On the Evolution of Random Boolean Functions

B. Bollobás[1, 2], Y. Kohayakawa[1, 2] and T. Łuczak[1, 3]

[1] Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge, 16 Mill Lane, Cambridge CB2 1SB, England

[2] Department of Mathematics,
Louisiana State University, Baton Rouge, LA 70803, USA

[3] Department of Discrete Mathematics,
Adam Mickiewicz University, ul. Matejki 48/49, Poznań, Poland

Abstract. Let a random induced subgraph $Q^p = Q^{n,p}$ of the cube Q^n be chosen by letting $\mathbb{P}(v \in V(G^p)) = p$, all such events being independent. We show that the component structure of Q^p undergoes a 'phase transition' at around $p = 1/n$, as conjectured by Weber. We show that if $p = (1+\epsilon)/n$ and $\epsilon > 0$ is fixed then a.e. Q^p contains a 'giant' component of order $(\eta + o(1))pN$, where $\eta = \eta(\epsilon) > 0$ is computed explicitly. This result is the natural analogue of a theorem of Ajtai, Komlós and Szemerédi concerning the behaviour of random spanning subgraphs of Q^n. We also show that the second largest component of a.e. Q^p is of order $O(n^{10})$.

1. Introduction

In this note we study random Boolean functions, *i.e.* random functions that are defined on the cube Q^n and take values in $\{0, 1\}$. Rather trivially, by identifying $\varphi : Q^n \to \{0, 1\}$ with $W_\varphi = \varphi^{-1}(1)$, a random Boolean function may be regarded as a random subset $W \subset V(Q^n)$ of the vertex set of the cube. More interestingly, one sees that certain natural properties of φ are directly reflected in the graph-theoretic properties of the graph $G^\varphi = Q^n[W_\varphi]$ induced by W_φ in the cube. Let us give some examples.

Suppose we can cover G^φ with ℓ subcubes Q_i $(1 \le i \le \ell)$, every Q_i being contained in G^φ. We then see that φ can be expressed as a disjunctive normal form (DNF) with ℓ conjunctions, that is it can be expressed by a DNF of *complexity*, or *length*, ℓ. The natural problem of determining the minimal complexity of a DNF representing φ has been studied in detail; see for instance Glagolev [9], Saposhenko ([11]–[14]) and Weber ([16]–[21]).

Another graph-theoretic property of $G^\varphi \subset Q^n$ that is of interest is the size of the edge-boundary of W_φ; more specifically, if we fix the cardinality of W_φ, we want to know whether there is a coordinate i ($1 \le i \le n$) such that the number $\partial_i(W_\varphi)$ of edges in the ith direction between vertices of W_φ and its complement $\varphi^{-1}(0) = Q^n \setminus W_\varphi$ is large in terms of $|W_\varphi|$ (see [10]). This question has to do with the strength of the influence of individual variables on the function φ. (The variable corresponding to i above has large influence on the behaviour of φ, since the fact that $\partial_i(W_\varphi)$ is large corresponds to the fact that the value of φ is highly sensitive to the value of the variable i.)

Finally, one rather basic question about G^φ concerns its connectedness: if we pick a random Boolean function φ, what is the probability that G^φ is connected? Or more generally, what can we say about the number of components of a typical G^φ?

Before we proceed, let us introduce the probabilistic model of Boolean functions that we shall use; terms like 'typical' will then have a precise meaning. For given $n \ge 1$ and $0 \le p \le 1$, our space of Boolean functions $\mathcal{G}_{\mathrm{ind}}(Q^n, p)$ has as its members all the induced subgraphs of Q^n, and a random element Q^p of $\mathcal{G}_{\mathrm{ind}}(Q^n, p)$ can be generated by simply letting $v \in V(Q^p)$ with probability p, all these events being independent. Thus if G_0 is an induced subgraph of the cube and its order $|G_0|$ is u, then

$$\mathbb{P}(Q^p = G_0) = p^u (1-p)^{N-u},$$

where $N = 2^n$. Toman [15] proved that the critical value for the connectedness of Q^p is $1/2$: for fixed values of p, a.e. Q^p is connected if $p > 1/2$ and it is a.s. disconnected if $p < 1/2$. For the critical case $p = 1/2$, Saposhenko ([12], [14]) and Weber [17] proved that a.e. Q^p has one large component L, and all the vertices of Q^p outside L are isolated, and moreover their number is, in the limit as $n \to \infty$, distributed according to the Poisson distribution with parameter $1/2$, and hence the probability that $Q^{1/2}$ is connected tends to $\mathrm{e}^{-1/2}$. (Considerable strengthenings of these results have been obtained by Dyer, Frieze and Foulds [6].)

Now, Weber [22] extended this result about the structure of $Q^{1/2}$ as follows. He proved that if $0 < p < 1/2$ is fixed then a.e. Q^p has one large component L of order $|Q^p| - (1 + o(1))p(2q)^n$, where $q = 1 - p$, and asymptotically there are $p(2q)^n$ small components of order between 1 and $\lfloor 1/\log(1/q) \rfloor$. In fact, in view of certain results concerning the random spanning subgraphs $Q_p \in \mathcal{G}(Q^n, p)$, one is inclined to expect considerably sharper results, namely a rather abrupt 'phase transition'. (The random graphs $Q_p \subset Q^n$ are obtained by independent selections of the edges of Q^n with probability p.) Erdős and Spencer [7] observed that if $p = (1-\epsilon)/n$ and $\epsilon > 0$ is fixed, then all components of Q_p have order $o(N)$. On the other hand, verifying a conjecture stated in [7], Ajtai, Komlós and Szemerédi [1] proved the following beautiful and surprising and result. If $p = (1+\epsilon)/n$ and $\epsilon > 0$ is fixed, then a.e. Q_p contains a 'giant' component of order at least cN, where $c = c(\epsilon) > 0$. This theorem has been extended considerably in [4], where, among others, it is shown that if $p = (1+\epsilon)/n$ and $60(\log n)^3/n \le \epsilon = \epsilon(n) = o(1)$, then the largest component of Q_p has order about $2\epsilon N$ almost surely. Furthermore, the second largest component of a.e. Q_p has order $O(n\epsilon^{-2})$, and hence apart from the giant all components of a.e. Q_p are very small indeed. From the results above, we see that the component structure of Q_p changes very suddenly at around the critical point $p = 1/n$.

As pointed out by Weber [22], a phase transition analogous to the one experienced by Q_p cannot take place in Q^p before $p = 1/n$, if it happens at all: if $\epsilon > 0$ is fixed and $p = (1-\epsilon)/n$ then a.e. Q^p is such that all its components have at most cn vertices for some $c = c(\epsilon)$. Weber also conjectured that a phase transition *does* occur at $p = 1/n$. Our aim in this note is to prove this conjecture. Among others, we shall show that if $\epsilon > 0$ is fixed then for $p = (1+\epsilon)/n$ a.e. $Q^p \in \mathcal{G}_{\mathrm{ind}}(Q^n, p)$ is such that its largest component has $(\eta + o(1))pN$ vertices, where $\eta = \eta(\epsilon) > 0$ depends only on ϵ. (We shall compute $\eta = \eta(\epsilon)$ explicitly.) Also, we shall show that the second largest component of a.e. Q^p has order polynomial in n.

The techniques we shall use here will resemble the ones from [4]. However, besides some subtle differences, there are some major ones and in fact we shall not have one of the main lemmas of that note: the method we used there to prove the rather powerful gap result does not work here, and hence we shall have to do quite a bit of work in order to get around this difficulty (cf. Lemma 5). Once this problem is overcome, we shall have no problems in proving the existence of the giant. In fact, much in the same way as in [4], we shall prove the existence of the giant component by first showing that a.e. Q^p has quite a few vertices in large components, and then by noticing that such components merge together very easily with the addition of very few vertices to Q^p.

Another pitfall arising from the fact that we cannot prove a good gap result will be that the order of the second largest component cannot be estimated easily; we shall have to deal with this problem in a completely different way (cf. the proof of Theorem 9).

This note is organised as follows. In Section 2 we give some preliminary lemmas concerning the distribution of the vertices of Q^p between its large and small components. In the following section we prove the key lemma, Lemma 5, and also show that the vertices in large components are 'everywhere dense' in the cube. In Section 4 we prove our main results: the one concerning the existence of the giant (Theorem 8), and the one on the second largest component (Theorem 9). We close this note with some remarks and open problems.

2. Preliminaries

In this section we shall estimate the number of vertices of Q^p that belong to largish components. Let $n \geq 2$ and $0 \leq p \leq 1$ be given. We shall make use of the branching process $\Pi_0 = \Pi_0(p) = (Z_t)_{t=0}^{\infty}$ that can be described as follows. In Π_0, we start with one particle that generates offspring according to the binomial distribution $\mathrm{Bi}(n, p)$ with parameters n and p, and all other particles generate offspring according to $\mathrm{Bi}(n-1, p)$. Let the probability that Π_0 does not die out be $\pi_0 = \pi_0(p)$. (For a brief discussion on branching processes see [4], Section 2.) Now, let $p = (1+\epsilon)/n$ where $\epsilon > 0$ is fixed. We shall show that a.e. $Q^p \in \mathcal{G}_{\mathrm{ind}}(Q^n, p)$ has $(\pi_0(p) + o(1))pN$ vertices in components of order at least $n^{1/2}$.

In order to estimate the probability that a fixed vertex $v \in Q^p$ belongs to a component of order at least $n^{1/2}$, we shall simulate the branching process $\Pi_0(p)$ in the cube. Let us fix $v \in Q^n$. We shall now describe an algorithm that generates a random connected induced subgraph $H^p(v)$ of Q^n that contains v. Note that, since we are generating an induced subgraph, it trivially suffices to specify its vertices.

Let $n_0 = \lceil n^{1/2} \rceil$. We start by letting $H^p(v)$ be the single vertex v. Note that the edges incident to a fixed vertex of the cube are naturally ordered by the coordinates to which they correspond, and hence so are its neighbours. Let the neighbours of v be in their natural ordering $v_1, \ldots, v_n$. We examine the vertices v_i in turn, one at a time, and insert them in $H^p(v)$ with probability p, and leave them out with probability $1-p$.

Possibly all the v_i are chosen not to be put in $H^p(v)$, and in this case our algorithm terminates and it outputs the single vertex v as $H^p(v)$. Assume that when looking at v_i we do choose to have it in $H^p(v)$. In this case, we insert the pair (v_i, v) at the back of a queue, and check whether the order $|H^p(v)|$ of $H^p(v)$ is now n_0; if this is the case, we abort the procedure and output this $H^p(v)$. If that is not the case we pass on to consider v_{i+1} if $i < n$, and if $i = n$ we proceed as follows.

Pick the first pair (w, u) in the queue. We now consider all the vertices adjacent to w, except u, in their natural order. Suppose we are examining x. We insert x in $H^p(v)$ with probability p and leave it out with probability $1 - p$. Suppose we do choose to have x in $H^p(v)$. Then we insert the pair (x, w) at the back of the queue, and check whether we now have $|H^p(v)| = n_0$ or $H^p(v)$ ceased to be acyclic. If either of those conditions holds, we abort the procedure and output this $H^p(v)$; if $|H^p(v)| < n_0$ and $H^p(v)$ is still acyclic, we pass on to consider the next vertex x' adjacent to w if such exists, and if not we collect another pair (w', u') from the front of the queue and repeat the above procedure with this new pair. If the queue happens to be empty, we abort the procedure and output the current $H^p(v)$.

Note that a vertex of the cube may be considered up to $n_0 - 1$ times in our algorithm, but at most one vertex of $H^p(v)$ has been considered more than once. More precisely, we see that $H^p(v)$ contains a vertex that was considered more than once only if $H^p(v)$ has a cycle, and in fact if $H^p(v)$ does contain a vertex w looked at more than once, then w was the last vertex put into $H^p(v)$, and any cycle contained in $H^p(v)$ goes through w. Note also that if H_0 is an induced tree of Q^n that has order not greater than n_0 and $v \in H_0$, then there is only one way in which our algorithm can generate H_0. We shall need the following lemma.

Lemma 1. *Let v be any vertex of Q^n. Let $0 < p \le 2/n$ be fixed and write $n_0 = \lceil n^{1/2} \rceil$.*

(i) The probability that $H^p(v)$ is acyclic and has fewer than n_0 vertices is less than $1 - \pi_0(p)$.

(ii) The probability that $H^p(v)$ contains a cycle is $O(n^{-1/2})$.

(iii) The probability that $H^p(v)$ is acyclic and has order n_0 is at least

$$\pi_0(p) + O(n^{-1/2}).$$

Proof. (i) Recall that our algorithm simulates the branching process $\Pi_0(p)$ up to a certain stage, and it only generates an $H^p(v)$ that is acyclic and has fewer than n_0 vertices if the corresponding branching process dies out, which happens with probability $1 - \pi_0(p)$.

(ii) Let $2 \le k \le n_0/2$. Lemma 8 of [4] tells us that the number of cycles of length $2k$ of Q^n that contain a fixed vertex of the cube is bounded from above by

$$\binom{2k}{k} k! n^k = O\left[\left(\frac{4kn}{\mathrm{e}}\right)^k\right].$$

Let us assume that our algorithm has generated an $H^p(v)$ that contains a cycle $C = C^{2k}$ of length $2k$, and let the last vertex added to $H^p(v)$ be $w \in C$. Let us first consider the case in which C does not contain v. In this case, each vertex of C has been examined by our algorithm exactly once, except possibly for w, which might have examined up to $n_0 - 1 \le n^{1/2}$ times. Hence the probability that there is such a C contained in $H^p(v)$ is at most

$$2kn_0 \binom{2k}{k} k! n^k \cdot (2/n)^{2k-1} 2n^{-1/2} = O(kn^{1/2}(16k/\mathrm{e}n)^k),$$

and summing these probabilities over k, we see that the probability that our algorithm has generated an $H^p(v)$ containing a cycle that does not pass through v is at most $O(1/n)$.

Let us now consider the case in which we have generated an $H^p(v)$ that contains a cycle $C = C^{2k}$ of length $2k$ that goes through v. In this case, each vertex of C has been examined by our algorithm exactly once, except for v, which has not been examined at all, and possibly w, which might have been examined up to $n_0 - 1 \leq n^{1/2}$ times. Hence, the probability that such a C exists is bounded above by

$$2k\binom{2k}{k}k!n^k \cdot (2/n)^{2k-2}2n^{-1/2} = O(kn^{3/2}(16k/\mathrm{e}n)^k),$$

and summing over k, we see that the probability that our algorithm has generated an $H^p(v)$ containing a cycle that does pass through v is at most $O(n^{-1/2})$, and this completes the proof of (ii).

(iii) This follows from (i) and (ii). □

We can now estimate from below the probability that a fixed vertex $v \in Q^p$ is in a component of order at least $n_0 = \lceil n^{1/2} \rceil$, and this lower bound will tell us that there are quite a few vertices in such components.

Corollary 2. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed, and set $n_0 = \lceil n^{1/2} \rceil$.*

(i) For any fixed vertex v of Q^n, we have that

$$\mathbb{P}\left(|C_v| \geq n_0 \mid v \in Q^p\right) \geq \pi_0(p) + O(n^{-1/2}),$$

where $C_v = C_v(Q^p)$ is the component of Q^p containing v.

(ii) The number of vertices of Q^p that belong to components of order at least n_0 is a.s. at least $(\pi_0(p) + o(1))pN$.

Proof. (i) Assume that $v \in Q^p$. Let $W \subset Q^n$ be the first $\min\{|C_v|, n_0\}$ vertices reached by the canonical breadth-first search run on C_v starting at v. Let the subgraph $Q^p[W]$ of Q^p induced by W be denoted by H_v. Clearly $|C_v| \geq n_0$ if and only if $|H_v| \geq n_0$. We shall show that the probability that H_v is acyclic and has at least n_0 vertices is at least $\pi_0(p) + o(1)$, which shows (i).

Let $H_0 \subset Q^n$ be an acyclic induced subgraph of the cube that contains v and has order n_0. Recall that there is only one way in which our probabilistic algorithm can generate H_0 as its output $H^p(v)$. It is easily seen that there is an integer $L = L(H_0) \geq 0$ such that

$$\mathbb{P}(H^p(v) = H_0) = \mathbb{P}(H_v = H_0)(1-p)^L \leq \mathbb{P}(H_v = H_0),$$

and hence (i) follows from Lemma 1(iii) by summing over all possible H_0.

(ii) This will follow from the fact that the events $\{v \in Q^p \text{ and } |C_v| \geq n_0\}$, $v \in Q^n$, are essentially independent. By (i) above, if $X = X(Q^p)$ is the number of vertices in components of order smaller than $n_0 = \lceil n^{1/2} \rceil$, then its expectation $\mathbb{E}(X)$ is at most $(1 - \pi_0(p) - O(n^{-1/2}))pN$. In order to prove our lemma, we shall show that X is concentrated around its expectation. For a vertex $v \in Q^n$, let C_v denote the component of Q^p containing v and set

$$X_v = \begin{cases} 1 & \text{if } |C_v| < n_0 \\ 0 & \text{otherwise;} \end{cases}$$

thus $X = \sum X_v$. Note that the r.v. X_v depends only on the vertices of the cube Q^n that are at distance at most $n_0 - 1$ from v, and hence if the Hamming distance between v and $w \in Q^n$ is at least $2n_0 - 1$, then X_v and X_w are independent. We can now easily show that the variance of X is very small. Clearly $p_0 = \mathbb{P}(X_v = 1)$ is independent of v and moreover

$$\sigma^2(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = \left[\sum_{(v,w)} \mathbb{P}(X_v X_w = 1)\right] - p_0^2 N^2,$$

where the sum is over all ordered pairs $(v, w) \in E = Q^n \times Q^n$. Given two vertices v and w of Q^n, denote their Hamming distance by $d_H(v, w)$. Set

$$E_0 = \{(v, w) \in Q^n \times Q^n : d_H(v, w) \leq 2n_0 - 2\},$$

and $E_1 = E \setminus E_0$. Note that $|E_0| \leq N\binom{n}{2n_0}$ and hence very crudely $|E_0| \leq N^{1+o(1)}$. Then

$$\begin{aligned}\sigma^2(X) &\leq \sum_{(v,w)\in E_1} p_0^2 + \sum_{(v,w)\in E_0} 1 - p_0^2 N^2 \\ &\leq (N^2 - N^{1+o(1)})p_0^2 + N^{1+o(1)} - p_0^2 N^2 \\ &\leq N^{1+o(1)}.\end{aligned}$$

The result now follows from Chebyshev's inequality. □

Let us now turn our attention to the number of vertices in small components. We shall show that essentially all the vertices that do not belong to components of order at least $n_0 = \lceil n^{1/2} \rceil$ are in components of order at most $\omega(n)$, where $\omega(n) \to \infty$ arbitrarily slowly.

Lemma 3. *Let $p = (1 + \epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed. Let $\omega(n) \to \infty$ as $n \to \infty$.*

(i) For any vertex $v \in Q^n$, we have that

$$\mathbb{P}\left(|C_v| \leq \omega(n) \mid v \in Q^p\right) \geq 1 - \pi_0(p) + o(1),$$

where $C_v = C_v(Q^p)$ is the component of Q^p containing v.

(ii) A.e. Q^p is such that the number of vertices in components of order not greater than $\omega(n)$ is at least $(1 - \pi_0(p) + o(1))pN$.

Proof. (i) We may and shall assume that $\omega(n) < n_0 = \lceil n^{1/2} \rceil$ for all n. We shall again use the probabilistic algorithm described at the beginning of this section. Recall that if H_0 is an induced acyclic subgraph of the cube that contains v and has order at most n_0, then there is only one way in which we can obtain H_0 as the output of our algorithm. Also, for such an H_0, there is an integer $L = L(H_0)$ such that

$$\mathbb{P}(C_v(Q^p) = H_0) \geq \mathbb{P}(C_v(Q^p) = H_0)(1 - p)^L = \mathbb{P}(H^p(v) = H_0).$$

Summing over all induced acyclic subgraphs $v \in H_0 \subset Q^n$ of order at most $\omega(n)$, we see that the probability that $C_v(Q^p)$ is acyclic and has order at most $\omega(n)$ is bounded from below by the probability that our algorithm generates as an output an acyclic $H^p(v)$ with order at most $\omega(n)$. Lemma 3(i) now follows from the claim below.

Claim. *We have that*

$$P_0 = \mathbb{P}\{H^p(v) \text{ is acyclic and } |H^p(v)| \leq \omega(n)\} \geq 1 - \pi_0(p) + o(1).$$

Let us start the proof of our claim by noticing that our algorithm generates an acyclic output $H^p(v)$ with order at most $\omega(n)$ if and only if our simulation of the process $\Pi_0(p) = (Z_t)_0^\infty$ dies out with total progeny $Z = \sum Z_t$ at most $\omega(n)$, and we were not forced to create a cycle during the simulation. Hence

$$P_0 \leq \mathbb{P}(Z \leq \omega(n)) \leq P_0 + \mathbb{P}(H^p(v) \text{ contains a cycle}),$$

and therefore $P_0 \geq \mathbb{P}(Z \leq \omega(n)) + O(n^{-1/2})$, by Lemma 1$(ii)$. It now suffices to show that

$$\mathbb{P}(Z \leq \omega(n)) \geq 1 - \pi_0(p) + o(1),$$

but this is standard (cf. the proof of Lemma 22 in [4]).

(ii) This follows easily from the fact that the events $\{v \in Q^p \text{ and } |C_v(Q^p)| \leq \omega(n)\}$, $v \in Q^n$, are essentially independent if $\omega(n)$ is small. (Cf. the proof of Corollary 2(ii) above.) □

Putting together Corollary 2(ii) and Lemma 3(ii), we have the following result.

Corollary 4. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed, and let $\omega(n) \to \infty$ as $n \to \infty$. Then a.e. Q^p has $(1+o(1))pN$ vertices, from which $(\pi_0(p)+o(1))pN$ belong to components of order at least $n^{1/2}$, and $(1-\pi_0(p)+o(1))pN$ belong to components of order at most $\omega(n)$.* □

We shall need to improve the above corollary in order to prove that a giant component exists in a.e. Q^p; roughly speaking, components of order $n^{1/2}$ are too small for us. Recall that the way in which we shall show that a giant component exists is by merging largish components into a unique very large one with the addition of a few vertices to Q^p. For this proof to work, the largish components have to be of order n^C for some large enough fixed C.

3. The vertices in the large components

In this section we shall look more closely at the vertices in 'largish' components. We know from Corollary 4 that there are $(\pi_0(p) + o(1))pN$ vertices in a.e. Q^p that belong to components of order at least $n^{1/2}$. The result below improves this substantially, by allowing us to replace $n^{1/2}$ by any polynomial of n. As remarked in the introduction, it is this lemma that substitutes the gap result from [4].

Lemma 5. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed, and let an integer $C \geq 1$ be given. Then there is a constant $\alpha = \alpha(\epsilon, C) > 0$ such that for any $v \in Q^n$ we have*

$$\mathbb{P}\left[|C_v| \geq \alpha(n^{1/2}/\log n)^C \;\middle|\; v \in Q^p\right] \geq \pi_0(p) + o(1),$$

where $C_v = C_v(Q^p)$ denotes the component of Q^p that contains v.

Proof. We shall prove our lemma by induction on C. If $C = 1$ then the result holds by Corollary 2(i), and hence we proceed to the induction step. Let $0 < \epsilon \leq 1$ and $C \geq 2$ be fixed, and assume that our result holds for $C - 1$ and for all $0 < \epsilon \leq 1$.

For a vertex $v \in Q^n$ let us denote by $\mathcal{G}^v_{\rm ind}(Q^n,p) \subset \mathcal{G}_{\rm ind}(Q^n,p)$ the set of the $Q^p \in \mathcal{G}_{\rm ind}(Q^n,p)$ such that $v \in Q^p$. Let $v \in Q^n$ be fixed. We shall generate a random $Q^p \in \mathcal{G}^v_{\rm ind}(Q^n,p)$ in an indirect way, and then prove that the component $C_v = C_v(Q^p)$ of Q^p containing v is large with high probability. Indeed, to take full advantage of independence we shall generate $Q^p \in \mathcal{G}^v_{\rm ind}(Q^n,p)$ in two rounds. More precisely, let $p_2 = 1/n\log n$, and set $p_1 = (p-p_2)/(1-p_2)$ so that $p = p_1 + p_2 - p_1p_2$. A way of generating a random $Q^p \in \mathcal{G}^v_{\rm ind}(Q^n,p)$ is to pick $G_i \in \mathcal{G}^v_{\rm ind}(Q^n,p_i)$ $(i = 1,\ 2)$ randomly, and then let Q^p be such that $V(Q^p) = V(G_1) \cup V(G_2)$.

Now, a way of generating $G_1 \in \mathcal{G}^v_{\rm ind}(Q^n,p_1)$ consists in choosing a random ordering $v_2, \dots, v_N$ of the vertices of $Q^n - v$ and then inserting $v_2 \in H$ with probability p_1 and leaving it out with probability $1-p_1$, then doing the same with v_3 and so on. If we are interested in knowing whether or not our G_1 will be such that $C_v(G_1)$ has order at least $n_0 = \lceil n^{1/2} \rceil$, we may choose the ordering $v_2, v_3, \dots$ so that we examine as few vertices of Q^n as possible and when, in the process of generating G_1, it becomes clear whether or not $|C_v(G_1)| \geq n_0$, we may stop. More precisely, let us consider the following simple probabilistic algorithm that generates a random connected induced subgraph $J^{p_1}(v)$ of Q^n containing v. For a subset $S \subset Q^n$ of the vertices of the cube let us denote the vertices of $Q^n \setminus S$ that are adjacent to some vertex of S by $\delta^+(S)$.

We start by letting $J^{p_1}(v)$ be the single vertex v, and set $A = \{v\}$. We now iterate the following procedure. Set $B = \delta^+(V(J^{p_1})) \setminus A$. If B is empty we abort the process and output the current $J^{p_1}(v)$. Suppose B is not empty, and let w be the first vertex of B in the lexicographic order. We now insert w into A, and add it into $J^{p_1}(v)$ with probability p_1 and leave it out with probability $1-p_1$. (Thus A is the set of vertices of Q^n that our algorithm has examined up to the current stage.) If w is not added into $J^{p_1}(v)$ then we restart this iterative procedure by updating B. Suppose we have decided to have w in $J^{p_1}(v)$. If with the addition of w our $J^{p_1}(v)$ became of order n_0, we abort the algorithm and output this $J^{p_1}(v)$, otherwise we continue iterating this procedure by updating B.

We shall generate our G_1 by first executing our algorithm above and then deciding whether or not the vertices in $Q^n \setminus A$ should be in G_1, where A is the set of vertices examined by our algorithm. We want to show that we succeed in generating a Q^p with $C_v(Q^p)$ of large order with high probability. Let us assume that we have run our algorithm and it has generated $J_0 = J^{p_1}(v)$ of order n_0; moreover, let us denote by A_0 the set of the vertices of Q^n that have been examined by our algorithm. Note that

$$\mathbb{P}(|J_0| = n_0) = \mathbb{P}(|C_v(G_1)| \geq n_0 \mid v \in G_1),$$

and hence, by Corollary 2(i), we have that $J_0 = J^{p_1}(v)$ has n_0 vertices with probability at least $\pi_0(p_1) + o(1)$, which equals $\pi_0(p) + o(1)$ since $p_1 = (1+\epsilon+o(1))/n$.

Let $V(J_0) = \{v_i : 1 \leq i \leq n_0\}$. By a simple result of Bondy [5] (see also [3], Chapter 2), there is a set $I \subset [n]$ with $|I| = n_0 - 1$ such that all the sets $v_i \cap I$ $(1 \leq i \leq n_0)$ are distinct. Let us define n_0 pairwise disjoint subcubes of Q^n, each containing exactly one vertex of J_0. We set

$$Q_i = \{w \in Q^n : w \cap I = v_i \cap I\}$$

for $1 \leq i \leq n_0$. Note that the dimension of the Q_i is

$$m_0 = n - n_0 + 1 = (1+o(1))n.$$

Let us denote by V_0 the set of the vertices of $\bigcup Q_i$ that are adjacent to some vertex of J_0. Note that V_0 is the union of the sets V_i given by

$$V_i = V_0 \cap V(Q_i) = \{w \in Q_i : w \text{ is adjacent to } v_i\},$$

$i = 1, \dots, n_0$. Let us also note that the vertices in A_0 examined by our algorithm is such that $A_0 \cap V(Q_i) \subset V_i$. For all i we clearly have $|V_i| = m_0$ and hence $|V_0| = n_0 m_0$, since the $V_i = V_0 \cap V(Q_i)$ are pairwise disjoint. Let us now randomly choose a subset V_0' of V_0 by letting for all $w \in V_0$

$$\mathbb{P}(w \in V_0') = p_2 = 1/n \log n,$$

all these events being mutually independent. Also, let us set $V_i' = V_i \cap V_0'$. Note that $\mathbb{E}(|V_0'|) = n_0 m_0 / n \log n \geq (1+o(1)) n^{1/2} / \log n$ and $\mathbb{E}(|V_i'|) = m_0 / n \log n = (1+o(1)) / \log n$. Rather crudely we see that with probability $1 - o(1)$ we have that

$$|V_0'| \geq (1/2) n^{1/2} / \log n$$

and

$$n_i = |V_i'| \leq n^{1/2}$$

for all $i = 1, \dots, n_0$. Let us assume that the set V_0' we have randomly chosen does satisfy the two conditions above. Let us now define a collection of $\sum n_i$ pairwise disjoint subcubes Q_{ij} of dimension $m_1 = m_0 - \lfloor n^{1/2} \rfloor = (1 + o(1))n$. Let us write

$$V_i' = \{v_{ij} : 1 \leq j \leq n_i\}$$

for all i. From the neighbours of v_i in Q_i, let us arbitrarily choose $\lfloor n^{1/2} \rfloor$ vertices to form a set $W_i \subset V_i \subset Q_i$ so that $V_i' \subset W_i$. Set $I_i = I \cup \bigcup_{w \in W_i} w \triangle v_i$. Finally we define

$$Q_{ij} = \{w \in Q_i : w \cap I_i = v_{ij} \cap I_i\}$$

for all i and j. Let us now randomly pick $Q_{ij}^p \in \mathcal{G}_{\text{ind}}^{v_{ij}}(Q_{ij}, p)$. Let us denote by C_{ij} the component of Q_{ij}^p that contains v_{ij}. By the induction hypothesis, there is a constant $\alpha' > 0$ such that

$$\mathbb{P}(|C_{ij}| \geq \alpha' (n^{1/2} / \log n)^{C-1}) \geq \pi_0(p) + o(1).$$

Let the r.v. X_{ij} be the indicator function of the event $|C_{ij}| \geq \alpha' (n^{1/2} / \log n)^{C-1}$, and set $X = \sum_{i,j} X_{ij}$. Recalling that $|V_0'| = \sum n_i \geq (1/2) n^{1/2} / \log n$, we have

$$\mathbb{E}(X) \geq (\pi_0(p) + o(1))(1/2) n^{1/2} / \log n,$$

and by standard estimates for the tail of the binomial distribution we have that

$$X \geq (\pi_0(p)/3) n^{1/2} / \log n$$

with probability $1 - o(1)$. Thus we have that

$$|C_v(Q^p)| \geq (\pi_0(p) \alpha' / 3)(n^{1/2} / \log n)^C$$

almost surely, and therefore we can take $\alpha(\epsilon, C) = \pi_0(p) \alpha' / 3$. This completes the induction step and hence the proof of our lemma. □

An immediate corollary of the above lemma and the results in the previous section is the following.

Corollary 6. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed, and let an integer $C \geq 1$ be given. Then a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ has $(\pi_0(p) + o(1))pN$ vertices in components of order at least n^C.*

Proof. By Lemmas 3(i) and 5, we have that

$$\mathbb{P}\left[n^{1/3} < |C_v(Q^p)| < n^C \;\middle|\; v \in Q^p \right] = o(1).$$

Let $X = X(Q^p)$ count the number of vertices of Q^n that belong to Q^p and such that the component $C_v = C_v(Q^p)$ of Q^p containing v has order $|C_v|$ strictly between $n^{1/3}$ and n^C. Then the expectation $\mathbb{E}(X)$ of X is $o(pN) = o(N/n)$ and hence a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ is such that $X = o(N/n)$, by Markov's inequality. Now our result follows from Corollary 4. □

Let us now look at the distribution of the vertices in components of large order.

Lemma 7. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed, and let an integer $C \geq 1$ be given. Then there is a constant $\beta = \beta(\epsilon, C) > 0$ such that for a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ all vertices of Q^n are at Hamming distance at most 3 of a component of Q^p of order at least βn^C.*

Proof. Let $0 < \epsilon \leq 1$ and $C \geq 1$ be given. Let us fix $v \in Q^n$, which we may assume without loss of generality to be the empty set. Let $k = \lceil (n^2 \log n)^{1/3} \rceil$ and set $m = n - k$. We now define $s = \binom{k}{3}$ pairwise disjoint subcubes of Q^n, all of them at distance 3 from v. Let the subsets of cardinality 3 of $[k]$ be $v_1, \ldots, v_s$ and then let

$$Q_i = \{w \in Q^n : w \cap [k] = v_i\}$$

for $i = 1, \ldots, s$. Note that the Hamming distance of Q_i to v is 3, and that it is realised by the vertex $v_i \in Q_i$. Note also that the dimension of the Q_i is $m = (1 + o(1))n$, and hence that $p = (1+\epsilon)/n > (1 + \epsilon/2)/m$. Now, by Lemma 5, we have that

$$\mathbb{P}(v_i \in Q^p \text{ and } |C_{v_i}(Q^p)| \geq \alpha m^C) \geq (\pi_0 + o(1))p > \pi_0/n$$

for some constants $\alpha = \alpha(\epsilon, C) > 0$ and $\pi_0 = \pi_0(\epsilon) > 0$. Since

$$\alpha m^C = (1 + o(1))\alpha n^C > (\alpha/2)n^C,$$

the probability that v fails to be at distance at most 3 ¿from a component of Q^p of order at least $(\alpha/2)n^C$ is at most

$$\left(1 - \frac{\pi_0}{n}\right)^s \leq \exp\left(-\frac{\pi_0}{n}\binom{k}{3}\right) \leq \exp\{(\pi_0/6)n \log n\} = o(N^{-1}).$$

Hence, if we let $\beta = \beta(\epsilon, C) = \alpha(\epsilon, C)/2$, a.e. Q^p is such that all vertices of Q^n are at distance at most 3 from a component of Q^p of order at least βn^C, as required. □

4. The emergence of the giant component

In this section we shall prove the main result of this note, namely that a.e. Q^p contains a component of order $(c+o(1))pN$ if $p=(1+\epsilon)/n$ and $\epsilon>0$ is fixed, *i.e.* a *giant* component. Moreover, we shall see that this giant component is unique: this will not only follow easily ¿from our estimates on the constant c above, but we shall in fact prove that the second largest component of a.e. such Q^p has order smaller than n^{10} (cf. Theorem 9).

Theorem 8. *Let $p=(1+\epsilon)/n$ where $0<\epsilon\le 1$ is fixed. Then a.e. $Q^p \in \mathcal{G}_{\mathrm{ind}}(Q^n,p)$ has a unique component, say L, of order $(\pi_0(p)+o(1))pN$, whilst all others are of order $o(N)$. Furthermore, we a.s. have that all vertices of Q^n are at Hamming distance at most 3 from L.*

Proof. Let $p_2=n^{-2}$, and set p_1 to be such that $p=p_1+p_2-p_1p_2$. Clearly $p_1=(1+\epsilon+o(1))/n$. Let us generate a random element Q^p of $\mathcal{G}_{\mathrm{ind}}(Q^n,p)$ by randomly selecting $G_i\in\mathcal{G}_{\mathrm{ind}}(Q^n,p_i)$ ($i=1$, 2) and then letting $V(Q^p)=V(G_1)\cup V(G_2)$. By Corollary 6 and Lemma 7 we know that a.e. $Q^{p_1}\in\mathcal{G}_{\mathrm{ind}}(Q^n,p_1)$ is such that (i) the number of vertices of Q^{p_1} in components of order at least n^{21} is

$$(\pi_0(p_1)+o(1))p_1N=(\pi_0(p)+o(1))pN$$

and (ii) all the vertices of Q^n are at distance at most 3 from a vertex of Q^{p_1} whose component has order at least n^{21}.

Let us call a component of $G_1=Q^{p_1}$ *large* if its order is at least n^{21}. Note that the existence of a component L satisfying the conditions of our theorem follows if we prove that with the addition of the vertices of G_2 to G_1 all large components of G_1 belong to a single component, and hence our task now is to show that such large components do merge together easily.

Let us fix $H=G_1=Q^{p_1}$ for which (i) and (ii) above hold. Let the number of large components in H be ℓ. Assume that we can split the large components of H into two classes such that there are no paths in Q^p, and hence in G_2, between vertices that belong to components in different classes. Let the number of components in one of the classes be k, and assume that $k\le\ell/2$. Let the set of the vertices in the components in one class be S and the corresponding set for the other class be T. Clearly we have that $|S|$ and $|T|$ are at least as large as kn^{21}.

Recall that all vertices of Q^n are at distance at most three from $S\cup T$. Arguing in the same manner as in the proof of Theorem 25 in [4], we can show that there is a collection of at least $kn^{14}/6$ internally vertex-disjoint paths of Q^n between S and T, all of them of length at most 7. By our assumption on Q^p, none of the paths above are paths in G_2. Note that this happens with probability at most

$$P_0=(1-n^{-12})^{kn^{14}/6}\le \mathrm{e}^{-kn^2/6}.$$

However, the number of partitions of the large components of H into two classes with one of them having k members is clearly at most $\binom{N/n^{21}}{k}$. Now note that

$$\sum_{k=1}^{\lfloor \ell/2\rfloor} P_0\binom{N/n^{21}}{k}\le\sum_{1}^{\lfloor \ell/2\rfloor}N^k\mathrm{e}^{-kn^2/6}\le\sum_{1}^{\lfloor \ell/2\rfloor}\left[N\mathrm{e}^{-n^2/6}\right]^k=o(1),$$

completing the proof that a.e. Q^p is such that all large components of H belong to a single component.

Let us now look at the order of the other components of Q^p. Assume $n^{1/2} \geq \omega(n) \to \infty$ is fixed, and let us first note that clearly the order of a.e. Q^p is $(1+o(1))pN$. Moreover, we also know from Corollary 4 that a.s. $(\pi_0(p)+o(1))pN$ of the vertices of Q^p belong to components of order at least $n^{1/2}$ while $(1-\pi_0(p)+o(1))pN$ belong to components of order at most $\omega(n)$. Since we do know that a.e. Q^p has a component L of order at least $(\pi_0(p)+o(1))pN$, we conclude that only $o(N)$ vertices of $Q^n - L$ may belong to components of order greater than $\omega(n)$, and hence the second largest component of Q^p is a.s. of order $o(N)$, as required. □

Let us now improve the statement concerning the order of the second largest component of Q^p given in the above theorem. To do so, we shall make use of the fact that the giant component L of Q^p is, as we saw above, 'everywhere dense' in Q^n in the sense that all vertices of Q^n lie very close to L.

Theorem 9. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed. Then a.e. $Q^p \in \mathcal{G}_{\rm ind}(Q^n, p)$ is such that its second largest component has order at most $3n^9(\log n)^3(\log\log n)^2$.*

Proof. We shall again generate Q^p in two rounds. Let $p_2 = 1/n\log n$, and let p_1 be such that $p = p_1+p_2-p_1p_2$. Then we can generate $Q^p \in \mathcal{G}_{\rm ind}(Q^n, p)$ by randomly choosing $G_i \in \mathcal{G}_{\rm ind}(Q^n, p_i)$ ($i = 1$, 2), and then letting $V(Q^p) = V(G_1) \cup V(G_2)$. Since $p_1 = (1+\epsilon+o(1))/n$, we know by Theorem 8 that G_1 has a component L of order $(\pi_0(p_1)+o(1))p_1N = (\pi_0(p)+o(1))pN$ such that all vertices of Q^n are at Hamming distance at most 3 from it; let us fix $H = G_1$ satisfying these conditions. Let us partition the vertices of Q^n into four pairwise disjoint classes by letting V_i be the set of the vertices of Q^n that are at Hamming distance i from L, where $0 \leq i \leq 3$. Let us generate G_2 in three stages. We randomly pick $W_i \subset V_i$ for $i = 1$, 2 and 3 so that $\mathbb{P}(v \in W_i) = p_2$, and all these events are mutually independent. We then let G^3, G^2 and $Q^p = G^1$ be the induced subgraphs of Q^n given by $V(G^3) = V(H) \cup W_3$, $V(G^2) = V(G^3) \cup W_2$ and $Q^p = G^1 = V(G^2) \cup W_1$. Let us first look at G^3. Let $J \subset Q^n[V_3]$ be a component of $G^3[V_3 \cap V(G^3)]$, the graph induced by $V_3 \cap V(G^3)$ in G^3, and assume that the order $|J|$ of J is at least $2n^5(\log n)^2\log\log n$. Let us consider the neighbours of J in G^2 that belong to V_2, that is $\Gamma_{G^2}(V(J)) \cap V_2$.

Since the order of J is large, we have that the number of cube-neighbours of J that belong to V_2 is large as well. More precisely, as $|J| \geq 2n^5(\log n)^2\log\log n$, we see rather crudely that

$$|\Gamma_{Q^n}(V(J)) \cap V_2| \geq 2n^4(\log n)^2\log\log n.$$

Hence we have that

$$\mathbb{E}(|\Gamma_{G^2}(V(J)) \cap V_2|) \geq \mathbb{E}(|\Gamma_{Q^n}(V(J)) \cap W_2|) \geq 2n^3(\log n)\log\log n,$$

and so, by well-known estimates for the tail of the binomial distribution,

$$\mathbb{P}\left(|\Gamma_{G^2}(V(J)) \cap V_2| < n^3(\log n)\log\log n\right) < \exp\left\{-n^3(\log n)(\log\log n)/8\right\}.$$

Since trivially G^3 has at most $N/(2n^5(\log n)^2\log\log n) < N$ components of order at least $2n^5(\log n)^2\log\log n$, we see that a.e. G^2 satisfies the following property: if K is a component of G^2 such that $V(K) \cap V_3$ induces at least one component of order at least $2n^5(\log n)^2\log\log n$, then $|V(K) \cap V_2| \geq n^3(\log n)\log\log n$.

Let us assume that our G^2 does satisfy the property above. Let $K \subset Q^n[V_2 \cup V_3]$ be a component of G^2 of order at least $3n^9(\log n)^3(\log\log n)^2$. We claim that a.s. K and L will belong to the same component in Q^p, which we recall is given by $V(Q^p) = V(G^2) \cup W_1$. Note that our theorem immediately follows from this claim. Indeed, if $K \neq L$ is a component of our Q^p then it is clearly contained in $Q^n[V_2 \cup V_3]$, and hence is a component of G^2.

To prove our claim, let us first show that $|V(K) \cap V_2| \geq n^3(\log n)\log\log n$. Assume that this is not the case. Let the components of the graph induced by $V(K) \cap V_3$ in Q^n be $J_1, \dots, J_s$ where $s \geq 1$. Note that clearly $s \leq n|V(K) \cap V_2|$, and hence

$$\begin{aligned} \max |J_i| &\geq (|K| - |V(K) \cap V_2|)/s \\ &\geq \frac{3n^9(\log n)^3(\log\log n)^2 - n^3(\log n)\log\log n}{n^4(\log n)\log\log n} \\ &\geq 2n^5(\log n)^2\log\log n. \end{aligned}$$

But then, by our assumption on G^2, if $|J_j| = \max |J_i|$ then

$$|V(K) \cap V_2| \geq |\Gamma_{G^2}(V(J_j)) \cap V_2| \geq n^3(\log n)\log\log n,$$

which is a contradiction. Let us now continue with the proof of our claim.

Let the maximal cardinality of a collection of internally vertex-disjoint paths of Q^n of length two from K to L be t. Note that rather crudely we have $t \geq n^2(\log n)\log\log n$, since every vertex of $V(K) \cap V_2$ is at Hamming distance 2 from L. Therefore the probability that K and L do not get joined through a vertex of W_1 is at most

$$\left(1 - \frac{1}{n\log n}\right)^t \leq \left(1 - \frac{1}{n\log n}\right)^{n^2(\log n)\log\log n} < \exp(n\log\log n).$$

However, the number of components of G^2 is trivially at most N, and hence all components K as above get merged into L almost surely. □

Let us remark that with some more care, one can prove that the order $L_2(Q^p)$ of the second largest component of Q^p is a.s. at most $\omega(n)n^7$, where $\omega(n) \to \infty$ arbitrarily slowly. However, since we believe that $L_2(Q^p) = O(n)$, we restricted ourselves to giving the weaker result above, whose proof is correspondingly simpler. Let us close this section by putting the above theorems together.

Theorem 10. *Let $p = (1+\epsilon)/n$ where $0 < \epsilon \leq 1$ is fixed. Let $\eta = \eta(\epsilon)$ be the unique solution of $x + \mathrm{e}^{-(1+\epsilon)x} = 1$ in the interval $0 < x < 1$. Then a.e. $Q^p \in \mathcal{G}_{\mathrm{ind}}(Q^n, p)$ is such that*

$$L_1(Q^p) = (\eta + o(1))pN,$$

and furthermore

$$L_2(Q^p) \leq 3n^9(\log n)^3(\log\log n)^2.$$

Proof. This follows from Theorems 8 and 9 and Lemma 5 in [4]. □

5. Concluding remarks and open problems

We have seen that if $p = (1+\epsilon)/n$ and $\epsilon > 0$ is fixed then a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ has a giant component. In view of the results in [4], it is natural to ask whether the giant component exists when $\epsilon = \epsilon(n) \to 0$ moderately slowly, say, if $\epsilon n^{1/2} \to \infty$. The best way of approaching this problem would be to prove a gap result similar to the one given in [4]. Unfortunately the techniques used in that note break down here, as we have already mentioned. However, one may check that the method used in this note do give the following result.

There is a function $\delta(n) = o(1)$ such that if $\epsilon = \epsilon(n) = n^{-1/3+\delta(n)}$ and $p = (1+\epsilon)/n$, then the largest component of a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ has order $(2+o(1))\epsilon pN$, while the second largest component has order polynomial in n.

We omit the details of the proof of the above assertion because they are somewhat technical, and it seems unlikey that this value of ϵ gives the actual point of emergence of the giant component in Q^p. Let us finally recall that we have shown that a.e. Q^p is such that its second largest component has order $O(n^{10})$, and in view of the well-known results on the second largest component of $G_{n,p} \in \mathcal{G}(K^n, p)$ (see [2]) and the results in [4], it seems very likely to us that the following holds.

Conjecture 11. *Let $p = (1+\epsilon)/n$ where $\epsilon > 0$ is fixed. Then the second largest component of a.e. $Q^p \in \mathcal{G}_{\text{ind}}(Q^n, p)$ has order $(1+o(1))\gamma n$, where $\gamma = \gamma(\epsilon) > 0$ depends only on $\epsilon > 0$. Furthermore, $\gamma = \gamma(\epsilon)$ decreases as ϵ increases.*

Acknowledgements. The first author was partially supported by the NSF under grant DMS-8806097. The second author was supported by FAPESP, University of São Paulo, Brazil, and by a grant from the Louisiana Education Quality Support Fund through the Board of Regents. The third author was partially supported by a SERC grant while visiting the University of Cambridge.

References

[1] Ajtai, M., Komlós, J., Szemerédi, E., Largest random component of a k-cube, *Combinatorica* **2** (1982), 1–7.

[2] Bollobás, B., The evolution of random graphs, *Trans. Amer. Math. Soc.* **286** (1984), 257–274.

[3] Bollobás, B., *Combinatorics*, Cambridge University Press, Cambridge 1986, $xii + 177$ pp.

[4] Bollobás, B., Kohayakawa, Y., Łuczak, T., The evolution of random subgraphs of the cube, to appear.

[5] Bondy, J.A., Induced subsets, *J. Combinatorial Theory (B)* **12** (1972), 201–202.

[6] Dyer, M.E., Frieze, A.M., Foulds, L.R., On the strength of connectivity of random subgraphs of the n-cube, in *Random Graphs '85*, Annals of Discrete Mathematics 33 (Karoński, M., Palka, Z., eds), North-Holland, Amsterdam 1987, pp. 17–40.

[7] Erdős, P., Spencer, J.H., Evolution of the n-cube, *Comput. Math. Applics* **5** (1979), 33-39.

[8] Harris, T.E., *The Theory of Branching Processes*, Springer-Verlag, Berlin 1963, $xiv + 230$ pp.

[9] Glagolev, W.W., Some estimations for disjunctive normal forms of Boolean functions (in Russian), *Problemy Kibernet.* **19** (1967), 75–94.

[10] Kahn, J., Kalai, G., Linial, N., The influence of a variable on a Boolean function, to appear.

[11] Saposhenko, A.A., On the greatest length of an irredundant disjunctive normal form of almost all Boolean functions (in Russian), *Mat. Zametki* **4** (1967), 649–658.

[12] Saposhenko, A.A., Metric properties of almost all Boolean functions (in Russian), *Diskretny Analiz* **10** (1967), 91–119.

[13] Saposhenko, A.A., On the complexity of disjunctive normal forms obtained by a greedy algorithm (in Russian), *Diskretny Analiz* **21** (1972), 62–71.

[14] Saposhenko, A.A., Geometric structure of almost all Boolean functions (in Russian), *Problemy Kibernet.* **30** (1975), 227–261.

[15] Toman, E., Geometric structure of Random Boolean functions (in Russian), *Problemy Kibernet.* **35** (1979), 111–132.

[16] Weber, K., The length of random Boolean functions, *Elektron. Informationsverarb. u. Kibernet.* **18** (1982), 659–668.

[17] Weber, K., Subcubes of random Boolean functions, *Elektron. Informationsverarb. u. Kibernet.* **19** (1983), 365–374.

[18] Weber, K., Prime implicants of random Boolean functions, *Elektron. Informationsverarb. u. Kibernet.* **19** (1983), 449–458.

[19] Weber, K., Irredundant disjunctive normal forms of random Boolean functions, *Elektron. Informationsverarb. u. Kibernet.* **19** (1983), 529–534.

[20] Weber, K., Subcube coverings of random spanning subgraphs of the n-cube, *Math. Nachrichten* **120** (1985), 327–345.

[21] Weber, K., Subcube coverings of random graphs in the n-cube, in *Random Graphs '83*, Annals of Discrete Mathematics 28 (Karoński, M., Ruciński, A., eds), North-Holland, Amsterdam 1985, pp. 319–336.

[22] Weber, K., On the evolution of random graphs in the n-cube, in *Graphs*, *Hypergraphs and Applications* (Sachs, H., ed), Leipzig, DDR 1985, pp. 203–206.