WHEN IS A RANDOM GRAPH PROJECTIVE?

TOMASZ ŁUCZAK AND JAROSLAV NEŠETŘIL

Abstract. We characterize all the values of $M = M(n)$ for which the random graph $\mathbb{G}(n, M)$ is a.a.s. projective.

1. Introduction

The theory of random discrete structures has contributed a lot to our understanding of many problems in graph theory; numerous examples of such an influence can be found in monographs [3] and [4]. However, until now relatively few authors have studied properties of products of random graphs. On the other hand, the behaviour of certain types of products of random graphs could, possibly, shed some light on the behaviour of Shannon capacities of graphs (see, for instance, [2] and Conjecture 5.1 in [1] with the following discussion), Hedetniemi's conjecture, and related problems. In this paper we make a small step towards studying properties of products of random graph, characterizing densities for which a random graph is projective.

Let us recall some basic definitions. A *homomorphism* of two graphs G and H is a map $f : V(G) \to V(H)$ for which $\{f(x), f(y)\} \in E(H)$ whenever $\{x, y\} \in E(G)$. A graph H is *rigid* if the identity map is the only homomorphism from H to H. For a graph $H = (V, E)$ and a natural number k, by H^k we denote the graph with vertex set $V^k = V \times \cdots \times V$, in which two vertices $(v_1, \ldots, v_k)$ and $(w_1, \ldots, w_k)$ are adjacent if and only if $\{v_i, w_i\} \in E$ for every $i = 1, \ldots, k$. Equivalently, H^k can be defined as the maximal graph on the set V^k for which all projections $\pi_i : (x_1, \ldots, x_n) \to x_i$ are homomorphisms. A homomorphism $f : H^k \to H$ is *idempotent* if $f(x, \ldots, x) = x$ for each $x \in V$. A graph H is *projective* if every idempotent homomorphism $g : H^k \to H$ is a projection, and is *strongly rigid* if every homomorphism $g : H^k \to H$ is a projection. It is easy to see that H is strongly rigid if and only if it

Date: September 23, 2003.

1991 *Mathematics Subject Classification.* 05C80.

Key words and phrases. random graphs, graph homomorphisms, projective graphs.

The first author was partially supported by KBN grant 2 P03A 016 23, the second author by a grant LN00A56 of the Czech Ministery of Education.

is rigid and projective. For more information on projective and rigid graphs and the role they play in the studies of category of graphs and their homomorphisms, we refer the reader to [9] and [11].

Larose and Tardif [5, 6], inspired by an earlier work of Rosenberg [10], asked whether most graphs on a large set are projective. In [7] we provided an elementary argument which settled this problem in the affirmative. In this note we would like to investigate this property for a random graph in much more detail.

Let us recall that *the random graph* $\mathbb{G}(n, M)$ is a graph chosen at random from the family of $\binom{\binom{n}{2}}{M}$ graphs with vertex set $[n] = \{1, 2, \dots, n\}$ and M edges. Equivalently, $\mathbb{G}(n, M)$ can be viewed as the $(M+1)$-stage of *the random graph process* $\mathcal{G}(n) = \{\mathbb{G}(n, M)\}_{M=0}^{\binom{n}{2}}$ which starts with the empty graph on the vertex set $[n]$, and for $1 \le M \le \binom{n}{2}$ a graph $\mathbb{G}(n, M)$ is obtained from $\mathbb{G}(n, M-1)$ by adding to the set of its edges a pair chosen at random from the family of all pairs $\{i, j\}$, $1 \le i < j \le n$, which are not edges of $\mathbb{G}(n, M-1)$ (for more elaborate treatment of these and other random graphs notions used here see [4]). We say that some property holds for $\mathcal{G}(n)$ *a.a.s.* if the probability that $\mathcal{G}(n)$ has this property tends to one as $n \to \infty$. Our aim is to determine the set of all values M for which the random graph $\mathbb{G}(n, M)$ is a.a.s. projective.

In order to state our results in the most precise form let us introduce two random variables related to $\mathcal{G}(n)$. By τ_1 we denote the minimum value of M such that the minimum degree of $\mathbb{G}(n, M)$ is at least two, and by τ_2 we mean the maximum value of M for which the maximum degree of $\mathbb{G}(n, M)$ is at most $n-3$. Now our main result can be stated as follows.

Theorem 1. *A.a.s. the random graph process* $\mathcal{G}(n) = \{\mathbb{G}(n, M)\}_{M=0}^{\binom{n}{2}}$ *is such that* $\mathbb{G}(n, M)$ *is projective if and only if either* $\tau_1 \le M \le \tau_2$, *or* $M = \binom{n}{2}$.

2. Proof of the main result

As typical in random graph theory we first introduce a family of graphs $\mathcal{B}$ such that for the choice of the parameter $M = M(n)$ we are interested in a.a.s. $\mathbb{G}(n, M) \in \mathcal{B}$, so that later on we can restrict ourselves only to graphs from $\mathcal{B}$. Here and below all logarithms are natural and all inequalities and estimates are assumed to hold only for n which is large enough.

Definition. *Let G be a graph with vertex set $[n]$. We say that G has property $\mathcal{B} = \mathcal{B}(n, d)$ if it is connected and the following holds.*

(i) *Any bipartite subgraph of H induced by two disjoint subsets S_1, S_2, $|S_1| = s_1$, $|S_2| = s_2$, $s_1, s_2 \geq \frac{200n}{d} \log d$, contains at least $0.81 s_1 s_2 d/n$ and at most $1.19 s_1 s_2 d/n$ edges. In particular, each subgraph induced in H by a subset S, $|S| = s$, $s \geq \frac{400n}{d} \log d$, contains at least $0.4s^2 d/n$ and at most $0.6s^2 d/n$ edges.*

(ii) *No subgraph of H of $s \leq \frac{n}{d} \log^2 d$, vertices contains more that $s \log^3 d$ edges.*

(iii) *If $d \geq \log^2 n$, then the degree of every vertex of H is at least $0.9d$ and at most $1.1d$; if $d \leq \log^2 n$, then each vertex of H has at least two but at most $3d$ neighbours. Furthermore, no vertex of degree at most $0.1d$ lie at a cycle shorter than five, and no two vertices of degree at most $0.1d$ lie within distance three from each other.*

(iv) *No two vertices of H have more than $1.1d^2/n + \log^2 d$ common neighbours, and no three vertices have more than $1.1d^3/n^2 + \log^2 d$ common neighbours. Furthermore, any two vertices of H have at least $\max\{0, 0.9d^2/n - \log^2 d\}$ common neighbours.*

(v) *Let S_1, S_2, S_3, S_4 be sets of vertices of H, each of $s \geq \frac{800n}{d} \log d$ vertices, such that $S_2 \cap S_4 = \emptyset$, and let $B_{1,2}$ and $B_{3,4}$ be bipartite graphs induced in H by the sets S_1, S_2, and S_3, S_4, respectively. Then no bijection $f : S_1 \cup S_2 \to S_3 \cup S_4$, with $f(S_1) = S_3$, $f(S_2) = S_4$, is a graph homomorphism from $B_{1,2}$ to $B_{3,4}$.*

(vi) *For every vertex v there exists a set W containing at most $\log^2 d$ neighbours of degree at least $0.1d$ such that v is the only vertex adjacent to all vertices from W.*

(vii) *Let v, w, u be three different vertices of H such that u has degree at least three. Then, there exists a vertex t which is a neighbour of u but which is adjacent neither to v, nor to u.*

(viii) *If $d \geq n^{0.9}$, then for every vertices v_1, v_2, v_3, v_4 of H there exist at least three vertices which are adjacent to v_1, v_2, v_3 and are not adjacent to v_4, and at least three vertices which are adjacent to v_1 and are not adjacent to v_2, v_3, v_4.*

Our next result states that, indeed, a typical random graph (with the number of edges we are interested in) has property $\mathcal{B}(n, 2M/n)$.

Lemma 2. *A.a.s. the random graph process $\mathcal{G}(n) = \{\mathbb{G}(n, M)\}_{M=0}^{\binom{n}{2}}$ is such that for each M, $\tau_1 \leq M \leq n^2/4$, $\mathbb{G}(n, M)$ has property $\mathcal{B}(n, 2M/n)$, and for each M, $n^2/4 \leq M \leq \tau_2$, the complement of $\mathbb{G}(n, M)$ has property $\mathcal{B}(n, n - 2M/n)$.*

Proof. Since the assertion can be easily verified using the first moment method and the well known estimates for the tails of binomial distribution (see, for instance, [4]) we omit it here. □

One of the basic tools in the proof of Theorem 1 is the following result of Larose and Tardif [5] which states that in order to check if H is projective it is enough to consider homomorphisms from $H \times H$ to H.

Theorem 3. *A graph H is projective if and only if it is 2-projective; i.e. if the only homomorphism $f : H \times H \to H$ satisfying $f(v, v) = v$ is a projection.* □

Let us start with the following observation.

Lemma 4. *Let H be a graph with property $\mathcal{B}(n, d)$ for some $10^{10} \le d \le n/2$ and let $g : H \times K_2 \to H$ be a graph homomorphism. Then either $g(v, 1) = g(v, 2) = v$ for each $v \in V(H)$ (i.e., the homomorphism g is a projection on $V(H)$), or, for some $v \in V(H)$, we have $|g^{-1}(v)| \ge \frac{800n}{d} \log d$.*

In particular, H is rigid.

Proof. For $i = 1, 2$, let $W_i = g(V(H), i)$, and $V_i = \{v :\ g(v, i) = v\}$. We consider the following three cases.

Case 1. $|V_i| \le \frac{200n}{d} \log d$ *and* $|W_i| \ge \frac{1300n}{d} \log d$, *for* $i = 1, 2$.

It is easy to see that in this case one can find four disjoint subsets S_1, S_2, S_3, S_4 of $V(H)$, each of $m = \lceil \frac{200n}{d} \log d \rceil$ vertices, such that $S_3 = g(S_1, 1)$ and $S_4 = g(S_2, 2)$. But this contradicts the property $\mathcal{B}(v)$.

Case 2. $|V_i| \ge \frac{200n}{d} \log d$ *for some* $i = 1, 2$.

Let $|V_1| \ge \frac{200n}{d} \log d$ and let $X \subseteq V(H) \setminus V_1$ denote the set of all vertices $x \in V(H) \setminus V_1$ for which there exists $y \in V(H) \setminus V_1$, $x \ne y$, such that $V_1 \cap N(x) = V_1 \cap N(y)$. If $|X| \ge \frac{600n}{d} \log d$, then one can find $X_1, X_2 \subseteq X$ such that $|X_1| = |X_2| \ge \frac{200n}{d} \log d$, and the bipartite graph induced in H by (V_1, X_1) and (V_1, X_2) respectively are isomorphic, which contradicts $\mathcal{B}(v)$. Hence $|X| \le \frac{600n}{d} \log d$ and, since $V_2 \supseteq V(H) \setminus (V_1 \cup X)$, we infer that $|V_2| \ge n - \frac{800n}{d} \log d$. A 'symmetric' argument gives $|V_1| \ge n - \frac{800n}{d} \log d$.

Note that $\mathcal{B}(i)$ and $\mathcal{B}(iii)$ imply that if the set of all vertices of degree at least $0.1d$ which do not belong to V_1 is non-empty, then there is $w \notin V_1$ with has in V_2 at least $0.01d$ neighbours. Hence, by $\mathcal{B}(iv)$, w is uniquely determined by its neighbours in V_2, and so $v \in V_1$. This contradiction shows that V_1, as well as V_2, contains all vertices of H of degree at least $0.1d$. But then, using $\mathcal{B}(iii)$ and $\mathcal{B}(iv)$, we infer that each vertex $w \notin V_1$ is uniquely determined by its neighbourhood in V_2. Hence $V_1 = V(H)$ and, by a similar argument, also $V_2 = V(H)$, i.e., the homomorphism g is a projection on $V(H)$.

Case 3. $|W_i| \le \frac{1300n}{d} \log d$ *for some* $i = 1, 2$.

Let us assume that $|W_1| \le \frac{1300n}{d} \log d$ and let U_2 denote the set of the vertices of H of degree at least $0.1d$. From $\mathcal{B}(i)$ and $\mathcal{B}(iii)$ we infer that $|U_2| \ge n - \frac{400n}{d} \log d$. Take any $w \in W_1$. If $|g^{-1}(w)| = m$ for some $m = m(w) \ge \frac{800n}{d} \log d$, we are done, so let us assume that this is not the case. Note that from $\mathcal{B}(ii)$ it follows that at most $m(w)/\log d$ vertices of H have in $g^{-1}(w)$ more than $2\log^4 d$ neighbours.

Hence, there are at most $n/\log d$ vertices $u_2 \in U_2$ such that the vertex $g(U_2, 2)$ is adjacent to fewer than $0.1d/2\log^4 d \ge d\log^{-5} d$ neighbours in W_1. Consequently, between the sets $W_1 = g((V(H), 1)$, $|W_1| \le \frac{1300n}{d} \log d$, and $g(U_2, 2)$, there are at least $|g(U_2, 2)| d \log^{-6} d$ edges, which contradicts $\mathcal{B}(i)$.

Finally, from the part of the assertion we have just proved it follows that for every non-trivial homomorphism $f : H \to H$ there exists a vertex $v \in V(H)$ such that $|f^{-1}(v)| \ge \frac{400n}{d} \log n$. But $\mathcal{B}(i)$ implies that the subgraph spanned in H by $f^{-1}(v)$ contains at least one edge, which is transformed by f into a pair $\{v, v\}$, while H contains no loops. This contradiction shows that the only homomorphism from H to H is the identity, i.e., H is rigid. □

Lemma 5. *Let H be a graph on n vertices which has property $\mathcal{B}(n, d)$, for some $d = d(n)$ such that $10^9 < d < n^{0.9}$, and let $f : H \times H \to H$ be a homomorphism such that for every $v \in V(H)$ we have $f(v, v) = v$. Then f is a projection.*

Proof. Note first that if for some $w \in V(H)$ and each $v \in V(H)$ we have $f(v, w) = v$, then $\mathcal{B}(vi)$ implies that for every w' adjacent to w we have $f(v', w') = v'$ for every $v' \in V(H)$, and so, since H is connected, f is a projection. Thus, let us assume that this is not the case. For every $v \in V(H)$, let $A(v)$ denote the largest set such that $|f(v, A(v))| = 1$ (if there are several such sets we take as $A(v)$ the lexicographically first one, to make $A(v)$ well defined). Furthermore, set

$$S = \{v \in V(H) : \; |A(v)| \ge \frac{400n}{d} \log d\}\,.$$

Since we have assumed that f is not an identity on any row of the set $V(H) \times V(H)$, from Lemma 4 it follows that the set $V(H) \setminus S$ is independent. Note also that because of $\mathcal{B}(i)$, if $v, v' \in S$ are two adjacent vertices of H, then also $f(v, A(v))$ is adjacent to $f(v', A(v'))$. Hence,

$$\tilde{f} : H[S] \to H : v \to f(v, A(v))$$

is a graph homomorphism. Since $\mathcal{B}(i)$ implies that $|S| \geq n - \frac{400n}{d} \log d$, one can argue as in the proof of Lemma 4 that $\tilde{f}$ is, in fact, an embedding (roughly speaking, $\mathcal{B}(v)$ implies that a lot of points of S must be mapped into themselves, which in turn, by $\mathcal{B}(iii)$ and $\mathcal{B}(iv)$, forces $\tilde{f}$ to be an embedding). Hence, for every $v \in S$, we have $f(v, A(v)) = v$.

Now suppose that $S \neq V(H)$ and let $w \notin S$. Since $V(H) \setminus S$ is independent and the minimum degree of H is at least two, there exist two vertices $v', v'' \in S$ which are adjacent to w.

From $\mathcal{B}(i)$ it follows that there exists a set W of at least $n - \frac{1600n}{d} \log d$ vertices such that each $w' \in W$ is adjacent to vertices from both $A(v')$ and $A(v'')$. Consequently, for $w' \in W'$ the vertex $f(w, w')$ is adjacent to both v' and v''. Since v' and v'' have at most $1.1d^2/n + \log^2 d$ common neighbours, $|f(w, W)| \leq 1.1d^2/n + \log^2 d$. But, as far as $d \leq n^{0.9}$, this implies that

$$|A(w)| \geq \frac{|W|}{1.1d^2/n + \log^2 d} > \frac{400n}{d} \log d,$$

and so $w \in S$. Consequently, $S = V(H)$.

In order to complete the proof we have to show that $A(v) = V(H)$ for every $v \in V(H)$. Thus, let us assume that this is not the case and let v_0 denote the vertex which minimizes $|A(v)|$ over all vertices with at least $0.1d$ neighbours. Set $\bar{A}(v_0) = n \setminus A(v_0)$, and $r = |\bar{A}(v_0)|$. We first show that $r = 0$. To this end we consider two following cases.

Case 1. $\bar{A}(v_0)$ *contains at least* $0.9r$ *vertices of degree at most* $0.1d$.

Take three neighbours v', v'', v''' of v_0 such that $|A(v')|$, $|A(v'')|$, $|A(v''')| \geq |A(v_0)|$ ($\mathcal{B}(iii)$ guarantees that it is possible). From our assumption and $\mathcal{B}(iii)$ it follows that there is a vertex $w \in \bar{A}(v_0)$ of degree at most $0.1d$ which has a neighbour in at least two of the sets $A(v')$, $A(v'')$ and $A(v''')$, say, $A(v')$, $A(v'')$ (in fact there must be at least $0.1r$ of such vertices w since otherwise two vertices of degree at most $0.1d$ would lie within distance three from each other). However, from $\mathcal{B}(iii)$ we infer that v' and v'' have only one common neighbour, which, of course, must be identical with v_0. Hence, $f(v_0, w) = v_0$ which contradicts the fact that $w \notin A(v_0)$.

Case 2. $\bar{A}(v_0)$ *contains fewer than* $0.9r$ *vertices of degree at most* $0.1d$.

Let W be the set of at most $\log^2 d$ neighbours of v_0 which determine the vertex v_0 uniquely (see $\mathcal{B}(vi)$). For each $v \in W$ let $C(v)$ be the set of all vertices of $\bar{A}(v_0)$ which are not connected to some vertex from

$A(v)$, i.e., $C(v)$ is the maximum set of vertices whose neighbourhoods contain no vertices from $A(v)$. From $\mathcal{B}(ii)$, $\mathcal{B}(iii)$, and the choice of v_0, it follows that for each $v \in W$ we have $|C(v)| \le \frac{200r}{d} \log^3 d$. Thus, $\sum_{v\in W} |C(v)| < r$, so there exists a vertex $w \notin A(v_0)$ which has neighbours in $A(w')$ for all $w' \in W$. Consequently, $f(v_0, w)$ is adjacent to all vertices $f(w', w') = w'$, $w' \in W$, and so we must have $f(v_0, w) = v_0$ contradicting the fact that $w \notin A(v_0)$. This completes the proof of the case.

Thus, we have shown that for all $v \in V(H)$ with degree at least $0.1d$ we have $f(v, v') = v$ for every v'. Now the assertion follows easily from the fact that the vertices of degree at most $0.1d$ induce in H an independent set ($\mathcal{B}(iv)$), and that, by $\mathcal{B}(iii)$, each such vertex of small degree is uniquely determined by its neighbourhood. □

Now we consider 'dense' random graphs $\mathbb{G}(n, M)$. Our aim is to show the following result.

Lemma 6. *Let H be a graph on n vertices such that either H has property $\mathcal{B}(n, d)$ for some $n^{0.9} \le d \le n/2$ or its complement H^c has property $\mathcal{B}(n, d)$ for some $10^{10} \le d \le n/2$. Furthermore, let $g : H \times H \to H$ be a graph homomorphism such that $f(v, v) = v$ for every $v \in V(H)$. Then f is a projection.*

The proof of Lemma 6 is an extension of the argument we used in [7]. We start with the following two claims. In each of them we assume that for H and f the assumptions of Lemma 6 hold.

Claim 1. *If $f(v, w) = u$ for some $v, w, u \in V(H)$, then either $v = u$, or $w = u$.*

Proof. Let us note first that if there exists a vertex s of H such that s is adjacent to both v and w and is not adjacent to u we are done. Indeed, then vertices (v, w) and (s, s) are adjacent in $H \times H$ but $u = f(v, w)$ is not adjacent to $s = f(s, s)$, contradicting the fact that f is a homomorphism. If both H and H^c are dense enough, then the existence of such s follows from $\mathcal{B}(viii)$. Furthermore, if H^c has the property $\mathcal{B}(n, d)$ for some $10^{10} \le d \le n/2$, then $\mathcal{B}(vii)$ implies that such a vertex s exists provided u has degree at least three in H^c. Thus, it remains to consider the case in which H^c has property $\mathcal{B}$ and u has degree two in H^c.

Observe that at least one of vertices v, w, say v, must be adjacent to u in H^c. Indeed, otherwise (v, w) is adjacent to (u, u) in $H \times H$ but $u = f(v, w)$ is not adjacent to $u = f(u, u)$ in H since H contains no loops. The vertex u has degree two in H^c, so, besides v, it has exactly one more neighbour t in H^c.

Let us consider first the case in which $t = w$, i.e., the vertices v and w are the only neighbours of u in H^c. By $\mathcal{B}(iii)$, v and w are not adjacent in H^c, and so they are adjacent in H; consequently (v, w) is adjacent to (w, v) in $H \times H$. But $u = f(v, w)$ is not adjacent in H to any of the vertices v, w, u; consequently, $u' = f(w, v) \neq v, w, u$. Arguing as above we infer that $u' \neq u$ is a vertex of degree two in H^c which is adjacent in H^c to one of vertices v or w, contradicting the fact that from $\mathcal{B}(iii)$ it follows that no two vertices of small degree in H^c lie within distance three from each other. Consequently, $t \neq w$.

Now, since by $\mathcal{B}(iii)$ t is not adjacent to v, either we can take $s = t$, or w is adjacent to t. But in the latter case (t, u) is adjacent to (v, w) in $H \times H$, and so $f(t, u) \neq t, u$. Hence, arguing as before, we infer that either u or t must be a neighbour of a vertex of degree two in H^c which contradicts $\mathcal{B}(iii)$. □

Claim 2. *Let $f(v, w) = v$ and $f(r, s) = s$ for some $v \neq w, r, s$ and $s \neq w, r$. Then at least one of vertices of v and s are of degree at most three in H^c and at least two out of three remaining vertices from the set $\{v, w, r, s\}$ lie within the distance two from this vertex in H^c.*

Proof. Observe first that if there exist vertices $\bar{v} \neq r, s$ and $\bar{s} \neq v, w$, such that $\bar{v}$ is adjacent in H to r, s and w, but not to v, while $\bar{s}$ is adjacent to v, w and r, but not to s, then we cannot have $f(v, w) = v$ and $f(r, s) = s$. Indeed, then $(\bar{s}, \bar{v})$ is adjacent in $H \times H$ to both (v, w) and (r, s), so $f(\bar{s}, \bar{v})$ must be adjacent in H to both v and s. However, neither $\bar{v}$ nor $\bar{s}$ have this property, which contradicts Claim 1. Consequently, in order to prove the claim we need to show that for every quadruple (v, w, r, s) of vertices H such a pair $(\bar{v}, \bar{s})$ exists, unless at least one of vertices of v and s are of degree at most three in H^c and at least two of out of three remaining vertices from the set $\{v, w, r, s\}$ are either adjacent to this vertex or lie at the distance two from it in H^c.

Let us consider the existence of $\bar{v}$ ($\bar{s}$ can be treated by a symmetric argument). The property $\mathcal{B}(viii)$ takes care of the case when both H and H^c are dense enough, so we may assume that H^c has property $\mathcal{B}(n, d)$ for some $d \leq n^{0.9}$. Suppose that v has at least $0.1d$ neighbours in H^c. By $\mathcal{B}(iv)$, at most

$$3(1.1d^2/n + \log^2 d + 1) < d$$

of them are either equal to one of the vertices w, r, s, or are adjacent to them in H^c. Thus, there exists $\bar{v} \neq w, r, s$, which is adjacent to w, r, s, but not to v, in H.

Now let us assume that the degree of v in H^c is smaller than $0.1d$. Note that v has at least two neighbours in H^c, and, since v belongs to no short cycles in H^c, each of vertices w, r, s can "spoil" at most one of them (e.g., if w is a neighbour of v in H^c it shares with v no other common neighbours; if w is not adjacent to v it has at least one common neighbour with v). Hence, we can always choose the vertex $\bar{v}$ unless the degree of v in H^c is two or three and each neighbour of v is either one of vertices w, s, r, or is adjacent to one of these vertices. □

Proof of Lemma 6. Let V' denote the set of vertices of degree at least $n-4$ in H (i.e., at most 3 in H^c). If the average degree of H is between $n^{0.9}$ and $n-n^{0.9}$ then, by $\mathcal{B}(iii)$, $V' = \emptyset$; if H^c has $\mathcal{B}(n,d)$ with $d < n^{0.9}$, then $\mathcal{B}(i)$ implies that $|V'| \le \frac{800n}{d} \log d < 0.01n$. Since Claim 1 implies that for every $v \in V(H)$ we have $|f^{-1}(v)| \le 2n-1$ and $|V'| \le 0.01n$, applying Claim 1 once again we infer that there exists $v_0 \in V(H) \setminus V'$ such that at least $n/3$ elements of $f^{-1}(v_0)$ is contained in one line. Thus, let $m = \lceil n/3 \rceil$ and assume that for some $v_0, v_1, \dots, v_m$, we have $f(v_0, v_i) = v_i$ for $i = 1, \dots, m$. Then, it is easy to see that Claim 2 implies that we must $f(v,w) = v$ for all $v \in V(H)$, $w \in V(H) \setminus V'$. Furthermore, let $s \in V'$. Choose $v, w \in V(H) \setminus V'$ which lie at distance at least three from s. Then, from Claim 2 it follows that for every $r \in V(H)$ we have $f(r,s) \ne s$; consequently, by Claim 1, for each such pair (r,s) we must have $f(r,s) = r$ and the assertion follows. □

Proof of Theorem 1. Observe first that any graph H with at least three vertices and the maximum degree at most one is not projective. For a graph containing an isolated vertex this fact follows easily from the definition. If $\{v, w\}$ is an isolated edge of H, then the edge $\{(v,w),(w,v)\}$ of $H \times H$ can be transformed into any other edge of the graph $H \times H$ which easily implies that H is not projective. Finally, if $\{v,w\}, \{w,u\}$ are edges of H and v has degree one, then one can modify a projection $f : H \times H \to H$ by setting $\tilde{f}(v,t) = f(u,t)$ (or, perhaps, $\tilde{f}(t,v) = f(t,u)$) for some vertices $t \in V(H)$. Consequently, a large graph with the minimum degree at most one is not projective and, consequently, in the random graph process $\mathcal{G}(n) = \{\mathbb{G}(n,M)\}_{M=0}^{\binom{n}{2}}$, the graph $\mathbb{G}(n,M)$ is not projective for $M < \tau_1$.

The fact that a.a.s. in the random graph process $\mathcal{G}(n)$ for all M, $\tau_1 \le M \le \tau_2$, $\mathbb{G}(n,M)$ is projective follows from Lemmas 2, 5, and 6.

Now consider any graph H on n vertices which contains a vertex v of degree $n-2$. Let w be a vertex of H which is not adjacent to v. Then one can modify a projection $f : H \times H \to H$ by putting $\tilde{f}(v,t) = f(w,t)$ (or, perhaps, $\tilde{f}(t,v) = f(t,w)$) for some vertices $t \in V(H)$. Hence, such a graph is clearly non-projective and since a.a.s. in the random graph process $\mathcal{G}(n)$, the graph $\mathbb{G}(n, M)$ contains a vertex of degree $n-2$ for each $\tau_2 < M < \binom{n}{2}$, for all such M's $\mathbb{G}(n, M)$ is not projective.

Finally, it is well known (see [8], or, for a somewhat simpler proof, [7]) that the graph $\mathbb{G}(n, \binom{n}{2}) = K_n$ is projective for all $n \geq 3$. □

It is not hard to show that a.a.s. the random graph process $\mathcal{G}(n) = \{\mathbb{G}(n, M)\}_{M=0}^{\binom{n}{2}}$ is such that $\mathbb{G}(n, M)$ is rigid whenever $\tau_1 \leq M \leq \tau_2$. (Note that Lemmas 2 and 4 imply this fact for $\tau_1 \leq M \leq n/2$, and show that for $n/2 \leq M \leq \tau_2$ a.a.s. $G(n, M)$ has no non-trival automorphisms; the fact that for $n/2 \leq M \leq \tau_2$ a.a.s. $G(n, M)$ is rigid can be proved in a similar way.) Hence, as an immediate consequence of Theorem 1, we get the following result.

Corollary 7. *A.a.s. the random graph process $\mathcal{G}(n) = \{\mathbb{G}(n, M)\}_{M=0}^{\binom{n}{2}}$ is such that $\mathbb{G}(n, M)$ is strongly rigid if and only if $\tau_1 \leq M \leq \tau_2$.*

We also remark that the asymptotic distributions of random variables $\tau_1 = \tau_1(n)$ and $\tau_2 = \tau_2(n)$ are well known and easy to find. Elementary calculations of moments (see, for instance, [3] and [4]) show that for every function $c(n)$ which tends to a constant c as $n \to \infty$ we have

$$\lim_{n\to\infty} \operatorname{Prob}\Big\{\tau_1(n) \leq \frac{n}{2}(\log n + \log\log n + c(n)\Big\} = \exp\big(-e^{-c}\big),$$

and

$$\lim_{n\to\infty} \operatorname{Prob}\Big\{\tau_1(n) \leq \frac{n}{2}(n - \log n - \log\log n - c(n)\Big\} = \exp\big(-e^{-c}\big).$$

Thus, one can easily write down the asymptotic probability that for a given function $M = M(n)$ the random graph $\mathbb{G}(n, M)$ is projective (or strongly rigid). Analogous results for the binomial random graph $\mathbb{G}(n, p)$ follow from Theorem 1, the above two equations for the limit distribution for τ_1 and τ_2, and the equivalence of the models $\mathbb{G}(n, M)$ and $\mathbb{G}(n, p)$ (see, [4], Proposition 1.12). Here we state it for the property that $\mathbb{G}(n, p)$ is projective.

Corollary 8. $\lim_{n\to\infty} \text{Prob}\{\mathbb{G}(n,p) \text{ is projective}\}$

$$= \begin{cases} 0 & \text{if} \quad np - \log n - \log\log n \to -\infty \\ \exp\left(-e^{-a}\right) & \text{if} \quad np - \log n - \log\log n \to a \\ 1 & \text{if} \quad np - \log n - \log\log n \to \infty \\ & \quad\text{and } n(1-p) - \log n - \log\log n \to \infty \\ \exp\left(-e^{-b}\right) & \text{if} \quad n(1-p) - \log n - \log\log n \to b \\ 0 & \text{if} \quad n(1-p) - \log n - \log\log n \to -\infty \\ & \quad\text{and} \quad n^2(1-p) \to \infty \\ e^{-c/2} & \text{if} \quad n^2(1-p) \to c \\ 1 & \text{if} \quad n^2(1-p) \to 0. \end{cases}$$ □

References

[1] N. Alon, The Shannon capacity of a union, Combinatorica, **18** (1998) 301–310.

[2] N. Alon, I. Dinur, E. Friedgut, B. Sudakov, Graph products, Fourier Analysis and spectral techniques, preprint

[3] B. Bollobás, "Random Graphs", Cambridge University Press, Cambridge, 2001, xviii+498 pp.

[4] S.Janson, T. Łuczak, A.Ruciński, *"Random Graphs,"* Wiley, New York, 2000, vii+333 pp.

[5] B. Larose, C. Tardif: Strongly rigid graphs and projectivity, Multiple-Valued Logic **7** (2001), 339–361.

[6] B. Larose, C. Tardif: Projectivity and independent sets in powers of graphs, J. Graph Theory **40** (2002), no. 3, 162–171.

[7] T. Łuczak, J. Nešetřil: On projective graphs, J. Graph Th., to appear.

[8] V. Müller: On coloring of graphs without short cycles, Discrete Math. **26** (1979), 165–179.

[9] J. Nešetřil: Structural combinatorics (Graphs homomorphisms and their use), Taiwanese J. Math. **3** (1999), 381–423.

[10] I.G. Rosenberg: Strongly rigid relations, Rocky Mountain Journal of Math., **3** (1973), 631-639.

[11] A. Pultr, V. Trnková: Combinatorial, Algebraic and Topological Representations of Groups, Semigroups and Categories, North Holland, Amsterdam, 1980.

Adam Mickiewicz University, Faculty of Mathematics and Computer Science, 61-614 Poznań, Poland

E-mail address: <tomasz@amu.edu.pl>

Department of Applied Mathematics, Institute of Theoretical Computer sciences (ITI), Faculty of Mathematics and Physics, Charles University, Praha, Czech Republic

E-mail address: <nesetril@kam.ms.mff.cuni.cz>