

Decoding communities in networks

Filippo Radicchi*

*Center for Complex Networks and Systems Research, School of Informatics, Computing, and Engineering,
Indiana University, Bloomington, Indiana 47408, USA*

(Received 5 July 2017; revised manuscript received 13 February 2018; published 28 February 2018)

According to a recent information-theoretical proposal, the problem of defining and identifying communities in networks can be interpreted as a classical communication task over a noisy channel: memberships of nodes are information bits erased by the channel, edges and nonedges in the network are parity bits introduced by the encoder but degraded through the channel, and a community identification algorithm is a decoder. The interpretation is perfectly equivalent to the one at the basis of well-known statistical inference algorithms for community detection. The only difference in the interpretation is that a noisy channel replaces a stochastic network model. However, the different perspective gives the opportunity to take advantage of the rich set of tools of coding theory to generate novel insights on the problem of community detection. In this paper, we illustrate two main applications of standard coding-theoretical methods to community detection. First, we leverage a state-of-the-art decoding technique to generate a family of quasioptimal community detection algorithms. Second and more important, we show that the Shannon's noisy-channel coding theorem can be invoked to establish a lower bound, here named as decodability bound, for the maximum amount of noise tolerable by an ideal decoder to achieve perfect detection of communities. When computed for well-established synthetic benchmarks, the decodability bound explains accurately the performance achieved by the best community detection algorithms existing on the market, telling us that only little room for their improvement is still potentially left.

DOI: [10.1103/PhysRevE.97.022316](https://doi.org/10.1103/PhysRevE.97.022316)**I. INTRODUCTION**

Real networks are often assumed to be organized in clusters or communities [1]. A community is naively defined as a subgroup of nodes with a density of internal connections larger than the density of external links. Most of the research in the area has focused on the development of algorithms aimed at detecting such objects. The philosophy of the approaches considered so far varies widely, with methods that rely on heuristics [2,3], spectral properties of operators [4], and optimization of quality functions [5–8], just to mention a few of them. Principled approaches, as those relying on generative network models [9–14], provide not only practical algorithms, but also a solid notion of a community. In this respect, they allow to generate insights on the problem of identification of communities in networks, as for example establishing the existence of a universal limitation affecting all community detection algorithms [9,15–18]. The limitation refers to the performance of a perfect algorithm in stochastic network models with planted community structure, and consists in the existence of a maximum level of fuzziness, generally named as detectability threshold, that can be tolerated by the algorithm to be able to detect, in the limit of infinite network sizes, a nonvanishing portion of the true community structure. As statistical inference approaches rely on stochastic network models [9–14], the detectability threshold of these models provides an indication of the parameter ranges where community detection algorithms are expected to be useful.

Although rigorous conditions for the establishment of the regime of detectability has been studied also for finite-size networks [19], the notion of detectability is much less useful in another important application of stochastic block models, that is, the numerical validation of community detection algorithms [2,20–22]. In this type of application in fact, the focus is not only on network models with small or medium size, but, more importantly, on the regime of exact recovery of the planted community structure.

The formal establishment of the regimes of partial and exact recovery in the stochastic block model has been the subject of a series of recent publications in coding theory [23–26]. In these papers, the problem of defining and identifying communities is interpreted as a classical communication process (Fig. 1), analogous to the one considered by Shannon [27]: group assignments of the nodes in the network represent a message that is first encoded, then transmitted along a noisy channel, and ultimately decoded. It is important to remark that the noisy-channel interpretation of the problem of community detection coincides with the one at the basis of statistical inference approaches [9–14]. The only difference is the angle from which one looks at it. Instead of interpreting a stochastic model as the generator of noisy edges, the stochastic model is seen as a source of noise that disrupts a network with community structure otherwise unambiguous. In this respect, edges in the network are not regarded as entities that define communities rather as redundant but altered information that is added to preexisting information on node memberships. Interpreting the task of detecting communities in graphs as a decoding process of a noisy signal has the great advantage to lead to rigorous mathematical statements, valid in the limit

*filiradi@indiana.edu

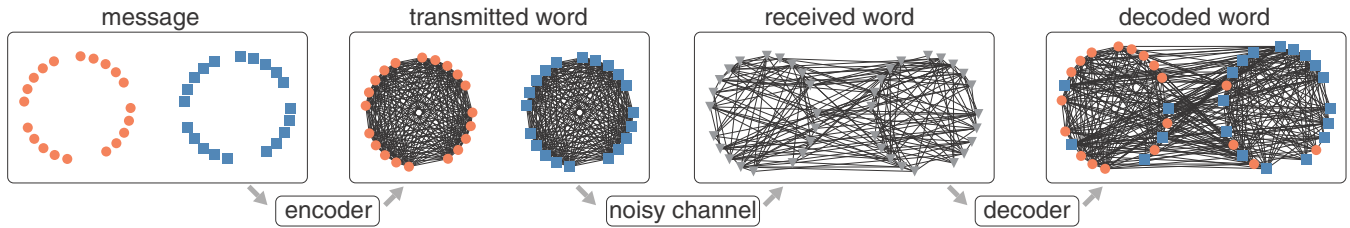


FIG. 1. Definition and detection of communities in networks as a communication process [23–25]. The message generated from the source contains information about the group assignments of the various nodes. The message is encoded in a network structure where all nodes belonging to the same group are connected one with the other, but no connections are present between any pair of nodes belonging to different groups. The codeword is transmitted along a noisy channel. The effect of the channel is twofold: it erases all information about group assignments, and deteriorates the network structure by adding and removing edges. The received word is decoded to reconstruct, even if only partially, the transmitted message.

of infinitely large graphs, regarding the identification of the regimes of partial and exact reconstruction of the planted community structure of the stochastic block model, regimes that are entirely determined by the amount of noise that characterizes the network model. Partial recovery corresponds to the aforementioned detectability [26]. The determination of the exact recovery threshold is instead a completely novel result, able to provide a precise indication of the range of parameter values of a stochastic block model where perfect recovery of the planted community structure is allowed [23]. The computation of the exact recovery threshold can be performed in general stochastic block models [24]. However, the mathematical result is derived in the limit of infinitely large systems. On finite systems, we expect the threshold to delineate conservative regimes of performance. How much is the threshold value underestimating the potential of algorithms on mid-sized networks as those used in typical numerical experiments [20,22]? Are there more predictive approximations for finite-size networks? Please note that this information is of fundamental importance. Without a theoretical baseline, we can assess the performance of algorithms only in pairwise comparisons. This means that we do not have the ability to judge their full potential, and determine if there is still room for improvement.

This paper aims at filling this gap. We provide numerical evidence that the exact recovery threshold [23–25] generates predictions that seem to be not very accurate in the description of the performance of algorithms in finite-size networks [20,22]. Specifically, we provide numerical evidence that existing community detection algorithms are able to achieve perfect recovery of communities in small or medium stochastic block models well beyond the exact recovery threshold [20,22]. We show, however, that the Shannon’s noisy-channel coding theorem [27] allows us to establish a less restrictive approximation for the regime of exact recovery which describes particularly well the maximum level of fuzziness tolerated by algorithms to achieve perfect detection in stochastic benchmarks [20,22]. We refer to the approximation obtained with the Shannon’s theorem as the decodability bound, being this quantity always a lower bound of the exact recovery threshold. The derivation of the decodability bound is very simple, as it requires only estimating the channel capacity of a generative network model. Further, the bound appears to be not very sensitive to important ingredients of a generative model with

planted community structure such as degree and community size distributions. The procedure seems therefore potentially generalizable to more complicated models. Please note that the decodability bound is still derived under the hypothesis that network size is infinite, thus its effectiveness in finite-size systems is not *a priori* granted. However, numerical results provide compelling evidence that no algorithm has been able to beat the decodability bound in the settings of the stochastic block model generally considered in the literature [20,22]. At the same time, we note also that the best algorithms available on the market have performances already very close to those predicted by the decodability bound, leaving therefore only little room for potential improvement. To reach our main results, we follow a path at the interface between community detection and traditional coding theory [28]. In particular, we deploy a family of error-correcting algorithms for community detection that rely on a traditional decoding technique [29,30]. Although these methods do not provide scalable algorithms, they do allow for straightforward calculations showing that the decoding algorithms are theoretically able to achieve almost perfect recovery at the decodability bound.

II. METHODS

A. Low-density parity-check codes

In this section, we describe a family of linear codes that can be used to interpret the problem of community detection in networks from a classical information-theoretic perspective. We stress that the code \mathcal{P} that we are going to present has been originally introduced in Ref. [23]. Here, in addition to rephrasing and expanding its description, we show that the code is only one member of a large family of equivalent codes.

Except for the final section, the entire paper focuses on the case of two communities only. This fact allows us to work with a binary alphabet and modulo-2 arithmetic. The message that the source wants to deliver is a vector $\vec{\sigma}^T = (\sigma_1, \dots, \sigma_N)$ of N bits, where $\sigma_i = 0, 1$ specifies the membership of node i , and N is the size of the graph. We refer to the bits σ as the information bits. Note that the transformation $\sigma_i \rightarrow (\sigma_i + 1)$ does not change the content of information. This means that the effective number of information bits generated by the source is $N - 1$. The encoder acts on the message in a very simple way. It basically generates a network where communities are disconnected cliques. From this perspective, edges are purely

redundant information, as the encoder generates $N(N-1)/2$ bits for every pair (i, j) of nodes to satisfy parity-check equations of the type

$$\sigma_i + \sigma_j + \theta_{i,j} = 0. \quad (1)$$

The bits θ are called the parity bits of the codeword. Note that, in any codeword, an edge corresponds to a parity bit $\theta = 0$, and every nonedge to a parity bit $\theta = 1$. This choice is made for convenience. We refer to the code described by the system of Eq. (1) as the pair code, or shortly as the code \mathcal{P} . The rate of this code is

$$R = \frac{\log_2(2^N/2)}{N(N-1)/2} = \frac{2}{N} \quad (2)$$

as the total number of possible messages is $2^N/2$ (the division by 2 arises from symmetry), and the total number of parity bits is $N(N-1)/2$. The code \mathcal{P} is linear, and can be written as a single matrix-vector equation $H\vec{\chi} = \vec{0}$, where $\vec{\chi}^T = (\sigma_1, \dots, \sigma_N, \theta_{1,2}, \dots, \theta_{N-1,N})$ is the codeword, $\vec{0}$ is a vector with the same dimension as $\vec{\chi}$ but where every single component is equal to zero, and

$$H = (V^T | \mathbb{I}_{N(N-1)/2}) \quad (3)$$

is the parity-check matrix of the code. In the above expression, \mathbb{I}_q is the identity matrix of dimensions $q \times q$, whereas V is a rectangular matrix with N rows and $N(N-1)/2$ columns that can be written as composed of N blocks

$$V = (V_1 | V_2 | \dots | V_i | \dots | V_N).$$

The i th block is defined as

$$V_i = \begin{pmatrix} 0_{[i-1] \times [N-i]} \\ J_{1 \times [N-i]} \\ \mathbb{I}_{N-i} \end{pmatrix},$$

where $0_{q \times t}$ is a matrix with q rows and t columns whose entries are all equal to zero, and $J_{q \times t}$ is a matrix with q rows and t columns whose entries are all equal to one. The parity-check matrix of the code \mathcal{P} has two nice properties. First, it appears in the so-called systematic form. This means that the actual generator matrix G of the code, the one used to generate codewords as $\vec{\sigma}^T G = \vec{\chi}^T$, can be written as $G = (\mathbb{I}_N | V)$. Second, H is a sparse matrix, as the density of ones is vanishing as N grows. Linear codes based on low-density parity-check matrices are usually denoted as LDPC codes, and they are at the basis of many error-correcting techniques [29,30].

After the message is encoded, the codeword $\vec{\chi}^T = (\vec{\sigma}^T, \vec{\theta}^T)$ is sent through a noisy communication channel. The effect of the channel is twofold. First, it erases completely the information bits σ . Second, it changes the value of some parity bits θ . What is received at the end of the channel is therefore a network with only partial information about the original community structure generated by the source. The way one can attempt to recover the content of the original message is finding the codeword that best represents, in terms of minimal distance, the received word. Several decoding algorithms can be used in this respect. A naive approach is for instance based on a spectral algorithm (see Appendix A). In this paper, we consider state-of-the-art error-correcting algorithms, typically used in decoding processes over arbitrary memoryless noisy channels

[28]. We will come back to it in a moment. Meanwhile, we would like to make some important remarks.

Although apparently very similar, the interpretation presented here is different from the one considered by Rosvall and Bergstrom [7]. The two approaches suffer from the detectability limit in the stochastic block model [12]. They stand, however, for different takes of the community detection problem. Their difference is analogous to the one present between the source coding theorem and the noisy-channel coding theorem [28]. In Ref. [7], the authors rephrased the community detection problem as a communication task over a channel with limited capacity. The goal of their approach was to provide the best encoding strategy to deliver information with such a limitation. Here instead, the focus is on the performance of the communication task depending on the noise of the channel. In this respect, it is very important to remark that, in most of practical situations, one has no clue of the type of noise that characterizes the channel. In these situations, the only possibility is to make and test hypotheses. This is pretty much in the same spirit as of community identification algorithms based on statistical inference [9,10], or, from the perspective of coding theory, maximum-likelihood decoders devised for specific noisy channels. We are not seriously concerned by the lack of knowledge about the noise of the channel, as the main goal of the paper is to generate insights on the problem of community detection in networks, rather than simply deploying practical algorithms.

The fact that the code is linear has one important feature [31]. One can create equivalent linear codes by performing special types of operations on the matrix H , as for example permutation of rows and columns, multiplications of rows by nonzero scalars, sum of rows, and so on. Equivalence means that the codes share the same set of codewords. For instance, summing the rows corresponding to the equations $\sigma_i + \sigma_j + \theta_{i,j} = 0$, $\sigma_i + \sigma_k + \theta_{i,k} = 0$, and $\sigma_j + \sigma_k + \theta_{j,k} = 0$, one obtains the equation

$$\theta_{i,j} + \theta_{i,k} + \theta_{j,k} = 0. \quad (4)$$

This equation involves only parity bits and not information bits. One can actually apply the same operation to all triplets of nodes to obtain an equivalent system of equations consisting in sums of triplets of parity bits only. We refer to this as the triplet code, or shortly as the code \mathcal{T} . The equivalence between \mathcal{P} and \mathcal{T} is particularly simple. If we find a codeword containing only parity bits for \mathcal{T} , we are able to trivially deduce the information bits of the corresponding codeword of \mathcal{P} . This can be done by simply fixing the value of one information bit $\sigma_{i^*} = 0, 1$, and use Eq. (1) to iteratively retrieve the values of the other information bits such that they satisfy their respective parity-check equation. This fact tells us that looking at higher-order local structures does not provide any significant benefit to the decoding process, that is, the identification of the communities in the network. We will see, however, that working with the code \mathcal{T} is useful to characterize performances of decoders.

B. Gallager decoders

A convenient way to graphically represent a LDPC code is to use a bipartite network called Tanner graph. The graph is constructed from the parity-check matrix H of the code.

Every row of H identifies a check node, and every column of H identifies a variable node. A variable node v is connected to a check node c if the entry $H_{c,v} = 1$; if $H_{c,v} = 0$, v and c are instead disconnected. Tanner graphs are particularly useful in the description of a probabilistic decoding strategy introduced by Gallager in the 1960's [29]. We provide in the Appendices D and E a detailed description of the algorithm as implemented for the specific cases of the \mathcal{P} and \mathcal{T} codes, respectively. Here, we just describe the spirit of the approach, and report the simplified equations for the code \mathcal{P} . The technique consists in a series of messages exchanged by check nodes and variable nodes connected in the Tanner graph. A variable node v sends to a connected check node c a message $m_{v \rightarrow c}$ representing the probability of the bit value that v should assume according to the other check nodes $c' \neq c$ connected to it. In turn, a check node c replies to a variable node v with a message $n_{c \rightarrow v}$ consisting in the probability of the bit value that the other variable nodes $v' \neq v$ attached to c would like to see from v . The algorithm is initialized from suitable initial conditions, i.e., our beliefs on the variable nodes, and run until convergence or up to a maximum number of iterations. The approach is exact in acyclic Tanner graphs, and thus particularly effective in the context of LDPC codes. Cycles in the Tanner graph deteriorate the performance of the algorithm, as they introduce dependencies among messages that are actually neglected

in the algorithm by Gallager. Most of the information theory research in this context is indeed centered on the construction of LDPC matrices (not necessarily equivalent) with small number of short loops, avoiding in particular loops of length four.

Going back to our specific problem, the matrix H defined in Eq. (3) generates a Tanner graph with girth equal to six (the girth is the length of the shortest loop in the graph). Such a property cannot be changed by creating equivalent parity-check matrices. In principle, one can apply the Gallager algorithm to any of the Tanner graphs generated starting from equivalent parity-check matrices, leading therefore to a class of algorithms. Typically, the more irregular, in terms of degree for check and variable nodes, the Tanner graph is, the lower is the total number of iterations required for the eventual convergence. On the other hand, increasing the degree heterogeneity of the Tanner graph increases also the complexity of the algorithm, whereas the solution obtained by the algorithm remains basically the same. If one applies the Gallager algorithm to the Tanner graph generated from the systematic parity-check matrix of Eq. (3), it is possible to simplify the implementation of the algorithm (Appendix D), and obtain the following system of equations that relates variables at iteration t of the algorithm to the values of the same variables at stage $t - 1$ of the algorithm:

$$\zeta_{i \rightarrow j}^{(t)} = \begin{cases} \ell_i & \text{for } t = 0, \\ \ell_i + \sum_{k \neq j} \log \frac{1 + \tanh\left(\frac{1}{2} \zeta_{k \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \ell_{i,k}\right)}{1 - \tanh\left(\frac{1}{2} \zeta_{k \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \ell_{i,k}\right)} & \text{for } t \geq 1, \end{cases} \quad (5)$$

where the logarithm is taken in the natural basis, and $\tanh(\dots)$ is the hyperbolic tangent function. $\ell_i = \log \frac{P(\sigma_i=0|s_i)}{P(\sigma_i=1|s_i)}$ is the *a priori* log-likelihood ratio (LLR) of the information bit σ_i , based on the information received s_i . It essentially stands for the logarithm of the ratio between the probabilities that σ_i is zero and σ_i is one, given our observation s_i at the end of the noisy channel. $\ell_{i,j} = \log \frac{P(\theta_{i,j}=0|A_{i,j})}{P(\theta_{i,j}=1|A_{i,j})}$ is exactly the same quantity but for the parity bit $\theta_{i,j}$, and $A_{i,j}$ is the element (i,j) of the adjacency matrix of the graph, i.e., one plus the (i,j) th parity bit received at the end of the channel. The messages $\zeta_{i \rightarrow j}^{(t)}$ are also LLRs. They are defined for every pair of nodes i and j , not just those actually connected. At every iteration t , the best estimate of the LLRs for the information and parity bits are given, respectively, by

$$\hat{\ell}_i^{(t)} = \ell_i + \sum_{k \neq i} \log \frac{1 + \tanh\left(\frac{1}{2} \zeta_{k \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \ell_{i,k}\right)}{1 - \tanh\left(\frac{1}{2} \zeta_{k \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \ell_{i,k}\right)} \quad (6)$$

and

$$\hat{\ell}_{i,j}^{(t)} = \ell_{i,j} + \log \frac{1 + \tanh\left(\frac{1}{2} \zeta_{j \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \zeta_{i \rightarrow j}^{(t-1)}\right)}{1 - \tanh\left(\frac{1}{2} \zeta_{j \rightarrow i}^{(t-1)}\right) \tanh\left(\frac{1}{2} \zeta_{i \rightarrow j}^{(t-1)}\right)}. \quad (7)$$

A hard-decision process is made at every stage t : the best estimates of the information bit i are $\hat{\sigma}_i = 0$ if $\hat{\ell}_i^{(t)} > 0$ and $\hat{\sigma}_i = 1$, otherwise. Similar rules hold for the determination of

the best estimate of the parity bits $\hat{\theta}$. These values are used to test convergence of the algorithm by simply checking whether the best estimates of the parity and information bits are such that all Eq. (1) is satisfied. In such a case, the algorithm stops. Otherwise, the algorithm is run up to a maximum number of iterations. The *a priori* LLRs ℓ_i and $\ell_{i,j}$ appearing in Eqs. (5), (6), and (7) play a fundamental role as they determine the fixed point which the algorithm will converge to. These parameters represent our prior belief about the message sent from the source on the basis of the corrupted word we received on the other side of the channel. If no other information is available, we can simply set $\ell_i = 0$ for all i , except for a single node i^* for which $\ell_{i^*} = \pm\infty$. The latter condition is given by the fact that the original message is perfectly symmetric, so that we can impose that a given information bit is certainly 0 (i.e., $\ell_{i^*} = +\infty$) or 1 (i.e., $\ell_{i^*} = -\infty$) without providing aid to our decoder. The values of the LLRs $\ell_{i,j}$ are instead functions of the features of the noisy channel, and the observed value of the element of the adjacency matrix $A_{i,j}$. Without any prior knowledge (or hypotheses) on how the parity bits were actually altered by the channel, the approach is thus not applicable.

The iterative algorithm just introduced resembles the one considered by Decelle *et al.* [9,32]. This is a natural consequence of the fact that both algorithms are trying to solve the same type of problem. There are, however, some differences. The most important one is conceptual, as ours is a straight adaptation of a well-established decoding technique to specific

decoding tasks. In this respect, the algorithm maintains a general character. For instance, the algorithm explicitly adapts to any noisy channel by simply choosing appropriately the values of LLRs ℓ . Also within the same noisy channel, the algorithm written for the code \mathcal{P} is just one of the potentially many algorithms that can be generated starting from equivalent parity-check matrices. Further, our algorithm includes an error-correcting component for the parity bit values [Eq. (7)]. Finally, the performance of the family of algorithms can be studied with a standard technique of coding theory named density evolution [29,33], as we are going to illustrate below. We should remark, however, that the algorithm has the practical disadvantage of working with a number of equations that scale quadratically with the system size, rather than linearly as the algorithm by Decelle *et al.* This is a consequence of the general nature of the algorithm, being not devised to perform the specific decoding task considered here. In this respect, we stress that other efficient and effective coding-theoretical algorithms specifically devised for the stochastic block model are available on the market [26,34].

III. RESULTS

A. Stochastic block model and the detectability threshold

In terms of performance, our algorithm behaves similarly to the one by Decelle *et al.* This fact is visible in Fig. 2(a), where we consider the application of the algorithm to the stochastic block model, finding once more the existence of the so-called detectability threshold [9,15]. The information-theoretic sufficient and necessary condition of the detectability threshold has been proven in Refs. [23–26]. In its simplest variant (the one considered here), the stochastic block model serves to generate networks with planted community structure,

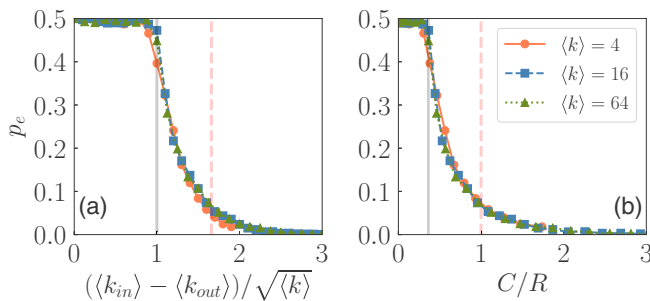


FIG. 2. Performance of the Gallager algorithm in the stochastic block model with two communities. (a) The plot shows the probability of error p_e for the information bits, i.e., the fraction of information bits that are not correctly decoded by the algorithm. We consider block models with $N = 10\,000$ divided in two equally sized groups with $n = N/2$ nodes. Each curve represents the results obtained for fixed average degree $\langle k \rangle = (n - 1)p_{\text{in}} + np_{\text{out}}$. The probability of error is computed as a function of difference between the average internal degree $\langle k_{\text{in}} \rangle = (n - 1)p_{\text{in}}$ and the average external degree $\langle k_{\text{out}} \rangle = np_{\text{out}}$. As the figure shows, the decoder is not able to recover any information in the regime $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle \leq \sqrt{\langle k \rangle}$ (gray full line). The probability of error is larger than zero at the decodability bound (red dashed line). (b) Same data as in panel (a), but the probability of error is plotted against the ratio C/R between channel capacity and rate of the code.

where N nodes are divided in two groups of sizes n and $N - n$, respectively. Nodes belonging to the same group are connected with probability p_{in} , while pairs of nodes belonging to different groups are connected with probability p_{out} . Using this knowledge of the channel, we can easily estimate the value of the LLRs $\ell_{i,j}$ required by the Gallager algorithm (Appendix B). The detectability threshold is generally studied for equally sized groups, so that $n = N/2$. One defines the average internal degree as $\langle k_{\text{in}} \rangle = (n - 1)p_{\text{in}}$, the average external degree as $\langle k_{\text{out}} \rangle = np_{\text{out}}$, and the average degree as $\langle k \rangle = \langle k_{\text{in}} \rangle + \langle k_{\text{out}} \rangle$. If the difference $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle$ is smaller than $\sqrt{\langle k \rangle}$, the algorithm is not able to detect any group. Groups start to be partially decoded only when $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle > \sqrt{\langle k \rangle}$.

B. Capacity of the noisy channel associated with the stochastic block model

The detectability threshold is one side of the medal. It tells us what is the minimum level of disorder that the channel should introduce to disrupt completely our ability to decode the original signal. One may, however, be interested in the behavior at regimes of lower noise, specifically to the value of maximum noise that can be tolerated to achieve perfect decoding, i.e., retrieve the original signal with no mistakes. This is often the case considered in the literature about performance of community detection algorithms [21,22]. It is also the typical case contemplated in information theory for reliable communication [28]. Recent literature has shown that exact recovery in the stochastic block model is still subjected to a threshold phenomenon [23,25]. The value of the threshold for the stochastic block model with two communities is given by $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle = \log N \sqrt{\frac{2\langle k \rangle}{\log N} - 1}$ (see Appendix H for the rephrasing of the original results of Refs. [23,25] according to the notation used in this paper). The above condition is valid in the limit of infinitely large stochastic block models with two equally sized communities decoded using a maximum likelihood decoder. The rationale behind the existence of such a finite-threshold effect is analogous to the one that describes the connectivity of the Erdős-Rényi model [35]. For instance, the logarithmic dependence of the threshold from the system size arises from the requirement of having no nodes with degree equal to zero, as those nodes cannot be correctly classified.

The threshold value is exact for infinitely large systems. However in numerical validations of community detection algorithms [20,22], system sizes are not very large. As we are going to show, the exact recovery threshold determines a too restrictive condition that does not provide an accurate estimate of the regime of exact recovery reached by the best algorithms. Such a condition must be relaxed to obtain more reliable predictions in finite-size systems. Here, we propose a simple way to do it. We compute a lower bound on the true value of the threshold using the Shannon’s noisy-channel coding theorem [27]. We refer to it as the decodability bound. The value of the bound differs from the one of the exact recovery threshold for a simple reason, already well emphasized in Ref. [24]: Shannon’s theorem is not the mathematically correct way to study exact recovery in community detection. The theorem applies in fact to the case where the channel properties are independent of the choice of the code. In the noisy-channel interpretation

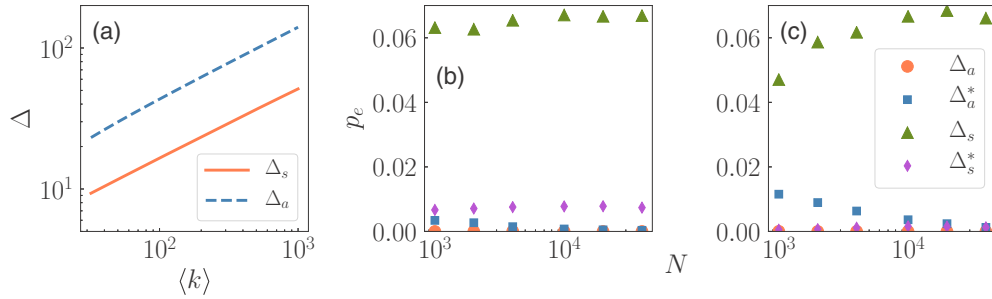


FIG. 3. Performance of the Gallager decoder at threshold. (a) Comparison between the exact recovery threshold (Δ_a , dashed blue line) and the decodability bound (Δ_s , orange full line) for a stochastic block model with $N = 10000$ nodes as a function of the average degree $\langle k \rangle$. (b) Probability of bit error p_e as a function of the network size N . We fix the value of the average degree $\langle k \rangle = 32$, and apply the Gallager decoder to 10 instances of the model. Results stand for average values of p_e over those realizations. Different colors and shapes correspond to different choices of $\langle k_{in} \rangle$. Orange circles are obtained at the exact recovery threshold; blue squares correspond to regimes of slightly larger amount of noise than the one corresponding to the exact recovery threshold, that is $\langle k_{in} \rangle$ is 0.9 times of the threshold value; green triangles are obtained at the decodability bound; purple diamonds are obtained slightly above the decodability bound by setting $\langle k_{in} \rangle$ is 1.1 times of its decodability bound value. (c) Same as in panel (b), but for $\langle k \rangle = 128$.

of community detection instead, the code is given, and there is no way of playing with it without necessarily changing the features of the channel. Given the lack of flexibility, the decodability bound is necessarily a lower bound of the true threshold. This tells us that exact recovery is impossible if the noise level is higher than what predicted by Shannon theorem. On the other hand, having a lower amount of noise than the one established by the bound does not provide a sufficient condition for perfect recovery. Both the exact recovery threshold and the decodability bound scale with the square root of the average degree of the graph (see Fig. 7). The difference between them grows logarithmically with the system size [see Figs. 7 and 3(a)]. As Shannon’s theorem is still derived in the limit of infinitely large systems, the decodability bound is potentially subjected to the same limitations as those of the exact recovery threshold. However, the different scaling with the system size of the decodability bound makes it a meaningful indicator for characterization of performances of community detection algorithms [20,22]. Another nice feature of the decodability bound is that it can be computed in a rather simple way by knowing just the properties of the stochastic network model without relying on any specific decoding protocol. In the following, we provide concrete support to these statements. For simplicity, we start describing how the decodability bound is computed in the stochastic block model with two communities. We will then proceed with calculations valid for other models, and numerical tests of the predictive power of the decodability bound.

In the interpretation of the community detection problem as a communication process, the stochastic block model is equivalent to an asymmetric binary channel [36]. We can compute the capacity of the channel as (see Appendix C)

$$C = H_2[\alpha^* p_{in} + (1 - \alpha^*) p_{out}] - \alpha^* H_2(p_{in}) - (1 - \alpha^*) H_2(p_{out}). \quad (8)$$

$H_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary entropy function. α^* is a function of p_{in} and p_{out} , and represents the value of the proportion of parity bits $\theta = 0$ in the transmitted codeword that maximizes the mutual information between

transmitted and received words. Knowing the capacity of the channel C and the rate R of the code [Eq. (2)], the decodability bound is determined by the condition $C/R = 1$. As the results of Fig. 2(b) show, the ratio C/R provides a natural scale to monitor the performance of the algorithm as a function of the channel noise, at the same footing as $(\langle k_{in} \rangle - \langle k_{out} \rangle) / \sqrt{\langle k \rangle}$ does. The two quantities are effectively related by the law $C/R \sim (\langle k_{in} \rangle - \langle k_{out} \rangle)^2 / \langle k \rangle$ (see Fig. 7).

The results of Figs. 3(b) and 3(c) highlight one of the potential reasons of why the decodability bound turns out to be more informative than the exact recovery threshold in finite-size systems. The figures show how the Gallager algorithm performs at different levels of noise as the system size increases. Slightly above the decodability bound but below the exact recovery threshold, the probability of information-bit error p_e is not exactly equal to zero. However, p_e is so small to become unnoticeable in numerical simulations. Further, the entity of the error becomes even smaller as the average degree increases.

C. Capacity-achieving codes

An issue that still remains open is understanding the performance of the LDPC codes we introduced earlier in the paper from a more formal point of view. In particular, we would like to better characterize their performances around the decodability bound. To address the issue, we rely on a popular technique, called density evolution, generally used to study the performances of LDPC decoders based on the Gallager algorithm. The advantage of the approach is that it allows us to study the performance of the algorithm without the need to run any simulation. The technique was introduced by Gallager himself in the analysis of the binary symmetric channel [29], and later generalized to arbitrary channels by Richardson and Urbanke [33]. The technique consists in assuming the LLR of the variable nodes as independent, and study the evolution of their probability density during the first t stages of the algorithm, with t smaller or equal than half of the girth of the underlying Tanner graph, i.e., until the assumption of independence among variables is justified. Estimating how

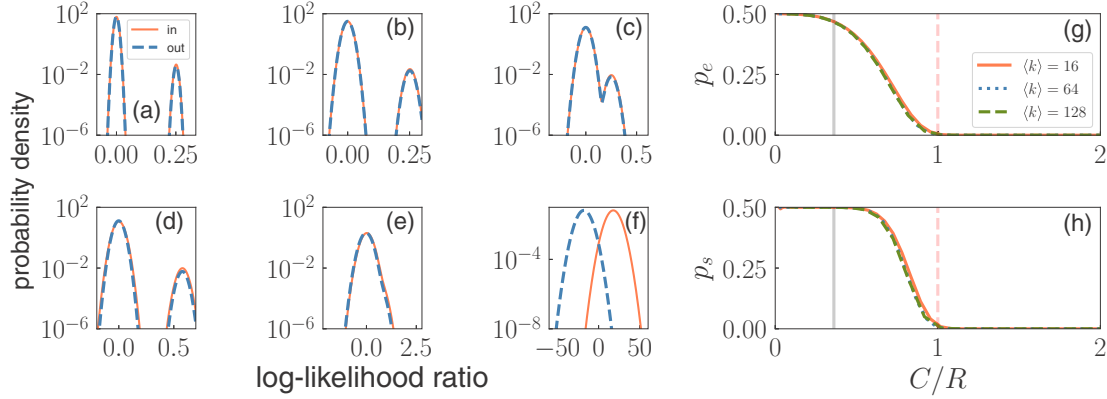


FIG. 4. Achieving the capacity of the stochastic block model. We consider a stochastic block model with $N = 10^5$, and groups of equal size $n = N/2$. (a) Probability density of the log-likelihood ratios (LLRs) after one iteration of the Gallager algorithm. The full orange line indicates the distribution for parity bits corresponding to internal pairs of nodes. The dashed blue line indicates the distribution for parity bits corresponding to external pairs of nodes. Here, we set $\langle k_{\text{in}} \rangle = (n-1)p_{\text{in}} = 36$ and $\langle k_{\text{out}} \rangle = np_{\text{out}} = 28$. The parameter values correspond to the regime where communities are not detectable. (b), (c) Same as in (a), but for the second and third iterations of the algorithm. (d)–(f) Same as in (a)–(c), but for $\langle k_{\text{in}} \rangle = (n-1)p_{\text{in}} = 41$ and $\langle k_{\text{out}} \rangle = np_{\text{out}} = 23$. In this regime communities are detectable, in the sense that good algorithms should be able to identify a nonvanishing portion of the nodes belonging to the two clusters. (g) Performance of the iterative algorithm after three iterations. We consider three different values of the average degree $\langle k \rangle$. The description of the figure is similar to the one of Fig. 2(b) with the difference that the probability of error p_e refers to parity bits only. (h) Probability p_s that a randomly chosen parity-check equation of the code \mathcal{T} is not satisfied as a function of the ratio C/R . We consider the same networks as those of (g).

LLR densities evolve requires repeated convolutions of distributions. The mathematical treatment of the density evolution for Gallager algorithm for the code \mathcal{P} is quite involved. However, for the equivalent code \mathcal{T} , it is greatly simplified (see Appendix F). In the limit of sufficiently large N , the distributions $P_{\text{in}}^{(t)}(\hat{\ell})$ and $P_{\text{out}}^{(t)}(\hat{\ell})$, respectively valid for the LLR of parity bits corresponding to pairs of nodes in the same group (internal pairs) and different groups (external pairs), are computed iteratively as convolutions of normal and delta distributions. These computations can be efficiently performed via numerical integration whose computational cost is virtually independent of the system size. From the LLR densities, we can further estimate (i) the probability of error on the best estimates of the parity bits, and (ii) the probability of error for the parity-check equations of the code \mathcal{T} [Eq. (4)]. These quantities serve to judge the overall performance of the algorithm. Everything can be carried out until $t = 3$ iterations, as the girth of the Tanner graph of the code equals six. This is a low number, yet sufficient to capture the general behavior of the algorithm.

Results of the density evolution analysis are reported in Fig. 4. First, we grasp why the detectability threshold emerges in the Gallager decoder. For $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle < \sqrt{\langle k \rangle}$, $P_{\text{in}}^{(t)}(\hat{\ell})$ and $P_{\text{out}}^{(t)}(\hat{\ell})$ are essentially identical, leading to the impossibility to properly disentangle internal from external parity bits. For $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle > \sqrt{\langle k \rangle}$ instead, the two distributions progressively separate one from the other, leading to partial (or even complete) recovery of the correct value of the parity bits. We note that decoding correctly a portion of the parity bits does not necessarily correspond to the correct recovery of a portion of the information bits [Fig. 4(g)]. If some of the parity-check equations of the \mathcal{T} code are violated [Fig. 4(h)], then some parity-check equations of the code \mathcal{C} are violated too. The relation between the two codes in terms of syndromes

is not trivial. Hence, one cannot conclude that a probability of parity-bit error smaller than 0.5 corresponds to a probability of information-bit error smaller than 0.5. On the other hand, \mathcal{P} and \mathcal{T} share the same codewords, thus, if the Gallager algorithm on the \mathcal{T} code converged finding a codeword, then convergence to the same codeword is guaranteed also for the code \mathcal{P} . In particular, if the codeword for \mathcal{T} is the one that perfectly disentangles parity bits corresponding to internal and external pairs, then the corresponding codeword for \mathcal{C} is the one that recovers perfectly the true values of information bits σ . As Fig. 4(h) shows, this situation happens approximately at the decodability bound, where both the probabilities of error for parity bits and parity-check equations are very close to zero. As a consequence, the algorithm is able to achieve performance very close to the channel capacity.

D. Stochastic block models with more than two groups

So far, we considered the simplest scenario of stochastic block models composed of two groups only. This is a rather special case, as the problem of identifying the memberships of the nodes can be mapped into a linear decoding task. Writing linear codes that apply to stochastic block models with more than two groups seems challenging. However, we can still provide insights to the problem of community detection by simply studying the channel characteristics, and relying on the Shannon's noisy-channel coding theorem to provide a lower bound for the maximal amount of noise admitted for exact recovery. From the graphical point of view, the situation of multiple groups is identical to the one of two groups (Fig. 1): we can imagine that the encoder generates a network of disconnected cliques, where every clique corresponds to a planted community. The effect of the channel is also the same as for the case of two groups: it erases completely the information

bits, and flips the values of some of the parity bits according to some stochastic rule. If the number of groups is Q , the rate of the code is given by

$$R = \frac{\log_2(Q^N/Q)}{N(N-1)/2} = \frac{2 \log_2 Q}{N}, \quad (9)$$

i.e., the generalization of Eq. (2) to the case of Q communities. We assume that the channel is still a binary asymmetric one, where parity bits $\theta = 0$ are flipped with probability $1 - p_{\text{in}}$, and parity bits $\theta = 1$ with probability p_{out} . This scenario includes naturally the case of the Girvan-Newman benchmark graphs [2]. Under these circumstances, we can extend all calculations valid for $Q = 2$ to arbitrary values of Q , arriving to the same expression for the capacity of the channel [Eq. (8)]. The only formal difference is in the value of α^* (see Fig. 6). The computation of this quantity requires to take derivatives with respect $Q - 1$ variables. However, the profile of mutual information is pretty much flat, reaching a maximum for a big number of different configurations. This fact allows us to assume that the maximum of the mutual information is also reached for equally sized groups, so that we can use

$$\alpha^* = \frac{N/Q - 1}{N - 1}. \quad (10)$$

In Fig. 5, we establish the value of the decodability bound for various models of interest in the literature about performance of algorithms in the detection of communities in synthetic graphs [20,22]. In Fig. 5(b), we consider the case of the Girvan-Newman (GN) benchmark graphs [2]. According to the Shannon's theorem, decoding exactly the community memberships is impossible as long as $C/R < 1$, with C computed using Eqs. (8) and (10), and R defined in Eq. (9). We estimate the bound in terms of the mixing parameter $\mu = \langle k_{\text{out}} \rangle / \langle k \rangle$ to make the results directly interpretable in terms of the numerical tests about performances of community detection algorithms on the same model (see Fig. 1 of Ref. [22]). The results of Fig. 5 are particularly illuminating in this regard. There are two regimes for which communities are in principle perfectly decodable: (i) a sufficiently assortative regime, where nodes have a number of internal edges that are sufficiently larger than the number of external connections, and (ii) a strongly disassortative regime, where external connections greatly outnumber internal connections. The bound in the assortative regime is located at $\mu \gtrsim 0.5$. Indeed, the best-performing algorithms in the analysis of Ref. [22] achieve almost perfect recovery until $\mu = 0.4$, while their performance drops down before reaching the point $\mu = 0.5$. The exact recovery threshold provides instead much more restrictive conditions [24]. According to it, the maximum amount of noise tolerable by the channel corresponds to $\mu \simeq 0.25$. However, most of the community detection algorithms are able to perfectly recover the planted community structure in the GN model well above $\mu \simeq 0.25$. To provide clear evidence of this fact, we replicated the results of Ref. [22] for Infomap [8], i.e., one of the top-performing algorithms. We extended the analysis also to the Lancichinetti-Fortunato-Radicchi (LFR) benchmark graphs [21], although this model is not exactly described by a stochastic block model (or a binary asymmetric channel from the perspective of coding theory). Yet, we are able to recover approximate estimates

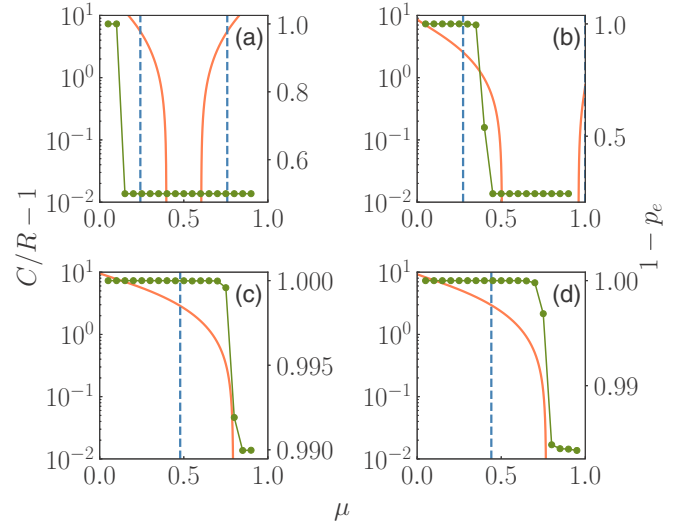


FIG. 5. Decodability bounds for the stochastic block model with multiple groups. We consider synthetic networks where N nodes are divided into Q groups of equal size. Pairs of nodes within the same group are connected with probability p_{in} , and pairs of nodes belonging to different groups are connected with probability p_{out} . The average value of the internal degree of a node is $\langle k_{\text{in}} \rangle = p_{\text{in}}(N/Q - 1)$, whereas the average value of the external degree is $\langle k_{\text{out}} \rangle = p_{\text{out}}N(Q - 1)/Q$. The probabilities p_{in} and p_{out} are subjected to the constraint $\langle k \rangle = \langle k_{\text{in}} \rangle + \langle k_{\text{out}} \rangle$. As the decodability bound is determined by the condition $C/R = 1$, with C/R ratio between the capacity of the channel and the rate of the code, we plot $C/R - 1$ as a function of the mixing parameter $\mu = \langle k_{\text{out}} \rangle / \langle k \rangle$. The latter quantity is used in place of the difference $\langle k_{\text{in}} \rangle - \langle k_{\text{out}} \rangle$ to make the results easily interpretable in the comparison with the performances of community detection algorithms on the same model [22]. The decodability bound is determined by the μ value where the orange full line drops down to values smaller than zero. As a term of comparison we plot, as vertical dashed blue lines, the value of exact recovery threshold [24] (see Appendix H for details on how the threshold is computed). As a paradigmatic example of a good community detection algorithm, we used Infomap [8], i.e., the top-performing algorithm according to the analysis of Ref. [22]. For every μ value, performance is measured in terms of $1 - p_e$, where p_e is the probability of parity-bit error (green squares). Exact recovery corresponds to $p_e = 0$. The results presented in the various panels refer to the average value of p_e computed over at least 10 independent realizations of the synthetic network model. (a) As in Fig. 2, we set $N = 10\,000$, $Q = 2$, and $\langle k \rangle = 64$. (b) Same as in (a), but for $N = 128$, $Q = 4$, and $\langle k \rangle = 16$. (c) Same as in (a) and (b), but for $N = 5000$, $Q = 100$, and $\langle k \rangle = 20$. (d) Same as in (a)–(c), but for $N = 5000$, $Q = 50$, and $\langle k \rangle = 20$. For the computation of the exact recovery threshold and the decodability bound, parameter values in (c) and (d) are chosen such that they are comparable with those used in Figs. 1 and 2 of Ref. [22]. In (c) and (d), Infomap is run on the LFR benchmark. Parameters of the model are chosen identical to those considered in Ref. [22].

about the regime of perfect performance of algorithms that well describe their behavior. In Figs. 5(c) and 5(d), for instance, we estimate the decodability regime for a stochastic block model with parameters that make the model comparable with the LFR benchmarks of types S and B , respectively, as defined in Ref. [22]. First, we recover threshold values that are just

slightly greater than those measured for the best-performing algorithms. The decodability bound is $\mu \gtrsim 0.75$, point at which all algorithms fail to correctly recover the planted partition. Second, as the threshold value for benchmarks of type *B* is smaller than the one found for benchmarks of type *S*, we are able to explain why such a slight difference in performance is also visible in practical algorithms (see also Fig. 2 of Ref. [22]). A third and final deduction from the plots is the disappearance of the disassortative regime of decodability visible instead in the GN benchmark graph. Still for the LFR model, the exact recovery threshold seems to not well represent the regime of perfect performance of the best algorithms for community detection available on the market. Also, from a comparison among the various panels of Fig. 5, it seems that the predictive power of the exact recovery threshold deteriorates as the number of communities in the stochastic model increases.

IV. CONCLUSIONS

The analogy between the problems of identifying communities in networks and communicating over a noisy channel is intrinsically present in all the methods for community detection based on statistical inference. In our contribution, we considered the analogy explicitly as already done in Refs. [23–25], and leveraged coding theory to achieve four main results. First, we built a family of equivalent linear codes based on low-density parity-check (LDPC) matrices, and show that they can be used to generate a class of LDPC community decoders. Second, we showed that the Shannon’s noisy-channel coding theorem sets a lower bound, named here as decodability bound, on the maximal amount of noise allowed for perfect community detection in the stochastic block model. Third, we connected the first two results, showing that LDPC community decoders are potentially able to reach the Shannon capacity of the stochastic block model. Fourth, whereas the above results are valid for the simplest case of stochastic block models with two communities only, we also showed that the decodability bound can be easily extended to the case of multiple communities providing a quantitatively accurate prediction of the regimes of performance of the best community detection algorithms available on the market [22]. This final result is certainly the most important from the practical point of view, as it seems to indicate that not much potential for improvement in performance is left. We stress that this conclusion can, at the moment, be supported only by numerical evidence. This fact restricts ourselves to consider the conclusion valid only for specific algorithms and specific settings of the stochastic block model. We do not exclude that the best-performing algorithms in the GN and LFR benchmarks will fail in other models, as a recent theoretical study [37] demonstrated that a single algorithm outperforming all other algorithms in every community detection task cannot exist. Further, as the mathematical proof of the Shannon’s noisy-channel coding theorem is valid only in the limit of infinitely large systems, there is no mathematical guarantee that the decodability bound must hold also for finite-size networks. Numerical evidence so far is supportive, but, until a mathematical explanation is provided, there is always the chance to find an algorithm able to beat the decodability bound.

ACKNOWLEDGMENTS

The author acknowledges financial support from the National Science Foundation (Grant No. CMMI-1552487), and from the US Army Research Office (Grant No. W911NF-16-1-0104).

APPENDIX A: SPECTRAL DECODER

An algorithm that approximates a minimum distance decoder can be deployed as follows. Our goal is to find the value of the information bits $\hat{\sigma}$ that lead to the minimum number of violated parity-check equations [Eq. (1) of the main text], given the word received. We can define a penalty function as

$$D = \sum_{i>j} A_{i,j}(1 - \delta_{\sigma_i, \sigma_j}) + \sum_{i>j} (1 - A_{i,j})\delta_{\sigma_i, \sigma_j} \\ \times E - 2 \sum_{i>j} A_{i,j}\delta_{\sigma_i, \sigma_j} + \sum_{i>j} \delta_{\sigma_i, \sigma_j},$$

where $\delta_{x,y} = 1$ if $x = y$, and $\delta_{x,y} = 0$ if $x \neq y$, $A_{i,j}$ is the i, j element of the adjacency matrix of the received network, and E is the total number of observed edges. Note that above sums are not performed in modulo 2. In the definition of the penalty function D , we are not allowing for any correction on the parity bits received. Thus, we can only act on the information bits. The best estimates of the bits $\hat{\sigma}$ are such that D is minimal. To approximate the solution, we can perform the transformation $\sigma_i = 0 \rightarrow \xi_i = 1$, and $\sigma_i = 1 \rightarrow \xi_i = -1$, so that $\delta_{\sigma_i, \sigma_j} = (1 + \xi_i \xi_j)/2$, and rewrite D as

$$D = E - \sum_{i>j} A_{i,j}(1 + \xi_i \xi_j) + \frac{1}{2} \sum_{i>j} (1 + \xi_i \xi_j) \\ \times \frac{N(N-1)}{4} + \frac{1}{2} \sum_{i>j} \xi_i \xi_j - \sum_{i>j} A_{i,j} \xi_i \xi_j$$

or in matrix-vector notation as

$$D = \frac{N(N-1)}{4} + \vec{\xi}^T (J/2 - \mathbb{I}/2 - A) \vec{\xi}, \quad (\text{A1})$$

where J is the all-one matrix, and \mathbb{I} is the identity matrix. The first term on the right-hand side of Eq. (A1) is a constant dependent only on the size of the network N . We need therefore to minimize only the rightmost term of the equation. An approximate solution for the configuration that minimizes D can be found by finding the largest eigenvector of the operator $A - J/2 + \mathbb{I}/2$, and set $\hat{\sigma}_i = 1$ if the corresponding component is smaller than zero, or $\hat{\sigma}_i = 0$, otherwise.

APPENDIX B: STOCHASTIC BLOCK MODEL AS A NOISY CHANNEL

In the stochastic block model, two nodes i and j belonging to the same group, with corresponding parity bit $\theta_{i,j} = 0$, are connected with probability p_{in} . The two nodes i and j belonging to different groups, with corresponding parity bit $\theta_{i,j} = 1$, are connected with probability p_{out} . This means that parity bits θ obey the rules of the following binary asymmetric

channel:

$$\begin{array}{c|c|c}
 \theta_{i,j} & A_{i,j} & P(A_{i,j}|\theta_{i,j}) \\
 \hline
 0 & 1 & p_{\text{in}} \\
 0 & 0 & 1 - p_{\text{in}} \\
 \hline
 1 & 1 & p_{\text{out}} \\
 1 & 0 & 1 - p_{\text{out}} \\
 \hline
 \end{array} . \quad (\text{B1})$$

We use the information about the noisy channel to determine the best estimate of $\theta_{i,j}$ given the observed value of $A_{i,j}$. We can write

$$P(\theta_{i,j}|A_{i,j}) = \frac{P(A_{i,j}|\theta_{i,j})P(\theta_{i,j})}{P(A_{i,j})}.$$

As we have no prior knowledge of the group assignments of the nodes, and therefore about true values of the parity bit $\theta_{i,j}$, we can set $P(\theta_{i,j}) = 1/2$. Additionally, we can write $P(A_{i,j} = 1) = (p_{\text{in}} + p_{\text{out}})/2$ and $P(A_{i,j} = 0) = 1 - (p_{\text{in}} + p_{\text{out}})/2$. Using our knowledge of the noisy channel, we can thus write

$$P(\theta_{i,j} = 0|A_{i,j} = 1) = \frac{p_{\text{in}}}{p_{\text{in}} + p_{\text{out}}}$$

and

$$P(\theta_{i,j} = 0|A_{i,j} = 0) = \frac{1 - p_{\text{in}}}{2 - (p_{\text{in}} + p_{\text{out}})}.$$

We can use those probabilities to determine the value of the log-likelihood ratios (LLRs)

$$\begin{aligned}
 \ell_{i,j} &= \log \frac{P(\theta_{i,j} = 0|A_{i,j})}{P(\theta_{i,j} = 1|A_{i,j})} \\
 &= \begin{cases} \log(p_{\text{in}}) - \log(p_{\text{out}}) & \text{if } A_{i,j} = 1, \\ \log(1 - p_{\text{in}}) - \log(1 - p_{\text{out}}) & \text{if } A_{i,j} = 0. \end{cases} \quad (\text{B2})
 \end{aligned}$$

APPENDIX C: CAPACITY OF THE CHANNEL

Messages are given by divisions of the network of N nodes into two blocks with size n and $N - n$, respectively. Once n is fixed, there will be $\binom{N}{n}$ equiprobable messages. One of those messages is encoded into a codeword $\vec{\theta}$ composed of

$$\Theta_0 = \binom{n}{2} + \binom{N-n}{2}$$

parity bits equal to zero, and

$$\Theta_1 = n(N - n)$$

parity bits equal to one. The length of the codeword is fixed and does not depend on n :

$$L = \Theta_0 + \Theta_1.$$

Strictly speaking the codeword contains also information bits. However, those bits are completely erased by the channel, thus for the computation of the capacity, we can think that the codeword is composed of parity bits only.

In the stochastic block model, the relation between transmitted and received parity bits is given by Eq. (B1). For simplicity, let us define $\phi_{i,j} = (1 + A_{i,j}) \bmod 2$. As the probability that an individual received bit $\phi_{i,j}$ is dependent only on the value

of the bit transmitted $\theta_{i,j}$, we can write

$$P(\vec{\phi}|\vec{\theta}) = \prod_{(i,j)} P(\phi_{i,j}|\theta_{i,j}).$$

As the probability associated to the value of a generic received parity bit ϕ is dependent only on the value of the transmitted bit θ , and for a fixed value of n all $\binom{N}{n}$ configurations are equiprobable, we can simply state that

$$P(\theta = 0|n) = \Theta_0/(\Theta_0 + \Theta_1) = \alpha$$

and

$$P(\theta = 1|n) = \Theta_1/(\Theta_0 + \Theta_1) = (1 - \alpha).$$

The parity bit ϕ is received as flipped with probability p_{out} if $\theta = 1$, while it will stay equal to θ with probability p_{in} if $\theta = 0$. The conditional entropy is then given by

$$H(\phi|\theta) = \alpha H_2(p_{\text{in}}) + (1 - \alpha) H_2(p_{\text{out}}),$$

where

$$H_2(f) = -f \log_2(f) - (1 - f) \log_2(1 - f)$$

is the binary entropy function. The probability that a received parity-check bit ϕ is zero is

$$P(\phi = 0) = \alpha p_{\text{in}} + (1 - \alpha) p_{\text{out}}.$$

Thus, the entropy of the received bit ϕ is

$$H(\phi) = H_2[\alpha p_{\text{in}} + (1 - \alpha) p_{\text{out}}].$$

The expression for the mutual information reads as

$$\begin{aligned}
 I(\theta; \phi) &= H_2[\alpha p_{\text{in}} + (1 - \alpha) p_{\text{out}}] \\
 &\quad - \alpha H_2(p_{\text{in}}) - (1 - \alpha) H_2(p_{\text{out}}). \quad (\text{C1})
 \end{aligned}$$

In Fig. 6, we display the profile of the mutual information for specific settings of the stochastic block model. To find the channel capacity, we need to maximize I with respect to α . For simplicity, we will assume α continuous. The derivative of the binary entropy function is

$$\frac{d}{dx} H_2(x) = \log_2(x^{-1} - 1).$$

The derivative of the mutual information is therefore

$$\begin{aligned}
 \frac{d}{d\alpha} I(\theta; \phi) &= (p_{\text{in}} - p_{\text{out}}) \log_2 \left[\frac{1}{\alpha p_{\text{in}} + (1 - \alpha) p_{\text{out}}} - 1 \right] \\
 &\quad - H_2(p_{\text{in}}) + H_2(p_{\text{out}}).
 \end{aligned}$$

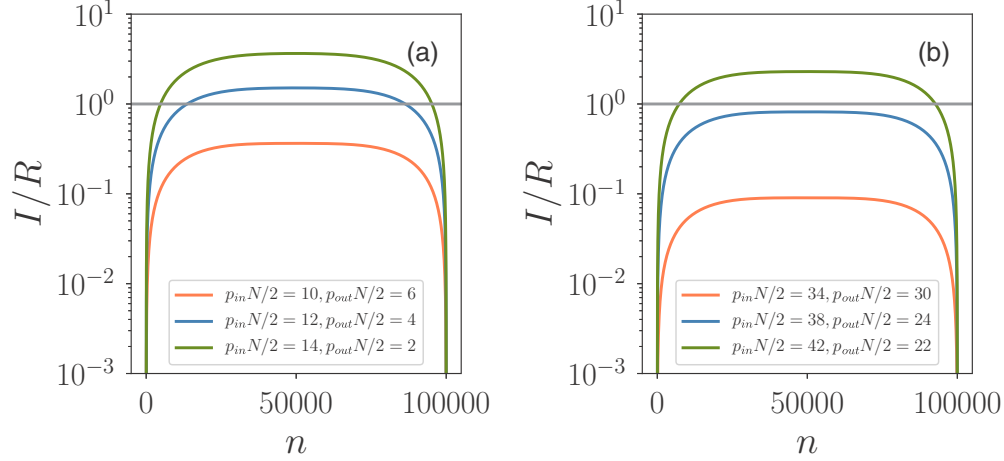


FIG. 6. (a) Mutual information I [Eq. (C1)] divided by the rate of the code $R = 2/(N + 2)$ as a function of the module size n (the size of the other module is $N - n$). We consider fixed values of the probabilities p_{in} and p_{out} . Here, $N = 10^5$. (b) Same as in (a), but for different values of p_{in} and p_{out} .

Setting the previous expression equal to zero, we have

$$(p_{in} - p_{out}) \log_2 \left[\frac{1}{\alpha^* p_{in} + (1 - \alpha^*) p_{out}} - 1 \right] - H_2(p_{in}) + H_2(p_{out}) = 0,$$

$$\log_2 \left[\frac{1}{\alpha^* p_{in} + (1 - \alpha^*) p_{out}} - 1 \right] = \frac{H_2(p_{in}) - H_2(p_{out})}{p_{in} - p_{out}},$$

$$\frac{1}{\alpha^* p_{in} + (1 - \alpha^*) p_{out}} - 1 = 2^{\frac{H_2(p_{in}) - H_2(p_{out})}{p_{in} - p_{out}}}.$$

For simplicity, let us define

$$z = 2^{\frac{H_2(p_{in}) - H_2(p_{out})}{p_{in} - p_{out}}},$$

thus,

$$\frac{1}{\alpha^* p_{in} + (1 - \alpha^*) p_{out}} = z + 1,$$

$$\alpha^* p_{in} + (1 - \alpha^*) p_{out} = \frac{1}{1 + z},$$

$$\alpha^*(p_{in} - p_{out}) = \frac{1 - p_{out}(1 + z)}{1 + z},$$

$$\alpha^* = \frac{1 - p_{out}(1 + z)}{(1 + z)(p_{in} - p_{out})},$$

so that we have

$$\alpha^* = \frac{1 - p_{out} \left(1 + 2^{\frac{H_2(p_{in}) - H_2(p_{out})}{p_{in} - p_{out}}} \right)}{\left(1 + 2^{\frac{H_2(p_{in}) - H_2(p_{out})}{p_{in} - p_{out}}} \right) (p_{in} - p_{out})}. \quad (C2)$$

The capacity of the channel is

$$C = H_2[\alpha^* p_{in} + (1 - \alpha^*) p_{out}] - \alpha^* H_2(p_{in}) - (1 - \alpha^*) H_2(p_{out}). \quad (C3)$$

In Fig. 7, we show that the ratio between channel capacity and code rate is a tight function of the parameters of the stochastic block model.

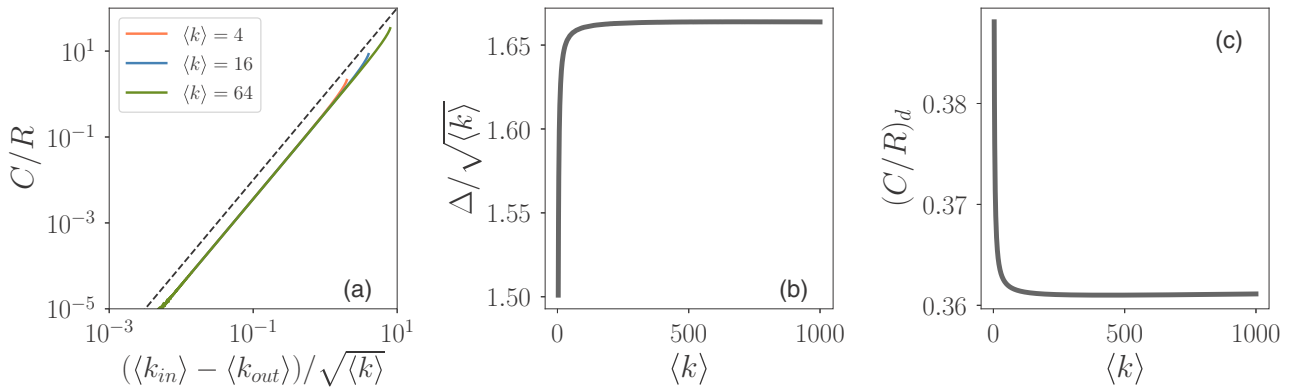


FIG. 7. (a) Relation between the ratio C/R , capacity divided by rate, and $(\langle k_{in} \rangle - \langle k_{out} \rangle)/\sqrt{\langle k \rangle}$ for the stochastic block model with $N = 10^6$ and two groups with identical size $n = N/2$. $\langle k_{in} \rangle = p_{in}(n - 1)$, $\langle k_{out} \rangle = p_{out}n$, and $\langle k \rangle = \langle k_{in} \rangle + \langle k_{out} \rangle$. We consider different values of $\langle k \rangle$. The black dashed line identifies a power law with exponent 2. (b) We compute Δ as the value of $\langle k_{in} \rangle - \langle k_{out} \rangle$ for which $C/R = 1$. As the plot shows, the value $\Delta/\sqrt{\langle k \rangle}$ saturates quickly at 1.66 as $\langle k \rangle$ grows. (c) We determined the value of the ratio C/R when $\langle k_{in} \rangle - \langle k_{out} \rangle = \sqrt{\langle k \rangle}$. We indicated this with $(C/R)_d$, and plotted the quantity as a function of the average degree $\langle k \rangle$. We observe a quick saturation $(C/R)_d \simeq 0.36$ as $\langle k \rangle$ grows.

APPENDIX D: ITERATIVE DECODING FOR THE PAIR CODE

We employ the Gallager algorithm to decode the received word. The technique involves messages sent back and forth between variable nodes to check nodes on the Tanner graph constructed from the parity-check matrix H of Eq. (3) of the main text. We have a total of $N + N(N - 1)/2$ variable nodes. The first N correspond to the actual nodes of the graph. The other $N(N - 1)/2$ variable nodes are instead given by all pairs of nodes in the graph. Check nodes amount to $N(N - 1)/2$, each corresponding to a pair of nodes in the graph.

To describe variable nodes, we use the following notation. The generic node i has associated log-likelihood ratio (LLR)

$$\ell_i = \log \frac{P(\sigma_i = 0|s_i)}{P(\sigma_i = 1|s_i)},$$

where $s_i = 0, 1$ is the received information bit, and σ_i is the transmitted information bit. Please note that in our problem we actually do not receive any information bit, as these are erased by the channel. Similarly, for a generic pair (i, j) of nodes, we define the LLR as

$$\ell_{i,j} = \log \frac{P(\theta_{i,j} = 0|A_{i,j})}{P(\theta_{i,j} = 1|A_{i,j})},$$

where $\phi_{i,j} = 1 + A_{i,j}$ is the received parity bit. Note that the former definition is perfectly symmetric under the exchange of i and j . It is clearly not defined, and actually not used, for $i = j$. This fact is assumed below.

ℓ_i and $\ell_{i,j}$ are our best estimates of the value of the variable nodes at stage $t = 0$ of the algorithm. At iteration t of the algorithm, the variable node i sends to the check node (i, j) the message

$$m_{i \rightarrow (i,j)}^{(t)} = \begin{cases} \ell_i & \text{if } t = 0, \\ \ell_i + \sum_{k \neq j, k \neq i} n_{(i,k) \rightarrow i}^{(t-1)} & \text{if } t \geq 1. \end{cases}$$

The message sent from the variable node (i, j) to the check node (i, j) is instead equal to $\ell_{i,j}$ in all rounds of the algorithm. In the above expression, $n_{(i,j) \rightarrow i}$ is the message sent back from the check node (i, j) to node i , and is defined as

$$n_{(i,j) \rightarrow i}^{(t)} = \log \frac{1 + \tanh(1/2 m_{j \rightarrow (i,j)}^{(t-1)}) \tanh(1/2 \ell_{i,j})}{1 - \tanh(1/2 m_{j \rightarrow (i,j)}^{(t-1)}) \tanh(1/2 \ell_{i,j})}.$$

The check node (i, j) sends a message back also to the variable node (i, j) equal to

$$n_{(i,j) \rightarrow (i,j)}^{(t)} = \log \frac{1 + \tanh(1/2 m_{i \rightarrow (i,j)}^{(t-1)}) \tanh(1/2 m_{j \rightarrow (i,j)}^{(t-1)})}{1 - \tanh(1/2 m_{i \rightarrow (i,j)}^{(t-1)}) \tanh(1/2 m_{j \rightarrow (i,j)}^{(t-1)})}.$$

Please note that the latter message is not used in the iterative algorithm. It is, however, used to check the convergence of the algorithm as it follows. At round $t > 0$ of the algorithm, the estimated values of the LLRs are

$$\hat{\ell}_i^{(t)} = \ell_i + \sum_{k \neq i} n_{(i,k) \rightarrow i}^{(t)},$$

$$\hat{\ell}_{i,j}^{(t)} = \ell_{i,j} + n_{(i,j) \rightarrow (i,j)}^{(t)}.$$

The estimate of the bits associated with the variable nodes is performed with a hard-decision choice, setting $\hat{\sigma}_i = 0$ if

$\hat{\ell}_i^{(t)} < 0$ and $\hat{\sigma}_i = 1$, otherwise. Similarly for the best estimate of the pair variable $\hat{\theta}_{i,j} = 0$ if $\hat{\ell}_{i,j}^{(t)} < 0$ and $\hat{\theta}_{i,j} = 1$, otherwise. Based on this choice, we can establish if the bit string decoded at iteration t is an actual codeword, i.e., $(\hat{\sigma}_i + \hat{\sigma}_j + \hat{\theta}_{i,j}) \bmod 2 = 0$, for all $i \neq j$. In such a case, we determine that the algorithm has converged. Otherwise, we run the algorithm up to a desired maximal number of iterations.

When applied to the stochastic block model, we can set $\ell_i = 0$ for all i , except for $\ell_{i^*} = \pm\infty$ for one node i^* . The values of $\ell_{i,j}$ are instead provided in Eq. (B2).

Simplification of the decoding algorithm

The structure of the equations above allows us to simplify the decoding algorithm. As messages sent by pair variables are unchanged, we can simply define

$$\zeta_{i \rightarrow j}^{(t)} = m_{i \rightarrow (i,j)}^{(t)}$$

to write $\zeta_{i \rightarrow j}^{(t=0)} = \ell_i$ and

$$\zeta_{i \rightarrow j}^{(t)} = \ell_i + \sum_{k \neq j} \log \frac{1 + \tanh(1/2 \zeta_{k \rightarrow i}^{(t-1)}) \tanh(1/2 \ell_{i,k})}{1 - \tanh(1/2 \zeta_{k \rightarrow i}^{(t-1)}) \tanh(1/2 \ell_{i,k})}$$

for $t \geq 1$. The best estimates of the LLRs at stage $t \geq 1$ are

$$\hat{\ell}_i^{(t)} = \ell_i + \sum_k \log \frac{1 + \tanh(1/2 \zeta_{k \rightarrow i}^{(t-1)}) \tanh(1/2 \ell_{i,k})}{1 - \tanh(1/2 \zeta_{k \rightarrow i}^{(t-1)}) \tanh(1/2 \ell_{i,k})}$$

and

$$\hat{\ell}_{i,j}^{(t)} = \ell_{i,j} + \log \frac{1 + \tanh(1/2 \zeta_{j \rightarrow i}^{(t-1)}) \tanh(1/2 \zeta_{i \rightarrow j}^{(t-1)})}{1 - \tanh(1/2 \zeta_{j \rightarrow i}^{(t-1)}) \tanh(1/2 \zeta_{i \rightarrow j}^{(t-1)})}.$$

APPENDIX E: ITERATIVE ALGORITHM FOR THE TRIPLET CODE

If instead of the pair code, we consider the triplet code

$$(\theta_{i,j} + \theta_{i,k} + \theta_{j,k}) \bmod 2 = 0,$$

we can still use the Gallager algorithm on the corresponding Tanner graph. The Tanner graph contains $N(N - 1)/2$ variable nodes. Each of those variable nodes is connected to $N - 2$ check nodes. The total number of check nodes is $N(N - 1)(N - 2)/6$, each for every triplet.

At iteration t of the algorithm, the variable node (i, j) sends to the check node (i, j, k) the message

$$m_{(i,j) \rightarrow (i,j,k)}^{(t)} = \begin{cases} \ell_{i,j} & \text{if } t = 0, \\ \ell_{i,j} + \sum_{s \neq i, j, k} n_{(i,j,s) \rightarrow (i,j)}^{(t-1)} & \text{if } t \geq 1. \end{cases}$$

The sum appearing above runs over all triplets connected to (i, j) , excluding the triplet (i, j, k) . In turn, check nodes reply

to variable nodes with

$$n_{(i,j,k) \rightarrow (i,j)}^{(t)} = \log \frac{1 + \tanh(1/2 m_{(i,k) \rightarrow (i,j,k)}^{(t-1)}) \tanh(1/2 m_{(j,k) \rightarrow (i,j,k)}^{(t-1)})}{1 - \tanh(1/2 m_{(i,k) \rightarrow (i,j,k)}^{(t-1)}) \tanh(1/2 m_{(j,k) \rightarrow (i,j,k)}^{(t-1)})}.$$

The reply depends only on the messages that the triplet (i, j, k) received from the other two pairs attached to it, namely, (i, k) and (j, k) . For $t \geq 1$, best estimates of the LLRs for variable nodes are

$$\hat{\ell}_{i,j}^{(t)} = \ell_{i,j} + \sum_k n_{(i,j,k) \rightarrow (i,j)}^{(t-1)} = \ell_{i,j} + \sum_k \log \frac{1 + \tanh(1/2 m_{(i,k) \rightarrow (i,j,k)}^{(t-1)}) \tanh(1/2 m_{(j,k) \rightarrow (i,j,k)}^{(t-1)})}{1 - \tanh(1/2 m_{(i,k) \rightarrow (i,j,k)}^{(t-1)}) \tanh(1/2 m_{(j,k) \rightarrow (i,j,k)}^{(t-1)})}.$$

APPENDIX F: DENSITY EVOLUTION FOR THE TRIPLET CODE ON THE STOCHASTIC BLOCK MODEL

For simplicity, we consider only the case of two equally sized groups, so that $n = N/2$. Our plan is to monitor the evolution of the probability densities of the log-likelihood ratios (LLRs) for internal and external pairs of nodes. An internal pair of nodes consists in two nodes i and j within the same group. We know that the true value of parity bit for such a pair is $\theta_{i,j} = 0$. An external pair of nodes consists in two nodes i and j belonging to different groups. The true value of the parity bit associated to this external pair is $\theta_{i,j} = 1$. At stage t of the iterative algorithm, the LLR densities of external and internal pairs are, respectively, indicated as $P_{\text{in}}^{(t)}(\hat{\ell})$ and $P_{\text{out}}^{(t)}(\hat{\ell})$. These densities describe the behavior of the LLRs over an infinite number of realizations of the stochastic block model. To monitor the evolution of the LLR densities as functions of the iteration t of the algorithm, we assume variables to be independent. This assumption is correct up to $t = 3$, as the girth of the underlying Tanner graph is 6. For a larger number of iterations, variables in the true algorithm become dependent on each other, and they do not longer obey the distributions derived under the independence assumption.

For a generic internal pair, the initial value of the LLR will be a random variable obeying the distribution

$$P_{\text{in}}^{(t=0)}(\hat{\ell}) = \delta\left(\hat{\ell} - \log \frac{p_{\text{in}}}{p_{\text{out}}}\right) p_{\text{in}} + \delta\left(\hat{\ell} - \log \frac{1 - p_{\text{in}}}{1 - p_{\text{out}}}\right) (1 - p_{\text{in}}),$$

where $\delta(x) = 1$ if $x = 0$, and $\delta(x) = 0$, otherwise.

For a generic external pair, the initial value of the LLR is a random variable obeying the distribution

$$P_{\text{out}}^{(t=0)}(\hat{\ell}) = \delta\left(\hat{\ell} - \log \frac{p_{\text{in}}}{p_{\text{out}}}\right) p_{\text{out}} + \delta\left(\hat{\ell} - \log \frac{1 - p_{\text{in}}}{1 - p_{\text{out}}}\right) (1 - p_{\text{out}}).$$

Every pair is connected to a total of $2n - 2$ parity checks. If the pair is internal, then the pair will be connected to $n - 2$ parity checks that include other two internal pairs, and n parity checks that include two external pairs (see Fig. 8). For an external pair instead, all parity checks necessarily include another external pair, and one internal pair.

At iteration $t \geq 1$, the distribution of the LLR for a generic internal pair is obtained as the sum of three independent con-

tributions. The first term is a single random variable extracted from $P_{\text{in}}^{(t=0)}$, namely, z_{in} . The second term is given by the sum of $n - 2$ random variables. The value of each of these variables is obtained by first extracting two random variables from $P_{\text{in}}^{(t-1)}$, namely $x_{\text{in}}^{(g)}$ and $y_{\text{in}}^{(g)}$, and then computing the quantity

$$q_{\text{in,in}}^{(g)} = \log \frac{1 + \tanh(x_{\text{in}}^{(g)}/2) \tanh(y_{\text{in}}^{(g)}/2)}{1 - \tanh(x_{\text{in}}^{(g)}/2) \tanh(y_{\text{in}}^{(g)}/2)}.$$

The value of the second term is given by

$$q_{\text{in,in}} = \sum_{g=1}^{n-2} q_{\text{in,in}}^{(g)}.$$

The third term is given by the sum of n random variables, generated from the sum of two random variables $x_{\text{out}}^{(g)}$ and $y_{\text{out}}^{(g)}$, extracted at random from the distribution $P_{\text{out}}^{(t-1)}$. For a given pair of random variables, we compute

$$q_{\text{out,out}}^{(g)} = \log \frac{1 + \tanh(x_{\text{out}}^{(g)}/2) \tanh(y_{\text{out}}^{(g)}/2)}{1 - \tanh(x_{\text{out}}^{(g)}/2) \tanh(y_{\text{out}}^{(g)}/2)}.$$

The value of the third term is finally given by

$$q_{\text{out,out}} = \sum_{g=1}^n q_{\text{out,out}}^{(g)}.$$

As the various quantities are determined independently, the distribution of the LLR for internal pairs after the t th iteration is

$$P_{\text{in}}^{(t)}(\hat{\ell}) = P^{(t=0)}(z_{\text{in}}) P^{(t-1)}(q_{\text{in,in}}) P^{(t-1)}(q_{\text{out,out}}) \times \delta(\hat{\ell} - z_{\text{in}} - q_{\text{in,in}} - q_{\text{out,out}}), \quad (\text{F1})$$

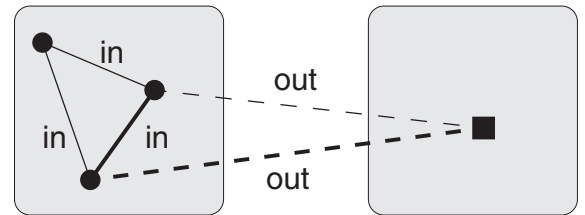


FIG. 8. Every internal pair of nodes is involved in two types of parity-check equations: (i) those formed with other two internal pairs, and (ii) those formed with two external pairs. Every external pair of nodes is instead involved in parity-check equations with one internal and one external pair.

where $P^{(t=0)}(z_{\text{in}})$, $P^{(t-1)}(q_{\text{in},\text{in}})$, and $P^{(t-1)}(q_{\text{out},\text{out}})$ are, respectively, the probability distributions of the variables z_{in} , $q_{\text{in},\text{in}}$, and $q_{\text{out},\text{out}}$ as defined above.

For external pairs, the computation of the distribution of the LLRs is very similar. There will be two contributions. The first is just a random variable extracted from $P_{\text{out}}^{(t=0)}$, namely, z_{out} . The second is computed by extracting two random numbers $x_{\text{in}}^{(g)}$ and $y_{\text{out}}^{(g)}$, respectively, from the distributions $P_{\text{in}}^{(t-1)}$ and $P_{\text{out}}^{(t-1)}$. One then evaluates the quantity

$$q_{\text{in},\text{out}}^{(g)} = \log \frac{1 + \tanh(x_{\text{in}}^{(g)}/2) \tanh(y_{\text{out}}^{(g)}/2)}{1 - \tanh(x_{\text{in}}^{(g)}/2) \tanh(y_{\text{out}}^{(g)}/2)}.$$

The value of the second term is finally given by

$$q_{\text{in},\text{out}} = \sum_{g=1}^{2n-2} q_{\text{in},\text{out}}^{(g)},$$

and the distribution of the LLR for external pairs is given by

$$P_{\text{out}}^{(t)}(\hat{\ell}) = P^{(t=0)}(z_{\text{out}}) P^{(t-1)}(q_{\text{in},\text{out}}) \delta(\hat{\ell} - z_{\text{out}} - q_{\text{in},\text{out}}). \quad (\text{F2})$$

1. Approximation for large networks

For $N \gg 1$, we expect that the distributions $P^{(t)}(q_{\text{in},\text{in}})$, $P^{(t)}(q_{\text{out},\text{out}})$, and $P^{(t)}(q_{\text{in},\text{out}})$ appearing at iterations $t \geq 1$ are

$$P_{\text{in}}^{(t+1)}(\hat{\ell}) = p_{\text{in}} \mathcal{N}\{\hat{\ell}; \mu_{\text{in}}^{(t)} + \log(p_{\text{in}}/p_{\text{out}}), \sigma_{\text{in}}^{(t)}\} + (1 - p_{\text{in}}) \mathcal{N}\{\hat{\ell}; \mu_{\text{in}}^{(t)} + \log[(1 - p_{\text{in}})/(1 - p_{\text{out}})], \sigma_{\text{in}}^{(t)}\} \quad (\text{F3})$$

and

$$P_{\text{out}}^{(t+1)}(\hat{\ell}) = p_{\text{out}} \mathcal{N}\{\hat{\ell}; \mu_{\text{out}}^{(t)} + \log(p_{\text{in}}/p_{\text{out}}), \sigma_{\text{out}}^{(t)}\} + (1 - p_{\text{out}}) \mathcal{N}\{\hat{\ell}; \mu_{\text{out}}^{(t)} + \log[(1 - p_{\text{in}})/(1 - p_{\text{out}})], \sigma_{\text{out}}^{(t)}\}, \quad (\text{F4})$$

where

$$\begin{aligned} \mu_{\text{in}}^{(t)} &= (n-2)\mu_{\text{in},\text{in}}^{(t)} + n\mu_{\text{out},\text{out}}^{(t)}, \\ (\sigma_{\text{in}}^{(t)})^2 &= (n-2)(\sigma_{\text{in},\text{in}}^{(t)})^2 + n(\sigma_{\text{out},\text{out}}^{(t)})^2, \\ \mu_{\text{out}}^{(t)} &= (2n-2)\mu_{\text{in},\text{out}}^{(t)}, \end{aligned}$$

and

$$(\sigma_{\text{out}}^{(t)})^2 = (2n-2)(\sigma_{\text{in},\text{out}}^{(t)})^2.$$

Equations (F3) and (F4) follow directly from Eqs. (F1) and (F2), as the distributions involved in the convolution are only normal and delta distributions. Equations (F3) and (F4) allow us to compute the probability of bit error as

$$p_e^{(t)} = \frac{1}{2} (\epsilon_{\text{in}} + \epsilon_{\text{out}}), \quad (\text{F5})$$

where we used the approximation $\alpha \simeq \frac{1}{2}$ for sufficiently large values of N , and

$$\epsilon_{\text{in}} = \int_{-\infty}^0 d\ell P_{\text{in}}^{(t)}(\ell)$$

and

$$\epsilon_{\text{out}} = \int_0^{+\infty} d\ell P_{\text{out}}^{(t)}(\ell).$$

We can further estimate the probability that one randomly chosen parity-check equation is violated as

$$p_s^{(t)} = 1 - \frac{w_{\text{in}}[(1 - \epsilon_{\text{in}})^3 + 3\epsilon_{\text{in}}^2(1 - \epsilon_{\text{in}})] + w_{\text{out}}[(1 - \epsilon_{\text{in}})\epsilon_{\text{out}}^2 + 2\epsilon_{\text{in}}\epsilon_{\text{out}}(1 - \epsilon_{\text{out}}) + (1 - \epsilon_{\text{in}})\epsilon_{\text{out}}^2]}{w_{\text{in}} + w_{\text{out}}}, \quad (\text{F6})$$

well described by normal distributions, so that

$$P^{(t)}(q_{\text{in},\text{in}}) \simeq \mathcal{N}(q_{\text{in},\text{in}}; (n-2)\mu_{\text{in},\text{in}}^{(t)}, \sqrt{n-2}\sigma_{\text{in},\text{in}}^{(t)}),$$

$$P^{(t)}(q_{\text{out},\text{out}}) \simeq \mathcal{N}(q_{\text{out},\text{out}}; n\mu_{\text{out},\text{out}}^{(t)}, \sqrt{n}\sigma_{\text{out},\text{out}}^{(t)}),$$

and

$$P^{(t)}(q_{\text{in},\text{out}}) \simeq \mathcal{N}(q_{\text{in},\text{out}}; (2n-2)\mu_{\text{in},\text{out}}^{(t)}, \sqrt{2n-2}\sigma_{\text{in},\text{out}}^{(t)}).$$

We used here $\mathcal{N}(x; \mu, \sigma)$ to indicate that the variable x is distributed according to a normal distribution with the average μ and standard deviation σ .

If we define

$$g(x, y) = \log \frac{1 + \tanh(x/2) \tanh(y/2)}{1 - \tanh(x/2) \tanh(y/2)},$$

we have

$$\mu_{\text{in},\text{in}}^{(t)} = \int dx \int dy P_{\text{in}}^{(t)}(x) P_{\text{in}}^{(t)}(y) g(x, y)$$

and

$$(\sigma_{\text{in},\text{in}}^{(t)})^2 + (\mu_{\text{in},\text{in}}^{(t)})^2 = \int dx \int dy P_{\text{in}}^{(t)}(x) P_{\text{in}}^{(t)}(y) [g(x, y)]^2.$$

Similar expressions can be written for $\mu_{\text{out},\text{out}}^{(t)}$, $\sigma_{\text{out},\text{out}}^{(t)}$, $\mu_{\text{in},\text{out}}^{(t)}$, and $\sigma_{\text{in},\text{out}}^{(t)}$. The updated values of the distributions $P_{\text{in}}^{(t+1)}(\hat{\ell})$ and $P_{\text{out}}^{(t+1)}(\hat{\ell})$ for stage $t+1$ of the algorithm are given by

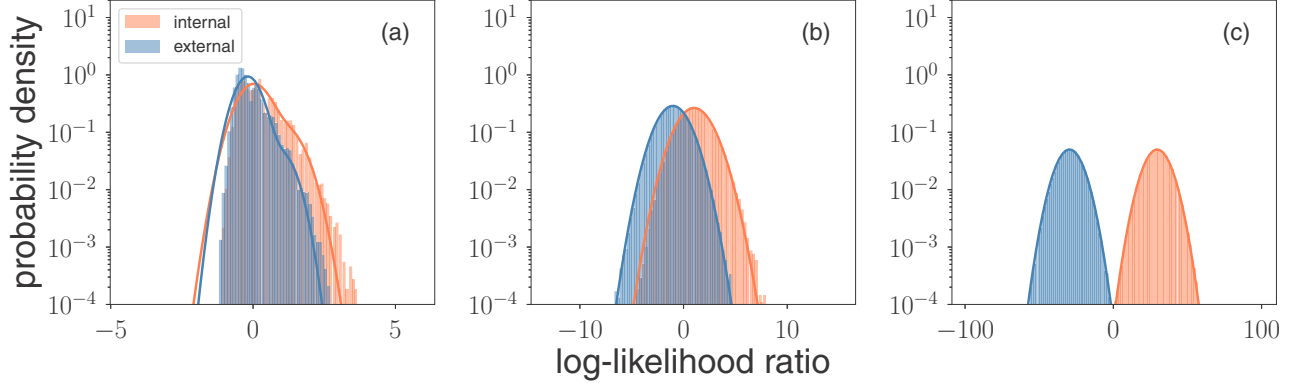


FIG. 9. Density distribution $P_{\text{in}}^{(t)}(\hat{\ell})$ of the log-likelihood ratio for internal pairs (orange), and density distribution $P_{\text{out}}^{(t)}(\hat{\ell})$ of the log-likelihood ratio for external pairs (blue) for a network with $N = 100$ nodes, and equally sized groups with $n = 50$ nodes. We consider $(n-1)p_{\text{in}} = \langle k_{\text{in}} \rangle = 6$ and $np_{\text{out}} = \langle k_{\text{out}} \rangle = 2$. The plot shows how the distributions change as functions of the iteration t of the algorithm: (a) $t = 1$, (b) $t = 2$, and (c) $t = 3$. Results of numerical simulations (bars) are compared with the normal approximations (lines) of Eqs. (F3) and (F4).

where

$$w_{\text{in}} = \frac{n(n-1)(n-2)}{3}$$

and

$$w_{\text{in}} = n^2(n-1).$$

In Figs. 9 and 10, we provide a comparison between theoretical and numerical estimates of the LLR density distributions.

APPENDIX G: CAPACITY OF STOCHASTIC BLOCK MODELS WITH MORE THAN TWO GROUPS

So far, we considered the simplest scenario of stochastic block models composed of only two groups. Under this assumption, the problem of identifying the memberships of the groups can be mapped into a decoding task of a linear code. Writing linear codes that apply to scenarios where the presence of multiple groups is allowed seems challenging. However, we can still provide insights to the problem by simply studying the channel characteristics, and relying on the Shannon theorem to provide indications about the regime of exact recovery. The nonconstructive nature of the Shannon theorem itself allows us to draw conclusions directly from the rate of the code and the channel features without the need of necessarily specifying

an encoding or decoding protocol. From the graphical point of view, the situation of multiple groups is identical to the one of two groups. Still, we can imagine that the encoder generates a network of disconnected cliques depending on the memberships of the nodes, and that the channel flips the values of those bits according to some stochastic rule.

Indicate with Q the total number of groups in the networks, and with n_i the number of nodes in group i . We clearly have that

$$\sum_{i=1}^Q n_i = N.$$

The total number of parity bits equal to zero in the transmitted codeword is

$$\Theta_0 = \sum_{i=1}^Q \frac{n_i(n_i-1)}{2} = \frac{1}{2} \sum_{i=1}^Q n_i^2 - \frac{N}{2}.$$

The total number of parity bits equal to one is instead

$$\Theta_1 = \frac{N(N-1)}{2} - \Theta_0.$$

Exactly as in the case of two groups, it is convenient to define

$$\alpha = \frac{\Theta_0}{\Theta_0 + \Theta_1}$$

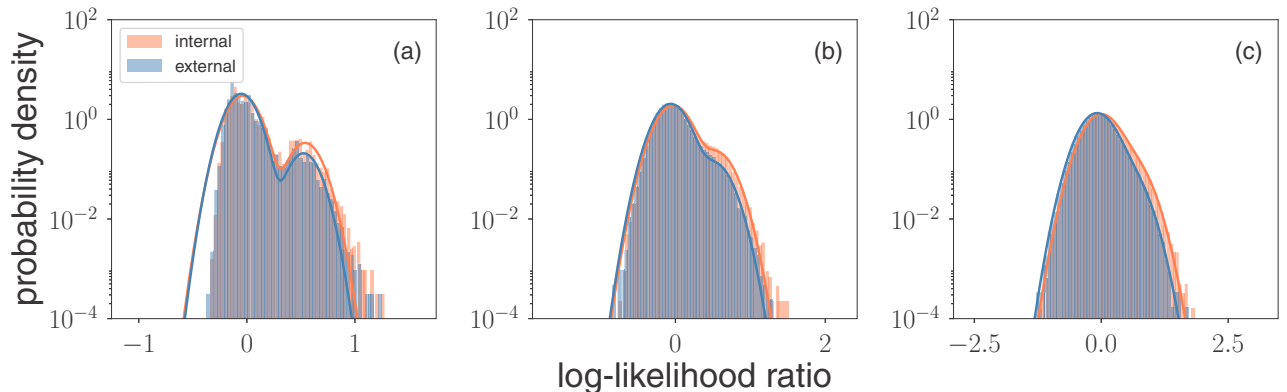


FIG. 10. Same as in Fig. 9 but for $(n-1)p_{\text{in}} = \langle k_{\text{in}} \rangle = 5$ and $np_{\text{out}} = \langle k_{\text{out}} \rangle = 3$.

as the relative amount of parity bits equal to zero. The rate of the code is given in Eq. (9).

For simplicity, let us focus on the case in which the channel acts on the codeword using the rules of a binary asymmetric channel [Eq. (B1)]. Under these conditions, everything we wrote for the case of two groups up to Eq. (C1) still holds. The fundamental difference here is that α depends on the size of the Q groups. In principle, the maximization of the mutual information requires to take derivatives with respect to $Q - 1$ variables. The profile of mutual information in this hyperdimensional space is similar to the one appearing in Fig. 6, looking flat over a big number of different configurations. This fact allows us to assume that the maximum of the mutual information is also reached for equally sized groups, $n_i = N/Q$ for all i , so that we can write

$$\Theta_0^* = \frac{N(N/Q - 1)}{2}$$

and

$$\alpha^* = \frac{N/Q - 1}{N - 1}. \quad (G1)$$

Finally, we can obtain the channel capacity as

$$C = H_2[\alpha^* p_{in} + (1 - \alpha^*) p_{out}] - \alpha^* H_2(p_{in}) - (1 - \alpha^*) H_2(p_{out}). \quad (G2)$$

APPENDIX H: COMPARISON WITH THE EXACT RECOVERY THRESHOLD

In Refs. [23,25], the authors provided an exact estimate of the threshold that the parameters of the stochastic block model must satisfy to have necessary and sufficient conditions for exact recovery of the modules. We report here only the results for the symmetric case, where a network with N nodes is divided into Q groups of size N/Q . Pairs of nodes in the

same group are connected with probability p_{in} , whereas pairs of nodes in different groups are connected with probability p_{out} . The condition reads as

$$(\sqrt{a} - \sqrt{b})^2 = Q, \quad (H1)$$

where

$$a = \frac{p_{in} N}{\log N} \quad \text{and} \quad b = \frac{p_{out} N}{\log N}.$$

As in our analysis we often consider the decodability of the model as a function of the difference between average internal and external degrees and fixed average total degree, in the following we rewrite Eq. (H1) in these terms. We note that

$$a = \frac{Q \langle k_{in} \rangle}{\log N} \quad \text{and} \quad b = \frac{Q \langle k_{out} \rangle}{(Q - 1) \log N}.$$

The solution of Eq. (H1) is

$$b^* = \frac{c \pm \sqrt{2cQ - Q^2}}{2},$$

where

$$c = \frac{Q \langle k_{in} \rangle + Q/(Q - 1) \langle k_{out} \rangle}{\log N}.$$

The value of a at threshold is

$$a^* = c - b^*.$$

For the case $Q = 2$, we can write the threshold as

$$|\langle k_{in} \rangle - \langle k_{out} \rangle| = \log N \sqrt{\frac{2 \langle k \rangle}{\log N} - 1}. \quad (H2)$$

For $Q > 2$, the value of the mixing parameter [22] for which perfect recovery is allowed is given by

$$\mu^* = \frac{(Q - 1) \log N b^*}{\langle k \rangle Q}. \quad (H3)$$

The condition for exact recovery is found imposing $\mu^* = \mu$.

[1] S. Fortunato, *Phys. Rep.* **486**, 75 (2010).
 [2] M. Girvan and M. E. Newman, *Proc. Natl. Acad. Sci. USA* **99**, 7821 (2002).
 [3] F. Radicchi, C. Castellano, F. Cecconi, V. Loreto, and D. Parisi, *Proc. Natl. Acad. Sci. USA* **101**, 2658 (2004).
 [4] M. E. J. Newman, *Phys. Rev. E* **88**, 042822 (2013).
 [5] M. E. J. Newman and M. Girvan, *Phys. Rev. E* **69**, 026113 (2004).
 [6] J. Reichardt and S. Bornholdt, *Phys. Rev. Lett.* **93**, 218701 (2004).
 [7] M. Rosvall and C. T. Bergstrom, *Proc. Natl. Acad. Sci. USA* **104**, 7327 (2007).
 [8] M. Rosvall and C. T. Bergstrom, *Proc. Natl. Acad. Sci. USA* **105**, 1118 (2008).
 [9] A. Decelle, F. Krzakala, C. Moore, and L. Zdeborová, *Phys. Rev. Lett.* **107**, 065701 (2011).
 [10] B. Karrer and M. E. J. Newman, *Phys. Rev. E* **83**, 016107 (2011).
 [11] T. P. Peixoto, *Phys. Rev. X* **4**, 011047 (2014).
 [12] T. P. Peixoto, *Phys. Rev. Lett.* **110**, 148701 (2013).
 [13] T. P. Peixoto, [arXiv:1705.10225](https://arxiv.org/abs/1705.10225).
 [14] C. Moore, [arXiv:1702.00467](https://arxiv.org/abs/1702.00467).
 [15] R. R. Nadakuditi and M. E. J. Newman, *Phys. Rev. Lett.* **108**, 188701 (2012).
 [16] F. Krzakala, C. Moore, E. Mossel, J. Neeman, A. Sly, L. Zdeborová, and P. Zhang, *Proc. Natl. Acad. Sci. USA* **110**, 20935 (2013).
 [17] F. Radicchi, *Phys. Rev. E* **88**, 010801 (2013).
 [18] F. Radicchi, *Europhys. Lett.* **106**, 38001 (2014).
 [19] J.-G. Young, P. Desrosiers, L. Hébert-Dufresne, E. Laurence, and L. J. Dubé, *Phys. Rev. E* **95**, 062304 (2017).
 [20] L. Danon, A. Diaz-Guilera, J. Duch, and A. Arenas, *J. Stat. Mech.: Theory Exp.* (2005) P09008.
 [21] A. Lancichinetti, S. Fortunato, and F. Radicchi, *Phys. Rev. E* **78**, 046110 (2008).
 [22] A. Lancichinetti and S. Fortunato, *Phys. Rev. E* **80**, 056117 (2009).
 [23] E. Abbe, A. S. Bandeira, and G. Hall, *IEEE Trans. Inf. Theory* **62**, 471 (2016).

- [24] E. Abbe and C. Sandon, in *IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS), 2015* (IEEE, Piscataway, NJ, 2015), pp. 670–688.
- [25] E. Abbe, [arXiv:1703.10146](https://arxiv.org/abs/1703.10146).
- [26] E. Mossel, J. Neeman, and A. Sly, *Combinatorica* (2017), doi:[10.1007/s00493-016-3238-8](https://doi.org/10.1007/s00493-016-3238-8).
- [27] C. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
- [28] D. J. MacKay, *Information Theory, Inference and Learning Algorithms* (Cambridge University Press, Cambridge, 2003).
- [29] R. Gallager, *IRE Trans. Inf. Theory* **8**, 21 (1962).
- [30] D. J. MacKay and R. M. Neal, *Electron. Lett.* **32**, 1645 (1996).
- [31] J. Bierbrauer, *Introduction to Coding Theory* (Chapman and Hall, New York, 2004).
- [32] A. Decelle, F. Krzakala, C. Moore, and L. Zdeborová, *Phys. Rev. E* **84**, 066106 (2011).
- [33] T. J. Richardson and R. L. Urbanke, *IEEE Trans. Inf. Theory* **47**, 599 (2001).
- [34] E. Abbe and C. Sandon, in *Advances in Neural Information Processing Systems 29*, edited by D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett (Curran Associates, Inc., 2016), pp. 1334–1342.
- [35] P. Erdős and A. Rényi, *Publ. Math. Inst. Hung. Acad. Sci.* **5**, 343 (1960).
- [36] I. Neri, N. Skantzos, and D. Bollé, *J. Stat. Mech.: Theory Exp.* (2008) P10018.
- [37] L. Peel, D. B. Larremore, and A. Clauset, *Sci. Adv.* **3**, e1602548 (2017).