The Sketching Complexity of Graph and Hypergraph Counting

John Kallaugher  
UT Austin  
Austin, USA  
jmgk@cs.utexas.edu

Michael Kapralov  
EPFL  
Lausanne, Switzerland  
michael.kapralov@epfl.ch

Eric Price  
UT Austin  
Austin, USA  
ecprice@cs.utexas.edu

Abstract—Subgraph counting is a fundamental primitive in graph processing, with applications in social network analysis (e.g., estimating the clustering coefficient of a graph), database processing and other areas. The space complexity of subgraph counting has been studied extensively in the literature, but many natural settings are still not well understood. In this paper we revisit the subgraph (and hypergraph) counting problem in the sketching model, where the algorithm’s state as it processes a stream of updates to the graph is a linear function of the stream. This model has recently received a lot of attention in the literature, and has become a standard model for solving dynamic graph streaming problems.

In this paper we give a tight bound on the sketching complexity of counting the number of occurrences of a small subgraph \( H \) in a bounded degree graph \( G \) presented as a stream of edge updates. Specifically, we show that the space complexity of the problem is governed by the fractional vertex cover number of the graph \( H \). Our subgraph counting algorithm implements a natural vertex sampling approach, with sampling probabilities governed by the vertex cover of \( H \). Our main technical contribution lies in a new set of Fourier analytic tools that we develop to analyze multiplexer communication protocols in the simultaneous communication model, allowing us to prove a tight lower bound. We believe that our techniques are likely to find applications in other settings. Besides giving tight bounds for all graphs \( H \), both our algorithm and lower bounds extend to the hypergraph setting, albeit with some loss in space complexity.

I. INTRODUCTION

Triangle counting is one of the most well-studied problems in streaming graph algorithms. In the standard “turnstile” version of this problem, one maintains a small-space “sketch” of a graph under a stream of insertions and deletions of edges, and at the end of the stream outputs a \( (1 \pm \varepsilon) \) multiplicative approximation to the number of triangles \( T \) in the graph; unless otherwise specified, we assume \( \varepsilon \) to be a small constant.

Turnstile streaming algorithms are almost invariably constructed as linear sketches, where the sketch maintained is a linear function of the indicator vector of edges; this makes it easy to process insertions and deletions. Linear sketches are also useful in other settings such as distributed computation, since sketches can be merged. There is evidence that any turnstile streaming algorithm can be efficiently implemented using linear sketches [LNW14a], [AHLW16], although these results do not quite apply to graph streams.

For worst-case graphs, counting triangles is impossible in sublinear space: \( \Omega(m) \) space is required to distinguish between a graph with 0 triangles and one with \( T = \Omega(m) \) triangles [BOV13]. However, the hard case is degenerate in that all the triangles share a common edge. If at most \( \Delta_E \) triangles share any single edge, then this bound becomes \( \Omega(m\Delta_E/T) \). In [PT12] an algorithm was given that counts triangles with

\[
O\left(m\left(\frac{1}{\sqrt{T}} + \frac{\Delta_E}{T}\right)\right)
\]

space, where the \( m/\sqrt{T} \) term improves upon a \( m/T^{1/3} \) term in [TKMF09], [TKM11]. In [KP17] this was shown to be tight for worst-case graphs, but the hard case is again degenerate: all the triangles share a common vertex. If \( \Delta_V \) bounds the maximum number of triangles to share a vertex, this bound becomes \( m\sqrt{\Delta_V}/T \). The algorithm in [KP17] requires

\[
\tilde{O}\left(m\left(\frac{1}{T^{2/3}} + \frac{\sqrt{\Delta_V}}{T} + \frac{\Delta_E}{T}\right)\right)
\]

space. A natural question is whether this \( \frac{m}{T^{2/3}} \) is necessary.

A. Linear Sketching

Suppose we have a problem of the following form: we receive a vector \( v \in \mathbb{Z}^n \) as a series of updates \( (v_i)_{i=1}^t \), so \( v = \sum_{i=1}^t v_i \), and we want to approximate some function \( f(v) \). A linear sketch for this problem is a linear transformation \( A \in \mathbb{Z}^{n \times d} \) and a post-processing function \( g \), so that \( g(Av) \) approximates \( f(v) \) (with the exact definition of “approximates” depending on the problem). The space complexity of such a sketch is the space needed to store the sketch vector, which is \( \Theta(d \log n) \).
bits if the maximum size of entries of $v$ is bounded by some $M = \text{poly}(n)$ (this holds even if intermediate stages of the stream exceed $M$, as the sketch vector may be stored mod $M$).

In [LNW14a], it was shown that any turnstile streaming algorithm (an algorithm that can solve a problem of the above form when the updates $v_i$ are allowed to be negative, but that is allowed to maintain arbitrary state) can be converted into a linear sketch with only logarithmic loss in space complexity. In [AHLW16], this result was extended to strict turnstile streaming algorithms, that is algorithms which require that $\sum_{i=1}^{s} v_i \geq 0$ for each $s \leq t$.

These results come with two important caveats. Firstly, they do not necessarily give an $O(d \log n)$-space streaming algorithm, as neither the linear transformation $A$ nor the post-processing function $g$ is known to be calculable in $O(d \log n)$ space. However, our sketching lower bounds will be based on communication complexity arguments that bound the size of the sketch vector, circumventing this issue.

Secondly, [LNW14a] assumes that the turnstile algorithm in question works regardless of the value of the partial sums $\sum_{i=1}^{s} v_i$, while [AHLW16] only requires that these sums be non-negative. Therefore, our lower bounds do not rule out the possibility of a turnstile algorithm that requires every partial sum to form a valid graph (i.e. edges can neither be deleted before they arrive, nor can they arrive multiple times before being deleted). However, existing turnstile algorithms do not typically require this property—in particular, any sampling-based algorithm, whether adaptive or non-adaptive, can handle it by the addition of a counter to each stored edge.

B. Our Results

a) Lower bound.: We show that any linear sketching algorithm for triangle counting requires $\Omega(\frac{m^{2/3}}{T^{1/3}})$ space, even for constant degree graphs. Such a result is not true for the insertion-only model, where triangles can be counted in graphs with max degree $d$ in $O(md^2/T)$ space by subsampling the edges at rate $d/T$ and storing all subsequent edges that touch the sampled edges [JG05].

Our result generalizes to counting the number of copies of any constant-size connected subgraph $H$. Such problems appear, for example, in estimating the size of database joins when planning queries [AGM08]. We show that the linear sketching complexity of distinguishing between 0 and $T$ copies of $H$ in constant-degree graphs is at least

$$\Omega\left(\frac{m}{T^{1/\tau}}\right)$$

where $\tau$ is the fractional vertex cover number of $H$, the minimum value such that there exists $f : V(H) \rightarrow [0,1]$ with $\sum_{v \in V(H)} f(v) \leq \tau$ and $f(u) + f(v) \geq 1$ for all $uv \in E(H)$.

b) Upper bound.: We also give a matching upper bound: by subsampling the vertices with probabilities dependent on their weight in the fractional vertex cover, we give an algorithm that estimates $T$ using $O(m/T^{1/\tau})$ words of space, as long as the graph has constant degree. Additionally, the constant-degree restriction can be lifted for many graphs: if an optimal fractional vertex cover of $H$ can place nonzero weight on every vertex (as occurs, for example, if $H$ is a cycle) then the algorithm works for degree up to $T^{1/(2\tau)}$ graphs.

c) Hypergraph counting.: Both our upper and lower bounds extend to counting hypergraphs $H$, but the exponent on $T$ no longer matches for all hypergraphs. The upper bound remains $O(m/T^{1/\mu})$, while the lower bound becomes $O(m/T^{1/\mu})$ for an exponent $\mu$ that equals the fractional vertex cover number $\tau$ on many hypergraphs but not all.

All of our results extend to $\varepsilon \ll 1$; the full statements of these results are given in Theorem 12 for the upper bound, Theorem 7 for the general lower bound, and Corollary 11 for the tight lower bound specific to non-hypergraphs.

C. Sampling and Sketching

Our upper bounds will take the form of non-adaptive sampling algorithms. By “sampling algorithm” we mean that the only state maintained between updates is a subset of the input edges, and by “non-adaptive” we mean that the probability of keeping an edge does not depend on which other edges have been seen so far in the stream.

Non-adaptive sampling algorithms may be modified into linear sketching algorithms by the use of $L_\infty$-sampler sketches. An $L_\infty$-sampler sketch is a linear sketch which, if $v$ is the frequency vector of the input stream, returns a non-zero co-ordinate of $v$, chosen uniformly at random (more generally, an $L_p$-sampler samples $v_i$ with probability proportional to $|v_i|^p$). A linear sketching algorithm for this problem was first presented in [CMR05], while [MW10] defined $L_p$ sampling and gave algorithms for all $p \in [0,2]$.

In [JST11], it was shown that, if the set to be sampled from has size $n$ and the sample is required

\cite{Note1}

Note that this does not mean that the edges are sampled independently of one another—for instance, if we choose a vertex at random and keep all edges incident on that vertex, the event that we keep the edge $uv$ is independent of whether the edge $vw$ is present in the stream, but it is not independent of the event that we keep the edge $uw$. 

557
to be within $\delta$ of uniform for some constant $\delta$, the space required is exactly $\Theta(\log^2 n)$. In [KNP+17], the optimal bound in terms of $n$ and $\delta$ was shown to be $\Theta\left(\min\left(n, \log\left(\frac{1}{\delta}\right) \log^2\left(\frac{n}{\log(1/\delta)}\right)\right)\right)$.

Therefore, as our sketching lower bound and sampling upper bounds match up to polylog factors, it follows that both are themselves tight up to polylog factors.

D. Our Techniques

The core of our lower bound proof is a new set of Fourier analytic techniques for analyzing multiplayer simultaneous communication protocols. Our approach is inspired by the Fourier analytic analysis of the Boolean Hidden Matching problem, but develops several new ideas that we think are likely to find applications beyond subgraph counting lower bounds. We now proceed to describe the Boolean Hidden Matching problem, the main ideas behind its analysis, and then describe our techniques.

The Boolean Hidden Matching problem of Gavinsky et al [GKK+07] is a two player one way communication problem where Alice holds a binary string $x \in \{0, 1\}^n$ that she compresses to a message $m$ of $s$ bits and sends to Bob. Bob, besides the message from Alice, gets two pieces of input: a uniformly random matching of size $n/10$ on the set $\{1, 2, \ldots, n\}$, along with a vector of binary labels $w_e \in \{0, 1\}, e \in M$. In the YES case of the problem the vector $w$ satisfies $w = Mx$, and in the NO case of the problem the vector $w$ satisfies $w = Mx \oplus 1^{\lfloor M/2 \rfloor}$, where we abuse notation somewhat by letting $M$ denote the edge incidence matrix of the matching $M$ (where each column corresponds to a vertex, and each edge to a row, with ones in the two co-ordinates corresponding to the vertices the edge is incident to).

The Boolean Hidden Matching problem and the related Boolean Hidden Hypermatching problem of Verbin and Yu [VY11] have been very influential in streaming lower bounds: streaming problems that have recently been shown to admit reductions from Boolean Hidden (Hyper)Matching include approximating maximum matching size [EHL+15], [AKLY15], [AKL17], approximating MAX-CUT value [KKS15], [KK15], [KKSV17], subgraph counting [VY11], [KP17], and approximating Schatten $p$-norms [LW16], among others. Most recent streaming lower bounds (with the exception of [KKSV17]) use reductions from Boolean Hidden (Hyper)Matching, without modifying the Fourier analytic techniques involved in the proof.

In this paper we develop several new Fourier analytic ideas that go beyond the Boolean Hidden Matching problem in several directions:

a) Analyzing simultaneous multiplayer communication: In the Boolean Hidden Matching problem Alice is the only player transmitting a message, but our communication problem features simultaneous communication from multiple players to a referee. We show how to use the convolution theorem from Fourier analysis to analyze the effect of combining information sent by multiple players in the one way simultaneous communication model. While the technique of combining information from two players using the convolution theorem was recently used by [KKSV17] to analyze a three-player game, to the best of our knowledge our work is the first to analyze games with an arbitrary number of players in this manner.

b) Analyzing a promise version of a communication problem via Fourier analysis: While in the Boolean Hidden Matching problem Alice’s string is sampled from the uniform distribution, in our problem multiple players receive correlated binary strings (conditioned on a linear constraint over the binary field). It turns out that this specific form of conditioning lends itself naturally to a Fourier analytic approach due to the linearity of the constraints imposed on the strings, and analysing such correlated settings gives us tight bounds on the subgraph counting version of our problem.

c) Sharing $M$ among the players: In the Boolean Hidden Matching problem, only Bob has the linear function $M$, while Alice must send her message based only on $x$. In our communication problem each (hyper)edge in $H$ corresponds to a player, and every player receives a linearized set of edges, together with parities of a hidden string $x$ over these edges. Similarly to the Boolean Hidden Matching problem, these parities are either correct (YES case) or flipped simultaneously. A crucial new component, however, is the fact that instead of $M$ being held by the recipient alone, each player holds part of it, and the parts the players hold are correlated.

Analyzing such correlations is in fact necessary even if one only wants to prove a simple lower bound on the space complexity of ‘sampling-type’ algorithms for triangle counting. We show how to analyze such correlations when $H$ is an arbitrary hypergraph through a purely combinatorial lemma. The weights lemma (Section III) is primarily concerned with the ability of the players to co-ordinate “weight” functions. This can be used to lower bound the space complexity of sampling-based protocols—we apply it to bound the Fourier coefficients of the referee’s posterior distribution on the players’ inputs when the players send arbitrary messages.
E. Related Work

The past decade has seen a large amount of work on the space complexity of graph problems in the streaming model of computation (see, e.g. the recent survey by McGregor [McG17]). The semi-streaming model of computation, which allows $O(n)$ space to process a graph on $n$ vertices, has been extensively studied, with space efficient algorithms known for many fundamental graph problems such as spanning trees [AGM12a], sparsifiers [AG09], [KL11], [AGM12b], [KLM+14], matchings [AG11], [AG13], [GKK12], [Kap13], [GO12], [HRVZ15], [Kon15], [AKLY15], spanners [AGM12b], [KW14]. Beyond the semi-streaming model, it has recently been shown that it is sometimes possible to approximate the cost of the solution to a graph problem in the streaming model even when the amount of space available does not suffice to store the vertex set of the graph (e.g. [KKS14], [EHL+15], [CCE+15], [Cor17], [MV18], [PS18]). The problem of designing lower bounds for graph sketches has received a lot of attention recently due to the success of graph sketching as an approach to solving dynamic graph streaming problems (e.g., [LNW14b], [AKLY15], [AKL17]). Similarly to our approach, such lower bounds normally make use of the simultaneous communication model.  

a) Subgraph counting.: The streaming subgraph counting problem was introduced in [BKS02] for the case where $H$ is a triangle. This was followed by alternative algorithms in [BFL+06], [JG05]. The lower bounds in [BOV13] and [KP17] were achieved by reductions to one-way communication complexity problems, the indexing problem and the Boolean Hidden Matching problem, respectively. Triangle detection has also been studied as a pure communication problem, for instance [FGO17], as well as in the adjacency-list [KMPT10], [BFL+06], [MVV16], multi-pass [BOV13], [CJ14], and query models [ELRS15].

Work on counting non-triangle subgraphs includes [BFLS07], which presented an algorithm for counting copies of $K_{3,3}$, [BDGL08], which studied subgraphs of size 3 and 4, [MMP11], which studied cycles of arbitrary size, and [KMSS12], which studied arbitrary subgraphs. The problem has also been studied in the query [JSP15], [ANRD15], [PSV17] and distributed [ESBD15], [ESBD16] models.

b) Join size estimation.: The size of a database join can be viewed as a “labeled” version of hypergraph counting, where each vertex of $G$ can only match a particular vertex (“attribute”) of $H$, and each hyperedge of $G$ can only match a particular hyperedge (“relation”) of $H$. (Both our upper and lower bounds apply in this labeled setting.) In [AGM08] it was shown for a database $G$ with $m$ hyperedges, the size of the join given by a query $H$ can be up to $\Theta(m^\rho)$, where $\rho$ is the fractional edge cover number of $H$.

This result is from a very different regime from ours because it involves very dense graphs and ours involves sparse ones. But one intriguing connection is through the $\Omega(m/T^{2/3})$ lower bound given in [KP17] for the restricted class of “triangle sampling” algorithms. Generalizing that proof for arbitrary $H$ would use [AGM08] to get a lower bound of $\Omega(m \left( \frac{1}{\rho \cdot \tau} \right)^{\frac{1}{3}})$, as opposed to our $\Omega(m/T^{1/\tau})$ bound. These are the same for some graphs, such as odd cycles, where $\rho = \tau = |V|/2$, and $\Omega(m/T^{1/\tau})$ is stronger for sparse graphs, but the two bounds are incomparable in general. It seems possible that the sample complexity for dense graphs will depend on $\rho$ in some fashion.

II. PROOF OVERVIEW

A. Lower Bound

For a fixed graph $H$ with fractional vertex cover $\tau$, we prove an $\Omega(n/T^{1/\tau})$ lower bound for determining whether a constant-degree graph on $\Theta(n)$ vertices has 0 or $\Theta(T)$ copies of $H$. For illustration, in this section we focus on the case where $H$ is a triangle.

We consider the three-party simultaneous-message communication problem illustrated in Figure 1, where each player is associated with an edge of $H$. First, we construct a set of $N = \Theta(n)$ vertices $V_u$ for each vertex $u \in H$. The player associated with edge $e = (u,v)$ receives an input consisting of $n$ disjoint edges on $V_u \times V_v$, along with binary labels associated with each edge. We are guaranteed that the three players’ inputs collectively contain $T$ triangles, with all the other edges disjoint. Each set of vertices are randomly permuted so that the players do not know which of their edges participate in triangles.

We also guarantee that the XOR of the labels associated with a triangle is the same for every triangle—either every triangle has an even number of 1s, or an odd number. The goal of the players is to send messages to a referee who knows the edges but not their labels, and for the referee to figure out if every triangle has an odd number of 1 labels.

We will show that a uniformly random instance of this problem requires $\Omega(n/T^{2/3})$ communication for the referee to succeed $2/3$ of the time. At the same time, it directly reduces to triangle counting: each player sketches their edges labeled 0 and sends the sketch to the referee. The referee adds the linear sketches up to get a sketch of all 0-labeled edges in the graph. This subgraph either contains zero triangles (if every triangle has an
Player 1

Player 2

Player 3

(a) Input for triangle-counting before permutation. Each player $e$ sees $n$ edges with associated binary labels (pictured as solid/dashed). The edges match up into $T$ triangles (center) and $n - T$ isolated edges (outside). The goal is to determine whether every triangle has an even number of solid edges, or an odd number.

(b) In the hard distribution, we randomly permute the vertices on top, on left, and on right. Each player sees their edges, with associated labels, in a random order; they do not see the pre-permutation vertex identities (represented by color).

Fig. 1: Lower bound instance for triangle counting

odd number of 1s) or very close to $T/4$ (otherwise), so successfully counting triangles will distinguish the two cases.

Our lower bound for the communication problem consists of two main pieces. First, we give a combinatorial lemma that bounds the players’ ability to co-ordinate any assignment of “weights” to edges or subsets of edges, based on the structure of the graph. Then we use Fourier-analytic techniques to extend this to a lower bound of the communication required by any protocol for the problem.

a) Combinatorial lemma: One approach the players could take to solve the problem would be for each player to look at their $n$ edges and pick a $p$ fraction to send to the referee. If the referee receives a complete triangle, he can solve the problem. What is the expected number of triangles the referee receives, if the players coordinate optimally?

The naive solution where players pick independently at random would yield $p^3T$ triangles. Vertex sampling—picking a $\sqrt{p}$ fraction of vertices, for example those of smallest index, and only sampling edges between picked vertices—increases this to $p^{3/2}T$. In [KP17], a simple counting argument showed that “oblivious” strategies, which decide whether to sample an edge based only on the edge and not the rest of the player’s input, cannot do better than this.

The combinatorial lemma we need for the Fourier-analytic proof is a stronger, generalized version of this sampling lemma. It considers players that receive some private randomness $\psi_e$ and partially-shared randomness $\phi_u$ for each $u \in e$, and output an arbitrary deterministic function

$$g_e = g_e(\psi_e, (\phi_u)_{u \in e}) \in [-1, 1]$$

of their inputs. If the $\phi_u$ are fully independent and the $\psi_e$ are $(|E| - 1)$-wise independent, and

$$\max_e \mathbb{E}_{\psi, \phi} [g_e^2] \leq p$$

for some $p$, then we show:

$$\mathbb{E}_{\psi, \phi} \prod_e g_e \lesssim p^{3/2}. \quad (1)$$

To relate this to sampling, we note that the communication problem in Figure 1 can be constructed with randomness in the form above: $\phi_u$ contains the permutation of the vertices $V_u$ associated with $u$, and $\psi_e$ contains player $e$’s edge labels $x_e$ (which are 2-wise independent) and the random order $\pi_e$ in which they see their edges. Consider picking a random triangle edge $s \in [T]$ and adding to $\psi_e$ the index of $s$ in player $e$’s list. (One can show that $\psi_e$ remains pairwise independent,
despite the shared dependence on \( s \).

If we only allow \( g_e \in \{0, 1\} \), then we can think of \( g_e \) as the event that player \( e \) samples their edge in the \( s \)th triangle. The condition on \( \mathbb{E} [g_e^2] \) says that each player can pick at most a \( p \) fraction of their edges, on average over their inputs. The conclusion is that the expected fraction of triangles completely sampled is at most \( p^{3/2} \).

This combinatorial lemma is different from the simple sampling lemma of [KP17] in several ways. First, it allows players to look at their entire inputs before deciding which edges to keep. Second, while the lemma of [KP17] was based on defining a fixed subset of edges to keep (so the number kept depended only on which edges were seen), in our lemma the players only need to keep a \( p \) fraction of their inputs on average, but the players do not have shared randomness. If they shared randomness, there would be a trivial counterexample: with probability \( p \) every player samples every edge, giving the referee \( p^2 \) triangles in expectation. Without shared randomness, they can still use the correlation of their input for nontrivial algorithms: for example, for \( p = 2^{1-n} \) they can send their entire input if every edge has the same label; because of the promise, if two players sample their inputs then the third is much more likely to. But this coordination is less effective than vertex sampling.

The combinatorial lemma is also more general, in ways that are important for the Fourier-analytic component of the proof. It allows for “fractional” choices of edges \( g_e \in [-1, 1] \), with an \( \ell_2 \) constraint. This allows for alternative competitive strategies—for example, placing \( \sqrt{p} \) weight on every edge also yields \( p^{3/2} \)—but no strictly better ones. Additionally, the lemma will extend to cases where instead of placing weight on individual edges, the players place weight on sets of \( k \) triangle edges for some \( k \geq 1 \). These will correspond to weight \( k \) Fourier coefficients.

b) Fourier-analytic argument: Our approach for lower bounding the communication problem is inspired by [GKK+07]. Let \( x_e \in \{0, 1\}^n \) be the player \( e \)'s labels before permutation (i.e., from Figure 1a). We consider the referee’s posterior distribution \( p \) on the triangle parities, \( x_1^T \oplus x_2^T \oplus x_3^T \). \( p \) is supported on \( \{0^T, 1^T\} \), and our goal is to show that it is nearly uniform.

First, we express the referee’s posterior distribution on the labels \( x = (x_e)_{e \in E} \). Let \( f_e(y) = 1 \) if player \( e \)'s message to the referee is consistent with \( x_e = y \), and 0 otherwise, and let \( f : \{0, 1\}^{|E|n} \rightarrow \{0, 1\} \) be given by \( f(x) = \prod_{e} f_e(x_e) \). The referee has two constraints on \( x \): the message consistency constraint \( f(x) \), and a parity constraint \( q(x) \). His posterior distribution is uniform on \( \text{supp}(f_q) \).

The first observation we make relates the referee’s total variation distance to the Fourier spectrum of \( f_q \). For indicator functions \( g : \{0, 1\}^m \rightarrow \{0, 1\} \), it makes sense to consider the renormalized Fourier transform

\[
\tilde{g}(s) := \frac{2^n}{|\text{supp}(g)|} \tilde{g}(s) = \mathbb{E}_{x \in \text{supp}(g)} [(-1)^{x \cdot s}].
\]

With this normalization, we observe that

\[
\Delta := \|p - \mathcal{U}(\{0^T, 1^T\})\|_{TV} = \frac{1}{2} \tilde{f}(e_1, e_1, e_1)
\]

where \( e_1 = (1, 0, \ldots, 0) \in \{0, 1\}^n \). Using the structure of \( \mathbb{g} \)'s spectrum and the Fourier convolution theorem, we turn this into

\[
\Delta = C \sum_{|t| = 1 \text{ mod } 2} \prod_{e} \tilde{f}_e(t n - T)
\]

where \( C \) is a normalising factor that is constant in expectation over the input. The bound is, for some constant \( D > 0 \),

\[
D \left( \frac{T}{k} \right)^{3/2} \left( \max_e \left( \frac{1}{n} \right) \mathbb{E} \left[ \sum_{s \in \{0, 1\}^n \text{ with } |s| = k} \tilde{f}_e(s)^2 \right] \right)^{3/2}
\]

which can be bounded in terms of the players’ \( c \) bits of communication by the KKL lemma (for small \( k \)) and Parseval’s identity (for high \( k \)). See the full version of the paper [KKP18] for statements of the bounds used. The dominant term when summing over \( k \) is \( k = 1 \) whence we get that the referee’s total variation distance has

\[
\mathbb{E}[\Delta] \lesssim T(c/n)^{3/2}.
\]

This implies the players must send at least \( n/T^{2/3} \) bits to distinguish the two cases with significant probability.

c) Changes for non-triangle graphs: For counting general (hyper)graphs, the combinatorial lemma as described gives a bound of \( p^{\text{MVC}_{1/2}(H)} \), where \( \text{MVC}_{1/2}(H) \) is a “modified” fractional vertex cover in which weight can be placed directly on edges for half price. For odd cycles such as triangles, \( \text{MVC}_{1/2}(H) \) equals the non-modified fractional vertex cover \( \tau \), giving the desired \( \Omega(n/T^{1/\tau}) \) bound.

For other graphs, such as the length-3 path, \( \text{MVC}_{1/2}(H) \) can be less than \( \tau \) leading to a suboptimal result. For these graphs we use a somewhat different proof, in which the referee is identified with a particular edge \( e^* \) in the graph. The other players’ inputs are then completely independent of one another, with no promise
on the XOR of their labels. We follow a slightly different Fourier-analytic approach that requires bounding

\[ E \left[ \prod_{e \notin e^*} \tilde{f}_e^2 \right] . \]

rather than \( E \left[ \prod_{e} \tilde{f}_e \right] . \) We apply the combinatorial lemma to the \( \tilde{f}_e \), on which we have an \( \ell_1 \) constraint, giving us the bound

\[ E \left[ \prod_{e \notin e^*} \tilde{f}_e^2 \right] \leq p^{MVC_1(H \setminus e^*)} \]

where the exponent is the non-modified fractional vertex cover of \( H \setminus e^* \). This gives a lower bound of \( \Omega(n/T^{1/MVC_1(H \setminus e^*)}) \). For every connected (non-hyper)graph \( H \) that is neither an odd cycle nor a single edge, this equals \( \Omega(n/T^{1/\tau}) \) for every connected graph with more than one edge. For hypergraphs, the individual lower bounds still hold, but their maximum is not necessarily \( \Omega(n/T^{1/\tau}) \).

For graphs that are single edges or odd cycles, \( MVC_{1/2}(H) = \tau \), and so the combination of these bounds gives \( \Omega(n/T^{1/\tau}) \) for every connected graph with more than one edge. For hypergraphs, the individual lower bounds still hold, but their maximum is not necessarily \( \Omega(n/T^{1/\tau}) \).

d) Dependence on \( \varepsilon \): The above approach is a lower bound for distinguishing \( T \) triangles from 0 triangles. Distinguishing \( T \) triangles from \((1 - \varepsilon)T \) triangles should require more space for small \( \varepsilon \). In the non-promise version of the proof used for graphs that are not odd cycles, we use the noise operator, an operator that takes a binary function and “noises” it by randomly flipping input bits, to get an \( \varepsilon^{-2/\tau} \) dependence. In the promise version, the bound we get is only \( \varepsilon^{-1/\tau} \).

B. Upper Bound

For purposes of this overview, we describe a sampling algorithm for the “labeled” version of the problem used in join size estimation, where edges and vertices in \( G \) correspond to edges and vertices in \( H \), and we only want to count subgraphs with matching labels. Since \( H \) has constant size, we can solve the non-labeled version by trying many random labelings.

Consider a hypergraph \( H \) with minimal fractional vertex cover \( f \), so \( f(u) \in [0, 1] \) for each vertex \( u \in V_H \) and \( \sum_u f(u) = \tau \). Let \( \chi : V_G \to V_H \) be the labels. For a parameter \( p \in (0, 1) \) to be determined later, we sample each vertex \( v \in V_G \) with probability \( p^{f(\chi(v))} \), and we keep a hyperedge \( e \in E_G \) if and only if we sample all \( v \in e \).

The chance we keep any given copy of \( H \) is \( \prod_{u \in H} p^{f(u)} = p^\tau \). Therefore, if we set \( p = 100/T^{1/\tau} \), the expected number of copies of \( H \) we see will be \( p^T \geq 100 \). On the other hand, the chance we keep any single edge \( e \) is \( \prod_{e \in E} p^{f(\chi(e))} \leq p \), because \( f \) covers the edge associated with \( e \) and so \( \sum_{e \in E} f(\chi(e)) \geq 1 \). This gives a algorithm with \( O(mp) = O(m/T^{1/\tau}) \) space that sees \( p^T \geq 100 \) copies of \( H \) in expectation; from this \( T \) can be estimated.

The only tricky bit is to show that the variance of the number of sampled copies of \( H \) is small. We bound this in terms of the maximum degree of \( G \) and the maximum correlation between sampling two copies of \( H \) in \( G \). If this correlation is 1 as can happen in general, the sampling algorithm only works for constant-degree graphs. However, if the vertex cover places at least 0.5 weight on each vertex of \( H \), then the correlation is at most \( \sqrt{\beta} = \Theta(T^{1/(2r)}) \). This lets the algorithm work for degree \( O(T^{1/(2r)}) \) graphs. In the case of triangles, this \( O(T^{1/3}) \) degree bound is the correct regime for \( O(m/T^{2/3}) \) samples to be possible—above this threshold, the maximum number of triangles sharing a single vertex can be larger than \( T^{2/3} \) and so the \( \Omega(m\sqrt{\Delta}/T) \) lower bound of \( [KP17] \) precludes it.

III. The Weights Lemma

**Definition 1.** For a weighted hypergraph \( H = (V, E) \) with weights \( w : E \to [0, \infty) \), we define the \( \lambda \)-modified fractional vertex cover number \( MVC_\lambda(H, w) \) to be:

\[ MVC_\lambda(H, w) = \min_f \left( \sum_{v \in V} f(v) + \lambda \sum_{e \in E} f(e) \right) \]

over all \( f : V \cup E \to [0, \infty] \) satisfying

\[ \sum_{v \in e} f(v) + f(e) \geq w(e) \quad \forall e \in E. \]

When \( w \) is omitted, it is assumed that \( w(e) = 1 \) for all \( e \). We note that \( MVC_\lambda(H) \) equals the standard fractional vertex cover number of \( H \) whenever \( \lambda \geq 1 \) and \( H \) has no empty hyperedges.

**Definition 2.** (Totally disconnected hypergraph). For a hypergraph \( H = (V_H, E_H) \) we say that \( H \) is totally disconnected if edges of \( H \) are pairwise disjoint, i.e. for every \( a, b \in E \) one has \( a \cap b = \emptyset \).

**Lemma 3.** Consider any hypergraph \( H = (V, E) \) and weight function \( w : E \to [0, \infty] \). Suppose that \( H \) is not totally disconnected as per Definition 2, i.e., there exist \( a, b \in E \) such that \( a \cap b \neq \emptyset \).

Consider any collection of random variables \( g_e \) (for \( e \in E \)) that can be expressed as deterministic functions of some random variables \( \phi_u \) (for \( u \in V \)) that are
independent, and $\psi_e$ (for $e \in E$) that are independent of the $\phi_u$ and $(|E| - 1)$-wise independent themselves, i.e.,
$$g_e = g_e(\psi_e, (\phi_u)_{u \in e}).$$

Let $q \in \{1, 2\}$ and $0 < p < 1$, and suppose for all $e \in E$ that $|g_e| \leq 1$ always and that
$$E[|g_e|^q] \leq p^w(e).$$
Then
$$E\left[\prod_{e \in E} g_e\right] \leq d^{1/q} p^{MVC_{1/q}(H, w)}$$
where $MVC_{1/q}(H, w)$ is the modified fractional vertex cover number per Definition 1, and $d$ is the maximum of 1 and the greatest degree of a vertex $v \in V$.

The proof is deferred to the full version of the paper [KKP18].

IV. HYPERGRAPH COUNTING WITH A PROMISE

In both of the games that follow, we will assume that the players are deterministic. This is without loss of generality by Yao’s minimax principle since the inputs are sampled from a fixed distribution.

A. Game

We will define a $|E| + 1$-player game PromiseCounting($H, n, T, \varepsilon$) (with $H$ a hypergraph, $n, T \in \mathbb{N}, \varepsilon \in \{1/T, 2/T, \ldots, 1\}$), as follows: There is one referee, who receives messages from every other player. No other communication takes place. Each player besides the referee corresponds to an edge $e \in E$.

Let $N = T + (n - T)|E|$. For each edge $e \in E$, let $L_e \subseteq [N]$ be an $n$-element set containing $[T]$ and $n - T$ elements disjoint from every other $L_e$, so that if $a \neq b$, $L_a \cap L_b = [T]$, and $\bigcup_{e \in E} L_e = [N]$. For each $e \in E$, let $\rho_e : [n] \to L_e$ be a fixed bijection such that $\rho_e([T])$ is the identity.

An instance of PromiseCounting($H, n, T, \varepsilon$) is as follows:

- For each edge $e \in E$:
  - A string $x_e \in \{0, 1\}^n$.
  - A permutation $\pi_e$ on $L_e$.
- For each vertex $v \in V$:
  - A permutation $\pi_v$ on $[N]$.
- A string $\tau \in \{0^T, 1^T\}$

The players have the following promise:
$$\bigoplus_{e \in E} x_e^{1:|T|} = \tau$$

We will write $X$ for the strings $(x_e)_{e \in E}$, $\Pi_E$ for the permutations $(\pi_e)_{e \in E}$, and $\Pi_V$ for the permutations $(\pi_v)_{v \in V}$. They have access to the following information:

- For each player $e \in E$:
  - $x_e \rho_e \pi_e$
  - $(\pi_v(\pi_e^{-1}(i)))_{v \in e, i \in L_e}$
- For the referee:
  - $\Pi = (\Pi_E, \Pi_V)$

Given the messages received from the players, the referee’s task will be to determine whether $\tau = 0^T$ or $\tau = 1^T$.

B. Hard Instance

We will lower bound the complexity of this problem under the following hard input distribution: $\tau$ is chosen uniformly from $\{0^T, 1^T\}$, and then the strings $(x_e)_{e \in E}$ are chosen uniformly from:
$$\left\{(x_e)_{e \in E} \in \{0, 1\}^{|E|} : \bigoplus_{e \in E} x_e^{1:|T|} = \tau\right\}$$

Every permutation $\pi_u, \pi_v$ is chosen uniformly at random and independently of each other and the strings.

C. Lower Bound

For each player $e$, write $m_e(x_e \rho_e \pi_e), (\pi_v(\pi_e^{-1}(i)))_{v \in e, i \in L_e}$ for the message the player sends to the referee on seeing $x_e \rho_e \pi_e$ and $(\pi_v(\pi_e^{-1}(i)))_{v \in e, i \in L_e}$.

Theorem 4. Let $H$ be a connected hypergraph with more than one edge. Let $c \in [n]$. Suppose that, for all inputs $(X, \Pi)$ to the game, no player sends a message of more than $c$ bits, and suppose that $cT \leq n/10$.

Let $p : \{0^T, 1^T\} \to [0, 1]$ be the referee’s posterior distribution on $\tau$. Let $\nu$ be the distribution of $U\{\{0^T, 1^T\}\}$, the uniform distribution on the two-element set $\{0^T, 1^T\}$. Let $\mu = MVC_{1/2}(H)$, and let $0 < \delta < 1$.

There exists a constant $\gamma$, depending only on $H$, such that, if $c \leq \gamma (q^{1/2} T)^{1/p}$:
$$E_{X, \Pi} \left[||p - \nu||_{TV}\right] \leq \delta$$

Corollary 5. Let $H$ be a connected hypergraph with more than one edge. Let $c \in [n]$. Suppose that, for all inputs $(X, \Pi)$ to PromiseCounting($H, n, T, \varepsilon$), no player sends a message of more than $c$ bits.

Let $\mu = MVC_{1/2}(H)$, and let $0 < \delta < 1$.

There exists a constant $\gamma$, depending only on $H$, such that, if $c \leq \gamma (q^{1/2} T)^{1/p}$, the players succeed at the game with probability at most $1/2 + \delta$. 

563
The proofs are deferred to the full version of the paper [KKP18].

V. HYPERGRAPH COUNTING WITH NO PROMISE

We also study a slightly different game, in which the XOR of the strings \( x_e \) may take any value, but the referee has a “target” string that is guaranteed to either be \( \bigoplus_{e \in E} x_e^1 \) or \( \bigoplus_{e \in E} x_e^2 \). This will give a different, and in general incomparable lower bound for subgraph counting. For further details, see the full version of the paper [KKP18].

VI. LINEAR SKETCHING LOWER BOUND

**Definition 6.** Let \( A \) be a randomized graph streaming algorithm, and let \( S \) be the set of possible states \( S \) of \( A \). We will say \( A \) has composable state if, for any fixed random seed for \( A \), there is a function \( c : S \times S \rightarrow S \) such that, if \( S_1 \) is the state of \( A \) after receiving the stream of edges \( E_1 \) as input, and \( S_2 \) is the state of \( A \) after receiving the stream of edges \( E_2 \) as input, \( c(S_1, S_2) \) is the state of \( A \) after receiving the concatenation of \( E_1 \) and \( E_2 \) as input.

**Theorem 7.** Let \( H = (V, E) \) be a (fixed) connected hypergraph with \( |E| > 1 \). Let \( T \in \mathbb{N} \), \( \varepsilon \in (1/\sqrt{T}, 1] \). Let \( A \) be a graph streaming algorithm that can distinguish between graphs \( G \) presented as a stream of edges with at least \( T \) copies of \( H \) and graphs with at most \( (1-\varepsilon)T \) copies of \( H \) with probability \( 99/100 \), provided \( G \) has no more than \( m \) edges. Let \( S(m) \) be the maximum space usage of \( A \) across all \( m \)-edge inputs.

Furthermore, let \( A \) have composable state. Then, for all \( m \geq O(T) \):

\[
S(m) = \Omega \left( \max \left( \frac{m}{(\varepsilon T)^{1/\mu_2}}, \frac{m}{(\varepsilon^2 T)^{1/\mu_1}} \right) \right)
\]

where \( \mu_2 = MVC_1(H) \) and \( \mu_1 = \max_{e \in E} MVC_1(H \setminus e) \), with constants that may depend on \( H \) but nothing else.

We will prove this by reductions to PromiseCounting and Counting.

**Lemma 8.** \( \forall m \geq O(T), S(m) = \Omega \left( \frac{m}{(\varepsilon T)^{1/\mu_2}} \right) \)

**Lemma 9.** \( \forall m \geq O(T), \forall e^* \in E, S(m) = \Omega \left( \frac{m}{(\varepsilon T)^{1/\mu_1}} \right) \) where \( \mu_1 = MVC_1(H \setminus e^*) \).

The proofs are deferred to [KKP18].

Theorem 7 then follows directly from the previous two lemmas.
To prove this gives tight bounds (for \( \varepsilon \) constant) for all 2-uniform hypergraphs (that is, all graphs), we will need the following lemma on graph covers:

**Lemma 10.** Let \( G = (V, E) \) be a connected graph with \(|E| > 1\). Then:

\[
\max(MVC_2(G), \max_{e \in E} MVC_1(G \setminus e)) = MVC_1(G)
\]

is the standard fractional vertex cover of \( G \).

The proof is deferred to [KKP18].

**Corollary 11.** Let \( H = (V, E) \) be a connected graph with \(|E| > 1\). Let \( \varepsilon \in (0, 1), T \in \mathbb{N} \). Let \( A \) be a graph streaming algorithm that can distinguish between graphs \( G \) presented as a stream of edges with \( T \) copies of \( H \), graphs with \((1 - \varepsilon)T\) copies of \( H \) with probability 99/100, provided \( G \) has no more than \( m \) edges. Let \( S(m) \) be the maximum space usage of \( A \) across all \( m \)-edge inputs.

Furthermore, let \( A \) have composable state. Then:

\[
\forall m \geq O(T), S(m) = \Omega\left(\frac{m}{(\varepsilon T)^{1/\tau}}\right)
\]

where \( \tau \) is the fractional vertex cover of \( H \), and the constant factor may depend on \( H \) but nothing else.

**VII. Upper Bound**

Our main result is

**Theorem 12.** For every hypergraph \( H = (V_H, E_H) \), \( \varepsilon \in (0, 1) \) there exists a sketching algorithm that, for any hypergraph \( G = (V_G, E_G) \) on \( n \) vertices with degrees bounded by \( d \), approximates the number of copies of \( H \) in \( G \) to within \( 1 + \varepsilon \) multiplicative factor with probability at least 99/100 using space \( s \leq C \cdot \varepsilon^{-2/\tau} \cdot mT^{-1/\tau} \), where \( T \) is the number of copies of \( H \) in \( G \) and \( \tau \) is the fractional vertex cover of \( H \) and \( C \) is a constant that depends on \( H \).

For graphs we get a more powerful result, which allows the graph \( G \) to have higher degrees:

**Theorem 13.** For every graph \( H = (V_H, E_H) \) that admits a minimum vertex cover that assigns nonzero weight to every vertex, for every \( \varepsilon \in (0, 1) \) there exists a sketching algorithm that, for any graph \( G = (V_G, E_G) \) on \( n \) vertices with degrees bounded by \( d \leq C' \varepsilon^{1/\tau} T^{1/(2\tau)} \), approximates the number of copies of \( H \) in \( G \) to within \( 1 + \varepsilon \) multiplicative factor with probability 99/100 using space \( C' \varepsilon^{-2/\tau} \cdot mT^{-1/\tau} \), where \( T \) is the number of copies of \( H \) in \( G \) and \( \tau \) is the fractional vertex cover of \( H \), and \( C, C' > 0 \) are constants that depend only on \( H \).

This result requires the minimum vertex cover to assign nonzero weight to every vertex; this happens for cycles but not stars.

Consider the fractional vertex cover of \( H \)

\[
\min \sum_{a \in V_H} x_a \quad \text{s.t.} \sum_{a \in e} x_a \geq 1 \text{ for all } e \in E_H,
\]

let \( x^* \in \mathbb{R}^{V_H} \) denote an optimal solution and let \( \tau \) denote its value.

Fix a mapping \( \chi : V_G \to V_H \) (see Algorithm 1, line 3). For a subset \( S \subseteq V_G \) we write \( \chi(S) \sim H \) if the subgraph induced by \( S \) equipped with labels \( \chi(S) \) contains a copy of \( H \), i.e. for every \( a \subseteq S \) one has that if \( \chi(a) \in E_H \), then \( a \in E_G \). Note that, if \( (A(H)) \) is the number of automorphisms of \( H \), the probability that a randomly chosen \( \chi \) will give \( \chi(S) \sim H \) is \((A(H))/k^k\).

**Algorithm 1** Subgraph counting by vertex sampling

1. \( \text{procedure SAMPLE}(H, p) \) \( \triangleright \) Input: hypergraph \( H \), sampling probability \( p \)
2. \( \chi \sim UNIF([k]^{|V_G|}) \) \( \triangleright \) Random mapping of \( V_G \) to \( V_H = [k] \)
3. \( \text{for } u \in V_G \text{ do} \)
4. \( a \leftarrow \chi(u) \)
5. \( X_u \leftarrow \text{independent Bernoulli r.v. with mean } p_{u,a} \)
6. \( E' \leftarrow \{ e \in E_G : \chi(e) = |e| \text{ and } \prod_{u \in e} X_u = 1 \} \) \( \triangleright \) Keep colorful edges only
7. \( Z \leftarrow k^k \cdot p^{-\tau} \cdot \sum_{S \subseteq V_G : \chi(S) \sim H} \prod_{u \in S} X_u \) \( \triangleright \)
8. Knowing \( E' \) and \( \chi \) suffices to compute \( Z \)
9. \( \text{return } Z/(A(H)) \)
10. \( \text{end procedure} \)

This result follows from a variance-based analysis. For details, see the full version [KKP18].

**ACKNOWLEDGMENTS**

This work was done in part while John Kallaugher and Eric Price were visiting the Simons Institute for the Theory of Computing. Michael Kapralov is supported in part by ERC Starting Grant 759471-Sublinear.
REFERENCES


