS PIPPENGER

Abstract. In a series of lectures given at the California Institute of Technology in 1952, John von Neumann laid the foundations of the theory of reliable computation by machines built from unreliable components. This paper surveys the developments that have taken place in the theory since that time.

1. Introduction. In January 1952, John von Neumann gave a series of five lectures at the California Institute of Technology. Notes of these lectures were revised by von Neumann and published in 1956 [**vN56**]. It is fair to say that von Neumann's paper founded the theory of reliable computation with unreliable components. The goal of this paper is to give an account of the developments that have taken place in that theory.

Von Neumann's paper, like his earlier *The general and logical theory of automata* [**vN51a**], his later *The computer and the brain* [**vN58**], and the posthumously published *Theory of self-reproducing automata* [**vN66**], was written in heady times, the fragrance of which can still be savored in Wiener's *Cybernetics* [**Wie48**]. It was a time of heightened optimism about the prospects for understanding communication, computation, observation, control, self-correction, and self-reproduction, both in natural and artificial systems, and a time of growing awareness of the interrelationships among them. Von Neumann's bibliography in [**vN56**] cites papers by Kleene [**Kl56**], McCulloch and Pitts [**McCP43**], Shannon [**Sh48**], Szilard [**Sz29**], and Turing [**Tu36**], and emphasizes the connections among mathematics, physics, and biology.

2. Von Neumann's model. To study reliable computation with unreliable components presupposes a satisfactory model for computation with reliable

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 68M15, 94C10; Secondary 03B48, 68Q80, 82A25, 82A60, 94B30.

This paper is in final form and no version of it will be submitted for publication elsewhere.

0082-0717/90 $1.00 + $.25 per page

components. The model used by von Neumann is roughly speaking the "neural net" of McCulloch and Pitts [McCP43], with the adjunction of a finite probability space to model the failures of components. Since the neural nets he discusses are all in fact "combinational" in nature, most later workers have used a model that is inherently combinational, such as the "network of gates" of Muller [Mul56], and we shall follow that practice here.

A precise discussion of errors in networks of gates requires a distinction between two types of errors, which (following a suggestion of Peter Gács) we shall call "failures" and "deviations". If the output of a gate is not what we expect from the inputs to that gate, we shall say that the gate "fails". If the output of a gate is not what we expect from the inputs to the network, we shall say that the output "deviates"; this may be due to a failure of that gate or to the propagation of failures from antecedent gates.

The occurrence of deviations may depend on the inputs to the network as well as on the locations of failures. We shall always be interested in the reliability of the network for the least favorable choice of the inputs. Thus we assume that an adversary to the network, with knowledge of the network, chooses the inputs to the network; then the failures are determined by a process to be described below.

The question of how to model failures is not completely straightforward; consider the following two quotations from [vN56].

> It is the author's conviction, voiced over many years, that error should be treated by thermodynamical methods, and be the subject of a thermodynamical theory, as information has been, by the work of L. Szilard and C. E. Shannon [...].
>
> The simplest assumption concerning errors is this: With every basic organ is associated a positive number ε such that in any operation, the organ will fail to function correctly with the (precise) probability ε. This malfunctioning is assumed to occur statistically independently of the general state of the network and of the occurrence of other malfunctions. A more general assumption, which is a good deal more realistic, is this: The malfunctions are statistically dependent on the general state of the network and on each other. In any particular state, however, a malfunction of the basic organ in question has a probability [...] which is $\leq \varepsilon$.

Here we have a statement of philosophy together with two concrete models. The philosophy is certainly consistent with that adopted by Wiener [Wie49] and Shannon [Sh48], in which "noise", the source of unreliability, is modeled as a random process with known parameters. Von Neumann's first model, with its parenthetical "precisely", adheres to this philosophy: the gates behave unreliably, but they can be relied upon to behave unreliably! If the value

of ε is sufficiently small, then von Neumann shows that such gates can be assembled to form a network that simulates (except with a modest probability of deviation) a given network of perfectly reliable gates. But gates with probability of failure precisely ε can also be assembled to form "random number generators" with known statistical properties. Now random number generators can in many cases be eliminated from networks of perfectly reliable gates (see Adleman [Ad78]), but it seems unlikely that this elimination can be accomplished without substantial increase in size. In any event, in this model it is certainly not true that a network that computes reliably in the presence of failures would necessarily continue to do so in their absence. Thus, in this first model, the failures add to as well as detract from the computational resources.

The second, more "realistic" model, is ambiguous because of the phrase "general state of the network". When this ambiguity is resolved in what seems the most natural way, the counterintuitive features of the first model disappear, and some new attractive features (which will be mentioned later) replace them. (For a more complete discussion of the relationships among these and other models, see Pippenger [Pi88b].) This second model is not completely consistent with the "thermodynamic" philosophy, however; the arbitrary dependence of probabilities on the general state of the network has an adversarial aspect akin to that of "Maxwell's demon".

Fortunately, it is not necessary to resolve the disparity between these two models. All of the negative results we shall discuss can be formulated for the first model, and all of the positive results for the second, so each result is automatically applicable to the other model.

An attractive feature of von Neumann's model is that it assumes the failure probability of the components to be fixed while contemplating arbitrarily large networks; thus, larger and larger networks must tolerate more and more failures. This may be contrasted with studies of networks that tolerate a fixed number of failures, independent of the size of the network, or which tolerate a large number of failures only if they are well dispersed. Such schemes include the well-known "triple-modular redundancy" (Lyons and Vanderkulk [LV62]) and "quadded logic" (Tryon [Tr60], [Tr62]), as well as some schemes related to error-correcting codes (see Armstrong [Ar61] and Ray-Chaudhuri [R61], for example). Von Neumann's model also assumes that all gates are unreliable; this contrasts with theories in which some reliable gates may also be used in critical portions of the network (see Muchnik and Gindikin [MucG62], Kirienko [Ki64, Ki70], Ulig [U74], and Ortyukov [Or78] for results along these lines).

Another feature of von Neumann's model is that it considers the evaluation of a Boolean function on one set of Boolean arguments, rather than considering the evaluation of one function on many disjoint sets of arguments. This feature is best understood by consulting works that take a contrary stand, such as Winograd and Cowan [WinC63], in the light of subsequent results

concerning the evaluation of functions on many disjoint sets of arguments (see Ulig [U74] and Paul [Pa76]).

3. Computability and complexity. The main result that is proved in von Neumann's paper is the following. Fix a basis B of Boolean functions (we shall always assume B to be finite, and "complete" in the sense of Post [Po41]). For all sufficiently small $\varepsilon > 0$, there exists a $\delta < 1/2$ with the following property. Every Boolean function is computed by a network over B that deviates with probability at most δ when its gates fail with probability at most ε. The supremum of the ε for which there exists such a $\delta < 1/2$ will be denoted $\varepsilon_0(B)$. For $0 < \varepsilon < \varepsilon_0(B)$, the infimum of the δ with the cited property will be denoted $\delta_0(B, \varepsilon)$.

Three prominent features of von Neumann's argument are (1) that $\varepsilon_0(B) < 1/2$ for all finite bases B, (2) that $\delta_0(B, \varepsilon) > \varepsilon$ for all $0 < \varepsilon < \varepsilon_0(B)$, and (3) the network of unreliable gates may have greater depth (or "delay"), by a constant factor depending on B, ε, and δ, than a network of reliable gates computing the same function. This situation is in marked contrast with that of reliable communication over an unreliable channel. There, a channel (say, a binary symmetric channel with error probability ε) has a positive capacity $C(\varepsilon) = 1 + \varepsilon \log_2 \varepsilon + (1 - \varepsilon) \log_2 (1 - \varepsilon)$ for all $\varepsilon < 1/2$, and any probability of incorrect decoding $\delta > 0$ is achievable (see Shannon [Sh48]). This contrast is evidently due to the fact that in the case of communication, it is assumed that coding and decoding can be performed without error, while in the case of computation, any coding and decoding must be done by components that are themselves subject to failure.

It is natural to ask whether this contrast is inherent, or whether it might be avoided by some more sophisticated argument. Pippenger [Pi88a] showed that for any finite, complete basis B, $\varepsilon_0(B)$ is bounded below $1/2$, at least if the computation is done by a formula with unreliable gates, rather than a network (a formula is a network in which the output of any gate serves as an input to at most one other gate). Furthermore, the ratio of the depth of the unreliable formula to that of a reliable formula is bounded above 1. Feder [F88] has extended these results to networks, and also shown that $\delta_0(B, \varepsilon)$ is bounded above ε in this case. Unfortunately, all of these negative results differ quantitatively from the positive results that emerge from von Neumann's analysis, even when this analysis is carried to its natural limit (see Pippenger [Pi87]). Indeed, while the negative results give bounds that are analytic functions of ε (like Shannon's capacity), the positive result gives a ratio of unreliable depth to reliable depth that is a "devil's staircase" function: a function that is monotonic and continuous, but constant throughout each of a countably infinite collection of intervals.

After establishing the possibility of reliable computation with unreliable components and ascertaining the effect on depth, von Neumann turned to assessing the effect on the size (or "cost") of the network. He came to the

conclusion that a function computed by a network of l reliable gates could be computed by a network of $O(l \log l)$ unreliable gates (where the constant implicit in the O-notation depends on B, ε, and δ). He drew this conclusion by considering a method of converting a network of reliable gates into one of unreliable gates by (1) replacing each reliable gate by an "executive organ" comprising $O(\log l)$ unreliable gates; (2) replacing each wire by a "bundle" of $O(\log l)$ wires; and (3) introducing "restoring organs" (comprising $O(\log l)$ unreliable gates) that correct the deviations caused by the executive organs. The analysis he gave is not entirely satisfactory, however; it considers the operation of the network for a single choice of the inputs, and assumes that certain interconnections are made "at random" in the restoring organ. Now there must be a particular pattern of interconnection that performs as well as the average pattern for a particular input, but there is no guarantee that the same pattern of interconnection will perform well for all inputs. Thus this argument cannot deal with a situation where the input to the network is chosen by an adversary with knowledge of the network, as we have assumed in our models.

A rigorous proof for these models was given by Dobrushin and Ortyukov [DO77b]. They also give an example of a function of n arguments (namely, the sum modulo 2 of n arguments) computed by a network of $O(n)$ reliable gates but requiring $\Omega(n \log n)$ unreliable gates. (As is customary in computer science, we use $\Omega(\ldots)$ to denote a lower bound that holds "eventually", rather than merely "frequently".) Pippenger [Pi85], on the other hand, gives an example of a function requiring $O(n)$ gates, whether reliable or unreliable. It seems to be difficult to give any simple criterion for when the extra logarithm appears.

It should be mentioned that the method of [DO77a] cannot give a lower bound larger than $\Omega(n \log n)$, and in particular cannot give $\Omega(l \log l)$ unless $l = O(n)$. It would be of interest to develop techniques that give larger lower bounds; since many such techniques are available for networks of reliable "monotone" gates (see Wegener [We87], for example), and since monotone gates suffice for the correction of deviations, it would be natural to try first to find such lower bounds for networks of unreliable monotone gates.

In discussing these results on the sizes of networks, we have not explicitly indicated the dependence of the results on B, ε, and δ. In the theory of networks of reliable gates, it is an important principle that changing B from one finite and complete basis to another can affect the size and depth of optimal networks by at most constant factors (see Muller [Mul56]). It is not at all obvious that this principle carries over to networks of unreliable gates; indeed, for the model in which gates fail with probability precisely ε it seems unlikely that it holds, since there appears to be no way to construct a network over a basis that imitates the behavior of a gate not in that basis. For the second model, however, it can be shown that changing B, ε, and δ (within obvious limits) can affect the size and depth of optimal networks by at most

constant factors (see Pippenger [**Pi88b**]). This justifies the imprecision of the O- and Ω-notation that we have used above and will use often throughout the rest of the paper.

4. Explicit constructions. As we have seen, both von Neumann's original plan for the restoring organ and Dobrushin and Ortyukov's implementation of it depend on random interconnections. This method of proof is familiar from Shannon's communication theory; it provides an existence proof but no explicit construction. Von Neumann was interested in the deterministic simulation of randomness from both a mathematical and a philosophical point of view, as is evident from the following well-known passage from [**vN51b**].

> Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, there is no such thing as a random number—there are only methods to produce random numbers, and a strict arithmetic procedure of course is not such a method. (It is true that a problem that we suspect of being solvable by random methods may be solvable by some rigorously defined sequence, but this is a deeper mathematical question than we can now go into.)

It is natural then, that he tried to supply an explicit construction for the restoring organ, and conjectured that a certain permutation (based on the reversal of binary digits) would serve as the basis for such a construction. From today's perspective, von Neumann's suggestion seems rather naive; it is vague enough to evade definitive refutation, but there is no evidence in its favor. In recent years, however, several provably correct explicit constructions have been given.

The first such explicit construction was given by Pippenger [**Pi85**]; it depends on the explicit construction of graphs with certain special spectral properties. These graphs (essentially "expanding graphs") have themselves been the subject of a long quest for explicit constructions. Contributions by Margulis [**Mar75**] and by Gabber and Galil [**GabG81**] were refined by Jimbo and Maruoka [**JM87**]; the use of Jimbo and Maruoka's graph in Pippenger's construction yields restoring organs with about 2^{57} gates per wire. Fortunately, subsequent work by Lubotzky, Phillips, and Sarnak [**LubPS88**] on "Ramanujan graphs" allows this constant to be deflated to about 2^9, still too large to be practical, but at least no longer ridiculous. Peter Gács has pointed out that another explicit restoring organ can be fashioned from the "approximate halvers" that constitute the fundamental building block of the celebrated Ajtai-Komlós-Szemerédi sorting network [**AKS83a**, **AKS83b**]; this also depends on explicit constructions for expanding graphs, and leads to similar constants to the ones cited above.

Before leaving the subject of explicit restoring organs, it should be mentioned that the explicit constructions for expanding graphs are all based on the action of a discrete group on a finite set, where the discrete group contains at least a free group on two generators. The proofs given by Gabber and Galil and by Jimbo and Maruoka both have a certain resemblance to von Neumann's proof that a group containing a free group on two generators cannot have an invariant mean [**vN29**]; so it may not be too arrogant to believe that von Neumann would have been delighted by this resolution of his problem.

5. Generic and linear functions. One of the central features of Shannon's theory of communication is that it associates with an unreliable channel a real number (called the "capacity" of the channel) that summarizes the information carrying ability of the channel in an absolute and quantitative way. It has been the dream of von Neumann's successors to associate with an unreliable gate a real number that summarizes the information processing ability of the gate in a similar way. This can clearly be done if we look at the depths of networks, as has been mentioned in §3. (The resulting number depends on some of the details of the model, but the situation is not substantially different in this respect from that of communication.) The $O(l \log l)$ estimate of von Neumann, together with the $\Omega(l \log l)$ bound of Dobrushin and Ortyukov [**DO77a**], would seem to dash all hopes of establishing similar results for the sizes of networks, since it suggests that reliable gates are stronger in a "non-Archimedian" way than unreliable ones. Recent results have, however, given rebirth to some of these hopes.

Muller [**Mul56**] showed that "almost all" Boolean functions of n Boolean arguments are computed by networks the minimum possible size of which is $\Theta(2^n/n)$. (Here $\Theta(\dots)$ denotes both $O(\dots)$ and $\Omega(\dots)$.) This result (like its precursor for networks of relay contacts, due to Shannon [**Sh49**]) is proved in two steps: an upper bound of $O(2^n/n)$ is proved by explicit construction that applies to all (rather than almost all) functions of n arguments; then a lower bound of $\Omega(2^n/n)$ is proved by a counting argument that compares the number of networks of a given size with the number of functions of a given number of arguments. The estimates given by Muller in this way differ by substantial constant factors; it was Lupanov [**Lup58**] who showed that more delicate methods give constant factors that asymptotically coincide, thus providing an exquisitely precise theory of the complexity of almost all functions. Lupanov's result is that almost all functions of n arguments are computed by networks the minimum possible size of which is asymptotic to $\rho(B)2^n/n$, where $\rho(B)$ is a constant that depends on the basis B in a known and easily determinable way.

Pippenger [**Pi85**] showed that all functions of n arguments are computed by networks with $O(2^n/n)$ unreliable gates. Comparing this with the lower bound of Muller shows that for almost all functions, the minimum possible

numbers of reliable and unreliable gates differ at most by a constant factor, depending on the basis B, the gate failure probability ε, and the network deviation probability δ. The methods used by Pippenger are comparable to those of Muller in their crudity; but Uhlig [**U87a, U87b**] has used the more delicate methods of Lupanov to derive an upper bound asymptotic to $\sigma(B,\varepsilon,\delta)2^n/n$, where $\sigma(B,\varepsilon,\delta) \to \rho(B)$ as $\varepsilon \to 0$. It would be of great interest to obtain an asymptotically matching lower bound of this form, for it would justify considering $\rho(B)/\sigma(B,\varepsilon,\delta)$ as a "capacity" for unreliable gates in the basis B.

Von Neumann's theory deals with the computation of an arbitrary Boolean function, rather than with particular functions (such as arithmetic operations) to which special methods may apply. Nevertheless, the computation of linear functions occupies a special place. The first hint that this is so appears in a paper of Elias [**E58**], in which he analyzes two-argument Boolean functions and points out an essential difference between "exclusive-or" (or addition modulo 2) and "inclusive-or". Specifically, certain forms of coding that are possible for exclusive-or (or its complement) are impossible for inclusive-or (and the functions obtained from it by complementing the function and its arguments in some combination). The negative result is developed in subsequent papers by Peterson and Rabin [**PeteR59**], Winograd [**Win62, Win63**], Pradhan and Reddy [**PrR72**], and Ahlswede [**Ah84**]. Winograd's result, for example, can be formulated as follows: let $\phi\colon \{0,1\}^k \to \{0,1\}^n$ be a code that preserves componentwise inclusive-or (that is, $\phi(x \vee y) = \phi(x) \vee \phi(y)$) and has minimum distance d. Then d/n and k/n cannot both be bounded away from zero as $n \to \infty$.

If inclusive-or is replaced by exclusive-or, the situation is quite different; indeed, most error-correcting codes are linear (over the field $GF(2)$), and thus preserve componentwise exclusive-or. A class of linear codes that is particularly well suited to computation with unreliable gates is the class of low-density parity-check codes, introduced by Gallager [**Gal63**]. This suitability was exploited by Taylor [**Ta68a**] for reliable storage of information with unreliable gates and memory cells, and in [**Ta68b**] for reliable componentwise exclusive-or with unreliable gates (the results in [**Ta68b**] concerning other operations are incorrect).

The result of Taylor on storage of information has been refined by Kuznetsov [**Kuz73**] to a form that is (within constant factors) optimal as regards both the amount of information stored and (the logarithm of) the length of time for which it is preserved. The only drawback of Kuznetsov's result is that, while explicit constructions have now been found for low-density parity-check codes (see Margulis [**Mar82**] and Imrich [**Im84**]), Kuznetsov's result still depends upon a random-coding argument. It would be of interest to replace this by an explicit construction. It would also be of interest to determine the complexity of the initial coding and final decoding required by this scheme.

Let us now consider the simultaneous computation of a set of m functions, each of which is the sum modulo 2 of some of their n arguments. If $m = 1$ and the function is the sum of all n arguments, then (as we have seen in §3), the minimum possible size with reliable components is $\Theta(n)$, but with unreliable components it is $\Theta(n \log n)$. If $n = m$, the minimum size depends of course on the particular functions. Lupanov [**Lup56**] has shown that for all such sets of functions, the minimum possible number of reliable gates is $O(n^2/\log n)$, and for "almost all" such sets it is $\Omega(n^2/\log n)$. Pippenger [**Pi85**] has shown that for all such sets, the minimum possible number of unreliable components is also $O(n^2/\log n)$. This provides yet another example of a situation in which the minimum possible numbers of reliable and unreliable components differ by at most a constant factor.

6. Variations. This section is devoted to a discussion of two other approaches to the problem of reliable computation with unreliable components, approaches that are based on models for computation and unreliability that are different from those von Neumann used.

The neural nets used by von Neumann have come to be viewed as a member of a class of models in which "gates" are interconnected to form networks. There is a similar but distinct class of models in which "contacts" are the basic components, and it was such a model that Shannon [**Sh38**] used in the paper that first applied Boolean algebra to logical networks. Such models were used by Shannon in other papers on logical networks (in particular, [**Sh49**]), including one with Moore [**MoSh56**] entitled *Reliable circuits using less reliable relays*. A great deal of additional work has been done for such models; most of this work assumes a fixed or slowly growing number of failures (see Andreev [**An86**] for references), but Petri [**Petr69**] retains the assumption used by Moore and Shannon of independent failures with fixed probability.

With contact networks, it is possible to tolerate component failure probabilities arbitrarily close to $1/2$; and for any such fixed component failure probability, it is possible to achieve network failure probabilities arbitrarily close to 0. This striking difference from gate networks may be attributed to the fact that in contract networks, more of the computation is done by the interconnection pattern (which is not subject to failure), rather than by the components. This is clearly a weakness of the failure model, for in practice there are certainly "open circuits" and "short circuits" that do not correspond to the failure of any single contact.

There is an analogous weakness in the failure model of von Neumann, in that "wires" are assumed to carry signals from gate to gate in a way that is not subject to failure. For wires of bounded length, this presents no problem, since a failure of the wire can be ascribed to the gate that drives it or the gate that senses it. But if gates occupy a fixed volume, large networks embedded in three-dimensional space will have large distances between most

pairs of gates, and unless special care is taken many wires will traverse such distances. (Random constructions, such as those proposed by von Neumann, and explicit constructions, such as those proposed by Pippenger and Gács, inevitably have long wires.) It may reasonably be argued that the probability of a signal successfully traversing a long wire decreases exponentially with its length, if the cross-section of the wire remains fixed as its length increases.

The prospect of formulating and justifying a model accounting for the physical disposition of gates in space and for the failures of communication among them may appear daunting, but there is a simple model that easily meets objections based on lengths of wires, and which can overcome a number of objections related to power supply and heat removal as well. This model is the "cellular automaton", or "iterative array", which was used by von Neumann in the context of self-reproduction [**vN66**]. In this model, computation is performed by an infinite collection of finite automata positioned periodically in one- or more-dimensional space. The state of each automaton at a given time step depends on its state and those of its neighbors at the immediately preceding time step; this dependence is the same for all automata and all time steps. This model requires no direct communication beyond neighbors and, once furnished with conventions for input and output, provides a satisfactory computing medium. The automata can, of course, be made unreliable in the same way as are gates.

This model bears a strong resemblance to many that are used in physics to study magnetization, condensation, percolation, and other phenomena that exhibit a "phase transition". (Most such physical models are "static", and are used to study equilibria, but many have "dynamic" counterparts; it is these that are analogous to cellular automata.) The distinguishing feature of a phase transition is that a qualitative change in the overall organization of the system occurs when a parameter passes a critical threshold. After consideration of many specific examples, the following principle became part of the folklore of statistical mechanics: phase transitions can occur in systems with two or more dimensions, but not in one-dimensional systems. In the context of cellular automata with unreliable components, this principle takes the form of the following conjecture: a one-dimensional cellular automaton with unreliable components is "ergodic", that is, tends to an equilibrium distribution that is independent of the initial state. Put simply, a one-dimensional unreliable cellular automaton cannot "remember".

This conjecture was disproved by Gács [**Gác86**]; the proof makes use of ideas from a rather vague attempt at disproof due to Kurdjumov [**Kur78**]. The essential feature of these constructions is that they simultaneously solve the problems of storage and computation with unreliable components; they do this recursively and depend upon "universality" and "fixed-point" arguments similar to those used by von Neumann in his discussion of self-reproduction [**vN51a**, **vN66**]. (If the requirement that the state transition rule be independent of time and position is dropped, reliable storage by a one-dimensional unreliable cellular automaton can be achieved by a much simpler scheme due to Cirelson [**C78**], which does not involve universal computation.)

In two or more dimensions, the situation is much simpler. Despite an early misstatement by Ising [**Is25**], it has been known since 1936 that two-dimensional static magnetic systems can exhibit a phase transition (see Peierls [**Pei36**], Kramers and Wannier [**KrW41**], and Onsager [**On44**] for a beautiful example). It remained to formulate an analog with suitable dynamics to achieve reliable storage and computation with unreliable components. This was done by Toom [**To74**] in 1974; in [**To80**] Toom gave a remarkably simple transition rule that is nonergodic: at each step, take a majority vote among your state, that of your northern neighbor, and that of your eastern neighbor. The use of Toom's rule for reliable computation by two- and three-dimensional unreliable cellular automata has been discussed by Gács [**Gác87**] and by Gács and Reif [**GácR88**], who have given an independent proof of the nonergodicity of Toom's rule based on a "renormalization" argument. Recently, Berman and Simon [**BS88**] have given a simplification of Toom's proof. This development leads to a most interesting open problem (formulated by Gács [**Gác86**]) that concerns "self-organization" with unreliable components. The two-dimensional nonergodic media constructed by Toom have distinct translation-invariant equilibrium distributions; is it possible for a one-dimensional medium to have this property?

This survey began with remarks on von Neumann's interest in the connections among computation, physics, and biology. It is fitting that it has concluded with examples of how ideas connected with phase transitions and self-reproduction have played a role in solving some of the problems arising from his legacy.

References

[Ad78] L. Adleman, *Two theorems on random polynomial time*, IEEE Sympos. on Foundations of Computer Science, vol. 19, IEEE Press, New York, 1978 pp. 75–83.

[Ah84] R. Ahlswede, *Improvements of Winograd's result on computation in the presence of noise*, IEEE Trans. Inform. Theory **30** (1984), 872–877.

[AKS83a] M. Ajtai, J. Komlós, and E. Szemerédi, *Sorting in c log n parallel steps*, Combinatorica 3 (1983), 1–19.

[AKS83b] ——, *An $O(n \log n)$ sorting network*, ACM Sympos. on Theory of Computing, vol. 15, ACM, New York, 1983, pp. 1–9.

[An86] A. E. Andreev, *A universal principle of self-correction*, Math. USSR-Sb. **55** (1986), 145–169.

[Ar61] D. B. Armstrong, *A general method of applying error correction to synchronous digital systems*, Bell System Tech. J. **40** (1961), 577–593.

[BS88] P. Berman and J. Simon, *Investigations of fault-tolerant networks of computers*, ACM Sympos. on Theory of Computing, vol. 20, ACM, New York, 1988, pp. 66-77.

[C78] B. S. Cirelson, *Reliable storage of information in a system of unreliable components with local interactions*, in Locally Interacting Systems and Their Applications in Biology (R. L. Dobrushin, V. I. Kryukov, and A. L. Toom, eds.), Springer-Verlag, New York, 1978.

[DO77a] R. L. Dobrushin and S. I. Ortyukov, *Lower bound for the redundancy of self-correcting arrangements of unreliable functional elements*, Problems Inform. Transmission **13** (1977), 59–65.

[DO77b] ——, *Upper bound for the redundancy of self-correcting arrangements of unreliable functional elements*, Problems Inform. Transmission, **13** (1977), 203–218.

[E58] P. Elias, *Computation in the presence of noise*, IBM J. Res. Develop. **2** (1958), 346–353.

[F88] T. Feder, *Reliable computation by networks in the presence of noise*, IEEE Trans. Info. Theory, **35** (1989), 569–571.

[GabG81] O. Gabber and Z. Galil, *Explicit constructions of linear-sized superconcentrators*, J. Comput. System Sci. **22** (1981), 407–420.

[Gác86] P. Gács, *Reliable computation with cellular automata*, J. Comput. System Sci. **32** (1986), 15–78.

[Gác87] ——, *Error-correction in two-dimensions: A trade-off in complexity* (to appear).

[Gác88] P. Gács and J. H. Reif, *A simple three-dimensional real-time reliable cellular array*, J. Comput. System Sci. **36** (1988), 125–147.

[Gal63] R. G. Gallager, *Low-density parity-check codes*, MIT Press, Cambridge, MA, 1963.

[Im84] W. Imrich, *Explicit construction of regular graphs without small cycles*, Combinatorica **4** (1984), 53–59.

[Is25] E. Ising, *Beitrag zur Theorie des Ferromagnetismus*, Z. Phys. **31** (1925), 253.

[JM87] S. Jimbo and A. Maruoka, *Expanders obtained from affine transformations*, Combinatorica **7** (1987), 343–355.

[Ki64] G. I. Kirienko, *O Samokorrektiruyushchikhsya Skhemakh iz Funktsionalnykh Elementov*, Problemy Kibernet. **12** (1964), 29–37.

[Ki70] ——, *Sintez Samokorrektiruyushchikhsya Skhem iz Funktsionalnykh Elementov dlya Sluchaya Rastushchego Chisla Oshibok v Skheme*, Diskret. Anal. **16** (1970), 38–43.

[Kl56] S. C. Kleene, *Representation of events in nerve nets and finite automata*, in Automata Studies (C. E. Shannon and J. McCarthy, eds.), Princeton Univ. Press, Princeton, N.J., 1956.

[KrW41] H. A. Kramers and G. H. Wannier, *Statistics of the two-dimensional ferromagnet*, Phys. Rev. **60** (1941), 252, 263.

[Kur78] G. L. Kurdjumov, *An example of a nonergodic one-dimensional homogeneous random medium with positive transition probabilities*, Soviet Math. Dokl. **19** (1978), 211–214.

[Kuz73] A. V. Kuznetsov, *Information storage in a memory assembled from unreliable components*, Problems Inform. Transmission **9** (1973), 254–264.

[LubPS88] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[Lup56] O. B. Lupanov, *O Ventilnykh i Kontaktno-Ventilnykh Skhemakh*, Dokl. Akad. Nauk SSSR **111** (1956), 1171–1174.

[Lup58] ——, *Ob Odnom Metode Sinteza Skhem*, Izv. Vyssh. Uchebn. Zaved. (Radiofizika) **1** (1958), 120–140.

[LV62] R. E. Lyons and W. Vanderkulk, *The use of triple-modular redundancy to improve computer reliability*, IBM J. Res. Develop. **6** (1962), 200–209.

[McCP43] W. S. McCulloch and W. Pitts, *A logical calculus of the ideas immanent in nervous activity*, Bull. Math. Biophys. **5** (1943), 115–133.

[Mar75] G. A. Margulis, *Explicit construction of concentrators*, Problems Inform. Transmission **9** (1975), 325–332.

[Mar82] ——, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica **2** (1982), 71–78.

[MoSh56] E. F. Moore and C. E. Shannon, *Reliable circuits using less reliable relays*, J. Franklin Inst. **262** (1956), 191–208, 281–297.

[MucG62] A. A. Muchnik and S. G. Gindikin, *The completeness of a system made up of nonreliable elements realizing a function of algebraic logic*, Soviet Phys. Dokl. **7** (1962), 477–479.

[Mul56] D. E. Muller, *Complexity in electronic switching circuits*, IRE Trans. Electr. Comput. **5** (1956), 15–19.

[vN29] J. von Neumann, *Zur allgemeinen Theorie des Masses*, Fund. Math. **13** (1929), 73–116.

[vN51a] ——, *The general and logical theory of automata*, in Cerebral Mechanisms in Behavior (L. A. Jeffress, ed.), Wiley , New York, 1951.

[vN51b] ——, *Various techniques used in connection with random digits*, J. Res. Nat. Bur. Standards (Appl. Math) **3** (1951), 36–38.

[vN56] ——, *Probabilistic logics and the synthesis of reliable organisms from unreliable components*, in Automata Studies (C. E. Shannon and J. McCarthy, eds.), Princeton Univ. Press, Princeton, N.J. 1956.

[vN58] ——, *The computer and the brain*, Yale Univ. Press, New Haven, CT, 1958.

[vN66] ——, *Theory of self-reproducing automata*, (A. W. Burks, ed.), Univ. of Illinois Press, Urbana, IL, 1966.

[On44] L. Onsager, *Crystal statistics*, I. *A two-dimensional model with an order-disorder transition*, Phys. Rev. **65** (1944), 117–149.

[Or78] S. I. Ortyukov, *Synthesis of asymptotically nonredundant self-correcting arrangements of unreliable functional elements*, Problems Inform. Transmission **13** (1978), 247–251.

[Pa76] W. J. Paul, *Realizing Boolean functions on disjoint sets of variables*, Theoret. Comput. Sci. **2** (1976), 383–396.

[Pei36] R. Peierls, *Ising's model of ferromagnetism*, Proc. Cambridge Philos. Soc. **32** (1936), 477.

[PeteR59] W. W. Peterson and M. O. Rabin, *On codes for checking logical operations*, IBM J. Res. Develop. **3** (1959), 163–168.

[Petr69] N. V. Petri, *The complexity of realizing a function of algebraic logic with contact circuit using unreliable contacts when high reliability is required*, Problemy Kibernet. **21** (1969), 159–169.

[Pi85] N. Pippenger, *On networks of noisy gates*, IEEE Sympos. on Foundations of Computer Science, vol. 26, IEEE Press, New York, 1985, pp. 30–38.

[Pi87] ——, *Analysis of error-correction by majority voting*, (to appear).

[Pi88a] ——, *Reliable computation by formulae in the presence of noise*, IEEE Trans. Inform. Theory **34** (1988), 194–197.

[Pi88b] ——, *Invariance of complexity measure for networks with unreliable gates*, J. ACM **36** (1989), 531–539.

[Po41] E. L. Post, *Two-valued iterative systems of mathematical logic*, Princeton Univ. Press, Princeton, N.J., 1941.

[PrR72] D. K. Pradhan and S. M. Reddy, *Error-control techniques for logic processors*, IEEE Trans. Comput. **21** (1972), 1331–1336.

[R61] D. K. Ray-Chaudhuri, *On the construction of minimally redundant reliable system designs*, Bell System Tech. J. **40** (1961), 595–611.

[Sh38] C. E. Shannon, *A symbolic analysis of relay and switching circuits*, Trans. AIEE **57** (1938), 713–723.

[Sh48] ——, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656.

[Sh49] ——, *The synthesis of two-terminal switching circuits*, Bell System Tech. J. **28** (1949), 59.

[Sz29] L. Szilard, *Über die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen*, Z. Phys. **53** (1929), 840–856.

[Ta68a] M. G. Taylor, *Reliable information storage in memories designed from unreliable components*, Bell System Tech. J. **47** (1968), 2299–2337.

[Ta68b] ——, *Reliable computation in computing systems designed from unreliable components*, Bell System Tech. J. **47** (1968), 2339–2366.

[To74] A. L. Toom, *Nonergodic multidimensional systems of automata*, Problems Inform. Transmission **10** (1974), 239–246.

[To80] ——, *Stable and attractive trajectories in multicomponent systems*, in Multicomponent Random Systems (R. L. Dobrushin and Ya. G. Sinai, eds.), Marcel Dekker, New York, 1980.

[Tr60] J. G. Tryon, *Redundant logic circuitry*, U.S. Patent 2,942,193, June 21, 1960.

[Tr62] ——, *Quadded logic*, in Redundancy Techniques for Computing Systems (R. H. Wilcox and W. C. Mann, eds.), Spartan Books, New York, 1962.

[Tu36] A. M. Turing, *On computable numbers*, Proc. London Math. Soc. (2) **42** (1936), 230–265.

[U74] D. Ulig (=Uhlig), *On the synthesis of self-correcting schemes from functional elements with a small number of reliable elements*, Math. Notes. Acad. Sci. USSR **15** (1974), 558–562.

[U87a] D. Uhlig, *On reliable networks from unreliable gates*, Lecture Notes in Comput. Sci., vol. 269, Springer-Verlag, New York, 1987, pp. 155–162.

[U87b] ——, *Reliable networks from unreliable gates with almost minimal complexity*, Lecture Notes in Comput. Sci., vol. 278, Springer-Verlag, New York, 1987 pp. 462–469.

[We87] I. Wegener, *The complexity of Boolean functions*, Wiley, New York, 1987.

[Wie48] N. Wiener, *Cybernetics: or control and communication in the animal and the machine*, MIT Press, Cambridge, MA, 1948.

[Wie49] ——, *Extrapolation, interpolation, and smoothing of stationary time series*, MIT Press, Cambridge, MA, 1949.

[Win62] S. Winograd, *Coding for logical operations*, IBM J. Res. Develop. **6** (1962), 430–436.

[Win63] ——, *Redundancy and complexity of logical elements*, Inform. and Control **5** (1963), 177–194.

[WinC63] S. Winograd and J. D. Cowan, *Reliable computation in the presence of noise*, MIT Press, Cambridge, MA, 1963.

UNIVERSITY OF BRITISH COLUMBIA, CANADA