

Computing with Noise: Phase Transitions in Boolean Formulas

Alexander Mozeika,¹ David Saad,¹ and Jack Raymond²

¹The Nonlinearity and Complexity Research Group, Aston University, Birmingham B4 7ET, United Kingdom

²Department of Physics, The Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong, China

(Received 26 August 2009; published 11 December 2009)

Computing circuits composed of noisy logical gates and their ability to represent arbitrary Boolean functions with a given level of error are investigated within a statistical mechanics setting. Existing bounds on their performance are straightforwardly retrieved, generalized, and identified as the corresponding typical-case phase transitions. Results on error rates, function depth, and sensitivity, and their dependence on the gate-type and noise model used are also obtained.

DOI: 10.1103/PhysRevLett.103.248701

PACS numbers: 89.70.Eg, 05.40.Ca, 05.70.Fh, 89.20.Ff

Noise is inherent in most forms of computing and its impact is more dramatic as the computing circuits become more complex and of large scale [1]. Classical computing circuits based on electromagnetic components suffer from thermal noise and production errors, quantum computers suffer from decoherence, and noisy processes, inherent in biological systems, remain poorly understood.

The first model of noisy computation was proposed by von Neumann [2] who used Boolean circuits composed of ϵ -noisy gates to gain insight into the robustness of biological neuronal networks. A *circuit* in this context is a directed acyclic graph in which nodes of in-degree zero are either Boolean constants or references to arguments, nodes of in-degree $k \geq 1$ are logical gates of k arguments and nodes of out-degree zero represent circuit outputs. A *formula* is a single-output circuit in which the output of each gate is input to at most one gate. An ϵ -noisy gate computes a Boolean function $\alpha: \{-1, 1\}^k \rightarrow \{-1, 1\}$, but for each input $S \in \{-1, 1\}^k$ there is an error probability ϵ , considered here to be independent for each gate, such that $\alpha(S) \rightarrow -\alpha(S)$. A circuit composed of noisy gates with $\epsilon > 0$ represents a given deterministic function with reliability δ —the maximum error probability over all possible circuit inputs. von Neumann showed that reliable computation, with $\delta < 1/2$, is possible [2] for small ϵ values and specific gates, and demonstrated how reliability can be improved using ϵ -noisy gates only.

In a more recent analysis Pippenger [3] demonstrated that formulas only compute reliably up to a certain gate error threshold and that reliable computation with noisy elements requires strictly greater depth. These bounds based on worst-case scenarios have subsequently been refined [4–6], and developed to include circuits [4]. Most existing results are restricted to specific gates and the restitution of gate properties employs specific constructions. Here we propose a more general *typical-case* analysis that accommodates general gates or gate distribution.

Random Boolean functions play an important role in information theory as they allow for the exploration of average case properties [7], in contrast to the traditionally

studied worst-case scenario. The generation of typical functions, sampled uniformly over the space of Boolean functions, is a research area in its own right; most conventional methods focus on the *ability* to construct arbitrary functions using basic gates or procedures but typically result in highly uncharacteristic functions when generated at random [8–10]. To generate typical functions we use a growth process where one defines an initial distribution over a set of simple Boolean gates; these are then combined repeatedly by Boolean connectives to define new formulas. One such process [11] was shown to result in typical Boolean functions even when a single-type gate is used [11]. As the resulting number of gates increases exponentially with the formula depth, we will use a layered variant of the original framework.

In this Letter we show how models of random formulas can be mapped onto a physical framework and employ methods of statistical physics, developed specifically to analyze the *typical* behavior of random disordered systems, to gain insight into the behavior of noisy Boolean random formulas. The stability of the circuit towards input-layer perturbations and its dependence on the input magnetization are studied to establish the main characteristics of the

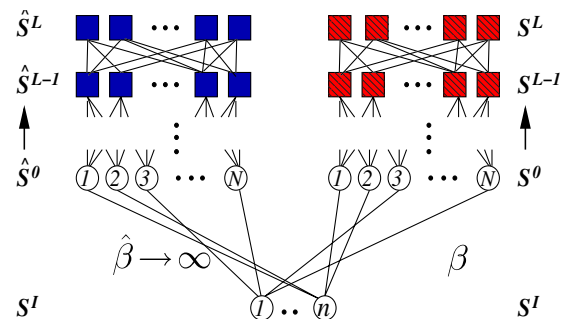


FIG. 1 (color online). The model of two coupled systems with identical topology and different inverse temperatures β and $\hat{\beta} \rightarrow \infty$. Gates are indicated by squares, S^I and input nodes by circles. Blue (dark gray) indicates noiseless gates, red (gray) indicates noisy gates.

generated formulas. To investigate the properties of noisy circuits we consider two copies of the same topology with different temperatures ($1/\beta$), representing the noisy ($\beta < \infty$) and noiseless ($\hat{\beta} \rightarrow \infty$) versions of the same circuit. The generating-functional methodology used here complements the cavity and variational approaches [12] that have been successfully applied to similar tasks, such as the reconstruction problem [13]. Because of the directed nature of the interactions, the generating-functional formulation is arguably more suitable here and in problems of similar characteristics. We show that the typical-case macroscopic behavior observed corresponds straightforwardly to the bounds obtained for specific cases [2–6]. Being very general, the framework is extended to consider further properties of random Boolean formulas for different gates and their dependence on noise level and formula depth.

The noisy computation model considered here, shown in Fig. 1, is a feed-forward layered $N \times (L + 1)$ Boolean circuit. The layers in the circuit are numbered from 0 (input) to L (output). Each layer $\ell \in \{1, \dots, L\}$ in the circuit is composed of exactly N ϵ -noisy, k -ary Boolean gates. Because of gate noise, the i th gate in the ℓ th layer operates in a stochastic manner according to the microscopic law

$$P(S_i^\ell | S_{i_1}^{\ell-1}, \dots, S_{i_k}^{\ell-1}) = \frac{e^{\beta S_i^\ell \alpha(S_{i_1}^{\ell-1}, \dots, S_{i_k}^{\ell-1})}}{2 \cosh[\beta \alpha(S_{i_1}^{\ell-1}, \dots, S_{i_k}^{\ell-1})]}, \quad (1)$$

where β relates to the gate noise ϵ via $\tanh \beta = 1 - 2\epsilon$. The gate-output S_i^ℓ is completely random/deterministic when $\beta \rightarrow 0/\infty$, respectively. The model is acyclic by definition so that given the state of the layer ℓ the gates of layer $\ell + 1$ operate independently of each other. This suggests that the probability of the microscopic state S^0, \dots, S^L , where $S^\ell \in \{-1, 1\}^N$, is a product of (1) over circuit sites and layers. The joint probability of microscopic states in two systems of identical topology but different gate noise is

$$P[\{S^\ell\}; \{\hat{S}^\ell\}] = P(S^0, \hat{S}^0 | S^L) \prod_{\ell=1}^L P(S^\ell | S^{\ell-1}) P(\hat{S}^\ell | \hat{S}^{\ell-1}), \quad (2)$$

where $P(S^\ell | S^{\ell-1}) = \prod_{i=1}^N P(S_i^\ell | S_{i_1}^{\ell-1}, \dots, S_{i_k}^{\ell-1})$. The conditional probability $P(\hat{S}^\ell | \hat{S}^{\ell-1})$ is similar to $P(S^\ell | S^{\ell-1})$ but with $\beta \rightarrow \hat{\beta}$. The source of disorder in our model are the random connections and boundary conditions. Random connections are generated by selecting the i th gate at layer ℓ and sampling exactly k (unordered) indices, $\{i_1, \dots, i_k\}$, uniformly from the set of all possible indices, which point to outputs of layer $\ell - 1$. This is carried out repeatedly and independently for all gates and layers except the input layer ($l = 0$). To cater for a possible higher level of correlation, the 0-layer boundary conditions are generated by selecting

randomly members of the finite set $S^l = \{S_1^l, \dots, S_{|S^l|}^l\}$; the indices n_i are sampled uniformly with $P(n_i) = 1/|S^l|$ and assigned to the input layer. This leads to the random boundary conditions $P(S^0, \hat{S}^0 | S^L) = \prod_{i=1}^N \delta_{S_i^0, S_{n_i}^L} \delta_{\hat{S}_i^0, \hat{S}_{n_i}^L}$.

The structure of the probability distribution (2) is similar to the evolution of disordered Ising spin systems [14] if layers are regarded as discrete time steps of parallel dynamics. The generating-functional method [15] provides

$$\Gamma[\boldsymbol{\psi}; \hat{\boldsymbol{\psi}}] = \left\langle e^{-i \sum_{\ell,i} \{\psi_i^\ell S_i^\ell + \hat{\psi}_i^\ell \hat{S}_i^\ell\}} \right\rangle, \quad (3)$$

where $\langle \dots \rangle$ denotes the average generated by (2). The generating functional (3), regarded also as a characteristic function, is used to compute moments of (2) by taking partial derivatives with respect to the generating fields $\{\psi_i^\ell, \hat{\psi}_j^{\ell'}\}$, e.g., $\langle S_i^\ell \hat{S}_j^{\ell'} \rangle = -\lim_{\psi, \hat{\psi} \rightarrow 0} \frac{\partial^2}{\partial \psi_i^\ell \partial \hat{\psi}_j^{\ell'}} \Gamma[\boldsymbol{\psi}; \hat{\boldsymbol{\psi}}]$. We

assume that the system becomes self-averaging for $N \rightarrow \infty$ [15] and compute $\overline{\Gamma[\boldsymbol{\psi}; \hat{\boldsymbol{\psi}}]}$, where $\overline{\dots}$ is the disorder average; this gives rise to the macroscopic observables

$$m(\ell) = \frac{1}{N} \sum_{i=1}^N \overline{\langle S_i^\ell \rangle}, \quad C(\ell) = \frac{1}{N} \sum_{i=1}^N \overline{\langle S_i^\ell \hat{S}_i^\ell \rangle}, \quad (4)$$

the average layer activity (magnetization) $m(\ell)$ on layer ℓ and overlap $C(\ell)$ between the two systems. Averaging (3) over the disorder [16] leads to the saddle-point integral $\overline{\Gamma[\dots]} = \int \{dP d\hat{P}\} e^{N\Psi[P, \hat{P}]}$ where Ψ is

$$\Psi = i \sum_{\ell} \sum_{S, \hat{S}} \hat{P}^\ell(S, \hat{S}) P^\ell(S, \hat{S}) + \sum_n P(n) \log \sum_{\{S^\ell, \hat{S}^\ell\}} M_n[\{S^\ell, \hat{S}^\ell\}] \quad (5)$$

and M_n is an effective single-site measure

$$M_n[\{S^\ell, \hat{S}^\ell\}] = \delta_{S^0, S^L} \delta_{\hat{S}^0, \hat{S}^L} \prod_{\ell=0}^{L-1} \left\{ \sum_{\{S_j, \hat{S}_j\}} \prod_{j=1}^k [P^\ell(S_j, \hat{S}_j)] \times e^{-i \hat{P}^\ell(S^\ell, \hat{S}^\ell)} \frac{e^{\beta S^{\ell+1} \alpha(S_1, \dots, S_k)}}{2 \cosh[\beta \alpha(S_1, \dots, S_k)]} \times \frac{e^{\hat{\beta} \hat{S}^{\ell+1} \alpha(\hat{S}_1, \dots, \hat{S}_k)}}{2 \cosh[\hat{\beta} \alpha(\hat{S}_1, \dots, \hat{S}_k)]} \right\}. \quad (6)$$

For $N \rightarrow \infty$ the averaged generating functional is dominated by the extremum of Ψ . Functional variation with respect to the order parameter $\hat{P}^\ell(S, \hat{S})$ provides the saddle-point equation $P^\ell(S, \hat{S}) = \sum_n P(n) \langle \delta_{S^\ell, S} \delta_{\hat{S}^\ell, \hat{S}} \rangle_{M_n}$, where $\langle \dots \rangle_{M_n}$ is the average with respect to (6). The physical meaning of $P^\ell(S, \hat{S})$ relates to the averaged joint probability of nodes in the two systems $P^\ell(S, \hat{S}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \overline{\langle \delta_{S_i^\ell, S} \delta_{\hat{S}_i^\ell, \hat{S}} \rangle_{S^l}}$, while the conjugate order parameter, which ensures normalization of $P^\ell(S, \hat{S})$, van-

ishes. This simplifies the effective measure (6), yielding the macroscopic observables

$$\begin{aligned}
 m(\ell + 1) &= \sum_{\{S_j\}} \prod_{j=1}^k \left[\frac{1}{2} \{1 + S_j m(\ell)\} \right] \tanh[\beta \alpha(S_1, \dots, S_k)] \\
 C(\ell + 1) &= \sum_{\{S_j, \hat{S}_j\}} \prod_{j=1}^k \left[\frac{1}{2} \{1 + S_j m(\ell) + \hat{S}_j \hat{m}(\ell) + S_j \hat{S}_j C(\ell)\} \right] \\
 &\quad \times \tanh[\beta \alpha(S_1, \dots, S_k)] \tanh[\hat{\beta} \alpha(\hat{S}_1, \dots, \hat{S}_k)].
 \end{aligned} \tag{7}$$

The magnetization $\hat{m}(\ell)$ is computed by (7) using $\hat{\beta}$; initial conditions are $m(0) = \hat{m}(0) = \frac{1}{|S^I|} \sum_{S \in S^I} S$, $C(0) = 1$.

The connectivity profile considered here results in a simple set of equations. The macroscopic behavior of the two systems is completely determined by the set of observables $\{m(\ell), \hat{m}(\ell), C(\ell)\}$ through the order parameter $P^\ell(S, \hat{S}) = \frac{1}{2}(1 + Sm(\ell) + \hat{S}\hat{m}(\ell) + S\hat{S}C(\ell))$, while the single system behavior is dominated by $\{m(\ell)\}$. Furthermore, since $\langle \prod_j S_j^\ell \rangle \rightarrow \prod_j \langle S_j^\ell \rangle$ for finite j , the spins in layer ℓ are uncorrelated when $N \rightarrow \infty$; this is due to the fact that the i th site is a root of a full k -ary tree, which grows from the input layer and points to Boolean variables in the set S^I . Loops in the circuit are rare, so that trees can be regarded as random independent Boolean formulas for a given input. The output of a typical formula at layer ℓ is determined by $P^\ell(S)$.

The order parameter $C(\ell)$ and the normalized Hamming distance $D(\ell)$ between states S^ℓ and \hat{S}^ℓ are related via the identity $D(\ell) = \frac{1}{2}(1 - C(\ell))$. This gives rise to the measure $\Delta(\ell) = \lim_{\beta, \hat{\beta} \rightarrow \infty} D(\ell)$, for the circuit's sensitivity with respect to its input. The probability $P(S_i^\ell \neq \hat{S}_i^\ell)$ for any node, which relates to the Hamming distance $D(\ell)$, facilitates the estimate of the noisy circuit's ℓ -layer error probability $\delta(\ell) = \max_{S^I} \lim_{\beta \rightarrow \infty} D(\ell)$, comparing the noisy and noiseless node values for all inputs. Obviously, in the absence of noise $\delta(\ell) = 0, \forall \ell$.

To obtain results for a specific case, which could be compared against those obtained in the information theory literature, we apply Eqs. (7) for a particular Boolean gate α , the k -input majority gate (MAJ- k). The reasons for choosing this gate are twofold. First, it was proved [5,6] to be optimal for noisy computation in formulas. Second, formulas constructed at random using majority gates can in principle compute any Boolean function [11] with *uniform probability*. A convenient representation of the MAJ- k gate is of the form $\text{MAJ}(S_1, \dots, S_k) = \text{sgn}[\sum_{j=1}^k S_j]$ with odd k . For the particularly simple example MAJ-3 one obtains for $\hat{\beta} \rightarrow \infty$

$$m(\ell + 1) = \frac{1}{2} \tanh \beta [3m(\ell) - m^3(\ell)], \tag{8}$$

$$\begin{aligned}
 C(\ell + 1) &= \tanh \beta \left[\frac{3}{2} m(\ell) \hat{m}(\ell) - \frac{3}{4} C(\ell) m^2(\ell) \right. \\
 &\quad \left. - \frac{3}{4} C(\ell) \hat{m}^2(\ell) + \frac{3}{4} C(\ell) + \frac{1}{4} C^3(\ell) \right].
 \end{aligned} \tag{9}$$

Insight on the functions implemented and the gate noise threshold can be obtained from Eq. (8), which describes the evolution of the magnetization from layer to layer. When expanded around the stationary solution $m(\infty) = 0$ it identifies the critical noise value $\epsilon^* = 1/6$, identical to the results of [2,5], below which the (unordered) $m(\infty) = 0$ solution becomes unstable and two stable (ordered) solutions $m(\infty) = \pm \sqrt{(1 - 6\epsilon)/(1 - 2\epsilon)}$ emerge. Studying the joint dynamics of (8) and (9) shows that for $\epsilon > 1/6$ the magnetization vanishes (exponentially) while for $\epsilon < 1/6$ the stationary solutions appear, corresponding to the positive and negative initial magnetizations $m(0)$, respectively. The boundary separating these phases, shown in Fig. 2(a), identifies the noise level below which the circuit can preserve 1 bit of input information $S^I = \{S\}$ for arbitrarily many layers; the error probability $P^\ell(-S) = \frac{1}{2}(1 - Sm(\ell))$ measures how well it is preserved after ℓ layers. Less complicated functions (fewer layers) can be computed with higher gate noise.

The analysis can easily accommodate other gates, in particular, MAJ- k . Using similar arguments one identifies the critical noise level $\epsilon^* = 1/2 - 2^{k-2}/\binom{k-1}{(k-1)/2}$ below which two stable solutions emerge. Computing formulas with limited error δ above the critical noise level ϵ^* , identical to the threshold reported in [6], becomes infeasible. Similarly, the transition point for formulas constructed of NAND gates identifies a threshold noise level $\epsilon^* = (3 - \sqrt{7})/4$, identical to the one derived in [17].

General properties of average formulas can be straightforwardly obtained from the site probability of average

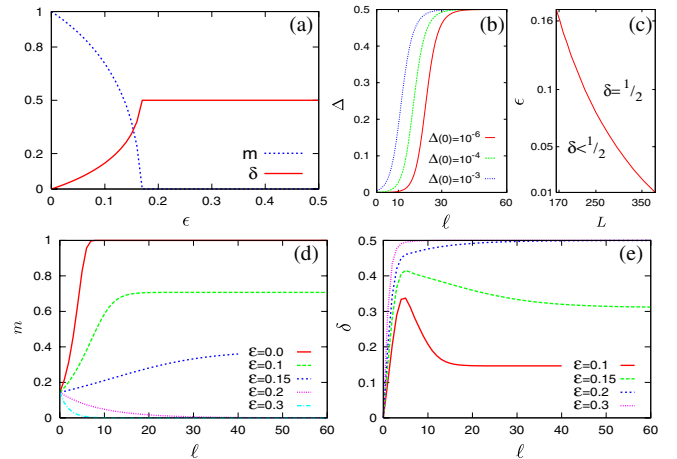


FIG. 2 (color online). Properties of MAJ-3 gate-based formulas: (a) Magnetization m and output error δ as a function of gate noise ϵ . (b) Sensitivity of $\Delta(\ell)$ to input mismatch $\Delta(0)$ for $m(0) = 0$. (c) Phase diagram for gate noise ϵ at layer L . For the MAJ-7 function, we plot the evolution, in layers (L), of (d) magnetization m and (e) output error δ .

formulas $P^\ell(S)$ at layer ℓ . Stationary solutions in the noiseless case show $m(\infty) = \pm 1$, in correspondence to the sign of the initial magnetization, giving rise to biased function outputs. For $m(0) = 0$ one obtains $m(\infty) = 0$, so that each site of the model can be associated with some random Boolean function output, evaluating to ± 1 with equal probability. Consequently, depending on the initial conditions, formulas converge to a *single* Boolean function or to the uniform distribution over some set of functions [7]. Our result is consistent with majority gate growth process [7,11] where for input $S^l = \{-1, 1, S_1^l, \dots, S_n^l, -S_1^l, \dots, -S_n^l\}$ stationary state formulas compute all Boolean functions of n variables while for $S^l = \{-1, 1, S_1^l, \dots, S_n^l\}$ (also without $-1, 1$) they converge to the MAJ- n function (odd n) or to the uniform distribution over slice functions (even n) [7]. Convergence to the stationary solution $m(\infty)$ is at depth $O(\log n)$ for $m(0) = 1/n$ where $n \in \mathbb{N}$ in agreement with [7].

Function error rates can be calculated through the study of Eq. (9) describing the evolution of the overlap between the two systems. Initial conditions are the same for both systems $m(0) = \hat{m}(0)$ and $C(0) = 1$. The magnetization in the noisy system ($\epsilon \leq 1/6$) converges to $m(\infty) = \pm\sqrt{(1-6\epsilon)/(1-2\epsilon)}$, depending on the sign of $m(0)$. Using these stationary values and Eq. (9) we find $C(\infty) \times (7-18\epsilon) - (1-2\epsilon)C^3(\infty) = \pm 6\sqrt{(1-2\epsilon)(1-6\epsilon)}$ leading to the error probability $\delta(\infty)$ plotted in Fig. 2(a).

The stationary solution $C(\infty) = 1$ of Eq. (9) for initial conditions $m(0) = 0$, $C(0) = 1$, and $\epsilon = 0$ is unstable under perturbations to $C(0)$, resulting in the stable stationary state $C(\infty) = 0$. Consequently, the circuit is input sensitive leading to an increasing Hamming distance $\Delta(\ell)$ for small perturbations $\Delta(0)$ as shown in Fig. 2(b). For $\epsilon > 0$ the circuit amplifies the noise and $\delta(L)$ grows but remains limited for sufficiently small ϵ as shown in Fig. 2(c).

To examine the computation performed at layer ℓ we consider the input set $S^l = \{S_1, \dots, S_7\}$, corresponding to the function MAJ-7 for the noiseless case, with lowest possible initial magnetization $m(0) = 1/7$ where changes between layers are smallest. Figure 2(d) shows the magnetization $m(\ell)$ for different gate noise levels; the convergence rate decreases with increasing ϵ . Close to the critical value the difference equation (8) can be approximated by the differential equation $\frac{d}{d\ell} m(\ell) = -m(\ell) + \frac{1}{2}(1-2\epsilon)[3m(\ell) - m^3(\ell)]$ for continuous ℓ . Its solution close to the phase boundary, obtained by expanding $\epsilon = 1/6 + \Delta\epsilon$ where $|\Delta\epsilon| \ll 1$, exhibits exponential convergence $|m(\ell) - m(\infty)| \approx e^{-\text{const}\Delta\epsilon\ell}$.

The function error $\delta(\ell)$, shown in Fig. 2(e) for different ϵ values, exhibits two distinct stages in the dynamics. Initially, the error increases until it reaches its maximum value at $\ell = 5$, before the MAJ-7 function is computed exactly at $\ell = 8$ for $\epsilon = 0$ [see Fig. 2(d)]; the location of this maximum is independent of ϵ . This suggests that

gate inputs at layers $\ell \leq 5$ are nonuniform, contributing to noise amplification, but become more uniform later leading to noise suppression and decreasing error. As we approach ϵ^* the number of layers needed for the error to reach stationarity increases; in the region $\epsilon = 1/6 \pm \Delta\epsilon$ it can be estimated from the asymptotic form derived for $m(\ell)$. The dynamic behavior of the error changes to monotonically increasing at $\epsilon^0 = \frac{1}{2} \left[\frac{1-m^2(0)}{3-m^2(0)} \right]$ above which noise cannot be reduced by additional layers. For $\epsilon \gg 1/6$ the error evolution becomes strictly monotonic it relaxes to its stationary value $1/2$ exponentially fast.

By mapping the problem of noisy computation onto a physical framework, we retrieved many of the existing bounds and extended them to include arbitrary gates and/or distribution of gates. In addition, we calculated the level of error and function bias expected at any depth, the sensitivity to input perturbations and expected convergence rate depending on the input bias, gate properties, and gate noise level. This framework enables one to discover typical properties of noisy computation that are inaccessible via traditional methods of information theory and will undoubtedly contribute to exciting new discoveries; for instance, in biologically inspired systems and circuits with hard (systematic) noise.

Support by the Leverhulme trust (F/00 250/H) is acknowledged.

-
- [1] S. Borkar, IEEE Micro **25**, 10 (2005).
 - [2] J. Von Neumann, *Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components* (Princeton University Press, Princeton, NJ, 1956), p. 4398.
 - [3] N. Pippenger, IEEE Trans. Inf. Theory **34**, 194 (1988).
 - [4] T. Feder, IEEE Trans. Inf. Theory **35**, 569 (1989).
 - [5] B. Hajek and T. Weller, IEEE Trans. Inf. Theory **37**, 388 (1991).
 - [6] W. Evans and L. Schulman, IEEE Trans. Inf. Theory **49**, 3094 (2003).
 - [7] A. Brodsky and N. Pippenger, Random Struct. Algorithms **27**, 490 (2005).
 - [8] H. Lefmann and P. Savický, Random Struct. Algorithms **10**, 337 (1997).
 - [9] B. Chauvin *et al.*, Comb. Probab. Comput. **13**, 475 (2004).
 - [10] D. Gardy and A. Woods, in *Proceedings of the 2005 International Conference on Analysis of Algorithms*, edited by C. Martínez [DMTCS Proc. AD, 139 (2005)].
 - [11] P. Savický, Discrete Math. **83**, 95 (1990).
 - [12] M. Mézard and A. Montanari, *Information, Physics, and Computation* (Oxford University Press, Oxford, 2009).
 - [13] M. Mezard and A. Montanari, J. Stat. Phys. **124**, 1317 (2006).
 - [14] J.P.L. Hatchett *et al.*, J. Phys. A **37**, 6201 (2004).
 - [15] C. De Dominicis, Phys. Rev. B **18**, 4913 (1978).
 - [16] A. Mozeika *et al.* (to be published).
 - [17] W. Evans and N. Pippenger, IEEE Trans. Inf. Theory **44**, 1299 (1998).