Connectivity Properties of Random Subgraphs of the Cube

B. Bollobás[1], Y. Kohayakawa[2], and T. Łuczak[3, 4]

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

[2] Instituto de Matemática e Estatística, Universidade de São Paulo,
Caixa Postal 20570, 01452–990 São Paulo, SP, Brazil

[3] Mathematical Institute of the Polish Academy of Sciences,
Poznań, Poland

[4] On leave from the Department of Discrete Mathematics,
Adam Mickiewicz University, ul. Matejki 48/49, Poznań, Poland

Abstract. The n-dimensional cube Q^n is the graph whose vertices are the subsets of $\{1, \ldots, n\}$ where two such vertices are adjacent if and only if their symmetric difference is a singleton. Clearly Q^n is an n-connected graph of diameter and radius n. Write $M = n2^{n-1} = e(Q^n)$ for the size of Q^n. Let $\widetilde{Q} = (Q_t)_0^M$ be a random Q^n-process. Thus Q_t is a spanning subgraph of Q^n of size t, and Q_t is obtained from Q_{t-1} by the random addition of an edge of Q^n not in Q_{t-1}. Let $t^{(k)} = \tau(\widetilde{Q}; \delta \geq k)$ be the hitting time of the property of having minimal degree at least k. It is shown in [5] that, almost surely, at time $t^{(1)}$ the graph Q_t becomes connected and that in fact the diameter of Q_t at this point is $n + 1$. Here we generalise this result by showing that, for any fixed $k \geq 2$, almost surely at time $t^{(k)}$ the graph Q_t acquires the extremely strong property that any two of its vertices are connected by k internally vertex-disjoint paths each of length at most n, except for possibly one, which may have length $n + 1$. In particular, the hitting time of k-connectedness is almost surely $t^{(k)}$.

1. Introduction

Let Q^n be the *n-dimensional cube*, the graph whose vertices are the subsets of $[n] = \{1, \dots, n\}$ and where two such vertices are adjacent if and only if their symmetric difference is a singleton. Note that Q^n is an n-connected graph and that both the diameter and the radius of Q^n are n. Write $N = 2^n = |Q^n|$ for the order of Q^n and $M = n2^{n-1} = e(Q^n)$ for the size of Q^n. Let $\widetilde{Q} = (Q_t)_0^M$ be a *random Q^n-processes*. This is a Markov chain whose states are spanning subgraphs of Q^n and Q_t $(1 \le t \le M)$ is obtained from Q_{t-1} by the addition of an edge of Q^n not in Q_t, with this edge chosen uniformly at random from all the possibilities. We are interested in the behaviour of $\widetilde{Q}$ for large n and, as is usual in the theory of random graphs, we use the terms 'almost surely' and 'almost every' to mean 'with probability tending to 1 as $n \to \infty$'.

If P is a non-trivial monotone increasing property of spanning subgraphs of Q^n we let $\tau_P = \tau(P) = \tau(\widetilde{Q}; P)$ be the hitting time of P in the process $\widetilde{Q} = (Q_t)_0^M$, that is

$$\tau_P = \tau(P) = \tau(\widetilde{Q}; P) = \min\{t : Q_t \text{ has } P\}.$$

Some basic properties P we shall consider here are (i) the property $\{\delta \ge k\}$ that the minimal degree should be at least k, (ii) the property $\{\text{diam} < \infty\}$ that the graph should be connected, (iii) the property $\{\text{rad} \le r\}$ that the radius should be at most r, (iv) the property $\{\text{diam} \le d\}$ that the diameter should be at most d, and (v) the property that the graph should be k-connected. In fact, we shall deal with a much stronger property than k-connectedness but to describe it we need to introduce some definitions.

For two vertices x, y of a graph G and an integer $k \ge 1$, let the *k-distance* $d^{(k)}(x, y)$ between x and y in G be the infimum of the natural numbers ℓ such that x and y are joined in G by k internally vertex-disjoint paths, each of length at most ℓ. Define the *k-diameter* $\text{diam}^{(k)}(G)$ of G by setting

$$\text{diam}^{(k)}(G) = \max\{d^{(k)}(x, y) : x, y \in G, \ x \ne y\}$$

when G is k-connected, and $\text{diam}^{(k)}(G) = \infty$ otherwise. Clearly $\text{diam}(G) = \text{diam}^{(1)}(G)$. Here we shall consider the property $\{\text{diam}^{(k)} \le \ell\}$ for spanning subgraphs H of Q^n where $k \ge 1$ will be fixed, independent of n, and $\ell \in \{n, n+1\}$. Thus, we shall be interested in finding a large number of short, internally vertex-disjoint paths between any pair of vertices of H.

2

Thus, generally speaking, our central problem here concerns a strong variant of the concept of connectivity. The reader is referred to Faudree [8] for a very recent survey on this variant and related topics. We remark that problems concerning the existence of families of internally vertex-disjoint paths of bounded length were first studied by Lovász, Neumann-Lara, and Plummer [11].

A simple corollary of the main results of [5] is that

$$\tau(\widetilde{Q}; \delta \geq 1) = \tau(\widetilde{Q}; \text{connectedness}) = \tau(\widetilde{Q}; \text{diam} \leq n+1) = \tau(\widetilde{Q}; \text{rad} = n), \qquad (1)$$

and that

$$\tau(\widetilde{Q}; \text{diam} = n) = \tau(\widetilde{Q}; \delta \geq 2), \qquad (2)$$

for almost every $\widetilde{Q}$. Our main results here assert that much more general identities than (1) and (2) hold almost surely. Indeed, for fixed $k \geq 2$, we show that

$$\tau(\widetilde{Q}; \delta \geq k) = \tau(\widetilde{Q}; \text{diam}^{(k)} \leq n+1), \qquad (3)$$

and that

$$\tau(\widetilde{Q}; \delta \geq k+1) = \tau(\widetilde{Q}; \text{diam}^{(k)} \leq n), \qquad (4)$$

for almost every $\widetilde{Q} = (Q_t)_0^M$. Thus, typically, at time $t^{(k)} = \tau(\widetilde{Q}; \delta \geq k)$ the graph Q_t acquires the rather strong property that any two of its vertices are connected by k internally vertex-disjoint paths each of length at most $n+1$, and at time $t^{(k+1)} = \tau(\widetilde{Q}; \delta \geq k+1)$ the graph Q_t almost surely acquires the property that any two of its vertices are connected by k internally vertex-disjoint paths each of length at most n.

Note that, trivially, if $H \subset Q^n$ is a subgraph of Q^n with minimal degree $\delta(H) < k$, then H is not k-connected and hence $\text{diam}^{(k)}(H) = \infty$. Thus $\tau(\widetilde{Q}; \delta \geq k) \leq \tau(\widetilde{Q}; \text{diam}^{(k)} < \infty) \leq \tau(\widetilde{Q}; \text{diam}^{(k)} \leq n+1)$ holds for every $\widetilde{Q}$. Thus the fact that (3) holds almost surely tells us that, in a typical Q^n-process $\widetilde{Q} = (Q_t)_0^M$, the property of Q_t having minimal degree at least k, a trivially necessary condition for Q_t having finite k-diameter, is almost always sufficient to guarantee that Q_t becomes such that $\text{diam}^{(k)}(Q_t) \leq n+1$. Similarly, if a spanning subgraph $H \subset Q^n$ of Q^n has a vertex x of degree k and $y \in \Gamma_H(x)$, then the k-distance $d^{(k)}(x, y^c)$ between x and $y^c = [n] \setminus y$ is at least $n+1$. Thus, clearly, we have that $\tau(\widetilde{Q}; \delta \geq k+1) \leq \tau(\widetilde{Q}; \text{diam}^{(k)} \leq n)$. Here we prove that the reverse inequality almost always holds (cf. (4)). In fact, we prove a little more. Namely, we show that,

3

when $t = \tau(\widetilde{Q}; \delta \geq k+1)$, our random graph Q_t is almost surely such that any two of its vertices are connected by k internally vertex-disjoint paths all of which have length at most n, except for possibly one, which may have length $n+1$.

Clearly, our results above imply that for almost every $\widetilde{Q}$ we have

$$\tau(\widetilde{Q}; k\text{-connectedness}) = \tau(\widetilde{Q}; \delta \geq k), \tag{5}$$

which is in itself a pleasant result, although in view of the analogous result for ordinary random graph processes (se Bollobás and Thomason [6]), and a result of Dyer, Frieze, and Foulds [7], it is not too unexpected. In [7], the authors study the connectivity of random subgraphs of the n-cube obtained by the random deletion of vertices and edges. An immediate corollary of their main result is that the limit distribution for the probability that Q_t should be k-connected is the same as the limit distribution for the probability that Q_t should have minimal degree at least k. Clearly (5) above extends this result.

This note is organised as follows. In the next section we state the basic lemma, Lemma 1, which is at the heart of our method. This lemma is proved in [5]. In this section we also give a technical lemma, Lemma 2, which follows from Lemma 1. In Section 3 we state and prove our main result, Theorem 5. For undefined terms and notation, the reader is referred to [2]. Moreover, we remark that this note is a sequel to [5], from where some of the techniques used here are drawn. Finally, for other work concerning random subgraphs of Q^n we refer the reader to [1, 3, 4, 9, 10] and the references therein.

2. The fundamental lemma

For the study of random Q^n-processes it is often convenient to look first at the binomial model Q_p of a random spanning subgraph of the cube Q^n. As usual, given a graph H and $0 \leq p \leq 1$, we write $\mathcal{G}(H, p)$ for the space of random spanning subgraphs H_p of H such that every edge of H belongs to H_p independently with probability p. Moreover, if $0 \leq t \leq e(H)$ is an integer, we let $\mathcal{G}(H, t)$ be the space of all spanning subgraphs of H with exactly t edges, all such subgraphs being equiprobable. We write H_t for a typical element of $\mathcal{G}(H, t)$. For a set X and $r \geq 0$ we let $X^{(r)}$ denote the set of all r-subsets of X. Furthermore, let $Q^{n[-l]}$ denote a graph obtained from Q^n by the deletion of some vertices in such a way that both $\emptyset$ and $[n]$ are left in $Q^{n[-l]}$ and, for every r $(1 \leq r < n)$, no more than l vertices from $[n]^{(r)}$ are missing. This section is devoted to the study of asymptotic

4

properties of the probability space $\mathcal{G}(Q^{n[-l]}, p)$, where $0 \leq p = p(n) \leq 1$. The key lemma in this note is Lemma 1 below, which roughly states that the probability that two large sets of vertices should not be connected by a short path in $Q_p^{[-l]} = Q_p^{n[-l]} \in \mathcal{G}(Q^{n[-l]}, p)$ is superexponentially small. The proof of this lemma appears in [5], and therefore is omitted.

Lemma 1. *Let $l \in \mathbb{N}$ be fixed, and suppose that $0 < \varepsilon = \varepsilon(n) \leq 1$ and that $(\log \log n)/n < p = p(n) < 1$. Then, for all $S \subset [n]^{(1)}$ and $T \subset [n]^{(n-1)}$ with $|S|, |T| \geq n^{(1+\varepsilon)/2}$, the probability that in $Q_p^{[-l]} \in \mathcal{G}(Q^{n[-l]}, p)$ there is no S—T path of length $n - 2$ is bounded from above by $\exp\{-\varepsilon pn(\log n)/\log \log n\}$.* □

A typical application of the above lemma is as follows. We consider $x = \emptyset$, $y = [n] \in Q^n$ and generate their neighbourhoods in Q_p, obtaining $\Gamma_{Q_p}(x) = S$ and $\Gamma_{Q_p}(y) = T$, say. Then, if both S and T are large, Lemma 1 tells us that x and y fail to be connected by a path of length n in Q_p with a superexponentially small probability only. Thus most pairs of antipodal, or in fact nearly antipodal, vertices x, $y \in Q_p$ of almost every Q_p are connected by paths of length $d_{Q^n}(x, y)$. However, it is technically a little harder to deal with pairs x, $y \in Q_p$ that are not so far away from each other. Roughly speaking, their neighbourhoods in Q_p may be 'facing' the 'wrong way', so that we cannot apply Lemma 1 directly. Lemma 2 below is a variant of Lemma 1 that is more readily applicable.

For brevity, here and in what follows we use the following somewhat unusual terminology. Suppose $P \subset Q^n$ is an x–y path of length $\ell = \ell(P)$. We say that P is a *short* path if either (i) $d_{Q^n}(x, y) \geq n - n^{2/3}$ and $\ell = d_{Q^n}(x, y)$, or (ii) $n/20 \leq d_{Q^n}(x, y) < n - n^{2/3}$ and $\ell \leq d_{Q^n}(x, y) + 4$, or else (iii) $d_{Q^n}(x, y) < n/20$ and $\ell \leq n/5$.

Clearly, a short x–y path has length at most n, and it has length n if and only if x and y are at distance n in Q^n, that is, if and only if $x = y^c = [n] \setminus y$.

Lemma 2. *Let $l \in \mathbb{N}$ be fixed. Suppose $x = \emptyset$ and $x \neq y \in Q^{n[-l]}$. Let $N_x \subset \Gamma_{Q^n}(x)$, $N_y \subset \Gamma_{Q^n}(y)$ with $|N_x|, |N_y| \geq 2n^{2/3}$ be given. Suppose $1/\log \log \log n \leq p = p(n) < 1$. Then, with probability $1 - \exp\{-\Omega(n \log \log n)\}$, the graph $Q_p^{[-l]} \in \mathcal{G}(Q^{n[-l]}, p)$ contains an N_x—N_y path P such that x, $y \notin P$ and such that if $P' = xPy$ is the natural x–y path extending P, then P' is a short x–y path and, moreover, contains at most six vertices from $[n]^{(r)}$ for every $0 \leq r \leq n$.* □

The above result, which may be proved by combining Lemma 1 with some arguments from Sections 2 and 3 of [5], is all we shall need in the sequel. Let us remark in passing that, as it can be easily seen, if $d_{Q^n}(x, y) = |y| \geq n/20$, then any short x–y path $P \subset Q^n$ contains at most three vertices from each layer $[n]^{(r)}$ $(0 \leq r \leq n)$. Moreover, note that above the constant implicit in the Ω-notation may depend on l. Instead of giving a detailed proof for Lemma 2, as this would not be particularly enlightening, we only remark that it can be derived from Lemma 1 in the same way that Lemma 4 in [5] is derived from Lemma 1 above. In particular, one needs to use a straightforward variant of Lemma 3 of [5] for $Q^{n[-l]}$.

3. The main result

Our aim here is to state and prove the main result of this note, Theorem 5. Before we start, for tidiness, we introduce some further definitions and notation. Let $H \subset Q^n$ be a spanning subgraph of Q^n, let x, $y \in Q^n$ be two given vertices, and let an integer $k \geq 1$ be fixed. Suppose $X \subset \Gamma_{Q^n}(x)$ and $Y \subset \Gamma_{Q^n}(y)$ are k-element sets of vertices. Then we define the properties $\mathcal{L}(x, y) = \mathcal{L}_k(x, y)$, $\mathcal{L}(x, Y) = \mathcal{L}_k(x, Y) = \mathcal{L}_k(x, y, Y)$, and $\mathcal{L}(X, Y) = \mathcal{L}_k(X, Y) = \mathcal{L}_k(x, y, X, Y)$ as follows.

(i) We say that H has $\mathcal{L}(x, y)$ if there are k short, internally vertex-disjoint x–y paths in H.

(ii) We say that H has $\mathcal{L}(x, Y)$ if there are k short x–Y paths $P_1, \ldots, P_k$ in $H - y$ satisfying $V(P_i) \cap V(P_j) = \{x\}$ for $1 \leq i < j \leq k$.

(iii) We say that H has property $\mathcal{L}(X, Y)$ if there are k short, vertex-disjoint X—Y paths in $H - \{x, y\}$.

Let us now define some events concerning $H = Q_p$ and Q_t. First, let $k \geq 1$ and $d \geq 1$ be given, and let $W_d = W_d(H) = \{w \in Q^n : d_H(w) \geq d\}$. We say that event $\mathcal{A}(d) = \mathcal{A}_k(d)$ holds in H if for all x, $y \in W_d$ the graph H has $\mathcal{L}(x, y)$. Event $\mathcal{B}(d) = \mathcal{B}_k(d)$ holds in H if, for all $x \in W_d$, $y \in Q^n$, and any k-set of vertices $Y \subset W_d \cap \Gamma_{Q^n}(y)$, the graph H has $\mathcal{L}(x, Y)$. Event $\mathcal{C}(d) = \mathcal{C}_k(d)$ holds in H if, for any two vertices x, $y \in Q^n$ with $d_{Q^n}(x, y) \geq 10$ and any two k-sets of vertices $X \subset W_d \cap \Gamma_{Q^n}(x)$, $Y \subset W_d \cap \Gamma_{Q^n}(y)$, the graph H has property $\mathcal{L}(X, Y)$.

The key lemma in the proof of our main result, Lemma 3, asserts that for suitably large $0 < p = p(n) < 1$ and quite small $d = d(n) \geq 1$ the events $\mathcal{A}_k(d)$, $\mathcal{B}_k(d)$, and $\mathcal{C}_k(d)$

hold with superexponential probability for any fixed $k \geq 1$.

In what follows, we shall often condition on the event that a certain fixed pair of vertices of Q^n should have large degree in Q_p. Thus, for convenience, we introduce the following notation. Let $x, y \in Q^n$ be fixed. For all $0 \leq d \leq n$ and $0 < p = p(n) < 1$, we write $\mathcal{G}_{x,y,d}(Q^n, p)$ for the conditional probability space obtained from $\mathcal{G}(Q^n, p)$ by conditioning on the event $\{d_{Q_p}(x), d_{Q_p}(y) \geq d\}$. Similarly, given a graph H, two vertices $x, y \in H$ in H, and $S \subset \Gamma_H(x)$, $T \subset \Gamma_H(y)$, we let $\mathcal{G}_{S,T}(H, p) = \mathcal{G}_{x,y;S,T}(H, p)$ be the conditional space obtained from $\mathcal{G}(H, p)$ by conditioning on the event $\{\Gamma_{H_p}(x) = S, \Gamma_{H_p}(y) = T\}$. We may now state and prove Lemma 3. (The constants in the Ω-notation below are allowed to depend on k.)

Lemma 3. *Suppose an integer $k \geq 1$ is fixed, and let $.498 < p = p(n) < 1$ and $d = d(n) = 3n^{2/3}$. Then*

(i) *the probability that $\mathcal{A}_k(d)$ holds in $Q_p \in \mathcal{G}(Q^n, p)$ is $1 - \exp\{-\Omega(n \log \log n)\}$,*

(ii) *the probability that $\mathcal{B}_k(d)$ holds in $Q_p \in \mathcal{G}(Q^n, p)$ is $1 - \exp\{-\Omega(n \log \log n)\}$,*

(iii) *the probability that $\mathcal{C}_k(d)$ holds in $Q_p \in \mathcal{G}(Q^n, p)$ is $1 - \exp\{-\Omega(n \log \log n)\}$.*

Proof. (i) Fix two vertices $x, y \in Q^n$ of Q^n. Consider the conditional space $\mathcal{G}_{x,y,d}(Q^n, p)$. To prove (i), it is enough to show that the probability that $Q_p \in \mathcal{G}_{x,y,d}(Q^n, p)$ fails to have $\mathcal{L}(x, y) = \mathcal{L}_k(x, y)$ is $\exp\{-\Omega(n \log \log n)\}$.

Without loss of generality, we may assume that $x = \emptyset$. Let $S \subset \Gamma_{Q^n}(x)$, $T \subset \Gamma_{Q^n}(y)$ with $|S|, |T| \geq d = d(n) = 3n^{2/3}$ be fixed and consider the conditional space $\mathcal{G}_{S,T}(Q^n, p)$. It suffices to show that

$$\mathbb{P}\{\mathcal{L}(x, y) \text{ fails in } Q_p \in \mathcal{G}_{S,T}(Q^n, p)\} = \exp\{-\Omega(n \log \log n)\}.$$

To prove this estimate, first consider the subgraph H_0 of Q^n spanned by the edges of the form uv, where either $u = x$ and $v \in S$, or else $u = y$ and $v \in T$. Find as many internally vertex-disjoint x–y paths in H_0 as possible, and suppose that there are k_0 such paths, say. Note that $0 \leq k_0 \leq 2$. Let $G^{(1)} = Q^{n[-2]}$ be the graph obtained from Q^n by the deletion of the internal vertices in these k_0 paths. We now proceed to find $k' = k - k_0$ short x–y paths in $G_p^{(1)} \in \mathcal{G}_{S_1,T_1}(G^{(1)}, p)$ inductively, where $S_1 = S \cap V(G^{(1)})$ and $T_1 = T \cap V(G^{(1)})$. To do this we use Lemma 2 in several $Q^{n[-l]}$. Let $p_0 = p/k'$.

Consider $H_1 = G_{p_0}^{(1)} \in \mathcal{G}_{S,T}(G^{(1)}, p_0)$. By Lemma 2, we have that with probability $1 - \exp\{-\Omega(n \log \log n)\}$, there is a short x–y path P_1 in H_1 satisfying $|V(P_1) \cap [n]^{(r)}| \leq 6$

for all r. Assume such a path does exist in H_1. Now we consider $G^{(2)} = Q^{n[-8]}$ obtained from $G^{(1)} = Q^{n[-2]}$ by the deletion of the vertices in $V(P_1) \setminus \{x, y\}$. Let $S_2 = S \cap V(G^{(2)})$ and similarly $T_2 = T \cap V(G^{(2)})$.

Now let $H_2 = G^{(2)}_{p_0} \in \mathcal{G}_{S_2, T_2}(G^{(2)}, p_0)$. Again by Lemma 2, with probability $1 - \exp\{-\Omega(n \log \log n)\}$, we find a short x–y path P_2 in H_2 with $|V(P_2) \cap [n]^{(r)}| \leq 6$ for all r. Assume such a path $P_2 \subset H_2$ exists, and consider $G^{(3)} = Q^{n[-14]}$ obtained from $G^{(2)} = Q^{n[-8]}$ by the deletion of the vertices in $V(P_2) \setminus \{x, y\}$. Let $S_3 = S \cap V(G^{(3)})$ and $T_3 = T \cap V(G^{(3)})$, and proceed as above to find P_3.

Iterating the above procedure k' times, we find the required paths $P_1, \ldots, P_{k'}$ with probability $1 - \exp\{-\Omega(n \log \log n)\}$ in $H_1 \cup \cdots \cup H_{k'}$. This completes the proof of (i).

(ii) A proof of Lemma 3(ii) may be obtained by coupling the above proof of (i) with ideas from the proof of Lemma 3(iii) below. Thus we omit the proof of (ii), and proceed to prove (iii).

(iii) Let x, $y \in Q^n$ be such that $d_{Q^n}(x, y) \geq 10$, and suppose that $x_1, \ldots, x_k \in \Gamma_{Q^n}(x)$, $y_1, \ldots, y_k \in \Gamma_{Q^n}(y)$ are $2k$ fixed vertices. We may and shall assume that $x = \emptyset$. Let $S_1, \ldots, S_k$ and $T_1, \ldots, T_k$ be such that $x \notin S_i \subset \Gamma_{Q^n}(x_i)$, $y \notin T_i \subset \Gamma_{Q^n}(y_i)$, and $|S_i|$, $|T_i| \geq 3n^{2/3} - 1$ $(1 \leq i \leq k)$. Let $\mathcal{N}$ be the event

$$\{\Gamma_{Q_p}(x_i) = S_i \text{ and } \Gamma_{Q_p}(y_i) = T_i \text{ for all } 1 \leq i \leq k\}.$$

To prove Lemma 3(iii), it suffices to show that

$$\mathbb{P}\big(\mathcal{C}(d) \text{ fails in } Q_p \in \mathcal{G}(Q^n, p) \,\big|\, \mathcal{N}\big) = \exp\{-\Omega(n \log \log n)\}.$$

Let $G^{(0)} = Q^n - \{x, y\} = Q^{n[-1]}$. We now seek k vertex-disjoint short paths in $G^{(0)}$, say $P_1, \ldots, P_k$, with P_i $(1 \leq i \leq k)$ connecting x_i to y_i in $G^{(0)}_p \in \mathcal{G}(G^{(0)}, p \mid \mathcal{N})$, the space obtained from $\mathcal{G}(G^{(0)}, p)$ by conditioning on $\mathcal{N}$. Let $p_0 = p/k$.

Let $G^{(1)} = G^{(0)} - \{x_i, y_i : 2 \leq i \leq k\}$, and pick $H_1 = G^{(1)}_{p_0} \in \mathcal{G}_{S_1, T_1}(G^{(1)}, p_0)$, the space obtained from $\mathcal{G}(G^{(1)}, p_0)$ by conditioning on $\{\Gamma_{G^{(1)}_{p_0}}(x_1) = S'_1, \Gamma_{G^{(1)}_{p_0}}(y_1) = T'_1\}$, where $S'_1 = S_1 \cap V(G^{(1)})$ and $T'_1 = T_1 \cap V(G^{(1)})$. Then, with probability $1 - \exp\{-\Omega(n \log \log n)\}$, there is a short x_1–y_1 path in H_1 with $|V(P_1) \cap [n]^{(r)}| \leq 12$ for all r. Indeed, to apply Lemma 2, we first consider the automorphism $\varphi = \varphi_{x_1}$ of the graph Q^n given by $u \mapsto u \triangle x_1 = (u \cup x_1) \setminus (u \cap x_1)$. Then $\varphi(x_1) = \emptyset$, and we may apply Lemma 2 to obtain, with large probability, a short $\varphi(x_1)$–$\varphi(y_1)$ path P'_1 in $\varphi(H_1)$ with $|V(P'_1) \cap [n]^{(r)}| \leq 6$ for all r. We

then take the short x_1–y_1 path $P_1 = \varphi(P_1')$ in H_1, and note that indeed $|V(P_1) \cap [n]^{(r)}| \leq 12$, since x_1 is a singleton and hence $\varphi^{-1}\{[n]^{(r)}\} \subset [n]^{(r-1)} \cup [n]^{(r+1)}$ for all r. Assume we have found such a path P_1 in H_1.

Now consider $G^{(2)} = G^{(0)} - (\{x_i, y_i : 1 \leq i \leq n,\ i \neq 2\} \cup V(P_1))$, $S_2' = S_2 \cap V(G^{(2)})$, $T_2' = T_2 \cap V(G^{(2)})$. We now pick $H_2 = G_{p_0}^{(2)} \in \mathcal{G}_{S_2', T_2'}(G^{(2)}, p_0)$ to find a suitable short x_2–y_2 path P_2. Iterating the procedure above k times we find, with probability $1 - \exp\{-\Omega(n \log \log n)\}$, the k paths $P_1, \ldots, P_k$ as required. This completes the proof (iii), and hence of Lemma 3. $\qquad\square$

We now give a result for $\widetilde{Q} = (Q_t)_0^M$ that is analogous to Lemma 3, and proceed to state and prove our main result.

Lemma 4. *Suppose an integer $k \geq 1$ is fixed, and $d = d(n) = 4n^{2/3}$. Then the probability that $\widetilde{Q} = (Q_t)_0^M$ is such that $\mathcal{A}_k(d)$, $\mathcal{B}_k(d)$, and $\mathcal{C}_k(d)$ hold for all Q_t with $t \geq .499M$ is $1 - \exp\{-\Omega(n \log \log n)\}$.*

Proof. The argument here is similar to the one in the proof of Corollary 6 in [5], and is based on Lemma 3 above. Let $.499 \leq t = t(n) \leq M$ and $p = p(n) = \left(1 - ((\log n)/M)^{1/2}\right) t/M$. Then $\mu = pM = \left(1 - ((\log n)/M)^{1/2}\right) t = (1 + o(1))t$, and, from standard estimates for the tail of the binomial distribution, we have $|e(Q_p) - \mu| \leq (1/2)((\log n)/M)^{1/2}\mu$ with probability $1 - n^{-1/20}$.

In particular, (*) $t - 2(M \log n)^{1/2} \leq e(Q_p) \leq t$ holds for every fixed $.499M \leq t \leq M$ with probability $1 - n^{-1/20}$. Let $\mathcal{G}_{\mathrm{c}}(Q^n, p)$ be the conditional probability space obtained from $\mathcal{G}(Q^n, p)$ conditioning on (*). Note that if $\mathcal{A}$ is any event concerning $Q_p \in \mathcal{G}(Q^n, p)$, then $\mathbb{P}_{\mathrm{c}}(\mathcal{A}) \leq (1 + o(1))\mathbb{P}(\mathcal{A})$, where $\mathbb{P}_{\mathrm{c}}$ denotes the probability in $\mathcal{G}_{\mathrm{c}}(Q^n, p)$. Let $d' = d'(n) = 3n^{2/3}$, and let $\mathcal{A}_0$ be the event that $\mathcal{A}_k(d')$, $\mathcal{B}_k(d')$, and $\mathcal{C}_k(d')$ hold. Then, by Lemma 3, we have $\mathbb{P}_{\mathrm{c}}(\mathcal{A}_0) = 1 - (1 + o(1))n^{-1/20}$. Now, we may generate $Q_t \in \mathcal{G}(Q^n, t)$ by first picking $Q_p \in \mathcal{G}_{\mathrm{c}}(Q^n, p)$, and then randomly adding $t' = t - e(Q_p)$ new edges to Q_p. One may check that $Q_{t'} \in \mathcal{G}(Q^n, t')$ is such that its maximal degree $\Delta(Q_{t'})$ satisfies $\Delta(Q_{t'}) \leq n^{2/3}$ with probability $1 - \exp\{-\Omega(n^{4/3}/\log n)\}$. Thus Q_t satisfies $\mathcal{A}_k(d)$, $\mathcal{B}_k(d)$, and $\mathcal{C}_k(d)$ with probability $1 - \exp\{-\Omega(n \log \log n)\}$. Thus these three properties hold for all Q_t in $\widetilde{Q} = (Q_t)_0^M$ with $t \geq .499M$ with probability $1 - M \exp\{-\Omega(n \log \log n)\} = 1 - \exp\{-\Omega(n \log \log n)\}$. $\qquad\square$

9

We have thus arrived at our main result.

Theorem 5. *Let an integer $k \geq 1$ be fixed. Almost every random Q^n-process $\widetilde{Q} = (Q_t)_0^M$ is such that*

(i) $t^{(k)} = \tau(\widetilde{Q}; \delta \geq k) = \tau(\widetilde{Q}; \operatorname{diam}^{(k)} \leq n+1)$,

(ii) $t^{(k+1)} = \tau(\widetilde{Q}; \delta \geq k+1) = \tau(\widetilde{Q}; \operatorname{diam}^{(k)} \leq n)$.

Proof. It is easily checked that if $t_0 = t_0(n) = \lceil .499M \rceil$, then a.e. $Q_{t_0} \in \mathcal{G}(Q^n, t_0)$ is such that any two vertices of degree less than $d = d(n) = 4n^{2/3}$ are at distance at least 10 and at most $n - 10$ in Q^n. Thus we may condition our Q^n-process $\widetilde{Q} = (Q_t)_0^M$ on being such that (1) Q_t has this property for all $t \geq t_0$. Now recall that by Lemma 4, for a.e. $\widetilde{Q} = (Q_t)_0^M$, we have (2) the events $\mathcal{A}_k(d)$, $\mathcal{B}_k(d)$, and $\mathcal{C}_k(d)$ hold in Q_t for all $t \geq t_0$. It now suffices to notice that, in any $\widetilde{Q}$ satisfying (1) and (2), assertions (i) and (ii) must necessarily hold.

Let us check (i). Suppose $\widetilde{Q} = (Q_t)_0^M$ satisfies (1) and (2), and let $t \geq t^{(k)}$. Let x, $y \in Q^n$ be two fixed vertices of Q^n. We shall check that the k-distance $d_{Q_t}^{(k)}(x,y)$ between x and y in Q_t is at most $n+1$. If $d_{Q_t}(x)$, $d_{Q_t}(y) \geq d$, then $\mathcal{A}_k(d)$ tells us that $\mathcal{L}_k(x,y)$ holds, and so $d_{Q_t}^{(k)}(x,y) \leq n$. Indeed, simply observe that any short path has length at most n. Now suppose that $d_{Q_t}(x) \geq d$ and $d_{Q_t}(y) < d$. Pick k vertices $y_1, \ldots, y_k \in \Gamma_{Q_t}(y)$ and note that, by (1), we have $d_{Q_t}(y_i) \geq d$ $(1 \leq i \leq k)$. Now $\mathcal{B}_k(d)$ tells us that $\mathcal{L}_k(x,Y)$ holds, where $Y = \{y_1, \ldots, y_k\}$, and hence $d_{Q_t}^{(k)}(x,y) \leq n+1$. In fact, more is true: either $d_{Q_t}^{(k)}(x,y) \leq n$, or else y has degree k in Q_t and $x^c \in \Gamma_{Q_t}(y)$, and moreover all the k internally vertex-disjoint x–y paths naturally given by $\mathcal{L}_k(x,Y)$ have length at most n, except for one, which has length $n+1$.

Finally, assume that $d_{Q_t}(x)$, $d_{Q_t}(y) < d$. Then by (1) we have that $10 \leq d_{Q^n}(x,y) \leq n-10$. Pick $2k$ vertices $x_1, \ldots, x_k \in \Gamma_{Q_t}(x)$, $y_1, \ldots, y_k \in \Gamma_{Q_t}(y)$. Again by (1) we have that $d_{Q_t}(x_i)$, $d_{Q_t}(y_i) \geq d$ for all $1 \leq i \leq k$. Now take $X = \{x_1, \ldots, x_k\}$, $Y = \{y_1, \ldots, y_k\}$, and note that then $\mathcal{C}_k(d)$ tells us that $\mathcal{L}_k(X,Y)$ holds in Q_t. Thus $d_{Q_t}^{(k)}(x,y) \leq n$. This completes the proof of (i). The proof of (ii) is similar. $\square$

We remark that above we in fact proved a statement stronger than (i) for almost every $\widetilde{Q} = (Q_t)_0^M$. Indeed, we showed that when $t = t^{(k)}$ the graph Q_t almost surely satisfies the following property: *for any pair x, $y \in Q_t$ of vertices of Q_t, either (a) $d^{(k)}(x,y) \leq n$, or else (b) one of x and y, say y, has degree k in Q_t and $x^c \in \Gamma_{Q_t}(y)$, and moreover x and y*

10

are connected by k internally vertex-disjoint paths all of which have length at most n, except for one, which has length $n + 1$.

Theorem 5 has the following immediate consequence.

Corollary 6. *For almost every random Q^n-process $\widetilde{Q} = (Q_t)_0^M$ and fixed integer $k \geq 1$, we have*

$$t^{(k)} = \tau(\widetilde{Q}; \delta \geq k) = \tau(\widetilde{Q}; k\text{-connectedness}) \qquad \square$$

Clearly, one can also define the *k-radius* $\mathrm{rad}^{(k)}(G)$ of a k-connected graph G, a generalisation of the ordinary radius, by setting

$$\mathrm{rad}^{(k)}(G) = \min_x \max_y \{d^{(k)}(x, y)\}.$$

Then one can easily combine the arguments in the proofs of Theorem 5 above and of Theorem 13 of [5] to show that in almost every random Q^n-process $\widetilde{Q} = (Q_t)_0^M$ the hitting time of the property of having k-radius at most n is $t^{(k)} = \tau(\widetilde{Q}; \delta \geq k)$. We omit the details.

References

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

[2] Bollobás, B., *Random Graphs*, Academic Press, London 1985, $xvi + 447$pp.

[3] Bollobás, B., Complete matchings in random subgraphs of the cube, *Random Structures and Algorithms* **1** (1990), 95–104.

[4] Bollobás, B., Kohayakawa, Y., Łuczak, T., The evolution of random subgraphs of the cube, *Random Structures and Algorithms* **3** (1992), 55–90.

[5] Bollobás, B., Kohayakawa, Y., Łuczak, T., On the diameter and radius of random subgraphs of the cube, to appear.

[6] Bollobás, B., Thomason, A.G., Random graphs of small order, in *Random Graphs '83*, Annals of Discrete Mathematics 28 (Karoński, M., Ruciński, A., eds), North-Holland, Amsterdam 1985, pp. 47–97.

[7] 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.

[8] Faudree, R.J., Some strong variations of connectivity, in *Combinatorics*, *Paul Erdős is Eighty*, Volume 1 (Miklós, D., Sós, V.T., Szőnyi, T., eds), Keszthely (Hungary) 1993, pp. 125–144.

[9] Kostochka, A.V., Sapozhenko, A.A., Weber, K., On random cubical graphs, in *Fourth Czechoslovakian Symposium on Combinatorics, Graphs and Complexity* (Nešetřil, J., Fiedler, M., eds), Annals of Discrete Mathematics 51, North–Holland, Amsterdam 1992, pp. 155–160.

[10] Kostochka, A.V., Sapozhenko, A.A., Weber, K., Radius and diameter of random subgraphs of the hypercube, *Random Structures and Algorithms* **4** (1993), 215–229.

[11] Lovász, L., Neumann-Lara, V., Plummer, M., Mengerian theorems for paths of bounded length, *Periodica Math. Hungar.* **9** (1978), 269–276.