Combinatorics, Probability and Computing (2001) 10, 219–237. Printed in the United Kingdom
© 2001 Cambridge University Press

An Entropy Approach to the Hard-Core Model on Bipartite Graphs

JEFF KAHN†

Department of Mathematics and RUTCOR,
Rutgers University, New Brunswick, NJ 08903, USA
(e-mail: jkahn@math.rutgers.edu)

Received 2 June 1999; revised 6 November 2000

We use entropy ideas to study hard-core distributions on the independent sets of a finite, regular bipartite graph, specifically distributions according to which each independent set I is chosen with probability proportional to $\lambda^{|I|}$ for some fixed $\lambda > 0$. Among the results obtained are rather precise bounds on occupation probabilities; a 'phase transition' statement for Hamming cubes; and an exact upper bound on the number of independent sets in an n-regular bipartite graph on a given number of vertices.

1. Introduction

Write $\mathscr{I}(G)$ for the collection of independent sets of a graph G. (An *independent set* is a set of vertices spanning no edges. For graph theory basics see, for example, [5]. A few conventions are mentioned at the end of this section.)

For G finite and $\lambda > 0$, the *hard-core distribution* (h.c.d.) with *activity* (or *fugacity*) λ on $\mathscr{I} = \mathscr{I}(G)$ is given by

$$p_\lambda(I) = p_\lambda^G(I) = \lambda^{|I|}[\textstyle\sum\{\lambda^{|I'|} : I' \in \mathscr{I}\}]^{-1} \qquad \text{for } I \in \mathscr{I}.$$

(For good introductions to the hard-core model see [3], [11]; see also [10] for more general background.) In particular, $\lambda = 1$ gives uniform distribution. One may also assign different activities λ_v to the different vertices v and take $\Pr(I)$ proportional to $\prod_{v\in I}\lambda_v$, but we will not do so here; again see [3], [11].

We will also say the above distribution is $\mathrm{hc}(\lambda)$, and refer to it as a distribution 'on G'. For infinite G a measure μ on $\mathscr{I}(G)$ is $\mathrm{hc}(\lambda)$ if, for $\mathbf{I}$ chosen according to μ and for each finite $W \subset V$, the conditional distribution of $\mathbf{I}\cap W$ given $\mathbf{I}\cap(V\setminus W)$ is μ-a.s. the same as $\mathrm{hc}(\lambda)$ on the independent sets of $\{w \in W : w \not\sim \mathbf{I}\cap(V\setminus W)\}$ (the vertices that can still

† Supported by NSF.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

be in $\mathbf{I}$ given $\mathbf{I} \cap (V \setminus W)$). General considerations (see [10]) imply that there is always at least one such μ. If there is more than one, the model is said to have a *phase transition.*

Here we are mainly interested in *bipartite* G, say with bipartition $V = V(G) = \mathscr{E} \cup \mathscr{O}$ (for 'even' and 'odd'). In this case one may loosely think of phase transition as saying that $\mathbf{I}$ is typically mostly even or mostly odd. The graphs we most often have in mind are, in the finite case, Hamming cubes $\{0,1\}^n$ and, more generally, tori (a torus being $(\mathbf{Z}/M)^d$ for some even M, with the usual nearest-neighbour adjacency), and in the infinite case $\mathbf{Z}^d$.

For $G = \mathbf{Z}^d$ Dobrushin [8] proved that there is a phase transition for sufficiently large λ (depending on d), but it is not even known that there is $\lambda(d)$ such that one has phase transition for $\lambda > \lambda(d)$ but not for $\lambda < \lambda(d)$. Nonetheless, we may define the *critical activity* for $\mathbf{Z}^d$ to be $\lambda_c(d) = \inf\{\lambda : \mathrm{hc}(\lambda) \text{ on } \mathbf{Z}^d \text{ has a phase transition}\}$. A central problem is then to better understand $\lambda_c(d)$, and in particular to prove the following.

Conjecture 1.1. $\lambda_c(d) \to 0 \quad (d \to \infty)$.

This has been the subject of some effort – if not publication – by a number of people in both the statistical mechanics and discrete mathematics communities over the last few years. Opinion regarding the conjecture was initially divided, but the consensus now seems to be that it is true, with $\lambda_c(d)$ probably as small as $O(\log d/d)$, or even $O(1/d)$ ($\Omega(1/d)$ is a lower bound).

In this paper we confine ourselves to (large) finite graphs, but remark at the outset that the natural (as yet unproved) extension of Theorem 1.3 from cubes to tori, in conjunction with Theorem 1.4, is easily seen to imply Conjecture 1.1.

For the remainder of the paper, unless stated otherwise, we will take G to satisfy the following assumption.

Assumption 1.2. *G is n-regular and bipartite with N vertices and bipartition $V = V(G) = \mathscr{E} \cup \mathscr{O}$.*

We will show that, for fixed λ and large n, $\mathrm{hc}(\lambda)$ on $\{0,1\}^n$ does have a 'phase transition' in the rough sense mentioned earlier, namely that $\mathbf{I}$ is typically drawn mostly from one side of the bipartition. There are two parts to this, the more difficult of which is as follows.

Theorem 1.3. *For any fixed $\lambda, \varepsilon > 0$, and $\mathbf{I}$ chosen according to p_λ on $\{0,1\}^n$, a.s.*

$$\min\{|\mathbf{I} \cap \mathscr{E}|, |\mathbf{I} \cap \mathscr{O}|\} < O(n^{-1/2+\varepsilon}2^n). \tag{1.1}$$

(As usual, 'a.s.' means with probability tending to 1 as $n \to \infty$.) Here and in several instances below (see the discussion following Example 1.8) it should be possible to improve terms like the $n^{-1/2+\varepsilon}$ in (1.1) to $\exp[-\Omega(n)]$.

Of course, Theorem 1.3 is only interesting if we know that $|\mathbf{I}|$ itself is typically large. It turns out that we can show something surprisingly precise in this direction, even for G satisfying only Assumption 1.2. To state this we need a little notation.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

For a probability distribution p on $\mathcal{I}(G)$, $\mathbf{I}$ chosen according to p, and $v \in V$, let $p(v) = \Pr(v \in \mathbf{I})$ (the *occupation probability* for v) and $\overline{p} = N^{-1} \sum_{v \in V} p(v) = \mathbf{E}|\mathbf{I}|/N$.

Set $\alpha_\lambda = \lambda/(2(1+\lambda))$. Thus α_λ would be the occupation probability (of any vertex) if our independent set were chosen with probability $1/2$ from each of $p_\lambda^{\mathcal{E}}$, $p_\lambda^{\mathcal{O}}$. Since we may think of 'phase transition' as saying that p_λ^G is close to this distribution, we may hope that, under suitable conditions, the occupation probabilities for p_λ^G are close to α_λ. In fact Corollary 1.5(a) says that this happens whenever we have Assumption 1.2.

Theorem 1.4. *Fix $\lambda > 0$ and let $\mathbf{I}$ be chosen according to p_λ^G (G satisfying Assumption 1.2). Then, for some constant C (depending on λ) and any $\xi > Cn^{-1/2}$,*

$$\Pr(||\mathbf{I}| - \alpha_\lambda N| > \xi N) = O(\xi^{-1} 2^{-\Omega(\xi^2 N)}).$$

Set

$$\zeta = \max\left\{\frac{1}{n}, \frac{\log N}{N}\right\}. \tag{1.2}$$

(In most examples of interest n is small compared to N, so $\zeta = 1/n$.)

Given Theorem 1.4, routine calculations (here left to the reader) yield the following result.

Corollary 1.5. *Under the conditions of Theorem 1.4,*

(a) $|\overline{p} - \alpha_\lambda| < O(\sqrt{\zeta})$,
(b) *a.s.* $||\mathbf{I}| - \alpha_\lambda N| < O(\sqrt{\zeta})N$.

So, for instance for large n, a *uniform* independent set from a G satisfying Assumption 1.2 has average occupation probability close to $1/4$. As far as I know this is not even obvious when $G = \{0,1\}^n$, and indeed this question for the cube, suggested by Rob van den Berg [2], was the starting point for the present investigation.

In many cases we can improve Theorem 1.4 and Corollary 1.5 a bit; however, in the absence of an appealing general formulation, we will do so here only for tori.

Theorem 1.6. *Let G range over tori (so G is either $(\mathbf{Z}/M)^{n/2}$ for some even $M > 2$ or $\{0,1\}^n$). Fix $\lambda > 0$ and $\beta < 1$, and let $\mathbf{I}$ be chosen according to p_λ^G. Then, for some constant C (depending on λ) and any $\xi \geq Cn^{-\beta}$,*

$$\Pr(||\mathbf{I}| - \alpha_\lambda N| > \xi N) = O(\xi^{-1} 2^{-\Omega(\xi^2 N)}).$$

Corollary 1.7. *Under the conditions of Theorem 1.6,*

(a) $|\overline{p} - \alpha_\lambda| < O(n^{-\beta})$,
(b) *a.s.* $||\mathbf{I}| - \alpha_\lambda N| < O(n^{-\beta})N$.

As we will see shortly (see the first remark at the end of this section), the seemingly minor improvement from $n^{-1/2}$ to $n^{-1+\varepsilon}$ is essential for the proof of Theorem 1.3.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

More generally, it seems interesting to decide how far the error term $O(\sqrt{\zeta})$ in Corollary 1.5 can be improved in various situations. The following simple construction shows that it cannot be improved too much in general.

Example 1.8. *Let H, H' be disjoint copies of $K_{n,n}$ with x, y (x', y') on opposite sides of H (H'), and let G be obtained from $H \cup H'$ by deleting the edges $\{x, y\}$, $\{x', y'\}$ and adding the edges $\{x, y'\}$, $\{x', y\}$. Then (it is easy to see that) for any fixed λ, $p_\lambda(x) = p_\lambda(y) = p_\lambda(x') = p_\lambda(y') = \alpha_\lambda - \Omega(1)$, and $\overline{p}_\lambda = \alpha_\lambda - \Theta(1/n)$.*

As far as we know, Theorem 1.6 and Corollary 1.7 could be true even for G satisfying only Assumption 1.2, which in view of Example 1.8 would be close to optimal. On the other hand, we feel certain that the correct error terms for tori are much smaller, and, moreover, that there should really be fairly general hypotheses – conceivably even symmetry is enough – that support such a conclusion. (For tori, an optimistic guess would be $\alpha_\lambda - \overline{p}_\lambda \approx n(1+\lambda)^{-n}$. For $K_{n,n}$, $\overline{p}_\lambda$ is actually slightly *larger* than α_λ.)

Preview

We now outline the contents of the paper and give some pointers to some of the proofs. In particular, the proof of Theorem 1.3, modulo results proved in later sections, is given following Proposition 1.12.

Most of what we do here is based on analysis of the entropies of various distributions on $\mathscr{I}(G)$. It may be that the method itself is the paper's most significant contribution. The basic idea is similar to that of [13] (which in turn was somehow inspired by Jaikumar Radhakrishnan's lovely entropy proof of the Minc Conjecture (Brégman's Theorem) [15]); but apart from [13] I do not know of any work taking a similar approach.

Section 2 includes entropy background and one technical lemma. Section 3 gives a quick indication of the basic method, embodied in some simple inequalities which are the starting point for most of what follows. Central to the approach are the events

$$Q_v = \{\mathbf{I} \cap N_v = \emptyset\},$$

where, for $v \in V$, $N_v = \{w : w \sim v\}$ (so Q_v is a prerequisite for $\{v \in \mathbf{I}\}$). Note that these events should show phase transitions and related behaviour more clearly than the events $\{v \in \mathbf{I}\}$, for example, since if there is a phase transition then $\mathbf{J} := \{v : Q_v \text{ occurs}\}$ should be roughly equal to one of $\mathscr{E}$, $\mathscr{O}$, whereas $\mathbf{I}$ will only pick out a small subset of one of these (if, as is usually the case, we think of λ as small).

In Section 4 we digress to give a simple and precise application of the method, namely, the following result.

Theorem 1.9. *If G is an n-regular bipartite graph on N vertices, then*

$$\log|\mathscr{I}(G)| \leq \frac{N}{2n}\log(2^{n+1}-1). \tag{1.3}$$

This is sharp whenever G is a disjoint union of $K_{n,n}$s. See Section 4 for some discussion and related questions, in particular the irritating Conjecture 4.1.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

In Section 5 we elaborate on the basic inequalities of Section 3 to give an upper bound in terms of $\bar{p}$ on the entropy, $H(\mathbf{I})$, of $\mathbf{I}$ drawn from an *arbitrary* distribution on $\mathscr{I}(G)$, as follows.

Proposition 1.10. *For G satisfying Assumption 1.2 and $\mathbf{I}$ drawn from any distribution p on $\mathscr{I}(G)$,*

$$H(\mathbf{I}) \leq (N/2)[1/n + H(2\bar{p})]. \tag{1.4}$$

This bound is then used to prove Theorem 1.4, the argument for which goes roughly as follows. Set $\mathscr{I}_k = \mathscr{I}_k(G) = \{I \in \mathscr{I} : |I| = k\}$. For any α we may apply (1.4) (later called (5.5)) to $\mathbf{I}$ chosen uniformly from $\mathscr{I}_{\alpha N}$, to obtain an upper bound on the total weight, $|\mathscr{I}_{\alpha N}|\lambda^{\alpha N}$, of Is of size αN. For α not too close to α_λ, this upper bound is much less than a trivial lower bound (see (5.6)) on the total weight of Is of size close to $\alpha_\lambda N$, and this gives Theorem 1.4.

The heart of the proof of Theorem 1.3 is contained in Section 6. Most of the work there is devoted to the proof of Lemma 6.1, the most important part of which (see (6.3)) says, roughly, that, for $d(v, w)$ small and even, the events Q_v, Q_w are strongly (positively) correlated. We defer the precise statement, together with a sketch of this part of the argument, to the beginning of Section 6. Note that this most interesting phase of the proof is valid for tori in general.

Given Lemma 6.1, we easily derive Theorem 1.6, as well as the following lemma, which is what we need for Theorem 1.3. Recall that $\mathbf{J} = \{v : Q_v \text{ occurs}\}$ and set $\mathbf{J}' := \{v \in \mathbf{J} : N_v \cap \mathbf{J} = \emptyset\}$ $(\supseteq \mathbf{I})$.

Lemma 1.11. *Let G be a torus and let $\mathbf{I}$ be chosen either uniformly from $\mathscr{I}_{\alpha N}(G)$ with $\alpha > \Omega(1)$ (and αN an integer), or according to p_λ^G with $\lambda > 0$ fixed. Then, for any fixed $\gamma < 1$ and sufficiently large n,*

$$a.s. \quad |\mathbf{J}'| > (1/2 - n^{-\gamma})N. \tag{1.5}$$

To derive Theorem 1.3 from Lemma 1.11, we just need to say that a $\mathbf{J}'$ as in (1.5) cannot have large intersection with both $\mathscr{E}$ and $\mathscr{O}$. This is where cube and general torus diverge: the weaker isoperimetric properties of the latter do not support such a statement, while for cubes an adequate inequality is given by the following observation, whose proof is given in Section 7.

Proposition 1.12. *If $\mathscr{X} \subseteq \{0,1\}^n$ is independent of size at least $(1-n^{-\beta})2^{n-1}$ with $\beta > 1/2$ fixed, then*

$$\min\{|\mathscr{X} \cap \mathscr{E}|, |\mathscr{X} \cap \mathscr{O}|\} < O(n^{1/2-\beta}\log^{-1/2} n)2^n.$$

Proof of Theorem 1.3. For λ, ε, $\mathbf{I}$ as in the theorem, with (w.l.o.g.) $\varepsilon < 1/2$ and $\gamma = 1-\varepsilon$, Lemma 1.11 and Proposition 1.12 imply that a.s.

$$\min\{|\mathbf{J}' \cap \mathscr{E}|, |\mathbf{J}' \cap \mathscr{O}|\} < O(n^{1/2-\gamma}\log^{-1/2} n)2^n.$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

The theorem follows since $\mathbf{I} \subseteq \mathbf{J}'$. □

Remarks. **(1)** Here we see the crucial difference between $O(n^{-1/2})$ and $O(n^{-1/2-\varepsilon})$ in our error terms; namely, Proposition 1.12 gives no information on $\mathbf{J}'$ if we relax the lower bound in Lemma 1.11 to $(1-n^{-1/2})N$ (and nothing like the proposition holds if we allow $\beta = 1/2$).

(2) Of course, we also have Theorem 1.3 for $\mathbf{I}$ uniform from $\mathscr{I}_{\alpha N}$ ($\alpha = \Omega(1)$).

Terminology

All our graphs are simple, with vertex and edge sets denoted V and E (or $V(G)$ and $E(G)$ if necessary). We use $x \sim y$ for adjacency of x, y (*i.e.*, $\{x, y\} \in E$), $d(x) = d_G(x)$ for the degree of (number of vertices adjacent to) x, and $d(x, y)$ for the distance between x and y.

We use $\mathbf{E}$ for expectation, and 'big O' notation (O, Θ, *etc.*) in the usual ways.

2. Preliminaries

In this section we recall the relevant entropy background and mention one easy technical lemma on concave functions. All of the material on entropy except Lemma 2.1, as well as a good discussion of what entropy 'means', can be found in [14, Chapter 1].

In what follows $\mathbf{X}$, $\mathbf{Y}$, *etc.* are discrete random variables (r.v.s), which in our usage are allowed to take values in any countable (here always finite) set. Throughout the paper we take $\log = \log_2$.

As usual, H is the (binary) entropy function, $H(\alpha) = \alpha \log(1/\alpha) + (1-\alpha)\log(1/(1-\alpha))$. The *entropy* of r.v. $\mathbf{X}$ is

$$H(\mathbf{X}) = \sum_x p(x) \log \frac{1}{p(x)} ,$$

where we write $p(x)$ for $\Pr(\mathbf{X} = x)$ (and extend this convention in natural ways below). The *conditional entropy* of $\mathbf{X}$ given $\mathbf{Y}$ is

$$H(\mathbf{X}|\mathbf{Y}) = \mathbf{E}H(\mathbf{X}|\mathbf{Y} = y) = \sum_y p(y) \sum_x p(x|y) \log \frac{1}{p(x|y)} .$$

For a random vector $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_n)$ (note this is also an r.v.), we have

$$H(\mathbf{X}) = H(\mathbf{X}_1) + H(\mathbf{X}_2|\mathbf{X}_1) + \cdots + H(\mathbf{X}_n|\mathbf{X}_1, \ldots, \mathbf{X}_{n-1}). \tag{2.1}$$

Some useful inequalities:

$$H(\mathbf{X}) \le \log |\mathrm{range}(\mathbf{X})|, \tag{2.2}$$

$$H(\mathbf{X}|\mathbf{Y}) \le H(\mathbf{X}), \tag{2.3}$$

and more generally,

$$\text{if } \mathbf{Y} \text{ determines } \mathbf{Z} \text{ then } H(\mathbf{X}|\mathbf{Y}) \le H(\mathbf{X}|\mathbf{Z}),$$

$$H(\mathbf{X}_1, \ldots, \mathbf{X}_n) \le \sum H(\mathbf{X}_i) \tag{2.4}$$

(*e.g.*, by (2.1) and (2.3)). We will often use these facts without reference in what follows.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

We need one less classical result due to J. Shearer (see [7, p. 33]). For a random vector $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_n)$ and $A \subseteq [n]$, set $\mathbf{X}_A = (\mathbf{X}_i : i \in A)$. Shearer's Lemma, which in particular generalizes (2.4), is as follows.

Lemma 2.1. *Let* $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_n)$ *be a random vector and* $\mathscr{A}$ *a collection of subsets (possibly with repeats) of* $[n]$*, with each element of* $[n]$ *contained in at least* m *members of* $\mathscr{A}$*. Then*

$$H(\mathbf{X}) \leq \frac{1}{m} \sum_{A \in \mathscr{A}} H(\mathbf{X}_A).$$

(The version stated in [7] is less general, but the proof given there yields Lemma 2.1.)

Finally, we need the following easy fact. Some version of this is presumably written somewhere, but, lacking a reference, we include a proof.

Lemma 2.2. *Fix an interval* $T \subseteq \mathbf{R}$*,* $a \in T$ *and a twice differentiable* $f : T \to \mathbf{R}$*, and suppose* $f''(x) \leq 0$*,* $f''(a) < 0$*, and* f'' *is continuous at* a*. Then, for any probability distribution* $\{p_1, \ldots, p_t\}$*, and* $\varepsilon_1, \ldots, \varepsilon_t \in [-1, 1]$ *with*

$$\sum_{i=1}^{t} p_i \varepsilon_i = 0 \tag{2.5}$$

and $a_i := a + \varepsilon_i \in T$ *for all* i*,*

$$f(a) - \sum p_i f(a_i) = \Omega\Big(\sum p_i \varepsilon_i^2 \Big). \tag{2.6}$$

(Note the implied constant depends on f and a.)

Proof. By Taylor's formula and our assumptions on f, there is some fixed positive ε (depending on f and a) such that if $|\varepsilon_i| \leq \varepsilon$ then

$$f(a_i) \leq f(a) + f'(a)\varepsilon_i + \frac{f''(a)}{3} \varepsilon_i^2 \, .$$

(Recall $f''(a) \leq 0$.) So, if $|\varepsilon_i| \leq \varepsilon$ for all i, then (using (2.5))

$$f(a) - \sum p_i f(a_i) \geq -f'(a) \sum p_i \varepsilon_i - \frac{f''(a)}{3} \sum p_i \varepsilon_i^2 = \Omega\Big(\sum p_i \varepsilon_i^2 \Big). \tag{2.7}$$

For general ε_is, notice that, for $0 < \delta \leq 1$,

$$f(a) - \sum p_i f(a + \varepsilon_i) \geq \delta^{-1} [f(a) - \sum p_i f(a + \delta \varepsilon_i)] \tag{2.8}$$

(since Jensen's inequality gives $f(a + \delta\varepsilon_i) \geq (1 - \delta) f(a) + \delta f(a + \varepsilon_i)$). So we may apply (2.8) with $\delta = \varepsilon$ (ε as above) and (2.7) (with the ε_is replaced by $\delta\varepsilon_i$s) to obtain

$$f(a) - \sum p_i f(a + \varepsilon_i) \geq \delta^{-1} \Omega\Big(\sum p_i \delta^2 \varepsilon_i^2 \Big),$$

which is still $\Omega(\sum p_i \varepsilon_i^2)$ since $\delta = \Omega(1)$. □

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

3. Basic inequalities

We begin with some general notation (some of which was already used above).

As earlier, we assume unless stated otherwise that we have Assumption 1.2, and always take $\mathbf{I}$ to be a random member of $\mathscr{I} = \mathscr{I}(G)$, with distribution to be specified.

We write $\mathscr{I}_k = \mathscr{I}_k(G)$ for $\{I \in \mathscr{I} : |I| = k\}$, and set $i(G) = |\mathscr{I}(G)|$, $i_k(G) = |\mathscr{I}_k(G)|$. We will usually take $k = \alpha N$, always assuming in this case that αN is an integer.

We write $\mathbf{1}_v$ for $\mathbf{1}_{\{v \in \mathbf{I}\}}$ and $p(v)$ for $\Pr(v \in \mathbf{I})$ $(= \mathbf{E}\mathbf{1}_v)$, extending this in the natural ways to expressions such as $p(v|Q)$.

We use N_v for the set of neighbours of (*i.e.*, vertices adjacent to) v, and set $\mathbf{X}_v = \mathbf{I} \cap N_v$. As mentioned earlier, a central role is played by the events $Q_v = \{\mathbf{X}_v = \emptyset\}$, in connection with which we define the probabilities $q(v) = \Pr(Q_v)$ and random sets $\mathbf{J} = \{v : Q_v \text{ occurs}\}$, $\mathbf{J}' = \{v \in \mathbf{J} : N_v \cap \mathbf{J} = \emptyset\}$.

We are interested in upper bounds on $H(\mathbf{I})$, thought of (as usual) as the amount of information in $\mathbf{I}$. Our basic idea is that, while each of $\mathbf{1}_v$, $\mathbf{X}_v$ contributes to $H(\mathbf{I})$, they cannot do so simultaneously. This notion is captured by Q_v: there is no information in $\mathbf{X}_v$ under Q_v, and none in $\mathbf{1}_v$ under $\overline{Q}_v$.

Concretely, we always begin with the following identity and inequalities, which hold for arbitrary $\mathbf{I}$ (each of the sums in the inequalities is over $v \in \mathscr{E}$):

$$H(\mathbf{I}) = H(\mathbf{I} \cap \mathscr{O}) + H(\mathbf{I} \cap \mathscr{E} | \mathbf{I} \cap \mathscr{O}); \tag{3.1}$$

$$H(\mathbf{I} \cap \mathscr{E} | \mathbf{I} \cap \mathscr{O}) \leq \sum H(\mathbf{1}_v | \mathbf{I} \cap \mathscr{O}) \leq \sum H(\mathbf{1}_v | \mathbf{1}_{Q_v}) \tag{3.2}$$

(these are equalities for h.c.d.s); and

$$\begin{aligned} H(\mathbf{I} \cap \mathscr{O}) &\leq \frac{1}{n} \sum H(\mathbf{X}_v) \\ &= \frac{1}{n} \sum [H(\mathbf{1}_{Q_v}) + H(\mathbf{X}_v | \mathbf{1}_{Q_v})] \\ &= \frac{1}{n} \sum [H(q(v)) + (1 - q(v)) H(\mathbf{X}_v | \overline{Q}_v)]. \end{aligned} \tag{3.3}$$

(For (3.3) we used Lemma 2.1, noting that the sets N_v cover each $x \in \mathscr{O}$ exactly n times.)

4. Number of independent sets

Proof of Theorem 1.9. We choose $\mathbf{I}$ uniformly from $\mathscr{I}(G)$ – so the left side of (1.3) is $H(\mathbf{I})$ – and apply (3.1)–(3.3). For uniform $\mathbf{I}$ the term $H(\mathbf{1}_v | \mathbf{1}_{Q_v})$ in (3.2) is just $q(v)$, and in (3.3) we use the naive bound (see (2.2)) $H(\mathbf{X}_v | \overline{Q}_v) \leq \log(2^n - 1)$. Thus, with v again ranging over $\mathscr{E}$,

$$\begin{aligned} H(\mathbf{I}) &\leq \sum q(v) + \frac{1}{n} \sum [H(q(v)) + (1 - q(v)) \log(2^n - 1)] \\ &= \frac{N}{2n} \log(2^n - 1) + \frac{1}{n} \sum \left[H(q(v)) + q(v) \log \frac{2^n}{2^n - 1} \right]. \end{aligned}$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

Differentiation gives the maximum of $H(x) + x \log \frac{2^n}{2^n - 1}$ at $x_0 := 2^n(2^{n+1} - 1)^{-1}$, so that

$$H(\mathbf{I}) \leq \frac{N}{2n} \left[\log(2^n - 1) + H(x_0) + x_0 \log \frac{2^n}{2^n - 1} \right],$$

which a little calculation shows to be equal to $\frac{N}{2n} \log(2^{n+1} - 1)$. (This can also be seen without calculation by observing that when $G = K_{n,n}$ and $q(v) = x_0 \ \forall v$, the argument gives away nothing.) □

Theorem 1.9 seems as if it ought to be obvious, but we do not see an entropy-free proof. An approximate version – $\log |\mathcal{I}(G)| < (1/2 + o(1))N$ (with $o(1) \to 0$ as $n \to \infty$) – for *general* n-regular, N-vertex G was proved by Noga Alon [1] in answer to a question of Andrew Granville (see [1] for motivation). This mainly requires proving the inequality for bipartite G (actually with regularity relaxed somewhat, which could also be done in Theorem 1.9), the general case then following easily via the Lovász Local Lemma. We feel certain that biparticity is similarly unnecessary for the precise result.

Conjecture 4.1. *If G is an n-regular graph on N vertices, then*

$$\log i(G) \leq \frac{N}{2n} \log(2^{n+1} - 1).$$

Again, one would think that this simple and natural conjecture, which was already suggested in [1], would have a simple and natural proof.

It is also natural to try to extend Theorem 1.9 and Conjecture 4.1 in other directions. First, one would like to allow variable degrees. It is easy to see that the theorem does not hold if we only assume average degree n, but perhaps the following is true.

Conjecture 4.2. *For any graph G without isolated vertices,*

$$\log i(G) \leq \sum_{\{x,y\} \in E(G)} (d(x)d(y))^{-1} \log(2^{d(x)} + 2^{d(y)} - 1).$$

(This is sharp for any disjoint union of complete bipartite graphs.) Straightforward generalization of the proof of Theorem 1.9 does give Conjecture 4.2 for biregular G.

Theorem 4.3. *If G is an (a, b)-regular bipartite graph on N vertices, then*

$$\log i(G) \leq \frac{N}{a + b} \log(2^a + 2^b - 1).$$

Here (a, b)-*regular* means $d(v)$ is a for $v \in \mathcal{E}$ and b for $v \in \mathcal{O}$.

We mention two more guesses, neither based on anything very substantial. First, we would like to say that among n-regular graphs on N vertices, disjoint $K_{n,n}$s maximize i_k for *every* k. To say this properly when $2n \nmid N$, define the polynomial $g_{n,k}(t)$ by

$$g_{n,k}(t) = i_k(t \cdot K_{n,n}), \qquad \text{for } t \in \mathbf{N},$$

where $t \cdot G$ means t disjoint copies of G.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

Conjecture 4.4. *If G is an n-regular graph on N vertices, then $i_k(G) \le g_{n,k}(N/(2n))$.*

Second, suppose we fix $\alpha < 1/2$ and consider $\sup\{H(\mathbf{I})/|V(G)|\}$, where the supremum is over n-regular G and $\mathbf{I}$ chosen from any distribution on $\mathscr{I}(G)$, subject only to the requirement that $\mathbf{E}|\mathbf{I}| = \alpha|V(G)|$. Could it be that this supremum is achieved by p_λ on $K_{n,n}$, with λ chosen to give occupation probabilities α?

Other remarks. It is *not* true that, for every λ, $K_{n,n}$ maximizes $H(p_\lambda^G)/|V(G)|$ over n-regular G (*e.g.*, take $n = 2$, G a 5-cycle and λ large). Conceivably it is true if we restrict to bipartite G, but even this seems unlikely. The particular question of estimating $|\mathscr{I}(G)|$ when G is a 'grid graph', $[m] \times [n] \subseteq \mathbf{Z}^2$ has received special attention; see [6] and its references.

5. A general upper bound

Proof of Proposition 1.10. Extending the notation $\overline{p}$, we set $\overline{p}_{\mathscr{E}} = (2/N)\sum_{v\in\mathscr{E}} p(v)$, and define $\overline{p}_{\mathscr{O}}$, $\overline{q}_{\mathscr{E}}$ and $\overline{q}_{\mathscr{O}}$ analogously. Sums in what follows are again over $v \in \mathscr{E}$ unless otherwise indicated.

First, using (3.2) and Jensen's inequality, we have

$$\begin{aligned} H(\mathbf{I}\cap\mathscr{E}|\mathbf{I}\cap\mathscr{O}) &\le \sum H(\mathbf{1}_v|\mathbf{1}_{Q_v}) = \sum q(v)H\left(\frac{p(v)}{q(v)}\right) \\ &\le \sum q(v)\cdot H\left(\frac{\sum p(v)}{\sum q(v)}\right) = \frac{N}{2}\overline{q}_{\mathscr{E}}H\left(\frac{\overline{p}_{\mathscr{E}}}{\overline{q}_{\mathscr{E}}}\right). \end{aligned} \tag{5.1}$$

Second, setting $B = \sum(1-q(v)) = (N/2)(1-\overline{q}_{\mathscr{E}})$, we have

$$H(\mathbf{I}\cap\mathscr{O}) \le \frac{1}{n}\sum[H(q(v)) + (1-q(v))H(\mathbf{X}_v|\overline{Q}_v)] \tag{5.2}$$

$$\le \frac{N}{2n} + \frac{1}{n}\sum(1-q(v))\sum_{x\sim v} H\left(\frac{p(x)}{1-q(v)}\right) \tag{5.3}$$

$$\begin{aligned} &\le \frac{N}{2n} + B\cdot H\left(\sum_v\sum_{x\sim v}\frac{p(x)}{nB}\right) \\ &= \frac{N}{2n} + (N/2)(1-\overline{q}_{\mathscr{E}})H\left(\frac{\overline{p}_{\mathscr{O}}}{1-\overline{q}_{\mathscr{E}}}\right), \end{aligned} \tag{5.4}$$

where the inequalities are instances of (3.3), (2.4) and Jensen's inequality respectively.

Inserting the preceding bounds in (3.1), we have, again using Jensen's inequality,

$$\begin{aligned} H(\mathbf{I}) &\le (N/2)[1/n + \overline{q}_{\mathscr{E}}H(\overline{p}_{\mathscr{E}}/\overline{q}_{\mathscr{E}}) + (1-\overline{q}_{\mathscr{E}})H(\overline{p}_{\mathscr{O}}/(1-\overline{q}_{\mathscr{E}}))] \\ &\le (N/2)[1/n + H(\overline{p}_{\mathscr{E}} + \overline{p}_{\mathscr{O}})] \\ &= (N/2)[1/n + H(2\overline{p})]. \end{aligned} \tag{5.5}$$

□

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

Remark. Of course, we could have written $H(\overline{q})/n$ in place of $1/n$ in (5.5).

Question 5.1. *Does Proposition 1.10 remain true if in Assumption 1.2 we drop the requirement that G be bipartite?*

Proof of Theorem 1.4. For $\alpha \in [0, 1/2]$, set $f(\alpha) = (N/2)[H(2\alpha) + 2\alpha \log \lambda]$ and $w(\mathscr{I}_{\alpha N}) = \lambda^{\alpha N}|\mathscr{I}_{\alpha N}|$ (the total weight of $\mathscr{I}_{\alpha N} = \mathscr{I}_{\alpha N}(G)$). Then, trivially,

$$\log w(\mathscr{I}_{\alpha N}) > \log \left(\binom{N/2}{\alpha N} \lambda^{\alpha N} \right) \geq f(\alpha) - \frac{1}{2} \log N + O(1). \tag{5.6}$$

On the other hand, (5.5) (applied to $\mathbf{I}$ uniform from $\mathscr{I}_{\alpha N}$) gives

$$\log w(\mathscr{I}_{\alpha N}) \leq f(\alpha) + N/(2n).$$

Now $f(\alpha)$ is maximized at α_λ, and for general α we have

$$f(\alpha) = f(\alpha_\lambda) - \Theta((\alpha_\lambda - \alpha)^2 N), \tag{5.7}$$

where the implied constants depend on λ.

It follows that, for a suitable constant C (again depending on λ) and $\xi > Cn^{-1/2}$,

$$\sum_{|\alpha - \alpha_\lambda| > \xi} w(\mathscr{I}_{\alpha N}) < \sum_{|\alpha - \alpha_\lambda| > \xi} 2^{f(\alpha_\lambda) - \Omega((\alpha_\lambda - \alpha)^2 N)} = O(\xi^{-1} 2^{f(\alpha_\lambda) - \Omega(\xi^2 N)}).$$

On the other hand, combining (5.7) with (5.6) we have

$$\sum \{w(\mathscr{I}_{\alpha N}) : \alpha_\lambda - N^{-1/2} < \alpha \leq \alpha_\lambda\} = \Omega(2^{f(\alpha_\lambda)}),$$

since each of the $N^{1/2}$ summands is $\Omega(2^{f(\alpha_\lambda)} N^{-1/2})$. Thus, for $\mathbf{I}$ chosen according to p_λ^G,

$$\Pr(||\mathbf{I}| - \alpha_\lambda N| > \xi N) = O(\xi^{-1} 2^{-\Omega(\xi^2 N)}). \qquad \square$$

6. Strong correlations for tori

Here we prove Lemma 1.11. We assume throughout that G is a torus (as in the statement of the lemma), and write q for the common value of the $q(v)$s.

As stated in the Introduction, our main task is proving the following result.

Lemma 6.1. *Fix $\alpha \in (0, 1/2]$ and let $\mathbf{I}$ be uniform from $\mathscr{I}_{\alpha N}(G)$. Then, for every fixed $\beta < 1$,*

$$H(\mathbf{I}) \leq (N/2)[O(n^{-(1+\beta)}) + H(2\alpha)], \tag{6.1}$$

$$q = 1/2 + O(n^{-\beta}), \tag{6.2}$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

and

$$\textit{for } d(v,w) \textit{ even}, \quad \Pr(Q_w|Q_v) = 1 - O(d(v,w)n^{-\beta}). \tag{6.3}$$

We assume until further notice (namely until after (6.31)) that $\mathbf{I}$ is uniform from $\mathscr{I}_{\alpha N}(G)$.

The proof of Lemma 6.1 is again based on playing off upper bounds on $H(\mathbf{I})$ – beginning with (1.4) – against a trivial lower bound ((6.4), which already appeared in (5.6) in the proof of Theorem 1.4). That these bounds nearly coincide implies that the upper bounds – and the inequalities of Section 2 on which they are based – do not give away very much, and this forces various parameters to be close to their 'ideal' values (see (6.7) for the first instance of this).

It is the availability of (6.4) that leads us to begin with uniform distribution on $\mathscr{I}_{\alpha N}$, though we are eventually more interested in p_λ. (Something similar to (6.4) for $\mathbf{I}$ drawn from p_λ follows from what we establish below, but we do not see that we can claim such a bound to begin with.)

Once we have Lemma 6.1, we easily derive Theorem 1.6 and Lemma 1.11. (Note that (6.1) is an improved version of (1.4) under the present stronger hypotheses, so may be expected to imply Theorem 1.6 as (1.4) implied Theorem 1.4.)

Perhaps the key idea, embodied in (6.3) and the weaker (6.8), is that we can establish strong correlations among the events Q_v, thus limiting the overall information in these events. This eventually sets up a bootstrapping procedure in which stronger correlations imply better upper bounds on $H(\mathbf{I})$ and *vice versa*, and iteration of this procedure gets us from (6.8) to (6.3).

It is also (6.3) that is needed for Lemma 1.11. Weaker versions of (6.1)–(6.3) are steps in the iteration (beginning with the use of (6.5) and (6.7) in obtaining (6.8)), and we also make some further use of (6.1) and (6.2) (respectively) in establishing Theorem 1.6 (as already mentioned) and (6.30), the odd-distance counterpart of (6.3).

First iteration

As mentioned above, we again exploit the fact that we can give similar lower and upper bounds on $H(\mathbf{I})$ ($=\log|\mathscr{I}_{\alpha N}|$). The lower bound is just (5.6) without the terms involving λ:

$$H(\mathbf{I}) > \log\binom{N/2}{\alpha N} \geq \frac{N}{2}H(2\alpha) - \frac{1}{2}\log N + O(1). \tag{6.4}$$

Our initial upper bound is (5.5) specialized to the present situation:

$$\begin{aligned} H(\mathbf{I}) &\leq (N/2)[1/n + qH(\alpha/q) + (1-q)H(\alpha/(1-q))] \\ &\leq (N/2)[1/n + H(2\alpha)]. \end{aligned} \tag{6.5}$$

We first show that q is close to $1/2$. From (6.4) and (6.5) we have

$$\begin{aligned} H(2\alpha) - (qH(\alpha/q) + (1-q)H(\alpha/(1-q))) &\leq \frac{1}{n} + \frac{\log N + O(1)}{N} \\ &= O(1/n). \end{aligned} \tag{6.6}$$

On the other hand, Lemma 2.2 implies that the left side of (6.6) is

$$\Omega(q\alpha^2(1/q-2)^2 + (1-q)\alpha^2(1/(1-q)-2)^2),$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

and combining this with (6.6) gives

$$q = 1/2 + O(n^{-1/2}). \tag{6.7}$$

Remark. The argument to this point is valid for general symmetric (*i.e.*, vertex-transitive) G, provided we replace the right sides of (6.6) and (6.7) by $O(\zeta)$ and $1/2 + O(\sqrt{\zeta})$, with ζ as in (1.2). It then follows via Theorem 1.4 that (6.7) is also true when $\mathbf{I}$ is drawn from p_λ^G with $\lambda = \Omega(1)$ (and, again, G is symmetric).

As mentioned above, correlation assertions along the lines of (6.3) are the key to bootstrapping; the first of these is:

$$\text{for } d(v,w) \text{ even}, \quad \Pr(Q_w|Q_v) = 1 - O(d(v,w)n^{-1/2}). \tag{6.8}$$

Write $v \approx w$ if $d(v,w) = 2$ and $\|v-w\|_\infty = 1$. (Of course, the second condition is automatic if G is a cube.) It is easy to see that (6.8) follows from

$$\text{if } v \approx w \quad \text{then} \quad \Pr(Q_w|Q_v) = 1 - O(n^{-1/2}),$$

which in view of (6.7) is the same as

$$\text{if } v \approx w \quad \text{then } \Pr(Q_v Q_w) = 1/2 + O(n^{-1/2}). \tag{6.9}$$

To prove (6.9) we will again exploit the relation between (6.4) and (6.5). Recall that we obtained (6.5) by combining the bounds (specializations of (5.1) and (5.4))

$$H(\mathbf{I} \cap \mathscr{E}|\mathbf{I} \cap \mathscr{O}) \le (N/2)qH(\alpha/q) \tag{6.10}$$

and

$$H(\mathbf{I} \cap \mathscr{O}) \le (N/2)[1/n + (1-q)H(\alpha/(1-q))]. \tag{6.11}$$

So again using (6.4) we have

$$(N/2)qH(\alpha/q) - H(\mathbf{I} \cap \mathscr{E}|\mathbf{I} \cap \mathscr{O}) = O(N/n), \tag{6.12}$$

$$(N/2)[1/n + (1-q)H(\alpha/(1-q))] - H(\mathbf{I} \cap \mathscr{O}) = O(N/n). \tag{6.13}$$

But we can insert some intermediate bounds in (6.10), summing now over $(v,w) \in \mathscr{E}^2$ with $v \approx w$ (and over $v \in \mathscr{E}$ in the fourth line), and letting $\iota = 1$ if $G = \{0,1\}^n$ and $\iota = 2$ otherwise:

$$\begin{aligned}
H(\mathbf{I} \cap \mathscr{E}|\mathbf{I} \cap \mathscr{O}) &\le \frac{1}{n(n-\iota)} \sum_v \sum_w H(\mathbf{1}_v, \mathbf{1}_w | \mathbf{1}_{Q_v}, \mathbf{1}_{Q_w}) \\
&\le \frac{1}{n(n-\iota)} \sum_v \sum_w [H(\mathbf{1}_v | \mathbf{1}_{Q_v}, \mathbf{1}_{Q_w}) + H(\mathbf{1}_w | \mathbf{1}_{Q_v}, \mathbf{1}_{Q_w})] \\
&\le \frac{1}{n(n-\iota)} \sum_v \sum_w [H(\mathbf{1}_v | \mathbf{1}_{Q_v}) + H(\mathbf{1}_w | \mathbf{1}_{Q_w})] \\
&= \sum H(\mathbf{1}_v | \mathbf{1}_{Q_v}) \\
&= (N/2)qH(\alpha/q).
\end{aligned}$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

(The first inequality is again Lemma 2.1.) Thus, using (6.12) and symmetry, we have, for $v \approx w$,

$$H(\mathbf{1}_v|\mathbf{1}_{Q_v},\mathbf{1}_{Q_w}) + H(\mathbf{1}_w|\mathbf{1}_{Q_v},\mathbf{1}_{Q_w}) - H(\mathbf{1}_v,\mathbf{1}_w|\mathbf{1}_{Q_v},\mathbf{1}_{Q_w}) = O(1/n) \tag{6.14}$$

and

$$H(\mathbf{1}_v|\mathbf{1}_{Q_v}) - H(\mathbf{1}_v|\mathbf{1}_{Q_v},\mathbf{1}_{Q_w}) = O(1/n). \tag{6.15}$$

Similarly, where in (5.3) we used $H(\mathbf{X}_v|\overline{Q}_v) \le \sum_{x\sim v} H(\mathbf{1}_x|\overline{Q}_v)$, we can insert (with the first two sums over unordered pairs)

$$\begin{aligned} H(\mathbf{X}_v|\overline{Q}_v) &\le \frac{1}{n-\iota}\sum\{H(\mathbf{1}_x,\mathbf{1}_y|\overline{Q}_v) : \{x,y\}\subseteq N_v,\ x\approx y\} &(6.16)\\ &\le \frac{1}{n-\iota}\sum\{H(\mathbf{1}_x|\overline{Q}_v)+H(\mathbf{1}_y|\overline{Q}_v) : \{x,y\}\subseteq N_v,\ x\approx y\} &(6.17)\\ &= \sum_{x\sim v} H(\mathbf{1}_x|\overline{Q}_v), \end{aligned}$$

and it follows, using (6.13) and symmetry, that the difference between the right sides of (6.17) and (6.16) is at most $O((1-q)^{-1})$, which is $O(1)$ by (6.7).

So, again using symmetry, we have, for any $x,y\in N_v$ with $x\approx y$,

$$H(\mathbf{1}_x|\overline{Q}_v) + H(\mathbf{1}_y|\overline{Q}_v) - H(\mathbf{1}_x,\mathbf{1}_y|\overline{Q}_v) = O(1/n). \tag{6.18}$$

We now turn to deriving (6.9) from (6.14), (6.15) and (6.18).

First, since for $x\sim v$, $H(\mathbf{1}_x|\overline{Q}_v) = H(\alpha/(1-q))$, (6.18) gives, for $x,y\in N_v$ with $x\approx y$,

$$H(\mathbf{1}_x,\mathbf{1}_y|\overline{Q}_v) = 2H(\alpha/(1-q)) - O(1/n), \tag{6.19}$$

which, we assert, implies $p(x,y|\overline{Q}_v) = (\alpha/(1-q))^2 + O(n^{-1/2})$, and thus

$$\text{for } x\approx y,\quad p(x,y) = \alpha^2/(1-q) + O(n^{-1/2}). \tag{6.20}$$

To justify the assertion we would like to apply Lemma 2.2 with $T=(0,\infty)$, $f=\log$, $a=1$, $t=4$, $p_1 = p(x,y|\overline{Q}_v)$, $a_1 = p(x|\overline{Q}_v)p(y|\overline{Q}_v)/p(x,y|\overline{Q}_v)$, $p_2 = p(x,\overline{y}|\overline{Q}_v)$, $a_2 = p(x|\overline{Q}_v)p(\overline{y}|\overline{Q}_v)/p(x,\overline{y}|\overline{Q}_v)$, *etc*. With these values the left side of (2.6) is $2H(\alpha/(1-q)) - H(\mathbf{1}_x,\mathbf{1}_y|\overline{Q}_v)$, which by (6.19) is $O(1/n)$. Thus Lemma 2.2 gives ε_1 $(=(a_1-1))=O(n^{-1/2})$ – which is equivalent to our assertion regarding $p(x,y|\overline{Q}_v)$ – *provided* we have $|\varepsilon_i|\le 1$ for all i.

But suppose $\varepsilon_s = \max\{\varepsilon_1,\dots,\varepsilon_4\} > 1$, and replace $\delta=\varepsilon$ in the second paragraph of the proof of Lemma 2.2 by $\delta=\varepsilon/\varepsilon_s$. The only use of the assumption $|\varepsilon_i|\le 1$ in the lemma is in the assertion $\delta=\Omega(1)$ in the last line of the proof; so with our revised δ we still have

$$O(1/n) > f(a) - \sum p_i f(a+\varepsilon_i) \ge \delta^{-1}\Omega\Big(\sum p_i\delta^2\varepsilon_i^2\Big) = \Omega(p_s\varepsilon_s). \tag{6.21}$$

In the present case,

$$p_s\varepsilon_s = p(\tilde{x}|\overline{Q}_v)p(\tilde{y}|\overline{Q}_v) - p(\tilde{x},\tilde{y}|\overline{Q}_v) = p(\tilde{x}|\overline{Q}_v)p(\tilde{y}|\overline{Q}_v) - p_s, \tag{6.22}$$

with $\tilde{x}$ either x or $\overline{x}$ and $\tilde{y}$ similarly. But if $\varepsilon_s\ge 1$ then the right side of (6.22) is at least $p(\tilde{x}|\overline{Q}_v)p(\tilde{y}|\overline{Q}_v)/2 = \Omega(1)$, contradicting (6.21). So the application of Lemma 2.2 is justified and we have (6.20). □

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

Second, we assert that (6.15) implies (for $v \approx w$)

$$p(v|Q_vQ_w) = p(v|Q_v) + O(n^{-1/2}) = \alpha/q + O(n^{-1/2}). \tag{6.23}$$

To see this, expand the left side of (6.15) as

$$\Pr(Q_v)[H(p(v|Q_v) - \Pr(Q_w|Q_v)H(p(v|Q_vQ_w)) - \Pr(\overline{Q}_w|Q_v)H(p(v|Q_v\overline{Q}_w))],$$

and use Lemma 2.2 with $f = H$, $a = p(v|Q_v)$, $t = 2$, $p_1 = \Pr(Q_w|Q_v)$ ($p_2 = 1 - p_1 = \Pr(\overline{Q}_w|Q_v)$), $a_1 = p(v|Q_vQ_w)$ and $a_2 = p(v|Q_v\overline{Q}_w)$) (noting that (6.20) implies $p_1 = \Omega(1)$).

Third, notice that the left side of (6.14) is

$$\Pr(Q_vQ_w)[H(p(v|Q_vQ_w)) + H(p(w|Q_vQ_w)) - H(\mathbf{1}_v, \mathbf{1}_w|Q_vQ_w)]$$

and, again, that (6.20) gives $\Pr(Q_vQ_w) = \Omega(1)$. So (6.14) implies, again using Lemma 2.2 as in the derivation of (6.20) (and (6.23) in the second line),

$$\begin{aligned} p(vw|Q_vQ_w) &= p(v|Q_vQ_w)p(w|Q_vQ_w) + O(n^{-1/2}) \\ &= (\alpha/q + O(n^{-1/2}))^2 + O(n^{-1/2}) \\ &= (\alpha/q)^2 + O(n^{-1/2}). \end{aligned} \tag{6.24}$$

Finally, combining (6.20), (6.24) and (6.7), we have (6.9):

$$\begin{aligned} \Pr(Q_vQ_w) &= \frac{p(vw)}{p(vw|Q_vQ_w)} = \frac{\alpha^2/(1-q) + O(n^{-1/2})}{(\alpha/q)^2 + O(n^{-1/2})} \\ &= q^2/(1-q) + O(n^{-1/2}) = 1/2 + O(n^{-1/2}). \end{aligned}$$

□

Bootstrapping

Fix $Z \subseteq V$ such that

$$|Z| < Nn^{-2} \quad \text{and} \quad \forall v \in V \ \exists z \in Z \quad \text{with } 10 \geq d(v,z) \equiv 0 \pmod 2. \tag{6.25}$$

(It is easy to see that such a Z exists. There is nothing special about 10 (which could be improved somewhat): any constant would do. The parity condition is not a restriction – it follows (with the bound on $|Z|$ replaced by $2Nn^{-2}$) if we just assume $d(v,Z) < 10$ for all v – but we will later use (6.25) in the form given.)

Suppose we have shown, for some fixed $\beta < 1$, that, for all $v, w \in V$,

$$\text{if } d(v,w) \text{ is even, then } \Pr(Q_w|Q_v) = 1 - O(d(v,w)n^{-\beta}). \tag{6.26}$$

We may then repeat the argument leading to (6.5), replacing (3.1) by

$$H(\mathbf{I}) \leq H(\mathbf{J} \cap Z) + H(\mathbf{I} \cap \mathscr{O}|\mathbf{J} \cap Z) + H(\mathbf{I} \cap \mathscr{E}|\mathbf{I} \cap \mathscr{O}).$$

The last term is bounded as before (as in (5.1) and (6.10)), and for the first we use the trivial

$$H(\mathbf{J} \cap Z) \leq |Z| < Nn^{-2}.$$

Our gain is in the second term, for which we replace $H(\mathbf{1}_{Q_v})$ ($= H(q(v))$) in (5.2) by $H(\mathbf{1}_{Q_v}|\mathbf{J} \cap Z)$. We may then replace the upper bound $H(q(v)) \leq 1$ used in (5.3) by $H(\mathbf{1}_{Q_v}|\mathbf{J} \cap Z) < H(O(n^{-\beta}))$, which follows from (6.25) and (6.26) (noting that the latter

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

implies that we also have $\Pr(Q_w|\overline{Q}_v) = O(d(v,w)n^{-\beta})$ when $d(v,w)$ is even). This substitution allows us to strengthen (6.5) to

$$H(\mathbf{I}) \le (N/2)[O(n^{-(1+\beta)}\log n) + H(2\alpha)]. \tag{6.27}$$

Repetition of the preceding arguments establishing (6.7) and (6.8) then leads us back to (6.26), but with β replaced by (say) any fixed $\beta' < (1+\beta)/2$, and iterating gives Lemma 6.1. □

We can now prove the first part of Lemma 1.11, *i.e.*, that (1.5) holds when $\mathbf{I}$ is uniform from $\mathscr{I}_{\alpha N}$. Fix $\beta \in (\gamma, 1)$. For use below (in (6.31)) we will prove a bit more than (1.5), namely,

$$\mathbf{E}[N/2 - |\mathbf{J}'|] = O(n^{-\beta}N). \tag{6.28}$$

Let Z again be as in (6.25). Then

$$\begin{aligned} H(\mathbf{I}) &\le H(\mathbf{J}\cap Z) + H(\mathbf{J}|\mathbf{J}\cap Z) + H(\mathbf{I}|\mathbf{J}') \\ &\le O(n^{-\beta}N) + \mathbf{E}\left[\log\binom{|\mathbf{J}'|}{\alpha N}\right], \end{aligned} \tag{6.29}$$

where we used (6.3) to bound $H(\mathbf{J}|\mathbf{J}\cap Z)$ (and should say, pickily, that we replace β in Lemma 6.1 by some β' in the interval $(\beta + \log\log n/(\log n), 1)$, so that $H(O(n^{-\beta'})) = O(n^{-\beta})$).

For the second term on the right side of (6.29), notice that

$$\log\binom{|\mathbf{J}'|}{\alpha N} < \log\binom{N/2}{\alpha N} - \Omega(N/2 - |\mathbf{J}'|),$$

so that

$$\mathbf{E}\left[\log\binom{|\mathbf{J}'|}{\alpha N}\right] < \log\binom{N/2}{\alpha N} - \Omega(N/2 - \mathbf{E}|\mathbf{J}'|).$$

Inserting this in (6.29) and combining with the trivial $H(\mathbf{I}) > \log\binom{N/2}{\alpha N}$, we have (6.28).

Remark. Given what we know at this point, we easily obtain an odd-distance version of (6.3); namely, for any fixed $\beta < 1$,

$$\text{for } d(v,w) \text{ odd}, \quad \Pr(Q_w|Q_v) = O(d(v,w)n^{-\beta}). \tag{6.30}$$

Again this will follow if we show $\Pr(Q_vQ_w) = O(n^{-\beta})$ when $v \sim w$. But this is immediate from (6.2) and (6.28) (and symmetry):

$$\Pr(Q_vQ_w) \le \Pr(v \in \mathbf{J}\setminus\mathbf{J}') = q - \frac{1}{N}\mathbf{E}|\mathbf{J}'| = O(n^{-\beta}). \tag{6.31}$$

We now turn to $\mathbf{I}$ chosen according to p_λ ($\lambda > 0$ fixed). First observe that, as suggested at the beginning of this section, repeating the proof of Theorem 1.4 with (5.5) replaced by (6.1) gives Theorem 1.6.

Theorem 1.6 then gives the second part of Lemma 1.11 (that for p_λ) and, incidentally, the analogues of (6.2) and (6.3) (but not (6.1)) for $\mathbf{I}$ drawn from p_λ as immediate consequences of their uniform versions. (For example, for Lemma 1.11, fix a small

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

positive ε, let $Q = \{|\mathbf{J}'| > (\frac{1}{2} - n^{-\gamma})N\}$, $R = \{||\mathbf{I}| - \alpha_\lambda N| > \varepsilon N\}$, and use

$$\Pr(\overline{Q}) = \Pr(R)\Pr(\overline{Q}|R) + (1 - \Pr(R))\Pr(\overline{Q}|\overline{R})) < 2^{-\Omega(N)} + o(1),$$

where the last term is given by the first part of Lemma 1.11.) □

7. Isoperimetry

Here we prove Proposition 1.12. It will be convenient to identify $\{0,1\}^n$ with $2^{[n]}$, the lattice of subsets of $[n]$. For $\mathscr{A} \subseteq 2^{[n]}$, set $\mathscr{A} \cap \mathscr{E} = \mathscr{A}_0$ and $\mathscr{A} \cap \mathscr{O} = \mathscr{A}_1$. We first 'shift' (see, *e.g.*, [9] for related procedures): for distinct $i, j \in [n]$ and $\mathscr{A} \subseteq 2^{[n]}$ define $S_{ij}(\mathscr{A})$ by setting, for each $A \subseteq [n] \setminus \{i,j\}$,

$$S_{ij}(\mathscr{A}) \cap \{A, A \cup \{i,j\}\} = \begin{cases} \{A\}, & \text{if } |\mathscr{A} \cap \{A, A \cup \{i,j\}\}| = 1 \\ & \quad \text{and } |A| \text{ is even,} \\ \{A \cup \{i,j\}\}, & \text{if } |\mathscr{A} \cap \{A, A \cup \{i,j\}\}| = 1 \\ & \quad \text{and } |A| \text{ is odd,} \\ \mathscr{A} \cap \{A, A \cup \{i,j\}\}, & \text{otherwise,} \end{cases}$$

and taking $B \in S_{ij}(\mathscr{A})$ if and only if $B \in \mathscr{A}$ when $|B \cap \{i,j\}| = 1$. (Thus we shift even sets down and odd sets up, maintaining parity.)

This clearly gives $|S_{ij}(\mathscr{A})_0| = |\mathscr{A}_0|$, $|S_{ij}(\mathscr{A})_1| = |\mathscr{A}_1|$, and it is easy to check that if $\mathscr{A}$ is independent then $S_{ij}(\mathscr{A})$ is as well. So, beginning with an independent $\mathscr{A}$, we may repeatedly apply such shifts to arrive at some independent $\mathscr{A}^*$ with $|\mathscr{A}^*_0| = |\mathscr{A}_0|$, $|\mathscr{A}^*_1| = |\mathscr{A}_1|$, and such that $\mathscr{A}^*_0$ and $\mathscr{A}^*_1$ are respectively an 'ideal' of $\mathscr{E}$ and a 'filter' of $\mathscr{O}$, meaning

$$A \in \mathscr{E} \text{ and } \mathscr{A} \subseteq B \in \mathscr{A}^*_0 \quad \Rightarrow \quad A \in \mathscr{A}^*_0, \tag{7.1}$$

$$A \in \mathscr{O} \text{ and } \mathscr{A} \supseteq B \in \mathscr{A}^*_1 \quad \Rightarrow \quad A \in \mathscr{A}^*_1. \tag{7.2}$$

Thus we may assume that we have (7.1) and (7.2) with $\mathscr{X}$ in place of $\mathscr{A}^*$.

Suppose now w.l.o.g. that $|\mathscr{X}_0| > 2^n/5$ and let $\mathscr{Y}_i$ be the set of neighbours of vertices in $\mathscr{X}_i$ $(i = 0, 1)$. Then, writing $E(\mathscr{W}, \mathscr{Z})$ for the set of edges joining $\mathscr{W}, \mathscr{Z} \subseteq \{0,1\}^n$ and $\overline{\mathscr{W}}$ for $\{0,1\}^n \setminus \mathscr{W}$, we have $n|\mathscr{X}_i| = |E(\mathscr{X}_i, \mathscr{Y}_i)| = n|\mathscr{Y}_i| - |E(\mathscr{Y}_i, \overline{\mathscr{X}}_i)|$, or $|\mathscr{Y}_i| - |\mathscr{X}_i| = |E(\mathscr{Y}_i, \overline{\mathscr{X}}_i)|/n$.

Thus (since independence of $\mathscr{X}$ implies $\mathscr{X}_i$ and $\mathscr{Y}_{1-i}$ are disjoint),

$$\begin{aligned} 2^n &\geq 2(|\mathscr{X}_0| + |\mathscr{X}_1|) + (|\mathscr{Y}_0| - |\mathscr{X}_0|) + (|\mathscr{Y}_1| - |\mathscr{X}_1|) \\ &\geq (1 - n^{-\beta})2^n + |E(\mathscr{Y}_0, \overline{\mathscr{X}}_0)|/n, \end{aligned}$$

or

$$|E(\mathscr{Y}_0, \overline{\mathscr{X}}_0)| \leq n^{1-\beta}2^n. \tag{7.3}$$

Now write $\langle \cdot \rangle$ for hereditary closure, that is,

$$\langle \mathscr{W} \rangle = \{A \subseteq [n] : \exists B \in \mathscr{W}, A \subseteq B\}.$$

To complete the proof we will show that (7.3) forces $\langle \mathscr{X}_0 \rangle$ to be large.

Set

$$\mathscr{Z} = \{A \subseteq [n] : d(A, \langle \mathscr{X}_0 \rangle) = 1,\ |A| \in [.4n, .6n]\}.$$

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

Notice that $\mathscr{Z} \cap \mathscr{O} \subseteq \mathscr{Y}_0$ and that if $A \subset B \in \mathscr{Z} \cap \mathscr{E}$ ('$A \subset B$' meaning $A \subset B$ and $|A| = |B| - 1$), then $A \in \mathscr{Y}_0$. Thus

$$E(\mathscr{Y}_0, \overline{\mathscr{X}}_0) \supseteq \{(A, B) : A \subset B \text{ and } [A \in \mathscr{Z} \cap \mathscr{O} \text{ or } B \in \mathscr{Z} \cap \mathscr{E}]\},$$

implying $|E(\mathscr{Y}_0, \overline{\mathscr{X}}_0)| \geq .2n|\mathscr{Z}|$, and, in view of (7.3), $|\mathscr{Z}| < O(n^{-\beta}2^n)$. Of course, this also implies the same kind of bound for the full boundary, $\partial\langle\mathscr{X}_0\rangle := \{A \subseteq [n] : d(A, \langle\mathscr{X}_0\rangle) = 1\}$; that is, $|\partial\langle\mathscr{X}_0\rangle| < O(n^{-\beta}2^n)$.

The proposition now follows from the well-known isoperimetric theorem of Harper ([12], see also, *e.g.*, [4, p. 126]), which says that, for given $m \leq 2^n$, $|\partial\mathscr{W}|$ is minimized over $\mathscr{W} \subseteq 2^{[n]}$ of size m by some $\mathscr{W}$ satisfying, for some k, $\{A : |A| \geq k+1\} \subset \mathscr{W} \subseteq \{A : |A| \geq k\}$. For consider

$$\mathscr{W} := 2^{[n]} \setminus (\langle\mathscr{X}_0\rangle \cup \partial\langle\mathscr{X}_0\rangle).$$

We have $|\partial\mathscr{W}| < O(n^{-\beta}2^n)$ (since $\partial\mathscr{W} \subseteq \partial\langle\mathscr{X}_0\rangle$), $|\mathscr{W}| < 4 \cdot 2^n/5$ (recall we assumed $|\mathscr{X}_0| > 2^n/5$), and $\mathscr{W} \supseteq \mathscr{X}_1$; and a routine calculation using Harper's Theorem gives

$$|\mathscr{X}_1| \leq |\mathscr{W}| < O(n^{1/2-\beta} \log^{-1/2} n)2^n. \qquad \square$$

Acknowledgement

I am indebted to Rob van den Berg and Jeff Steif for helpful discussions; to Rob also for suggesting investigation of the cube in the first place and for pointing out an error in an early version of this material; and to Noga Alon for telling me about [1].

Note added in proof

Ideas in a subsequent paper of the author – Range of cube-indexed random walk, *Israel J. Math.*, to appear – can be adapted to improve terms such as $n^{-\beta}$ in (6.3) and Corollary 1.7 to $\exp[-\Omega(n)]$.

References

[1] Alon, N. (1991) Independent sets in regular graphs and sum-free subsets of finite groups. *Israel J. Math.* **73** 247–256.
[2] van den Berg, J. Private communication.
[3] van den Berg, J. and Steif, J. E. (1994) Percolation and the hardcore lattice gas model. *Stoch. Proc. Appl.* **49** 179–197.
[4] Bollobás, B. (1986) *Combinatorics*, Cambridge University Press, Cambridge.
[5] Bollobás, B. (1998) *Modern Graph Theory*, Springer, New York.
[6] Calkin, N. J. and Wilf, H. S. (1998) The number of independent sets in a grid graph. *SIAM J. Discrete Math.* **11** 54–60.
[7] Chung, F. R. K., Frankl, P., Graham, R. and Shearer, J. B. (1986) Some intersection theorems for ordered sets and graphs. *J. Combin. Theory Ser. A* **48** 23–37.
[8] Dobrushin, R. L. (1968) The problem of uniqueness of a Gibbs random field and the problem of phase transition. *Functional Anal. Appl.* **2** 302–312.
[9] Frankl, P. (1987) The shifting technique in extremal set theory. In *Surveys in Combinatorics* (C. Whitehead, ed.), Cambridge University Press, Cambridge, pp. 81–110.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press

[10] Georgii, H.-O. (1988) *Gibbs Measures and Phase Transitions*, de Gruyter, Berlin.
[11] Häggström, O. (1997) Ergodicity of the hard-core model on $\mathbf{Z}^2$ with parity-dependent activities. *Ark. Mat.* **35** 171–184.
[12] Harper, L. H. (1966) Optimal numberings and isoperimetric problems on graphs. *J. Combin. Theory* **1** 385–394.
[13] Kahn, J. and Lawrenz, A. (1999) Generalized rank functions and an entropy argument. *J. Combin. Theory Ser. A* **87** 398–403.
[14] McEliece, R. J. (1977) *The Theory of Information and Coding*, Addison-Wesley, London.
[15] Radhakrishnan, J. (1997) An entropy proof of Bregman's theorem. *J. Combin. Theory Ser. A* **77** 161–164.

https://doi.org/10.1017/S0963548301004631 Published online by Cambridge University Press