Erdős-Pyber theorem for hypergraphs and secret sharing

László Csirmaz · Péter Ligeti · Gábor Tardos

Abstract A new, constructive proof with a small explicit constant is given to the Erdős-Pyber theorem which says that the edges of a graph on n vertices can be partitioned into complete bipartite subgraphs so that every vertex is covered at most $O(n/\log n)$ times. The theorem is generalized to uniform hypergraphs. Similar bounds with smaller constant value is provided for fractional partitioning both for graphs and for uniform hypergraphs. We show that these latter constants cannot be improved by more than a factor of 1.89 even for fractional covering by arbitrary complete multipartite subgraphs or subhypergraphs. In the case every vertex of the graph is connected to at least $n - m$ other vertices, we prove the existence of a fractional covering of the edges by complete bipartite graphs such that every vertex is covered at most $O(m/\log m)$ times, with only a slightly worse explicit constant. This result also generalizes to uniform hypergraphs. Our results give new improved bounds on the complexity of graph and uniform hypergraph based secret sharing schemes, and show the limits of the method at the same time.

Keywords graph covering · partition cover number · bipartite graph · uniform hypergraph · secret sharing.

Mathematics Subject Classification (2010) 05C99 · 05C65 · 05D40 · 94A60

1 Introduction

While graph decomposition is an interesting topic by itself [1,3,8–11,14], our interest comes mainly from a particular application in cryptography. Upper bounds on the worst case complexity of secret sharing schemes often use graph decomposition techniques [2,13,16]. In this respect the most cited result is the Erdős-Pyber theorem [7], which states that the edges of any graph on n vertices can be partitioned into the edge sets of complete bipartite subgraphs such that every vertex is contained in $O(n/\log n)$ of these subgraphs. (In this paper log denotes the

L. Csirmaz
Central European University, Budapest, Hungary
e-mail: csirmaz@renyi.hu

P. Ligeti
Department of Computeralgebra and ELTECRYPT Research Group,
Eötvös Loránd University, Budapest, Hungary
e-mail: turul@cs.elte.hu

G. Tardos
Rényi Institute of Mathematics, Budapest, Hungary
e-mail: tardos.gabor@renyi.mta.hu

base 2 logarithm.) An immediate consequence is that for any graph there is a secret sharing scheme realizing that graph with complexity $O(n/\log n)$ – the best upper bound known for the share size in general graphs. Any improvement in the the Erdős-Pyber theorem implies immediately a similar improvement in this bound. In this paper we give an alternate proof of the Erdős-Pyber theorem which yields an improved explicit constant term. For the consequence on secret sharing a so called *fractional partition* is enough in place of a the edge partition in the Erdős-Pyber theorem. For this fractional version our results are stronger by a factor of 2 and we further prove that they are near-optimal: there exists graphs, where even the average vertex cover number is always more than half of our upper bound, and this holds for every fractional cover of the edges, even if arbitrary complete multipartite graphs are allowed to participate in the fractional cover.

We generalize all these results to uniform hypergraphs, and our results remain equally sharp.

Motivated by the question of what makes a graph "hard" for secret sharing schemes, Beimel et al. [2] considered very dense graphs, that is, graphs where every node has high degree. We generalize our results to graphs on n vertices with minimum degree $n - m$ and show that in this case the edges can be partitioned into complete bipartite graphs such that every vertex is covered by only $O(m/\log m)$ of them (again, with a small explicit constant). Setting $m = n$ we get yet another proof of the Erdős-Pyber theorem, but this time the constant term is slightly higher than in our first proof.

The paper is organized as follows. In Sect. 2 we recall some definitions and notations, and present our results. Our constructive proof of the Erdős-Pyber theorem is given in Sect. 3. The generalization for d-uniform hypergraphs is proved in Sect. 4, Sect.5 deals with the case of dense graphs. Finally, in Sect. 6 we prove that our results are the best possible up to a small constant multiplier.

2 Preliminaries and results

2.1 Graph decomposition

Let $\mathcal{F}$ be a collection of graphs. An $\mathcal{F}$-graph is a graph which is isomorphic to an element of $\mathcal{F}$. An *$\mathcal{F}$-cover* of a graph $G = (V, E)$ is a collection of subgraphs of G that are $\mathcal{F}$-graphs, and the union of whose edge sets is E. An $\mathcal{F}$-cover is an *$\mathcal{F}$-partition* if the edge sets of the subgraphs are pairwise disjoint. Given an $\mathcal{F}$-cover of G, the *load* of a vertex $v \in V$ is the number of subgraphs containing it. The *vertex $\mathcal{F}$-cover number* and the *vertex $\mathcal{F}$-partition number* of a graph G is the smallest r such that for some $\mathcal{F}$-cover (or $\mathcal{F}$-partition, respectively) of G all vertex loads are at most r. We denote these numbers by $\mathsf{vc}_{\mathcal{F}}(G)$, and $\mathsf{vp}_{\mathcal{F}}(G)$, respectively, and the value is $+\infty$ when no such a cover or partition exists. For more information on this notation and a discussion of its relevance, see, e.g., [12].

In the *fractional*, or weighted version, each $\mathcal{F}$-subgraph of a graph $G = (V, E)$ has a non-negative weight, and the total weight of the subgraphs containing an edge $e \in E$ should be at least 1 (cover), or exactly 1 (partition). In this case the load of a vertex is the sum of the weights of the $\mathcal{F}$-subgraphs containing it, and the corresponding *fractional vertex $\mathcal{F}$-cover number* and *fractional vertex $\mathcal{F}$-partition number* are denoted by $\mathsf{vc}^*_{\mathcal{F}}(G)$, and $\mathsf{vp}^*_{\mathcal{F}}(G)$, respectively. It is clear that

$$\mathsf{vc}^*_{\mathcal{F}}(G) \le \mathsf{vc}_{\mathcal{F}}(G) \le \mathsf{vp}_{\mathcal{F}}(G), \quad \text{and} \quad \mathsf{vc}^*_{\mathcal{F}}(G) \le \mathsf{vp}^*_{\mathcal{F}}(G) \le \mathsf{vp}_{\mathcal{F}}(G). \tag{1}$$

The most frequently investigated case is when $\mathcal{F}$ is the collection of complete bipartite graphs, denoted here by CB. In the classical work of Fishburn and Hammer [8] $\mathsf{vc}_{\mathsf{CB}}(G)$ is called the bipartite degree of G. Dong and Liu showed in [6] that $\mathsf{vc}_{\mathsf{CB}}(K_n) = \mathsf{vp}_{\mathsf{CB}}(K_n) = \lceil \log n \rceil$,[1] and that $\mathsf{vp}_{\mathsf{CB}}(G) \le 4$ for planar graphs. Pinto [14] calls $\mathsf{vc}_{\mathsf{CB}}(G)$ and $\mathsf{vp}_{\mathsf{CB}}(G)$ the local biclique

[1] Note that log denotes base 2 logarithm.

cover and partition number of G, respectively, and shows that there are graphs with $\mathsf{vc}_{\mathsf{CB}}(G) = 2$ while $\mathsf{vp}_{\mathsf{CB}}(G)$ can be arbitrary large. V. Watts investigates fractional partitions and covers in [17].

Other well studied graph families are the collection of stars, and the collection of cycles. We will use another important graph family, that of the *complete multipartite graphs*. These graphs are the complements of disjoint unions of complete graphs and we denote their collection by CM.

2.2 d-uniform hypergraphs

Let $d \geq 2$ be an integer. A *d-uniform hypergraph* $\mathcal{H}$ is a pair (V, E), where V is the set of vertices, and E is the set of edges, often called *hyperedges*, and each edge is a d-element subset of V. A *subhypergraph* of $\mathcal{H}$ is a d-uniform hypergraph (V', E') with $V' \subseteq V$ and $E' \subseteq E$.

A d-uniform hypergraph $\mathcal{H}$ is a *complete d-uniform k-partite hypergraph*, a (d, k)*-cuph* for short, if its vertex set can be partitioned into k parts such that the edge set consists of the subsets of the vertices that intersect d of the parts, each in a single vertex. We call the parts of this partition the *partite sets* of $\mathcal{H}$. When $k = d$ we call a (d, d)-cuph simply a d-cuph.

With a slight abuse of notation, the family of complete d-uniform multipartite hypergraphs ((d, k)-cuphs) is also denoted by CM, and the family of d-cuphs is denoted by CB. In these definitions we consider d to be fixed but the class CM contain (d, k)-cuphs for arbitrary k. Note that in the $d = 2$ case we get back the the standard notion of complete multipartite and bipartite graphs, respectively.

When $\mathcal{F}$ is a collection of d-uniform hypergraphs, the notion of $\mathcal{F}$-cover and $\mathcal{F}$-partition as well as the load of a vertex generalizes easily for d-uniform hypergraphs. The values $\mathsf{vc}_{\mathcal{F}}(\mathcal{H})$, $\mathsf{vp}_{\mathcal{F}}(\mathcal{H})$ and their fractional versions are defined similarly as has been done for standard graphs. Inequalities in (1) remain valid in this case.

2.3 Secret sharing

A secret sharing scheme, introduced in [4,15], is a probabilistic method by which a dealer, who holds a secret, distributes shares to a set of participants, so that only *authorized* subsets of the participants are able to reconstruct the secret from their shares. The collection of all authorized subsets is called the *access structure*. We only consider *perfect schemes*, in which unauthorized subsets of participants should learn nothing about the secret, that is, the collection of their shares should be independent of the secret. Secret sharing schemes are considered as one of the main building blocks in modern cryptography [13]. Most research on secret sharing focuses on the ratio between the size of the largest share and the size of the secret. Size is measured here by way of entropy. The *complexity*, or information ratio of an access structure is the infimum of this ratio over all schemes realizing the structure. In this paper we consider access structures where all minimal authorized subsets have the same size $d \geq 2$. These access structures can be described by d-uniform hypergraphs, where each vertex represents a participant, and d vertices form a hyperedge if and only if the respective d-element set of participants is authorized. For such a hypergraph $\mathcal{H}$, the complexity of the access structure based on $\mathcal{H}$ is denoted by $\sigma(\mathcal{H})$. Hypergraphs with at least one edge have complexity at least 1. Hypergraphs with complexity exactly 1 are called *ideal*. The complete d-uniform multipartite hypergraphs, that is (d, k)-cuphs, are ideal [13]. When $d = 2$ all other non-trivial graphs have complexity at least $3/2$ [5], for $d \geq 3$ the characterization of ideal d-uniform hypergraphs is an open problem.

Our interest in graph decomposition stems from Stinson's Decomposition Theorem [16] which is an indispensable tool in giving upper bounds on the complexity of access structures. While Stinson's theorem is more general, we state here in a special case.

Theorem 1 (Stinson [16]) *Let $\mathcal{F}$ be any collection of ideal d-uniform hypergraphs. For any d-uniform hypergraph $\mathcal{H}$ we have $\sigma(\mathcal{H}) \le \mathsf{vc}^*_{\mathcal{F}}(\mathcal{H})$.* □

As complete d-uniform multipartite graphs are ideal, the complexity of the hypergraph $\mathcal{H}$ can be upper bounded by $\mathsf{vp}_{\mathsf{CM}}(\mathcal{H})$.

2.4 Our results

In the asymptotic notation $O(\cdot)$ and $o(\cdot)$ we assume that d is fixed and n and in the case of Theorem 4 and Corollary 5, also m tend to infinity.

Erdős and Pyber proved in [7] that for any (standard) graph G on n vertices, the edge set of G can be partitioned into complete bipartite graphs so that every vertex of G is contained in at most $O(n/\log n)$ of the bipartite graphs. Using the notation introduced above, their result can be expressed equivalently as $\mathsf{vp}_{\mathsf{CB}}(G) = O(n/\log n)$. They also remarked that this estimate is the best possible. We give a constructive proof of the Erdős-Pyber theorem with an improved explicit constant factor.

Theorem 2 *Let G be a graph on n vertices. Then*

$$\mathsf{vp}_{\mathsf{CB}}(G) \le \big(1+o(1)\big)\frac{n}{\log n},$$

moreover

$$\mathsf{vp}^*_{\mathsf{CB}}(G) \le \big(0.5+o(1)\big)\frac{n}{\log n}.$$

We prove a generalization of this theorem to d-uniform hypergraphs with higher values of d as follows.

Theorem 3 *Let $d \ge 2$ be an integer, and $\mathcal{H}$ be a d-uniform hypergraph on n vertices. Then*

$$\mathsf{vp}_{\mathsf{CB}}(\mathcal{H}) \le \big(\frac{1}{(d-2)!}+o(1)\big)\frac{n^{d-1}}{\log n},$$

and

$$\mathsf{vp}^*_{\mathsf{CB}}(\mathcal{H}) \le \big(\frac{1}{d!}+o(1)\big)\frac{n^{d-1}}{\log n}.$$

In case a graph G is dense and each vertex is connected to almost all other vertices, the bound on $\mathsf{vc}^*_{\mathsf{CB}}(G)$ in Theorem 2 can be strengthened. Similar strengthening works for dense hypergraphs. Note that we can choose $m = n$ to get a result for arbitrary graphs or hypergraphs, and even in this case the bounds are only slightly worse than the ones implied by Theorems 2 and 3.

Theorem 4 *Let G be a graph on n vertices such that every vertex has degree at least $n - m$. Then we have*

$$\mathsf{vp}^*_{\mathsf{CB}}(G) \le \big(0.725+o(1)\big)\frac{m}{\log m}.$$

If the d-uniform hypergraph $\mathcal{H}$ on n vertices satisfies that every set of $d-1$ vertices that appears together in an edge appears in at least $n - m$ edges, then

$$\mathsf{vp}^*_{\mathsf{CB}}(\mathcal{H}) \le \left(\frac{1.45}{d!}+o(1)\right)\frac{n^{d-2}m}{\log m}.$$

Our results can be applied to get universal bounds on the complexity of graph and uniform hypergraph based structures.

Corollary 5 *For any graph G on n vertices, $\sigma(G) \leq (1/2 + o(1))\frac{n}{\log n}$. If the graph G has minimum degree $n - m$, then $\sigma(G) \leq (0.725 + o(1))\frac{m}{\log m}$.*

For any d-uniform hypergraph $\mathcal{H}$ on n vertices, $\sigma(\mathcal{H}) \leq (\frac{1}{d!} + o(1))\frac{n^{d-1}}{\log n}$. If every set of $d-1$ vertices in $\mathcal{H}$ that appears in a hyperedge appears in at least $n - m$ of them, then we also have $\sigma(\mathcal{H}) \leq (\frac{1.45}{d!} + o(1))\frac{n^{d-2}m}{\log m}$.

Note that, in general, the complexity $\sigma(G)$ and $\sigma(\mathcal{H})$ relates the size of the largest share to size of the secret, and optimal ratio may only be achievable if both of these quantities are high. Without going in the technical details of implementing Stinson's decomposition let us note that the ideal access structures in CB (complete bipartite graphs or d-cuphs) admit an ideal secret sharing scheme with a binary secret, but to achieve the ratio given in Corollary 5 for graphs or d-uniform hypergraphs one does indeed need to work with non-binary secrets. If, however, we use edge covers rather than fractional edge covers, then the decomposition does not increase the size of the secret. In particular, any access structure given by a graph G or hypergraph $\mathcal{H}$ can be realized by a secret sharing scheme with uniform binary secret variable and the shares having size at most $\mathsf{vc}_{\mathsf{CB}}(G)$ or $\mathsf{vc}_{\mathsf{CB}}(\mathcal{H})$, respectively. In light of Theorems 2, 3, and 4 the share to secret ratio of these secret sharing schemes is at most $d(d-1)$ times the bounds claimed in Corollary 5 for d-uniform access structures.

From the other direction we show that the fractional results in Theorems 2 and 3 cannot be improved by more than a factor of 1.89 even if we consider fractional covering instead of fractional partition and arbitrary complete multipartite hypergraphs instead of d-cuphs.

Theorem 6 *For every $d \geq 2$ and $n \geq n_0(d)$ there is a d-uniform hypergraph $\mathcal{H}$ on n vertices such that*

$$\mathsf{vc}^*_{\mathsf{CM}}(\mathcal{H}) \geq \frac{0.53}{d!} \cdot \frac{n^{d-1}}{\log n}.$$

This theorem indicates that new and different ideas are required to improve the general upper bound on the complexity of graphs and hypergraphs given by Corollary 5.

3 Graphs - proof of the Erdős-Pyber theorem

With the choice $k = \lceil \log n - 2 \log \log n \rceil$ the following lemma implies Theorem 2. We formulate this lemma because for the generalizations for hypergraphs we will need its bound on the total number of subgraphs used in the partition. For the same choice of k it is $O(n^2/\log^3 n)$.

Lemma 1 *Let G be a graph on n vertices and let $1 \leq k \leq n$. There exists a CB-partition of G involving less than $2^k n/k$ complete bipartite subgraphs such that load of every vertex is at most $2^{k-1} + \lceil n/k \rceil$.*

Furthermore, there exists a fractional CB-partition of G involving less than $2^k n/k$ complete bipartite subgraphs, each with weight $1/2$ or 1, such that the load of every vertex is at most $2^{k-2} + \lceil n/k \rceil/2$.

Proof Let us orient each edge e of G arbitrarily, so now one of its vertices is $h(e)$, the *head* of e, while the other is the *tail* $t(e)$ of e. We write $N^+(v)$ for the set of *outneighbors* of the vertex v, i.e., $N^+(v) = \{h(e) : e \in E, t(e) = v\}$. Let us partition the vertex set into classes $H_1, \ldots, H_{\lceil n/k \rceil}$ in such a way that each class has at most k elements. For a nonempty subset $S \subseteq H_i$ of a class H_i we consider the complete bipartite graph G_S whose two partite sets are S and $T_S = \{v \in V : N^+(v) \cap H_i = S\}$. Figure 1 illustrates an example of such graph. The

graphs G_S are clearly subgraphs of G, their number is less than $2^k n/k$ as claimed and their edge sets partition the edge set E as $e \in E$ appears in the unique subgraph G_S, where H_i is the class containing $h(e)$ and $S = N^+(t(e)) \cap H_i$. Furthermore a vertex $v \in H_i$ appears in the $2^{|H_i|-1} \le 2^{k-1}$ sets $S \subseteq H_i$ and further it also appears in the partite set T_S of G_S for $S = N^+(v) \cap H_j \neq \emptyset$, for at most $\lceil n/k \rceil$ additional graphs. This proves the first claim of the lemma.

For the second claim we ignore the orientation and work with the full neighborhood $N(v) = \{w \in V : \{v, w\} \in E\}$ of a vertex. We still use the same partition of the vertex set. For a nonempty set $S \subseteq H_i$ we define G'_S to be the complete bipartite graph with partite sets S and $T'_S = \{v \in V : N(v) \cap H_i = S\}$. It is clear that these graphs are subgraphs of G, their number is the same as the number of the graphs G_S, and every edge $\{v, w\} \in E$ appears in exactly two of these graphs, namely if $v \in H_i$ and $w \in H_j$, then $\{v, w\}$ appears in $G'_{N(v)\cap H_j}$ and in $G'_{N(w)\cap H_i}$. Thus, assigning the weight $1/2$ to each of these graphs we obtain a fractional CB-partition of G. The weight 1 will only show up if two of the complete bipartite graphs are the same with the role of their partite sets reversed. As before, a vertex $v \in H_i$ appears in at most 2^{k-1} sets $S \subseteq H_i$ and at most $\lceil n/k \rceil$ sets T'_S, where $S = N(v) \cap H_j \neq \emptyset$ for some j. □

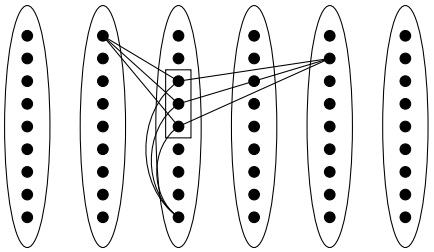

Fig. 1 A $K_{3,3}$ subgraph with a 3-element S from the third class

4 Uniform hypergraphs

In this section we prove Theorem 3. We note that the out of the d partite sets of the d-cuphs used in the CB-partition or fractional CB-partition constructed in the proof at least $d-2$ are singletons. The weight of any d-cuph in the fractional CB-partition is a multiple of $1/(d^2-d)$.

Proof (of Theorem 3) Let $\mathcal{H} = (V, E)$. We start with something similar to orientation: we partition every edge $e \in E$ into two sets $A(e)$ and $B(e)$ with $|A(e)| = d-2$ and $|B(e)| = 2$. For $A \subseteq V$, $|A| = d-2$ we define a subset $E_A = \{e \in E : A(e) = A\}$ of E and a graph $G_A = (V, \{B(e) : e \in E_A\})$. See Figure 2 for an example in a 6-uniform hypergraph. Clearly, the sets E_A partition E. We apply the claim on CB-partition in Lemma 1 separately to each of the graphs G_A using $k = \lceil \log n - 2 \log\log n \rceil$. This yields a partition of the edge set of G_A into the edge sets of the subgraphs $G_{A,i}$. As calculated before the statement of the lemma, for every A we have $O(n^2/\log^3 n)$ graphs $G_{A,i}$ and the load of any vertex is at most $(1+o(1))n/\log n$.

Let $S_{A,i}$ and $T_{A,i}$ be the partite sets of $G_{A,i}$ and let us define $\mathcal{H}_{A,i}$ to be the d-cuph with partite sets $S_{A,i}$, $T_{A,i}$ and the $d-2$ singleton sets contained in A. For a fixed A the edge sets of the d-cuphs $\mathcal{H}_{A,i}$ partition E_A. Thus, all the hypergraphs $\mathcal{H}_{A,i}$ give a CB-partition of $\mathcal{H}$.

Let us now fix a vertex $v \in V$ and estimate its load. The vertex v appears in all $\mathcal{H}_{A,i}$ with $v \in A$: this contributes $O(n^{d-3} \cdot n^2/\log^3 n)$ to the load. We further have $\binom{n-1}{d-2}$ sets A that do not contain v and at most $(1+o(1))n/\log n$ graphs $G_{A,i}$ for each such set A in which v

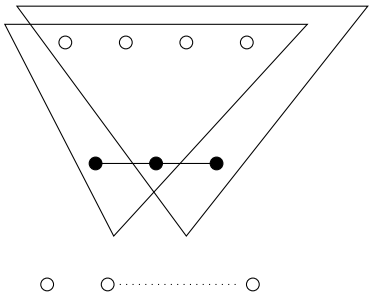

Fig. 2 A 6-uniform hypergraph with $G_A = K_{2,1}$

appears making v also appear as a vertex of $\mathcal{H}_{A,i}$. This brings the total load on v up to at most $(1/(d-2)! + o(1))n^{d-1}/\log n$ proving the first statement of the theorem.

To obtain a good fractional CB-partition of $\mathcal{H}$ we disregard the partition $e = A(e) \cup B(e)$ created earlier. For $A \subseteq V$ with $|A| = d-2$ we define $E'_A = \{e \in E : A \subseteq e\}$ and the graph $G'_A = (V, \{e \setminus A : e \in E'_A\})$. Every edge $e \in E$ appears in exactly $\binom{d}{2}$ of the sets E'_A. Now we apply the claim on fractional CB-covering in Lemma 1 for each of the graphs G'_A with the same choice of k as before. We obtain a fractional CB-partition of G'_A with the complete bipartite graphs $G'_{A,i}$ with weight $w_{A,i}$ such that the total number of these graphs is $O(n^2/\log^3 n)$ and the maximum load does not exceed $(1/2 + o(1))n^2/\log n$. We define the d-cuphs $\mathcal{H}'_{A,i}$ as before: its partite sets are the partite sets of $G'_{A,i}$ plus the singleton sets contained in A. We set the weight of $\mathcal{H}'_{A,i}$ to be $w_{A,i}/\binom{d}{2}$. This gives a fractional CB-partition of $\mathcal{H}$. Calculating the maximum load of this fractional CB-partition as before finishes the proof of the theorem. □

5 Very dense graphs

In this section we prove Theorem 4. S. Jukna in [10, Theorem 1] proves similar results for bipartite graphs with the difference that he bounds the total number of covering bipartite graphs rather than the maximum load. The first part of Theorem 4 will follow from the following lemma, which will also be used to bootstrap the proof for the d-uniform case.

Lemma 2 *Let G be a graph on n vertices such that every vertex has degree at least $n-m$. For each $0 < p < 1$ we have*

$$\mathsf{vp}^*(G) \le \frac{1}{2}\big(p^{-1} + (1-p)^{-m}\big). \tag{2}$$

Moreover, the total weight of all graphs taking part in the fractional partition is $1/(2p(1-p)^m)$.

Proof The proof uses some ideas from [2, Lemma 3.7]. Let V be the vertex set of G. Choose the random complete bipartite subgraph H_0 of G as follows. The partite sets of H_0 are A and B_0. Construct A by adding each vertex v of G to the set independently with probability p. Let B_0 consists of all vertices in $V \setminus A$ which are connected to all elements in A. Clearly, H_0 is a subgraph of G. Now let H be a random subgraph of H_0, a complete bipartite graph with partite sets A and B, where B is a subset of B_0 that contains the vertex $v \in B_0$ with probability $(1-p)^{d_v - n + m}$ independently from each other, where d_v is the degree of v in G. Note that we assumed that $d_v \ge n - m$, so this selection makes sense. This two-step process produces a random complete bipartite subgraph H of G.

Let us fix a vertex $v \in V$. We have $v \in B_0$ if and only if the vertices not adjacent to v (including v itself) are not in A, thus $\mathbf{Pr}(v \in B_0) = (1-p)^{n-d_v}$. By our construction, $v \in B$ implies $v \in B_0$ and we have $\mathbf{Pr}(v \in B | v \in B_0) = (1-p)^{d_v - n + m}$. Thus, overall, we have $\mathbf{Pr}(v \in B) = (1-p)^m$. Note also, that $v \in B$ is independent of $u \in A$ for all vertices u adjacent

to v. Thus, for every uv edge of G we have $\mathbf{Pr}(u \in A, v \in B) = p(1-p)^m$. The same uv edge is also contained in H if $u \in B$ and $v \in A$, thus the total probability of an edge uv of G to be covered by H is exactly $2p(1-p)^m$.

Let us associate with each complete bipartite subgraph H^* of G the weight $\mathbf{Pr}(H = H^*)/(2p(1-p)^m)$. The calculation above verifies that this is a fractional CB-partition. The load of every vertex v is exactly

$$\frac{\mathbf{Pr}(v \in A \cup B)}{2p(1-p)^m} = \frac{p + (1-p)^m}{2p(1-p)^m} = \frac{1}{2}\big(p^{-1} + (1-p)^{-m}\big),$$

as was required. The total weight of the complete bipartite subgraphs is $1/(2p(1-p)^m)$ as the sum of probabilities is exactly 1. □

Proof (of Theorem 4) We choose $p^{-1} = m \log e/(\log m - 2 \log\log m)$ where e is the base of the natural logarithm. With this choice the right hand side of (2) is

$$\big(\frac{\log e}{2} + o(1)\big)\frac{m}{\log m} < \big(0.725 + o(1)\big)\frac{m}{\log m},$$

which proves the first claim of Theorem 4. Note that the total weight of all graphs taking part of the fractional partition is $1/(2p(1-p)^m) = O(m^2/\log^2 m)$.

To turn this fractional partition result on graphs to one on hypergraphs we do the same as in the proof of Theorem 3. Let $\mathcal{H} = (V, E)$ be a d-uniform hypergraph. For a $(d-2)$-set A of vertices consider the edge set $E_A = \{e \in E \mid A \subseteq e\}$ and the graph $G_A = (V, \{e \setminus A \mid e \in E_A\})$. Ignoring the isolated vertices in G we get a graph on less than n vertices and with minimum degree at least $n - m$. Applying our result above we obtain a fractional CB-partition of G_A with complete bipartite graphs $G_{A,i}$ with weight $w_{A,i}$. The claimed fractional CB-partition of $\mathcal{H}$ is formed by the hypergraphs $\mathcal{H}_{A,i}$ with weights $w_{A,i}/\binom{d}{2}$, where the partite sets of $\mathcal{H}_{A,i}$ are those of $G_{A,i}$ and the singleton sets contained in A. Calculation of the load of this partition finishes the proof of the theorem. □

6 Lower bound for the load of fractional covers

To show Theorem 6 and see that the fractional results in Theorems 2 and 3 are optimal within a factor of less than 2 we turn to random hypergraphs. Let $\mathcal{H}^d(n,p)$ denote the random d-uniform hypergraph on n vertices in which each d-subset of the vertices is an edge with probability p and these events are independent. For a d-uniform hypergraph $\mathcal{H} = (V, E)$ we write $\rho(\mathcal{H}) = |E|/|V|$ and call it the *density* of $\mathcal{H}$. Note that $d\rho(\mathcal{H})$ is the *average degree* in $\mathcal{H}$.

Lemma 3 *Let $d \geq 2$ be an integer and $0 < p < 1$. With probability tending to 1 as n goes to infinity the maximum density of a (d,k)-cuph subhypergraph of $\mathcal{H}^d(n,p)$ (for any k) is at most $-\log n/\log p$.*

Proof We use the first moment method. Let $\mathcal{H} = (V, E)$ be a (d,k)-cuph with $\rho(\mathcal{H}) > -\log n/\log p$. We can get rid of the empty partite sets and assume that all k partite sets of $\mathcal{H}$ are non-empty. For a fixed size $s = |V|$ and k we have $\binom{n}{s}$ possibilities to choose V as a subset of the fixed vertex set of $\mathcal{H}^d(n,p)$ and less than $s^k/k!$ ways split it into the partite sets that determine $\mathcal{H}$. For a fixed $\mathcal{H}$ the chance that it is a subhypergraph of $\mathcal{H}^d(n,p)$ is $p^{|E|} = p^{\rho(\mathcal{H})s} < n^{-s}$. Thus the probability of the existence (in fact the expected number) of suitably dense (d,k)-cuph subhypergraph (for any k) can be estimated as less than

$$\sum_{s,k} \binom{n}{s} \frac{s^k}{k!} n^{-s} < \sum_{s,k} \frac{s^k}{s!k!} = \sum_s \frac{e^s}{s!} = e^e,$$

where e is the base of the natural logarithm. However d-uniform hypergraphs of any given fixed size s have a bounded density, so as n increases and our threshold $-\log n/\log p$ passes this density we can ignore small values of s. This yields a sum that tends to zero as claimed. □

Theorem 7 *Let $d \geq 2$ be an integer, $0 < p < 1$ and $\varepsilon > 0$. With probability tending to 1 as n goes to infinity we have $\mathsf{vc}^*_{\mathsf{CM}}(\mathcal{H}^d(n,p)) \geq (-p\log p/d! - \varepsilon)n^{d-1}/\log n$.*

Proof Let $\mathcal{H}^d(n,p) = (V,E)$ and let the hypergraphs $\mathcal{H}_i = (V_i, E_i)$ with the weights w_i form a fractional CM-cover of $\mathcal{H}^d(n,p)$. By Lemma 3 we may assume that $\rho(\mathcal{H}_i) = |E_i|/|V_i| \leq -\log n/\log p$ for all i. This means $w_i|E_i| \leq -w_i \log n|V_i|/\log p$. Summing these inequalities we get

$$|E| \leq \sum_{e\in E}\sum_{i:e\in E_i} w_i = \sum_i w_i|E_i| \leq -\frac{\log n}{\log p}\sum_i w_i|V_i| = -\frac{\log n}{\log p}\sum_{v\in V} l_v,$$

where l_v is the load of the vertex v. Thus, for the maximum load l we have

$$l \geq -\frac{\log p}{\log n}\rho(\mathcal{H}^d(n,p)).$$

Here the expectation of $\rho(\mathcal{H}^d(n,p))$ is $\mathrm{Exp}[|E|]/n = p\binom{n}{d}/n = (p/d! + o(1))n^{d-1}$. Note further that the distribution of $|E|$ is binomial, and therefore it is concentrated around its expectation. That is, with probability tending to 1 we have $\rho(\mathcal{H}^d(n,p)) \geq (p/d! + \varepsilon/\log p)n^{d-1}$. This gives $l \geq (-p\log p/d! - \varepsilon)n^{d-1}/\log n$. As we proved this bound for the maximal load of an arbitrary fractional CM-cover of $\mathcal{H}^d(n,p)$ it also applies to $\mathsf{vc}^*_{\mathsf{CM}}(\mathcal{H}^d(n,p))$ (still with probability tending to 1), and finishes the proof of the theorem. □

Proof (of Theorem 6) By Theorem 7 for any p and $\varepsilon > 0$ and large enough n there exists a hypergraph $\mathcal{H}$ on n vertices with $\mathsf{vc}^*_{\mathsf{CM}}(\mathcal{H}) \geq (-p\log p/d! - \varepsilon)n^{d-1}/\log n$, namely the random graph $\mathcal{H}^d(n,p)$ works with high probability. Here $-p\log p$ is maximized for $p = 1/e$, where e is the base of the natural logarithm. This choice for p proves the theorem. □

Acknowledgment

This research has been partially supported by the Cryptography Lendület program of the Hungarian Academy of Sciences. The first author also acknowledges the support from the grant TAMOP-4.2.2.C-11/1/KONV-2012-0001. The second author was supported by the OTKA grant PD100712. The last author also acknowledges the support of the grant OTKA NN-102029 and the NSERC Discovery grant.

References

1. N. Alon, Covering graphs by the minimum number of equivalence relations, Combinatorica, **2** no. 3, 201–206 (1986)
2. A. Beimel, O. Ferràs, Y. Mintz, Secret sharing schemes for very dense graphs, Lecture Notes in Computer Science, vol. 7417 (Advances in Cryptology - CRYPTO 2012), pp. 144–161, ISSN: 0302-9743 (2012)
3. S. Bezrukov, D. Fronček, S. J. Rosenberg, P. Kovář, On biclicque coverings, Discr. Math, **208**, 319–323 (2008)
4. G. R. Blakley, Safeguarding cryptographic keys, in R.E. Merwin, J. T. Zanca and M. Smith (eds.) *Proc. of the 1979 IFIPS National Computer Conference*, **48**, 313–317 (1979)
5. C. Blundo, A. De Santis, R. De Simone, U. Vaccaro: Tight bounds on the information rate of secret sharing schemes, Des. Codes Cryptogr., **11**, 107–122, (1997)
6. J. Dong, Y. Liu, On the decomposition of graphs into complete bipartite graphs, Graph. and Combin., **23**, 255–262 (2007)
7. P. Erdős, L. Pyber, Covering a graph by complete bipartite graphs, Discr. Math, **170**, no. 1–3, 249–251 (1997)

8. P.C. Fishburn, P.L. Hammer, Bipartite dimensions and bipartite degrees of graphs Discr. Math, **160**, 127148 (1996)
9. H. Hajuabolhassan, F. Moazami, Some new bounds for cover-free families through biclique cover, arXiv 1008.3691 (2011), Accessed Nov. 2013
10. S. Jukna, On set intersection representation of graphs, J. Graph Theor., **61**, 55–75 (2009)
11. G. Katona, E. Szemerédi, On a problem of graph theory, Studia Math. Hung., **2** 23–28 (1967)
12. K. Kanuer, T. Ueckerdt, Three ways to cover a graph arXiv:1205.1627 (2012), Accessed Nov 2013
13. C. Padro, Lecture Notes in Secret Sharing IACR preprint `http://eprint.iacr.org/2012/674` (2012), Accessed Nov 2013
14. T. Pinto, Biclique covers and partitions, arXiv 1307.6363, (2013), Accessed Nov 2013
15. A. Shamir, How to share a secret, Comm. ACM, **22**, 612–613 (1979)
16. D. R. Stinson: Decomposition construction for secret sharing schemes, *IEEE Trans. Inf. Theory* **40**, 118–125 (1994) .
17. V. L. Watts, Fractional biclique covers and partitions of graphs, Electron. J. Combin., **13** (2006)