k-connectivity of uniform s-intersection graphs

Mindaugas Bloznelis*, Katarzyna Rybarczyk*

*Faculty of Mathematics and Informatics, Vilnius University, 03225 Vilnius, Lithuania, E-MAIL: mindaugas.bloznelis@mif.vu.lt

*Faculty of Mathematics and Computer science, Adam Mickiewicz University, 60769 Poznań, Poland, E-MAIL: kryba@amu.edu.pl

Abstract

Let \( W_1, \ldots, W_n \) be independent random subsets of \([m] = \{1, \ldots, m\}\). Assuming that each \( W_i \) is uniformly distributed in the class of \( d \)-subsets of \([m]\) we study the uniform random intersection graph \( G_s(n, m, d) \) on the vertex set \( \{W_1, \ldots, W_n\} \), defined by the adjacency relation: \( W_i \sim W_j \) whenever \( |W_i \cap W_j| \geq s \). We show that as \( n, m \to \infty \) the edge density threshold for the property that each vertex of \( G_s(n, m, d) \) has at least \( k \) neighbours is asymptotically the same as that for \( G_s(n, m, d) \) being \( k \)-connected.

1 Introduction

Let \( H = H(n, m, d) \) be a random bipartite graph with bipartition \((V, W)\), where \(|V| = n, |W| = m\), and where each vertex from \( V \) chooses \( d \) neighbours in \( W \) uniformly at random and independently of the other vertices of \( V \). Given a natural number \( s, 1 \leq s < d \), the uniform random intersection graph \( G_s = G_s(n, m, d) \) is defined as the graph on the vertex set \( V \), where \( u, v \in V \) are adjacent (denoted by \( u \sim v \)) if they share at least \( s \) common neighbours in \( H \). We refer to the vertices of \( V \) as sensors, and the vertices of \( W \) we call keys. This random graph model has been widely studied in the literature mainly as a model of secure wireless sensor network that uses random predistribution of keys (see [1], [7], [10], [11], [12], [17]). Our study is motivated by fact that \( k \) connectivity of \( G_s \) is an important characteristics of the reliability of the sensor network as well as its resilience against attacks by an adversary controlling a certain number of sensors (see [6]).

Key words and phrases: random intersection graph, k-connectivity, wireless sensor network.
Mathematics Subject Classification 2010: primary 05C80, 05C40, secondary 05C07.
We study the threshold for the property \( \mathcal{C}_k \) that \( G_s \) is \( k \)-connected, i.e., that \( G_s \) is connected and that the removal of any set of at most \( k - 1 \) vertices does not disconnect the graph. Here \( k = 1, 2, \ldots \) is arbitrary, but fixed. For this purpose we consider a sequence of random graphs \( \{ G_s(n,m,d), n = 1, 2, \ldots \} \), where \( m = m(n) \rightarrow \infty \) as \( n \rightarrow \infty \), and the numbers \( s = s(n) \) and \( d = d(n) \) may depend on \( n \). In particular, they may tend to infinity as \( n \rightarrow \infty \), but at a slow rate, see (1) below. We assume that \( s(n) < d(n) \). By \( \delta(G) \) we denote the minimum degree of a graph \( G \). We denote by \( p = p(n,m,d,s) \) the edge-probability in \( G_s(n,m,d,s) \). We always assume that expressions \( o(\cdot), O(\cdot) \) refer to the case where \( n \rightarrow \infty \), and all inequalities are assumed to hold for \( n \) which is large enough.

A necessary condition for a graph to be \( k \)-connected is that it has no vertex of degree less than \( k \). Our first result shows that the thresholds for the properties \( \mathcal{C}_k \) and \( \delta(G_s(n,m,d)) \geq k \) coincide.

**Theorem 1.** Let \( k \geq 1 \) be an integer. Let \( \gamma \in (0,1) \). Let \( m, n \rightarrow +\infty \). Assume that

\[
( (s+2)(d^s)^5(\ln n)^2)^{(3d-s)/(3(d-s))} \leq (\ln n)^{1-\gamma} 
\]  

and for some \( \theta > 1 \) we have

\[
\ln n - \ln^{1/2} n \leq np \leq \theta \ln n. 
\]  

Then

\[
\left| \mathbf{P}(G_s(n,m,d) \in \mathcal{C}_k) - \mathbf{P}(\delta(G_s(n,m,d)) \geq k) \right| \leq n^{-\gamma + o(1)} \frac{d^s}{s(s+2)} \left( \frac{d}{s} \right)^{-4}. 
\]

Our next theorem gives the threshold for the property \( \delta(G_s(n,m,d)) \geq k \).

**Theorem 2.** Let \( k \geq 1 \) be an integer. Let \( m, n \rightarrow +\infty \). Assume that

\[
d^2 = o(m \ln^{-1} n), 
\]

\[
(s^{-1} - d^{-1}) \ln n - (s^{-1} + (k-1)d^{-1}) \ln \ln n \rightarrow +\infty. 
\]

Then for

\[
np = \ln n + (k-1) \ln \ln n + x_n \quad \text{with} \quad x_n = o(\ln n) 
\]

we have

\[
\lim_{n \rightarrow \infty} \mathbf{P}(\delta(G_s(n,m,d)) \geq k) = \begin{cases} 
0 & \text{if } x_n \rightarrow -\infty, \\
 e^{-\frac{x_n}{(k-1)}} & \text{if } x_n \rightarrow x, \\
1 & \text{if } x_n \rightarrow +\infty.
\end{cases} 
\]

Combining (3) and (7) we obtain the threshold for the property \( \mathcal{C}_k \).

**Theorem 3.** Let \( k \geq 1 \) be an integer. Let \( m, n \rightarrow +\infty \). Suppose that for some \( \gamma \in (0,1) \) condition (1) is satisfied. Assume that (4), (5) hold. Then for \( p \) satisfying (6) we have

\[
\lim_{n \rightarrow \infty} \mathbf{P}(G_s(n,m,d) \in \mathcal{C}_k) = \begin{cases} 
0 & \text{if } x_n \rightarrow -\infty, \\
 e^{-\frac{x_n}{(k-1)}} & \text{if } x_n \rightarrow x, \\
1 & \text{if } x_n \rightarrow +\infty.
\end{cases} 
\]

We remark that in the statements of Theorems 2 and 3 the edge-probability \( p \) can be replaced by the expression only involving \( d, s \) and \( m \)

\[
\hat{p} = \frac{(d^s)^2}{s!(m)_s},
\]
where \((a)_b = a(a-1)\cdots(a-b+1)\) for any positive integer \(b\). Indeed, as we shall see in Lemma 1 below, condition (4) implies that \(p = \hat{p}(1-o(ln^{-1} n))\). Therefore, for \(n\hat{p} = ln n + (k-1)ln ln n + x_n\), with \(x_n = O(ln n)\), we have \(np = n\hat{p} + o(1)\). In particular, Theorems 2 and 3 remain true with \(p\) replaced by \(\hat{p}\).

In the following corollary of Theorem 2 conditions (4) and (5) are replaced by a simpler, but more stringent condition \(d = o(ln^{1/2} n)\).

**Corollary 1.** Let \(k \geq 1\) be an integer. Let \(m, n \to +\infty\). Assume that \(d = o(ln^{1/2} n)\). Suppose that \(n\hat{p} = ln n + (k-1)ln ln n + x_n\), with \(x_n = o(ln n)\). Then (7) holds.

In the particular case where \(s \equiv 1\) is constant we have the following result.

**Corollary 2.** Let \(k \geq 1\) be an integer. Let \(0 < \alpha < 0.2\). Let \(m, n \to +\infty\). Assume that \(s \equiv 1\) and \(d = O(ln^n n)\). Suppose that \(n\hat{p} = ln n + (k-1)ln ln n + x_n\). Then (8) holds.

We note that the condition \(x_n = o(ln n)\) does not appear in Corollary 2.

Theorem 3 and Corollary 2 say that the edge density threshold for the property that \(G_s(n,m,d)\) is \(k\)-connected is the same as that of the binomial random graph \(G(n,p)\), where edges are inserted independently, see [5], [9], [13].

Our results are obtained under the assumption that \(s < d\). In the case where \(s = d\) the random graph \(G_s(n,m,d)\) is a union of disjoint cliques. It is connected (also \(k\)-connected) whenever all sensors have chosen the same collection of keys. This happens with probability \(\binom{m}{d}^{(n-1)}\), which does not depend on \(k\).

**Related work.** For \(k = 1\) the edge density threshold for the property \(\delta(G_s(n,m,d)) \geq 1\) has been shown in [12]. For \(s \equiv 1\) the connectivity and \(k\)-connectivity of \(G_1(n,m,d)\) has been studied in [1], [7], [17], [20], [21]. For \(s > 1\) the connectivity threshold of \(G_s(n,m,d)\) has been shown in [3].

Our proof of Theorem 1 differs from those of [1], [7], [17], [20], [21]. It relies on an expansion property of \(G_s(n,m,d)\) established in [3].

## 2 Proofs

Before the proof we introduce some notation and formulate an auxiliary lemma. For a set \(\Omega\) and a natural number \(t\), we denote by \(\binom{\Omega}{t}\) the collection of \(t\)-element subsets of \(\Omega\). The set of keys adjacent to a sensor \(v \in V\) in \(H\) is denoted \(W_v\). We say that a sensor \(v\) covers a set of keys \(B\) if \(B \subset W_v\). Subsets of \(W\) of size \(s\) are called joints.

**Lemma 1.** *(see, e.g., Lemma 6 of [4])* Given integers \(1 \leq s \leq d \leq m\), let \(W_1, W_2\) be independent random subsets of the set \(W = \{1, \ldots, m\}\) such that \(W_1\) and \(W_2\) are uniformly distributed in the class of subsets of \(W\) of size \(d\). Then

\[
\left(1 - \frac{(d-s)^2}{m+1-d}\right) \hat{p} \leq P(|W_1 \cap W_2| = s) \leq P(|W_1 \cap W_2| \geq s) \leq \hat{p}.
\]

**Proof of Theorem 3.** The result follows by Theorem 1 and Theorem 2. The fact that (1) indeed implies that the quantity in the right-hand side of (3) tends to 0 is shown in [3] (see the proof of Theorem 1 in [3]).

**Proof of Corollary 1.** We shall show that conditions (4), (5), (6) of Theorem 2 are satisfied. The bound \(n\hat{p} = O(ln n)\) implies that \(\hat{p}^{-1} \geq cn ln^{-1} n\), for some constant \(c > 0\). Furthermore, the inequality \((d)_s > s!\) implies \((m)_s > \hat{p}^{-1}\). Hence, we have \(m^s \geq cn ln^{-1} n\). The later inequality implies (4), since \(m \geq e^{s^{-1}(1+o(1))} ln n \geq e^{ln^{1/2} n} > d^2 ln^2 n\), for \(s < d = o(ln^{1/2} n)\).
Let us show (5). For $s \leq 2^{-1}d$ we have $s^{-1} - d^{-1} \geq 2^{-1}s^{-1}$. The quantity on the left side of (5) is bounded from below by
\[ 2^{-1}s^{-1}\ln n - (k+1)s^{-1}\ln \ln n. \]
Hence, it tends to $+\infty$, since $s < d = o(\ln^{1/2} n)$. For $s > 2^{-1}d$ we write $s^{-1} - d^{-1} \geq (d-1)^{-1} - d^{-1} > d^{-2}$. Now the quantity on the left side of (5) is bounded from below by
\[ d^{-2}\ln n - (k+1)d^{-1}\ln \ln n. \]
It tends to $+\infty$, since $d = o(\ln^{1/2} n)$.

Finally, (4) and Lemma 1 imply $p = \hat{p}(1 - \mathcal{O}(d^2/m)) = \hat{p} - o(n^{-1})$. Hence, the relation $n\hat{p} = \ln n + (k-1)\ln \ln n + x_n$, with $x_n = o(\ln n)$, implies (6). \hfill \Box

Proof of Corollary 2. First we consider the case where $x_n = o(\ln n)$. In this case we have $n\hat{p} = \mathcal{O}(\ln n)$ and we derive (4), (5), (6) from the bound $d = o(\ln^\alpha n)$ as in the proof of Corollary 1 above. The bound $d = o(\ln^\alpha n)$ also implies (1). Hence, conditions of Theorem 3 are satisfied and we obtain (8). Using a coupling argument we extend the result to the case where the condition $x_n = o(\ln n)$ is violated. We note that except for some particular cases, we do not know how to construct a proper coupling of random intersection graphs. One exception is the case $s = 1$, where such a coupling is available. In [1] (see also the proof of Corollary 1 in [3]) it is shown that if $m'' = hm'$ for some integer $h$ then there is a common probability space on which $G_1(n,m',d) \subseteq G_1(n,m'',d)$ with probability 1. In particular, we have $P(G_1(n,m',d) \in \mathcal{C}_k) \leq P(G_1(n,m'',d) \in \mathcal{C}_k)$. If, in addition, $m'$ and $m''$ are such that the first probability tends to 1 (the second probability tends to 0), then the second probability tends to 1 (the first probability tends to 0) as well. Therefore it is enough to set $m'' = m (m' = m)$ and $m' (m'')$ such that the edge probability in $G_1(n,m',d) (G_1(n,m'',d))$ follows (6) with $x_n \to \infty (x_n \to -\infty)$. \hfill \Box

Proof of Theorem 1. We use the same notation as in [3]. Consider an $H(n,m,d)$ such that (1) and (2) hold. The set of keys adjacent to a sensor $v \in V$ in $H$ is denoted by $W_v$. Given $s$, let $H_s = H_s(n,m,d)$ be a bipartite graph with bipartition $(V, (W_v)^s)$, where $v \in V$ and $B \in (W_v)^s$ are adjacent whenever $v$ covers $B$. Hence, $H(n,m,d)$ defines $H_s(n,m,d)$ and $H_s(n,m,d)$ defines $G_s = G_s(n,m,d)$. We note that every sensor covers $\binom{d}{s}$ joints and the probability that a given sensor covers a joint chosen uniformly at random is $\binom{d}{s}/(m)^{s-1}$. We denote $r = \binom{d}{s}$ and $p_s = r^{-1}/(m)^{s-1}$. A joint $B \in (W_v)^s$ is called \textit{thin} if the number $\sum_{v \in V} |B \subseteq W_v|$ of sensors that cover $B$ is less than $\tilde{k} = r^{-2}(\ln \ln n)^{-1}\ln n$; otherwise, $B$ is \textit{fat}. A sensor $v \in V$ is \textit{tiny} if every $B \in (W_v)^s$ is thin and it is \textit{heavy} if every $B \in (W_v)^s$ is fat. Otherwise, $v$ is \textit{small}. A subset $S \subseteq V$ is heavy if all its members are heavy. We remark that our choice of $\tilde{k}$ ensures that any set of heavy sensors has a large neighbourhood in $G_s$, see the property $A_5$ below.

We fix $k$ and consider the following properties of a graph $H_s$ (cf. [3]).

$A_2$: no two tiny sensors are within distance 8 from each other (8 hops in graph $H_s$);

$A_3$: every fat joint is covered by at most $(s+1)r$ small sensors;

$A_4$: there are fewer than $(2p_s)^{-1} - (k-1)$ small sensors;

$A_5$: for any heavy set of sensors $S \subseteq V$ of size $|S| \leq 2n/3$ we have
\[ |N(S)| \geq \min\{((s+1)r^2 + r + 1)|S|, 2p_s^{-1}\}. \]

Here $N(S) = \{u \in V \setminus S : u \sim v \text{ for some } v \in S\}$ denotes the neighbourhood of $S$ in $G_s$. 4
Let $\mathcal{A}$ denote the event that the random graph $H_s$ satisfies all the properties $\mathcal{A}_2$, $\mathcal{A}_3$, $\mathcal{A}_4$, $\mathcal{A}_5$. In [3] it was shown that $P(\mathcal{A}) = 1 - o(1)$. More precisely, we have, see Lemmas 4 and 5 in [3],

$$1 - P(\mathcal{A}_i) \leq (1 + o(1)) n^{-\gamma \frac{d_n}{(d_n+2r)^2}} + n^{-r/(0.4+o(1))}, \quad i = 2, 3, 4, 5. \tag{9}$$

We remark that although our definition of the property $\mathcal{A}_4$ differs from that of [3], where only the case $k = 1$ is considered, the argument of the proof of the upper bound for $1 - P(\mathcal{A}_4)$ in Lemma 4 in [3] applies to an arbitrary, but fixed $k$. Hence (9) holds.

Now we derive (3). For this purpose we show that the event $\mathcal{A} \cap \{\delta(G_s) \geq k\}$ implies

$$\forall S \subset V \quad 1 \leq |S| \leq (n + 1)/2 \quad \text{we have} \quad N(S) \geq k. \tag{10}$$

(10) implies the $k$-connectivity property of $G_s$. In order to show that $\mathcal{A} \cap \{\delta(G_s) \geq k\}$ implies (10) we partition $V = V_T \cup V_S \cup V_H$, where $V_T$, $V_S$ and $V_H$ denote the sets of tiny, small and heavy sensors respectively. For $S \subset V_T$ (10) follows from $\delta(G_s) \geq k$ and the property $\mathcal{A}_2$. For $S \subset V_T \cup V_S$ with $S \cap V_S \neq \emptyset$ we find a fat joint covered by a small sensor, say $v'$, from $S$. By $\mathcal{A}_3$, this fat joint is covered by at least $k - (s + 1)r > k$ heavy sensors which are neighbours of $v'$ from outside $S$. Here, the latter inequality follows from (1). Now consider a set $S$ such that $S_H := S \cap V_H$ is nonempty. In the case where $s_H := |S_H|$ is less than $k$, we fix a fat joint of a heavy vertex $v'' \in S_H$ and (in view of $\mathcal{A}_3$) we find at least $k - (s + 1)r$ heavy sensors that cover this joint.

Among these heavy sensors at least $k - (s + 1)r - s_H \geq k - (s + 1)r - k > s_H$ are from outside $S$, where the latter inequality follows from (1). Hence $N(S) \geq k$. Now assume that $s_H \geq k$. Heavy vertices of $S_H$ all together contain at most $s_H r \times (s + 1) r$ small sensors, by property $\mathcal{A}_3$. In the case where $((s + 1) r^2 + r + 1)|S_H| < 2p_s^{-1}$, the property $\mathcal{A}_5$ yields that the set $N(S_H)$ has at least $((s + 1) r^2 + r + 1)s_H$ sensors and we know that there are at most $(s + 1) r^2 s_H$ small sensors among them. Hence $N(S_H)$ contains at least $(r + 1)s_H \geq (r + 1)k > k$ heavy sensors and, obviously, these are from outside of $S$. Finally, in the case where $((s + 1) r^2 + r + 1)s_H \geq 2p_s^{-1}$, the inequality $|N(S_H)| \geq 2p_s^{-1}$ implies that $N(S_H)$ contains at least $k$ heavy sensors, because by $\mathcal{A}_4$ the total number of small sensors the graph $G_s$ is less than $2p_s^{-1} - k$.

\[ \square \]

**Proof of Theorem 2.** Denote $\lambda_n = e^{-x_n}/(k-1)!$ and $\lambda = e^{-x}/(k-1)!$. Let $X_n$ denote the number of vertices of $G_s(n, m, d)$ of degree at most $k$. In view of the identity $P(\delta(G_s(n, m, d)) \geq k) = P(X_n = 0)$ it suffices to show (7) with $P(\delta(G_s(n, m, d)) \geq k)$ replaced by $P(X_n = 0)$. For this purpose we prove that, for $t = 1, 2, \ldots$,

$$\lim_{n \to +\infty} \lambda_n^t E(X_n)_t = 1. \tag{11}$$

Let us show that (11) implies (7). For $x_n \to +\infty$, (11) implies $E X_n = o(1)$ and we obtain

$$1 - P(X_n = 0) = P(X_n \geq 1) \leq E X_n = o(1),$$

by Markov’s inequality. For $x_n \to -\infty$, (11) implies $(E X_n)^2 / E X_n^2 = 1 - o(1)$ and we obtain $1 - P(X_n = 0) = P(X_n \geq 1) = 1 - o(1)$ using the Paley-Zygmund inequality $P(X_n \geq 1) \geq (E X_n^2) / E X_n^2$. Finally, for $x_n \to x$, (11) implies $E(X_n)_t = t^x (1 + o(1))$, for every $t = 1, 2, \ldots$. By the method of moments, we obtain that $X_n$ converges in distribution to the Poisson distribution with mean $\lambda$. Hence, $P(X_n = 0) = e^{-\lambda}$.

Let us prove (11). Given $t$, the number $(\binom{V}{t})$ counts $t$-subsets of the set of vertices having degrees at most $k - 1$, thus $(X_n)_t = t! \sum_{V' \subset V, |V'| = t} \mathbb{I}_{\mathcal{B}_V'}$, where $\mathbb{I}_{\mathcal{B}_V'}$ is the indicator of the event $\mathcal{B}_V := \{\text{all vertices from } V' \text{ have degrees at most } k - 1\}$. It follows now, by symmetry, that

$$E(X_n)_t = t! \binom{n}{t} P(\mathcal{B}), \quad \text{where } \mathcal{B} := \mathcal{B}_{V^*}, \quad V^* := \{v_1, \ldots, v_t\}$$

5
Thus in order to prove (11) we are left with proving
\[ P(B) = (1 + o(1)) \left( \frac{\lambda n}{n} \right)^t. \] (12)

In the proof of (12) we approximate \( P(B) \) by the probability that \( W_{v_1}, \ldots, W_{v_t} \) are disjoint, all vertices from \( V^* \) are of degree exactly \( k - 1 \) and their neighbourhoods are disjoint. Therefore we consider the following events.

\( C_0 \): each vertex from \( V^* \) has degree \( k - 1 \), \( W_{v_1}, \ldots, W_{v_t} \) are disjoint and every \( v \in V \setminus V^* \) has at most one neighbour in \( V^* \) and if such a neighbour exists, it shares with \( v \) exactly \( s \) keys, while any other member of \( V^* \) has no common keys with \( v \);  

\( C_1 \): the set of vertices from \( V \setminus V^* \), having at least one neighbour in \( V^* \), can be divided into disjoint subsets \( V_1, \ldots, V_t \subseteq V \setminus V^* \) such that for every \( i = 1, \ldots, t \) we have \( |V_i| \leq k - 1 \) and all members of \( V_i \) are neighbours of \( v_i \) (we note that any vertex from \( V_i \) is allowed to be a neighbour of \( v_j \in V^* \) for \( j \neq i \)).

We have \( C_0 \subset B \subset C_1 \), i.e., event \( C_0 \) implies event \( B \), and event \( B \) implies event \( C_1 \). Hence,
\[ P(C_0) \leq P(B) \leq P(C_1). \] (13)

Thus in order to prove (12) it is enough to show that
\[ P(C_0) = (1 + o(1)) \left( \frac{\lambda n}{n} \right)^t, \quad P(C_1) \leq (1 + o(1)) \left( \frac{\lambda n}{n} \right)^t. \] (14)

The proof of (14) is technical. In order to avoid cumbersome formulae we introduce the notation
\[ T = \frac{(n\hat{\rho})^t(k-1)!}{((k-1)!)^t} e^{-tn\hat{\rho}}, \quad \tau = \frac{d^2}{m}. \]

We observe, that \( \hat{\rho} \leq \tau^s/s! \leq \tau^s \). Let us show that \( p = \hat{\rho} - o(n^{-1}) \). We note that (4) implies \( 1 > \frac{d^2}{m} \). Hence, \( \frac{d^2}{m} > \frac{d^2-d+1}{m-d+1} \). Next, the inequalities \( d^2 - d + 1 > (d-1)^2 \geq (d-s)^2 \) imply \( d^2 > \frac{(d-s)^2}{m-d+1} \). Combining this inequality with the inequalities \( \hat{\rho} \geq p \geq \hat{\rho}(1 - \frac{(d-s)^2}{m-d+1}) \) (see Lemma 1) we obtain \( \hat{\rho} \geq p \geq \hat{\rho}(1 - \frac{d^2}{m}) \). Hence, \( p = \hat{\rho}(1 - O(\tau)) \). Now, the bound \( \tau = o(\ln n) \), see (4), implies \( \hat{\rho} = O(p) \), and the bound \( p = O(n^{-1} \ln n) \), see (6), implies the desired bound \( p = \hat{\rho} - O(\hat{\rho}r) = \hat{\rho} - O(pr) = \hat{\rho} - o(n^{-1}) \). In particular, we have \( n\hat{\rho} = \ln n + (k-1) \ln \ln n + x_n + o(1) \). The latter relation implies
\[ T = \left( \frac{\lambda n}{n} \right)^t (1 + o(1)). \] (15)

Evaluation of \( P(C_0) \). We have
\[ P(C_0) = \frac{N_1}{N_2} N_3 p_1^{(k-1)t} (1 - p_2)^{n-t-(k-1)t}, \] (16)
where \( N_2 = \frac{m}{d} \) counts all possible collections \( W_{v_1}, \ldots, W_{v_t} \) of the sets of keys that can be assigned to \( v_1, \ldots, v_t \), while \( N_1 = \frac{m}{d} \) counts the collections of non-intersecting sets. Furthermore, \( N_3 = \frac{(n-t)!}{((k-1)!)^t (n-t-(k-1)t)!} \) counts the number of ways to assigning neighbourhoods (each of size \( k - 1 \)) to the vertices \( v_1, \ldots, v_t \), and \( p_1 = \frac{\binom{d}{k-1} \binom{m-td}{d-s}}{\binom{m}{d}} \) is the conditional probability that, given non intersecting sets \( W_{v_1}, \ldots W_{v_t} \), the vertex \( v \in V \setminus V^* \) and the vertex \( v_t \in V^* \) share exactly \( s \) keys, while any other member of \( V^* \) has no common keys with \( v \). Finally, \( p_2 \) denotes
Now we estimate the value of \(1 - \) which is adjacent to some vertex \(v \) from \(V^*\).

Let us we evaluate (16). A direct calculation shows that

\[
\frac{N_1}{N_2} N_3 p_1^{(k-1)t} = \frac{(m)_{td} (n - t)_{(k-1)t}}{(m)_{td}^t ((k-1)!)^t} \left( \frac{(d)_{s}^2 (m - td)_{d-s}}{(m)_{d}} \right)^{(k-1)t}
\]

\[
e^{-\mathcal{O}(\tau)} \frac{n(n-1)}{((k-1)!)^t} \frac{(d)_{2}^2 (m - td)_{d-s}}{s! m_d} e^{\mathcal{O}(\tau)} (1 + o(1))
\]

(17)

In the last step we used the fact that \(d^2 = o(m)\) implies \(\tau = o(1)\) and \(e^{\mathcal{O}(\tau)} = 1 + o(1))\).

Now we estimate the value of \((1 - p_2)^{n-t-(k-1)t}\). Let \(u \in V \setminus V^*\) be fixed and \(W_{v_1} \cap W_{v_2} = \emptyset\).

By inclusion-exclusion,

\[
t \mathbb{P}(u \sim v_1 | W_{v_1}) - \left(\frac{3}{2}\right) \mathbb{P}(u \sim v_1, u \sim v_2 | W_{v_1}, W_{v_2}) \leq p_2 \leq t \mathbb{P}(u \sim v_1 | W_{v_1}).
\]

Note that

\[
\mathbb{P}(u \sim v_1, u \sim v_2 | W_{v_1}, W_{v_2}) \leq \frac{(d)_{s}^2 (m - 2s)}{(m)_{d}}
\]

and so \(\mathbb{P}(u \sim v_1, u \sim v_2 | W_{v_1}, W_{v_2}) \leq \hat{p}^2\). Here \(\binom{3}{2}^2\) counts pairs \((B_1, B_2)\) of joints \(B_1 \in W_{v_1}, B_2 \in W_{v_2}\) and \(\binom{m-2s}{d-2s} \binom{m}{d}^{-1}\) is the probability that \(W_u\) covers a given pair \((B_1, B_2)\) of disjoint joints. On the other hand

\[
\mathbb{P}(u \sim v_1 | W_{v_1}) = p = \hat{p}(1 + \mathcal{O}(\tau))
\]

implies \(p_2 = t \hat{p}(1 + O(\tau + \hat{p})) = t \hat{p}(1 + O(\tau))\). Therefore we have

\[
(1 - p_2)^{n-t-(k-1)t} = \exp\{n - t - (k - 1)t \ln(1 - p_2)\} = \exp\{-tn\hat{p}\}(1 + o(1)).
\]

(18)

In the second identity of (18) we expanded the logarithm in powers of \(p_2\) and used \(np_2^2 = \mathcal{O}(np^2) = \mathcal{O}(\hat{p} \ln n)\) and \(\hat{p} \ln n \leq \tau \ln n = o(1)\), see (4). Finally, we substitute (17) and (18) to (16). Then, by (15), we get the first relation of (14).

**Upper bound for \(\mathbb{P}(C_1)\).** We first collect some auxiliary results. We define random variables

\[
Z_1 = |W_{v_1} \cap W_{v_2}|, \quad Z_2 = |W_{v_1} \cup W_{v_2} \cap W_{v_3}|, \ldots, \quad Z_{t-1} = |W_{v_1} \cup \cdots \cup W_{v_{t-1}} \cap W_{v_t}|
\]

and the random vector \(\bar{Z} = (Z_1, \ldots, Z_{t-1})\). We note that \(d \leq |W_{v_1} \cup \cdots \cup W_{v_t}| \leq td\), for \(i \leq t\).

Thus for \(i < t\) and for any integer \(0 \leq z \leq d\) we have

\[
\mathbb{P}(Z_i = z | W_{v_1}, \ldots, W_{v_t}) \leq \frac{(td)^z (m - d)_{d-z}}{z! (m)_{d} (d)_{z}} \frac{(m-z)_{d-z}}{z!} e^{\mathcal{O}(\tau)}
\]

(19)

Now we evaluate \((m-d)_{d-z}/(m)_{d} = m^{-z} e^{\mathcal{O}(\tau)}\) and bound, for \(s \leq z \leq d\),

\[
\frac{(td)^z}{z!} (d)_{z} \leq \frac{t^z d^z}{z!} (d)_{z} \leq e(\epsilon t)^z \frac{(d)_{s}^2}{s!} \frac{z/s}{e(\epsilon t)^z (d)_{z}}
\]

(20)

In the last step we used the inequality \(d^z \leq e^{z+1}(d)_{z}\), which follows by Stirling’s approximation, and the simple inequalities \((d)_{z}^s \leq (d)_{s}z^s\) and \((s!) \leq (z!)^s\). From (19) and (20) we obtain

\[
\mathbb{P}(Z_i = z | W_{v_1}, \ldots, W_{v_t}) \leq e(\epsilon t)^z \left( \frac{(d)_{s}^2}{s! m_d^s} \right) e^{\mathcal{O}(\tau)} = e(\epsilon t)^z (\hat{p})^{z/s}(e + o(1))
\]

(21)
uniformly in \(1 \leq i \leq t-1\), \(W_{v_1}, \ldots, W_{v_t}\) and \(s \leq z \leq d\). Given an arbitrary vector \(\vec{z} = (z_1, \ldots, z_{t-1})\) with coordinates from \(\{0, 1, \ldots, d\}\), let \(\vec{z}_s = (\mathbb{I}_{\{z_1 \geq s\}} z_1, \ldots, \mathbb{I}_{\{z_{t-1} \geq s\}} z_{t-1})\). The set of indices of non-zero coordinates of \(\vec{z}_s\) is denoted \(J_s = \{i_1, i_2, \ldots, i_r\}\). Here we assume that \(i_1 < \cdots < i_r\). For any given \(\vec{z}_s\), we have
\[
P(\vec{Z}_s = \vec{z}_s) \leq \prod_{j=1}^{r} P(Z_{i_j} = z_{i_j} | Z_{ih} = z_{ih}, 1 \leq h < j) \leq \prod_{i \in J_s} \left((\epsilon t)^{z_i} (\hat{p})^{z_i/s} (e + o(1))\right). \tag{22}\]
In the second inequality we used the fact that upper bound (21) obviously extends to conditional probabilities \(P(Z_{i_j} = z_i | Z_{ih} = z_{ih}, 1 \leq h < j)\). Denote \(S(\vec{z}) := \sum_{i \in J_s} z_i\). From (22) we obtain
\[
P(\vec{Z} = \vec{z}_s) \leq \exp\{S(\vec{z}) (s^{-1} \ln \hat{p} + \ln t + 2)\}(1 + o(1)). \tag{23}\]
We call a joint \(B\) occupied, if it is covered by some \(W_{v_i}\), for \(1 \leq i \leq t\). We observe that if the event \(\{\vec{Z} = \vec{z}\}\) holds then the number of occupied joints is at least \(N_\vec{z} = t(\frac{d}{s}) - \sum_{j=1}^{t-1} (\frac{z_j}{s})\). In particular, we have \(N_\vec{z} = t(\frac{d}{s})\) in the case where \(J_s = \emptyset\). For \(J_s \neq \emptyset\) we have
\[
N_\vec{z} = \left(t - \sum_{i \in J_s} \frac{(z_i)_s}{(d)_s}\right) \frac{d}{s} \geq \left(t - d^{-1} S(\vec{z})\right) \frac{d}{s}. \tag{24}\]
Now fix \(u \in V \setminus V^*\) and, assuming that the realized sets \(W_{v_1}, \ldots, W_{v_t}\) satisfy the condition \(\vec{Z} = \vec{z}\), consider the conditional probability (denoted \(p_\vec{z}\)) of the event that \(u\) is adjacent to some \(v_j \in V^*\), given \(W_{v_1}, \ldots, W_{v_t}\). Observing that \(p_\vec{z}\) is the probability that a random subset of \(W\) of size \(d\) covers an occupied joint we obtain
\[
p_\vec{z} \geq N_\vec{z} \left(\frac{m - td}{d - s} \right)^{m-1} \geq \left(t - d^{-1} S(\vec{z})\right) \hat{p} e^{O(r)}. \tag{25}\]
In the second inequality of (25) we applied (24) and the relation \(\left(\frac{m}{d}\right)^{m-1} = \hat{p} e^{O(r)}\).
Now we are ready to show an upper bound for \(P(C_1)\). By the law of total probability,
\[
P(C_1) = \sum_{\vec{z}} P(C_1 | \vec{Z} = \vec{z}) P(\vec{Z} = \vec{z}) = I_1 + I_2, \tag{26}\]
where \(I_1 = \sum_{\vec{z}, J_s = \emptyset} P(C_1 | \vec{Z} = \vec{z}) P(\vec{Z} = \vec{z})\) and \(I_2 = \sum_{\vec{z}, J_s \neq \emptyset} P(C_1 | \vec{Z} = \vec{z}) P(\vec{Z} = \vec{z})\).
We first estimate the conditional probabilities \(P(C_1 | \vec{Z} = \vec{z})\). Recall that \(C_1\) occurs when the set of neighbours of \(V^* = \{v_1, \ldots, v_t\}\) can be divided into disjoint subsets \(V_{i_1}, \ldots, V_{i_t}\) such that \(|V_i| \leq k - 1\) and elements of \(V_i\) are neighbours of the \(i\)-th vertex of \(V^*\), \(1 \leq i \leq t\). Denote \(l_i = |V_i|, 1 \leq i \leq t, \text{and } l := l_1 + \cdots + l_t\).
For any \(\vec{z}\) we have, by the union bound,
\[
P(C_1 | \vec{Z} = \vec{z}) \leq \sum_{l = 0}^{t(k-1)} T_l(\vec{z}), \quad T_l(\vec{z}) := \sum_{l_1 + \cdots + l_t = l} \frac{(n-t)!}{l_1! \cdots l_t!} p_\vec{z}^{l_1} (1 - p_\vec{z})^{n-l-t}. \tag{27}\]
In the definition of \(T_l(\vec{z})\), \(\frac{(n-t)!}{l_1! \cdots l_t!}\) is the number of ways we may choose sets \(V_{i_1}, \ldots, V_{i_t}\), given their cardinalities. Moreover, given \(V_{i_1}, \ldots, V_{i_t}\) and \(v_j \in V^*\), and \(u \in V_{i_1} \cup \cdots \cup V_{i_t}\), the number \(\hat{p}\) is an upper bound for the probability that \(u\) covers a joint belonging to \(v_j\) (see Lemma 1), and \(1 - p_\vec{z}\) is an upper bound on the probability that given \(u' \in V \setminus (V^* \cup V_{i_1} \cup \cdots \cup V_{i_t})\) does not cover any joint of any vertex from \(V^*\).
Let us construct an upper bound for $I_1$. For this purpose we estimate every $T_l(\bar{z})$, with $J_1 = \emptyset$. The latter relation implies $S(\bar{z}) = 0$ and we have $p_\bar{z} \geq t \hat{\rho} e^{O(\tau)} = \hat{\rho} + o(n^{-1})$, see (25), (4), and $(1 - p_\bar{z})^{(k-1)} = 1 - o(1)$. We obtain

$$T_l(k-1)(\bar{z}) = \frac{(n - t)(k-1)}{(k-1)!} (\hat{\rho}^{(k-1)}(1 - p_\bar{z})^{n-kt} \leq (1 + o(1))T.$$ 

For $l = t(k - 1) - j$, where $j \geq 1$, we have for some constant $C_{l,k,j}$ depending only on $t, k, j$

$$T_l(\bar{z}) \leq C_{l,k,j} T(n\hat{\rho})^{-j}.$$ 

Combining this inequality and the relation $n\hat{\rho} = (1 + o(1)) \ln n$ we obtain from (27) that $P(C_1|\bar{Z} = \bar{z}) \leq T(1 + o(1))$. We note that the latter inequality holds uniformly in $\bar{z}$ satisfying $J_1 = \emptyset$. Hence, we have

$$I_1 \leq T(1 + o(1)). \tag{28}$$

Now we construct an upper bound for $I_1$. Given $\bar{z}$ with $J_1 = \{i_1, \ldots, i_r\} \neq \emptyset$ we estimate $T_l(\bar{z})$. From (25) combined with the relation $e^{O(\tau)} = 1 + O(\tau) = 1 + o(\ln^{-1} n)$ we obtain

$$(1 - p_\bar{z})^{n-1-t} \leq (1 - p_\bar{z})^{n-kt} \leq \exp\{- (n - kt)p_\bar{z}\} \leq \exp\{- n\hat{\rho}(t - d^{-1} S(\bar{z})) + o(1)\}.$$ 

The latter inequalities imply

$$T_l(k-1)(\bar{z}) \leq (1 + o(1))T e^{-n\hat{\rho}(t - d^{-1} S(\bar{z}))}, \tag{29}$$

and

$$T_l(\bar{z}) \leq C_{l,k,j} T(n\hat{\rho})^{-j} e^{-n\hat{\rho}(t - d^{-1} S(\bar{z}))}, \quad l = t(k - 1) - j, \quad j \geq 1. \tag{30}$$

Combining (27), (29), (30) we obtain the inequality

$$P(C_1|\bar{Z} = \bar{z}) \leq (1 + o(1)) T e^{-n\hat{\rho}(t - d^{-1} S(\bar{z}))}.$$ 

Observing that $S(\bar{z})$ in the right hand side depends only on $\bar{z}$, we conclude that

$$I_2 \leq (1 + o(1)) T \sum_{\bar{z} \neq \emptyset} e^{-n\hat{\rho}(t - d^{-1} S(\bar{z}))} P(\bar{Z}_s = \bar{z}_s). \tag{31}$$

Here the sum runs over all $\bar{z}_s$ that are not equal to $\emptyset = (0, \ldots, 0)$. Next, we invoke (23) to obtain

$$e^{-n\hat{\rho}(t - d^{-1} S(\bar{z}))} P(\bar{Z}_s = \bar{z}_s) \leq e^{S(\bar{z})\xi}, \quad \xi := d^{-1} n\hat{\rho} + s^{-1} \ln \hat{\rho} + \ln t + 2.$$ 

We remark that (5) implies $\xi \to -\infty$. Hence $\sum_{i \geq 1} e^{\xi i} = o(1)$. Now, given $\xi$ with $\sum_{i \geq 1} e^{\xi i} < 1$, define independent random variables $Y_1, \ldots, Y_{t-1}$ with the common distribution $P(Y_j = i) = e^{\xi i}$, $i = 1, 2, \ldots$, and $P(Y_j = 0) = 1 - \sum_{i \geq 1} e^{\xi i}$. The inequalities

$$\sum_{\bar{z}_s \neq 0} e^{S(\bar{z})\xi} \leq \max_{1 \leq j \leq t-1} P(Y_j \geq s) \leq (t - 1) P(Y_1 \geq 1)$$

imply

$$\sum_{\bar{z}_s \neq 0} e^{S(\bar{z})\xi} \leq (t - 1) \sum_{z \geq 1} e^{\xi z} = o(1).$$

We conclude that $I_2 = o(T)$. Combining this bound with (28) and (26) we obtain the second inequality of (14).

\[\square\]

**Acknowledgements.** Authors thank referees for their remarks. M. Bloznelis acknowledges support of Lithuanian Research Council grant MIP-067/2013. K. Rybarczyk is partially supported by the National Science Centre grant - DEC- 2011/01/B/ST1/03943.
References


