Improving Sign-Random-Projection via Count Sketch

Abstract

Computing the angular similarity between pairs of vectors is a core part of various machine learning algorithms. The seminal work due to Charikar [Charikar, 2002] (*a.k.a.* Sign-Random-Projection (SRP) or SimHash) provides an unbiased estimate for the same. However, SRP suffers from the following limitations: (i) large variance in the similarity estimation, (ii) and high running time while computing the sketch. There are improved variants that address these limitations. However, they are known to improve on only one aspect in their proposal, for *e.g.* [Yu et al., 2014] suggest a faster algorithm, [Ji et al., 2012, Kang and Wong, 2018] provide estimates with a smaller variance. In this work, we propose a sketching algorithm that addresses both aspects in one algorithm – a faster algorithm along with a smaller variance in the similarity estimation. Moreover, our algorithm is space-efficient as well. We present a rigorous theoretical analysis of our proposal and complement it via experiments on synthetic and real-world datasets.

1 INTRODUCTION

High-dimensional datasets are ubiquitous in many real-life applications. Performing analytics on such datasets is tedious and, at times impossible due to the *curse of dimensionality*. The dimensionality reduction or sketching algorithms suggest provably algorithmic techniques that compress the high dimensional dataset into low dimensions while preserving pairwise similarity measures such as JL lemma [Johnson and Lindenstrauss, 1983] for real-valued vectors and pairwise euclidean distance, Minhash [Broder et al., 1998] for sets and pairwise Jaccard similarity.

In this work, we focus on the sketching algorithm for real-valued data that approximates pairwise cosine similarity. The seminal work due to Charikar [Charikar, 2002] suggest an algorithm for this task which has been extensively used in applications such as detecting near-duplicates [Manku et al., 2007, Henzinger, 2006], Spam-email detection [Ho et al., 2014]. Their algorithm compresses large-dimensional datasets into low-dimensional binary vectors such that the Hamming distance between the sketched vectors gives an unbiased estimate of the pairwise cosine similarity. Let $\vec{a}, \vec{b} \in \mathbb{R}^D$ such that the angle between them is $\theta_{(\vec{a},\vec{b})}$, and let $\mathcal{H} = \{h^{(i)}(\cdot)\}_{i\geq 1}$ denote the family of hash function stated as follows:

$$h^{(i)}(\vec{a}) = \begin{cases} 1, & \text{if } \langle \vec{a}, \vec{r_i} \rangle \geq 0. \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

where $\vec{r_i} = \langle r_{i1}, \ldots, r_{ij}, \ldots, r_{iD} \rangle \in \mathbb{R}^D$ such that $r_{ij} \sim \mathcal{N}(0,1)$. Repeating the step stated in Equation (1) K times, and concatenating the corresponding hash values gives a K dimensional binary vector corresponding to the input vector. Let X be the estimator random variable for the estimate of cosine similarity by SRP defined as:

$$\begin{aligned} X &= \frac{\pi}{K} \sum_{i=1}^{K} X^{(i)}, \text{where } X^{(i)} = \mathbb{1}_{h^{(i)}(\vec{a}) \neq h^{(i)}(\vec{b})}. \\ \mathbb{E}[X] &= \theta_{(\vec{a},\vec{b})}. \\ \text{Var}[X] &= \frac{\theta_{(\vec{a},\vec{b})}\left(\pi - \theta_{(\vec{a},\vec{b})}\right)}{K}. \end{aligned} \tag{2}$$

SRP can also be seen as a multiplication of the projection matrix (of dimension $K \times D$) with input vectors. Thus, the running time and space required (by the projection matrix) to compute the sketch per data point is $O(DK)$. This highlights the following limitations of SRP: (i) higher running time and space requirement, especially when the data dimension D is large, and (ii) high variance, when sketch dimension K is smaller, and also when pairwise angle of data points is close to $\pi/2$.

Submitted to the 38th Conference on Uncertainty in Artificial Intelligence (UAI 2022). **To be used for reviewing only**.

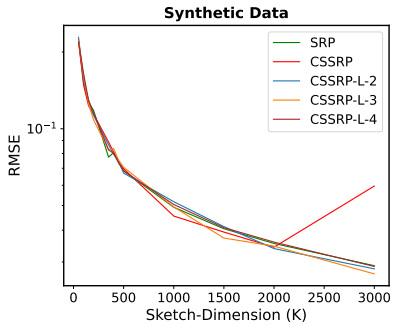

Figure 1: RMSE for similarity estimation on a pair of points. Original dimension of points is 10^4. A smaller RMSE indicates better performance.

Previously known improved variants of SRP**:** There are several results that address some of these limitations of SRP. The result of [Yu et al., 2018, 2014] a.k.a. CBE gives a faster and space efficient algorithm for the task, but its variance remains the same as of SRP, whereas method proposed by [Kang and Wong, 2018] (MLE) and [Ji et al., 2012] (SuperBit) reduces the variance but at the cost of higher running time than SRP. We present an elaborated discussion in Section 2.

To the best of our knowledge, there is no work that addresses all the limitations of SRP in the same sketching algorithm. In this work, we propose one such algorithm. Our key contributions are summarized as follows:

• Our first algorithm is COUNT-SKETCH SIGN-RANDOM-PROJECTION (CSSRP) that compresses high dimensional points into low dimensional binary vectors and closely approximates pairwise cosine similarity, offer a faster running time and simultaneously provide a significantly smaller variance than SRP. At a high level, the CSSRP is inspired from COUNT SKETCH [Charikar et al., 2004a] algorithm, where we first apply the COUNT SKETCH algorithm on the input vectors and then compute the sign of the resultant sketch vector. The similarity estimation step remains exactly the same as SRP (Definition 2). Note that our algorithm can be seen as projecting the input vector on a $K \times D$ projection matrix (whose each column has exactly one non-zero entry at the index randomly sampled from $\{1, \ldots K\}$, and takes value between $\{\pm 1\}$ with probability $1/2$), and computing the sign of the resultant K-dimensional vector. However, the mentioned improvement of CSSRP holds when the sketch dimension $K = o(D)$ (Theorems 5, 6).

• To alleviate the limitation of CSSRP mentioned above, we propose another sketching algorithm, namely - COUNT SKETCH SIGNED RANDOM PROJECTION-L (CSSRP $-$ L) (Definition 8). The basic difference CSSRP $-$ L and CSSRP is in the process of generating the random projection matrix - each column of the projection matrix for CSSRP $-$ L has exactly l non-zero values (randomly sampled between $\{\pm 1\}$ with probability $1/2$) at randomly chosen positions, where $l \ll K$. CSSRP $-$ L offers significant variance reduction even for large K where $K = o(lD)$ (Theorems 9, 10). We summarise a quick comparison between CSSRP and CSSRP $-$ L using the standard RMSE metric in Figure 1. It is evident that for small values of K, CSSRP has a smaller RMSE. However, at higher values of K, its RMSE starts increasing, which gets settled by CSSRP $-$ L, even for very small values of l say $2, 3$. Furthermore, both proposals are space-efficient and require $O(D)$ and $O(lD)$ space for projection matrices, for CSSRP and CSSRP $-$ L, respectively, which is significantly less than that required by most baseline algorithms.

• We present our theoretical analysis in Section 4, and complement it via experiments (in Section 5) on synthetic and real-world datasets, on the metrics such as running time, similarity search, and variance analysis via box-plot. We observed a significant speedup (upto $3896\times$) in running time, while simultaneously offering a better performance on the remaining experiments. Our observation is that for small values of the sketch dimension K, CSSRP offers both significant speedup and smaller variance, whereas for large values of K CSSRP $-$ L performs similarly even for small values of $l = \{2, 3, 5\}$. We summarise a tabular comparison among the baselines on asymptotic sketching time, space complexity, and variance in Table 1.

2 RELATED WORKS

Our work focused on computing fast and accurate pairwise similarity between input vectors, which has been extensively studied; we summarized some of the related works below:

CBE: [Yu et al., 2014] proposed a faster algorithm to compute pairwise cosine similarity. Their algorithm employs a special kind of matrix called circulant matrix, which consists of a random vector $\vec{r} = (r_0, \ldots, r_i, \ldots, r_D)$, where $r_i \in \mathcal{N}(0, 1)$, and $d - 1$ vectors obtained via applying circular shift in $\vec{r}$. Their projection matrix is the matrix obtained via multiplication of the circulant matrix and a random diagonal matrix, whose entries are in $\{-1, +1\}$ with probability $1/2$. This projection matrix enables the use of the Fast Fourier transform, which reduces the sketching time to $O(D \log D)$. Moreover, if implemented carefully, the space complexity of their algorithm is $O(D)$. However, its variance remains the same as of the SRP. In comparison, our proposal is not only faster both asymptotically and empirically *w.r.t.* CBE but simultaneously offers a smaller variance.

SuperBit: [Ji et al., 2012] proposed an algorithm that offers smaller variance than SRP. Their main idea is to use a projection matrix that consists of orthogonal vectors obtained via the Gram-Schmidt process in $O(DK^2)$ time, which makes its running time high. In comparison, our proposal is much faster both asymptotically and empirically (speedup

Algorithm	Sketching Time	Space Complexity	Variance
SRP [Charikar, 2002]	$O(DK)$	$O(DK)$	$\theta(\pi-\theta)/K$
CBE [Yu et al., 2014]	$O(D\log D)$	$O(D)$	$\theta(\pi-\theta)/K$
SuperBit [Ji et al., 2012]	$O(DK^2)$	$O(DK)$	$(\pi^2/K^2)\cdot(K(\theta/\pi)+K(K-1)(\theta/\pi)\times p_{21})-\theta^2$
MLE [Kang and Wong, 2018]	$O(DK)$	$O(DK)$	$(2\pi/K)\cdot\left(\frac{1}{\theta+\theta_{\vec{x},\vec{e}}-\theta_{\vec{y},\vec{e}}}+\frac{1}{\theta_{\vec{x},\vec{e}}+\theta_{\vec{y},\vec{e}}-\theta}+\frac{1}{2\pi-\theta_{\vec{x},\vec{e}}-\theta_{\vec{y},\vec{e}}-\theta}+\frac{1}{\theta+\theta_{\vec{y},\vec{e}}-\theta_{\vec{x},\vec{e}}}\right)$
CSSRP (this work)	$O(D)$	$O(D)$	$(\pi^2/K^2)\cdot(K(\theta/\pi)+K(K-1)(\theta/\pi)\times\eta)-\theta^2$
CSSRP − L (this work)	$O(lD)$	$O(lD)$	$(\pi^2/K^2)\cdot(K(\theta/\pi)+K(K-1)(\theta/\pi)\times\eta_l)-\theta^2$

Table 1: Comparison among the baselines on asymptotic sketching time, space complexity, and variance. [Kang and Wong, 2018] conditioned the estimate on a weighted vector $\vec{e}$, hence variance includes the angle formed between the vector pairs and $\vec{e}$. Note that for $\vec{a},\vec{b}\in\mathbb{R}^D$, in SuperBit, p_{21} is defined as $\Pr[h^{(k_2)}(\vec{a})\neq h^{(k_2)}(\vec{b})|h^{(k_1)}(\vec{a})\neq h^{(k_1)}(\vec{b})]$, where $h^{(k)}(\cdot)$ is the hash function used in SRP (Equation (1)) *s.t.* the rows of the matrix R are orthonormal to each other. η and η_l are defined in Theorems 6 and 10, respectively.

upto $3896\times$, see Table 2 and Figure 5), and simultaneously space efficient as well. However, variance expression of both the methods looks similar.

MLE: [Kang and Wong, 2018] suggest employing *maximum-likelihood-estimation* technique on top of the sketch obtained from SRP. Inspired by Li et al. [2006a], their techniques include formulating the similarity estimation problem into computing the real roots of a cubic polynomial. In comparison, our proposal is both faster (asymptotically and empirically) as well as space efficient.

In order to understand the comparison among the baselines on their theoretical variances, we plot their respective expressions stated in Table 1. To do so, we generate several data pairs of $10K$ dimension such that their pairwise angles are between 30° and 150°. We summarise it via a scatter plot in Figure 2. It is evident that variances of SRP and CBE remain the highest among all, followed by MLE. Further, the variances of SuperBit, and our proposals CSSRP and CSSRP − L remains the lowest, and are comparable with each other.

Our proposals are based on correlated hash functions. We note that such hash functions have been explored earlier to get an accurate estimation for random projection and angular kernel estimation [Choromanski et al., 2017]. Also, the COUNT SKETCH projection matrix used in CSSRP have been used earlier to get a faster algorithm for several machine learning tasks such as low-Rank approximation and regression [Clarkson and Woodruff, 2017, 2013]. Furthermore, our proposal CSSRP − L uses a projection matrix whose entries are sampled from sparse Bernoulli distribution. We note that such projection matrices have been used in the context of random projection [Kane and Nelson, 2014, Li et al., 2006b, Dasgupta et al., 2010] to get a faster algorithm.

3 BACKGROUND

Definition 1 (Count-Sketch Charikar et al. [2004b], Weinberger et al. [2009]). *Let $\vec{\alpha}=(\alpha_1,\ldots,\alpha_k,\ldots,\alpha_K)\in\mathbb{R}^K$ be the sketch of input vector $\vec{a}\in\mathbb{R}^D$, obtained from Count-sketch algorithm. Then, the k-th feature of $\vec{\alpha}$*

$$\alpha_k=\sum_{j=1}^{D}a_j g(j)\mathbb{1}_{kj}, \tag{3}$$

where $g:[D]\mapsto\{-1,+1\}$, and $h:[D]\mapsto[K]$ are hash functions from 2-universal hash families, and $\mathbb{1}_{kj}$ is indicator of the event $h(j)=k$.

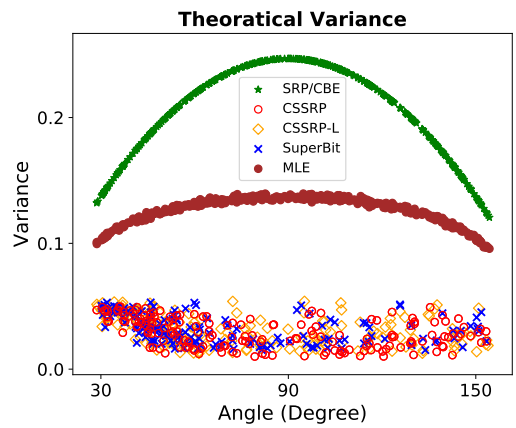

Figure 2: Illustration of theoretical variances of the baselines.

Notations	
$\vec{a},\vec{b}\in\mathbb{R}^D$	Input vectors
a_i	i-th feature of $\vec{a}$
$\vec{\alpha},\vec{\beta}\in\mathbb{R}^K$	Sketch vectors
D	Original dimension
K	Sketch dimension
R	Projection matrix
$\theta_{(\vec{a},\vec{b})}$	Angle between $\vec{a}$ and $\vec{b}$
$\vec{r}_k$	k-th row of projection matrix
$r_{kj}=g(j)\mathbb{1}_{kj}$	(k,j)-th index of projection matrix
$h(\vec{a})$	$=(sign(\alpha_1)\ldots sign(\alpha_k)\ldots sign(\alpha_K))$

COUNT-SKETCH operation can also be represented as a matrix projection. Let R be a random matrix such that $r_{kj}=g(j)\cdot\mathbb{1}_{kj}$, for all $k\in[K]$, $j\in[D]$.

$$R = \begin{bmatrix} \vec{r}_1 \\ \vdots \\ \vec{r}_k \\ \vdots \\ \vec{r}_K \end{bmatrix}_{K \times D}, \text{ where } \vec{r}_k = (r_{k1}, \ldots, r_{kj}, \ldots, r_{kD}),$$

Therefore, $\vec{\alpha} = R\vec{a}^T$.

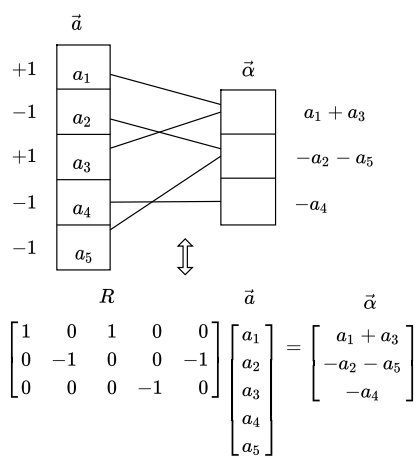

Figure 3: Count-Sketch as matrix projection.

4 IMPROVING SRP USING COUNT-SKETCH

At a high level our proposal is computing the sketch of input vectors using Count-sketch (see Definition 1) and taking the sign of the resultant vector. We state it as follows.

Definition 2 (COUNT-SKETCH SIGN-RANDOM-PROJECTION-CSSRP)**.** *We denote our proposal as a hash function $h(\cdot)$ that takes a vector $\vec{a} \in \mathbb{R}^D$ as input, first compress it (say vector $\vec{\alpha} \in \mathbb{R}^K$) using Count-sketch (Definition 1), and then compute the sign of the compressed vector.*

$$\begin{aligned} h(\vec{a}) &= sign(\vec{\alpha}) \\ &= (sign(\alpha_1), \ldots, sign(\alpha_k), \ldots, sign(\alpha_K)) \\ h^{(k)}(\vec{a}) &= sign(\alpha_k). \end{aligned}$$

where, $sign(\alpha_k)$ returns 1 if $x \geq 0$, and 0 otherwise.

In what follows, we prove that our proposal gives an unbiased estimate of the pairwise cosine similarity, further show that the variance of our estimate is smaller than that of SRP.

Our proof techniques relies in showing that the projection matrix (see Figure 3) corresponding to COUNT-SKETCH algorithm, approximates sparse Bernoulli distribution, and further we show that features of the sketch vector obtained from COUNT-SKETCH asymptotically converges to the Gaussian distribution when the sketch dimension $K = o(D)$.

Note that the pairwise angular similarity is only meaningful if all dimensions of the data are more or less equally important; otherwise, the exceptionally large entries will dominate. Therefore, our assumption is that the fourth moment of the input vectors is bounded i.e. $\mathbb{E}[a_i^4] < \infty$, $\mathbb{E}[b_i^4] < \infty$ and $\mathbb{E}[a_i^2 b_i^2] < \infty$, for $\vec{a},\ \vec{b} \in \mathbb{R}^D$ (as discussed in Sections $4, 5$ of [Li et al., 2006b]). However, the proof of asymptotic normality and analyzing its rate of convergence only require a bounded third moment or even a much weaker condition.

We adopt the following two lemmas from [Li et al., 2006b] to support our proofs. Our all results hold asymptotically as $D \to \infty$.

Lemma 3. *[Adapted from Lemma 4 of Li et al. [2006b]] Let $\vec{r} = (r_1, \ldots, r_j, \ldots, r_D) \in \mathbb{R}^D$ s.t.*

$$r_j \sim \begin{cases} 1 & \text{with probability } \frac{1}{2K} \\ 0 & \text{with probability } \frac{K-1}{K} \\ -1 & \text{with probability } \frac{1}{2K} \end{cases} \tag{4}$$

and $\vec{a} \in \mathbb{R}^D$. Denote $\alpha = \sum_{j=1}^D r_j a_j = \langle \vec{r}, \vec{a} \rangle$. Then if $D \to \infty$ and $K = o(D)$, we have $\alpha \overset{\mathcal{L}}{\Longrightarrow} \mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$ with the rate of convergence

$$|F_\alpha(y) - \Phi(y)| \leq 0.8\sqrt{K} \frac{\sum_{i=1}^D |a_i|^3}{(\sum_{i=1}^D a_i^2)^{3/2}} = 0.8\sqrt{\frac{K}{D}} \frac{\mathbb{E}[|a_i|^3]}{(\mathbb{E}[a_i^2])^{3/2}} \to 0, \tag{5}$$

where $\overset{\mathcal{L}}{\Longrightarrow}$ denotes "convergence in distribution", $F_\alpha(y)$ is the empirical cumulative density function of α, and $\Phi(y)$ is the CDF of $\mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$.

Lemma 4. *Let $\vec{r} \in \mathbb{R}^D$ with the probability distribution in Lemma 3, and $\vec{a}, \vec{b} \in \mathbb{R}^D$. Suppose we denote $\alpha = \sum_{j=1}^D r_j a_j = \langle \vec{r}, \vec{a} \rangle$, and $\beta = \sum_{j=1}^D r_j b_j = \langle \vec{r}, \vec{b} \rangle$. As $D \to \infty$, we have*

$$\sqrt{K} \begin{bmatrix} ||\vec{a}|| & \vec{a}\vec{b}^T \\ \vec{a}\vec{b}^T & ||\vec{b}|| \end{bmatrix}^{-\frac{1}{2}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \overset{\mathcal{L}}{\Longrightarrow} \mathcal{N}\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right), \tag{6}$$

with $\mathbb{E}\left[||sign(\alpha) - sign(\beta)||_1\right] = \frac{\theta_{(\vec{a},\vec{b})}}{\pi}$.

With the help of Lemmas 3 and 4, in the following we show that CSSRP gives an unbiased estimate of pairwise cosine similarity.

Theorem 5. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h(\vec{a})$ and $h(\vec{b})$ be their K-dimensional binary vector obtained via our proposal (Definition 2). If $K = o(D)$, then as $D \to \infty$ we have the following*

$$\mathbb{E}\left[\frac{\pi}{K}||h(\vec{a}) - h(\vec{b})||_1\right] = \theta_{(\vec{a},\vec{b})}. \tag{7}$$

Proof. We first consider each row $\vec{r}_k, 1 \leq k \leq K$ of the random matrix in Figure 3. The goal is to find the distribution of each $\vec{r}_k$, and hence compute

$$\mathbb{E}\left[\sum_{k=1}^{K} |h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|\right] = \sum_{k=1}^{K} \mathbb{E}\left[|h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|\right].$$

Suppose we denote $Z_k := |h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|$. While each Z_k are not independent due to our construction of R, let us briefly consider how each $\vec{r}_k$ is distributed.

When $k = 1$, we have that each entry in $\vec{r}_1$ comes from a Sparse Bernoulli distribution with

$$r_{1j} \sim \begin{cases} 1 & \text{with probability } \frac{1}{2K} \\ 0 & \text{with probability } \frac{K-1}{K} \\ -1 & \text{with probability } \frac{1}{2K} \end{cases}$$

where $\mathbb{E}[r_{1j}] = 0$, with $\text{Var}[r_{1j}] = \frac{1}{K}$. Here, we note that each entry in $\vec{r}_1$ is i.i.d.

We can also compute the moment generating function of each r_{1j} and get

$$\mathbb{E}\left[e^{sr_{1j}}\right] = \frac{K-1}{K} + \frac{\exp\{s\} + \exp\{-s\}}{2K}. \tag{8}$$

Now let us consider the case $k = 2$, and compute the moment generating function for each r_{2j}. By using the Law of Total Expectation, we have that

$$\begin{aligned}
\mathbb{E}\left[e^{sr_{2j}}\right] &= \mathbb{E}\left[e^{sr_{2j}} \mid r_{1j} = 0\right]\mathbb{P}\left[r_{1j} = 0\right] \\
&\quad + \mathbb{E}\left[e^{sr_{2j}} \mid r_{1j} = 1\right]\mathbb{P}\left[r_{1j} = 1\right] \\
&\quad + \mathbb{E}\left[e^{sr_{2j}} \mid r_{1j} = -1\right]\mathbb{P}\left[r_{1j} = -1\right]. \\
&= \left(\frac{\exp\{s\} + \exp\{-s\}}{2(K-1)} + \frac{K-2}{K-1}\right)\frac{K-1}{K} \\
&\quad + \frac{1}{2K} + \frac{1}{2K}. \\
&= \frac{\exp\{s\} + \exp\{-s\}}{2K} + \frac{K-2}{K} + \frac{1}{K}. \\
&= \frac{\exp\{s\} + \exp\{-s\}}{2K} + \frac{K-1}{K}.
\end{aligned} \tag{9}$$

which is the same moment generating function as the sparse Bernoulli distribution.

Moreover, we also note that each element in $\vec{r}_2$ are i.i.d., i.e. each r_{2i} is independent of r_{2j} (albeit dependent on r_{1i}). Now, consider $\vec{r}_k, 2 < k \leq K$, and consider each r_{kj}. By Law of Total Expectation, and conditioning on previous vectors:

$$\begin{aligned}
\mathbb{E}\left[e^{sr_{kj}}\right] &= \mathbb{E}\left[e^{sr_{kj}} \mid \text{all zeros for } r_{k'j}, k' < k\right] \times \\
&\quad \mathbb{P}\left[\text{all zeros for } r_{k'j}, k' < k\right] \\
&+ \mathbb{E}\left[e^{sr_{kj}} \mid 1 \text{ appears for at most one } r_{k'j}, k' < k\right] \times \\
&\quad \mathbb{P}\left[1 \text{ appears for at most one } r_{k'j}, k' < k\right] \\
&+ \mathbb{E}\left[e^{sr_{kj}} \mid -1 \text{ appears for at most one } r_{k'j}, k' < k\right] \times \\
&\quad \mathbb{P}\left[-1 \text{ appears for at most one } r_{k'j}, k' < k\right]. \\
&= \left(\frac{K-k}{K-k+1} + \frac{\exp\{s\} + \exp\{-s\}}{2(K-k+1)}\right)\frac{K-k+1}{K} \\
&\quad + \frac{k-1}{2K} + \frac{k-1}{2K}. \\
&= \frac{K-k}{K} + \frac{\exp\{s\} + \exp\{-s\}}{2K} + \frac{k-1}{K}. \\
&= \frac{\exp\{s\} + \exp\{-s\}}{2K} + \frac{K-1}{K}.
\end{aligned} \tag{10}$$

which gives the same moment generating function as the sparse Bernoulli distribution.

Now, we can use Lemma 3 to show that $\alpha_k = \langle \vec{r}_k, \vec{a} \rangle$ and $\beta_k = \langle \vec{r}_k, \vec{b} \rangle$ converge in distribution to $\mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$ and $\mathcal{N}\left(0, \frac{||\vec{b}||^2}{K}\right)$ respectively as D grows large. Moreover, by Lemma 4, we see that $\mathbb{E}\left[|h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|\right] = \mathbb{E}\left[|sign(\alpha_k) - sign(\beta_k)|\right] = \frac{\theta_{(\vec{a},\vec{b})}}{\pi}$ for each $1 \leq k \leq K$. Hence we must have that $\mathbb{E}\left[\sum_{k=1}^{K} |h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|\right] = K\frac{\theta_{(\vec{a},\vec{b})}}{\pi}$, and on rearranging, we have

$$\mathbb{E}\left[\frac{\pi}{K}\sum_{k=1}^{K} |h^{(k)}(\vec{a}) - h^{(k)}(\vec{b})|\right] = \theta_{(\vec{a},\vec{b})} \tag{11}$$

which is what we wanted to show. □

We give a bound on the variance of CSSRP. We defer its proof to the appendix due to space limit.

Theorem 6. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h(\vec{a})$ and $h(\vec{b})$ be their K-dimensional binary vector obtained via our proposal (Definition 2). If $K = o(D)$, then as $D \to \infty$ we have the following*

$$\begin{aligned}
&\text{Var}\left[\frac{\pi}{K}||h(\vec{a}) - h(\vec{b})||_1\right] \\
&= \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\frac{\theta_{(\vec{a},\vec{b})}}{\pi} \times \eta\right) - \theta^2_{(\vec{a},\vec{b})}.
\end{aligned}$$

where, $k_1 \neq k_2$, $k_1, k_2 \in [K]$, and
$\eta = \Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \mid \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right]$.

Remark 7. *Recall that the variance of* SRP *is*

$$\text{Var}\left[\text{SRP}\right] = \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\left(\frac{\theta_{(\vec{a},\vec{b})}}{\pi}\right)^2\right) - \theta^2_{(\vec{a},\vec{b})}.$$

We remark that the variance of CSSRP *stated in Theorem 6 is smaller than that of* SRP *because $\eta \leq \frac{\theta}{\pi}$. We validate this empirically by plotting η for several values of θ and summarise it in Figure 4. We notice that η always remains smaller than $\frac{\theta}{\pi}$, and leads to variance reduction as also supported in Figure 2.*

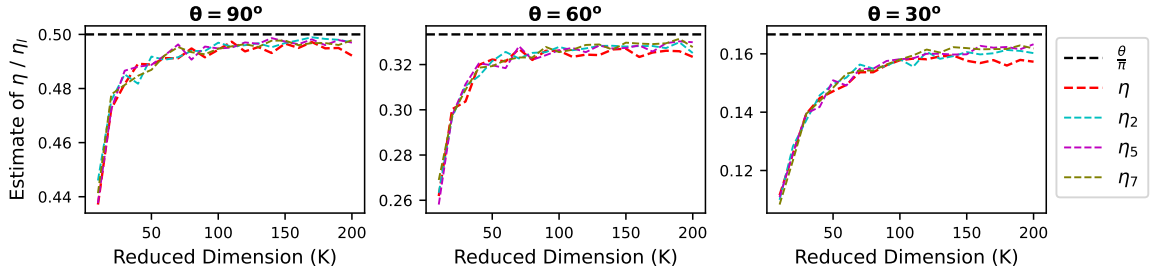

Figure 4: Empirical estimation of η and η_l via synthetically generated data points for various pairwise angles θ, and reduced dimensions K.

4.1 ANOTHER IMPROVED ESTIMATOR - $\text{CSSRP} - \text{L}$:

We note that the stated in Theorems 5 and 6 holds when $K = o(D)$. We wish to show that our results hold for higher values of K as well. Our sketching algorithm $\text{CSSRP} - \text{L}$ stated below achieves the same.

Definition 8 ($\text{CSSRP} - \text{L}$)**.** *Let R' be a $K \times D$ projection matrix such that each column of R' has exactly l non-zero entries. These l positions are sampled uniformly at random and each of them takes value $\{\pm 1\}$ with probability $1/2$*

$$R' = \begin{bmatrix} \vec{r}'_1 \\ \vdots \\ \vec{r}'_k \\ \vdots \\ \vec{r}'_K \end{bmatrix}_{K \times D} . \tag{12}$$

We denote our proposal $\text{CSSRP} - \text{L}$ as a two step procedure: in the first step, we project input vectors $\vec{a},\ \vec{b} \in \mathbb{R}^D$ on the matrix R'. Let $\vec{\alpha}'$ and $\vec{\beta}'$ denote resultant vector, that is,

$$\vec{\alpha}' = R'\vec{a}^T, \text{and } \vec{\beta}' = R'\vec{b}^T.$$

In the second step, the final binary sketch is obtained by taking the sign of the resultant vectors obtained via projection. That is

$$\begin{aligned} h'(\vec{a}) &= sign(\vec{\alpha}') \\ &= (sign(\alpha'_1), \ldots, sign(\alpha'_k), \ldots, sign(\alpha'_K)). \\ h'^{(k)}(\vec{a}) &= sign(\alpha'_k), \ \ for \ \ k \in [K]. \end{aligned}$$

where $sign(\alpha'_k)$ returns 1 if $x \geq 0$, and 0 otherwise.

In the following theorem, we show that our proposal gives an unbiased estimate of pairwise angular similarity. Its proof is built on similar lines to the proof of Theorem 5. We defer it to the appendix.

Theorem 9. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h'(\vec{a})$ and $h'(\vec{b})$ be their K-dimensional binary vector obtained via our improved estimator proposal (stated in Definition 8). If $K = o(lD)$, then as $D \to \infty$ we have the following*

$$\mathbb{E}\left[\frac{\pi}{K}||h'(\vec{a}) - h'(\vec{b})||_1\right] = \theta_{(\vec{a},\vec{b})}. \tag{13}$$

We give a bound on the variance of our proposal $\text{CSSRP} - \text{L}$ estimator, its proof is analogous to that of Theorem 6.

Theorem 10. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h'(\vec{a})$ and $h'(\vec{b})$ be their K-dimensional binary vector obtained via our improved estimator (Definition 8). If $K = o(lD)$, then as $D \to \infty$ we have the following*

$$\begin{aligned} &\text{Var}\left[\frac{\pi}{K}||h'(\vec{a}) - h'(\vec{b})||_1\right] \\ &= \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\frac{\theta_{(\vec{a},\vec{b})}}{\pi} \times \eta_l\right) - \theta^2_{(\vec{a},\vec{b})} \end{aligned}$$

where, $k_1 \neq k_2$, $k_1, k_2 \in [K]$, and
$\eta_l = \Pr\left[\left(h'^{(k_2)}(\vec{a}) \neq h'^{(k_2)}(\vec{b})\right) \mid \left(h'^{(k_1)}(\vec{a}) \neq h'^{(k_1)}(\vec{b})\right)\right]$.

Remark 11. *Similar to Remark 7, the variance of $\text{CSSRP} - \text{L}$ (Theorem 10) is smaller than that of SRP as $\eta_l \leq \frac{\theta}{\pi}$. Its numerical simulation is mentioned in Figure 4. Further, when l is equal to K, then rows of the matrix R' defined in Equation (12) become independent, and our proposal $\text{CSSRP} - \text{L}$ (Definition 8) becomes exactly similar to SRP.*

5 EXPERIMENTS

Hardware description: We conducted our experiments on a machine with the following configuration CPU: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs); Memory: 8GB; OS: Window 10; Model: MSI GL62M 7RDX.

We use synthetic and real-world dataset for our experiments. In the synthetic dataset, the value of each feature is randomly sampled from $[0, 1]$. Description of real-world dataset is summarized in Table 3.

5.1 BASELINES AND END TASKS

We evaluate the performance of our proposals Count-Sketch-Signed Random Projection (CSSRP) and Count-Sketch-Signed Random Projection-L ($\text{CSSRP} - \text{L}$) to that of the

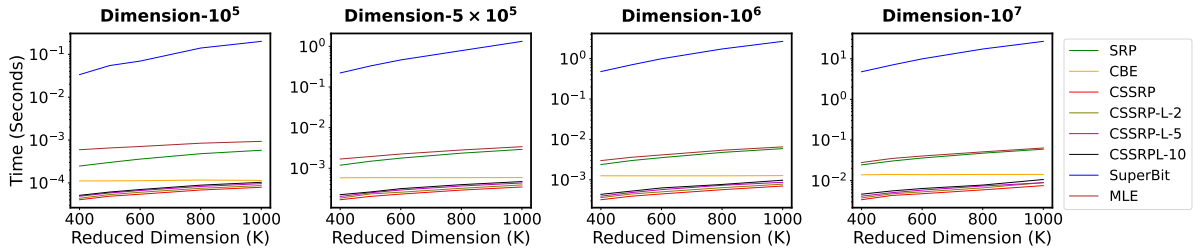

Figure 5: Comparison among the baselines on average running time which consist of both dimensionality reduction time as well as pairwise similarity computation time for a pair. Note that $\text{CSSRP} - \text{L} - 2$ denotes $\text{CSSRP} - \text{L}$ algorithm with $l = 2$, and so on.

Estimators	**Dimension-10^5**	**Dimension-5×10^5**	**Dimension-10^6**	**Dimension-10^7**
SRP [Charikar et al., 2004a]	**7.32**×	**8.41**×	**8.44**×	**8.65**×
CBE [Yu et al., 2014]	**1.45**×	**1.70**×	**1.811**×	**2.074**×
MLE [Kang and Wong, 2018]	**11.80**×	**9.79**×	**9.32**×	**9.24**×
SuperBit [Ji et al., 2012]	**2541.35**×	**3820.91**×	**3826.56**×	**3896.71**×
$\text{CSSRP} - \text{L} - 2$ (this work)	1.09×	1.12×	1.15×	1.20×
$\text{CSSRP} - \text{L} - 5$ (this work)	1.22×	1.25×	1.29×	1.39×
$\text{CSSRP} - \text{L} - 10$ (this work)	1.31×	1.35×	1.40×	1.55×

Table 2: Numerical speedup of CSSRP *w.r.t.* other baselines on a fixed reduced dimension 1000.

Table 3: Description of real-world datasets.

Dataset	**# of points**	**Dimension**
Gisette [Lichman, 2013]	13,500	5,000
Arcene [Lichman, 2013]	900	10,000
Gene RNA-Seq [Lichman, 2013]	801	20,531
PEMS-SF[Dua and Graff, 2017]	440	138,672

Signed Signed-random-projection (SRP) [Charikar, 2002], Circulant Binary Embedding (CBE) [Yu et al., 2014], Maximum Likelihood Estimation (MLE) [Kang and Wong, 2018], and Super-Bit LSH (SuperBit) [Ji et al., 2012]. Note that the MLE estimator requires an extra vector for similarity computation, and we use the first principal component vector for the same, as mentioned in [Kang and Wong, 2018]. We use the following metrics for evaluations: (i) running time to generate the sketch, (ii) variance analysis via boxplot, (iii) similarity search.

5.2 RUNNING TIME:

Experimental setting: We aim to compare the running time of all the baselines. To do so, we generate high dimensional synthetic datasets of dimensions ranging from 10^5 to 10^7. We compress the datasets for different values of reduced dimension using various baselines, and record the sum of dimensionality reduction time and pairwise similarity computation time. Note that the sketching approach of MLE remains same as that of SRP, however its similarity estimation step is different, and involves computing the root of a cubic polynomial. Therefore to have a fair comparison among all the baselines, we included both dimensionality reduction time as well as similarity computation time. We compute average running time required by a pair of points, over various reduced dimensions, and summarise it in Figure 5. We also note the corresponding speedup obtained via our proposal CSSRP *w.r.t.* baselines, and report it in Table 2.

Insight: We observed that CSSRP is a way much faster than all the baselines, and we observed a significant numerical speedup (upto 3800×). We would like to highlight that our CSSRP is also faster (speed up 1.45× to 2×) than CBE Yu et al. [2014], which is a faster variant of SRP. Further, the running time of our other proposal $\text{CSSRP} - \text{L}$ remains somewhat comparable to CSSRP. Note that the SuperBit method remains the slowest among all the baselines; this is due to the step of generating orthonormal vectors (via *Gram-Schmidt* orthogonalization process) required for the projection matrix.

5.3 SIMILARITY SEARCH:

Experimental setting: In this experiment, aim is to check if points proximity are maintained after dimensionality reduction. We discuss our experimental setting as follows. We split the dataset randomly into two parts 90% and 10% – we refer the former as the training partition, while the latter one as the query partition. For each point in the query partition, we record top-k similar points (under cosine similarity) from training partition for the uncompressed datasets. We denote this set by S. We compress the dataset (both query and training partition) using several baselines on various reduced dimensions, and record top-k similar points (on the sketch) of the query points from the sketch of the training partition. We denote this set by $S^{'}$. We use two evaluation metrics – *recall*:= $|S \cup S^{'}|/|S|$, and *accuracy*= $|S \cap S^{'}|/|S \cup S^{'}|$. We compute them for all the points in the query partition, and record their average. We summarize our findings in Figure 6 for accuracy, and Figure 8 (in appendix) for recall.

Insight: We observed that at small reduced dimensions

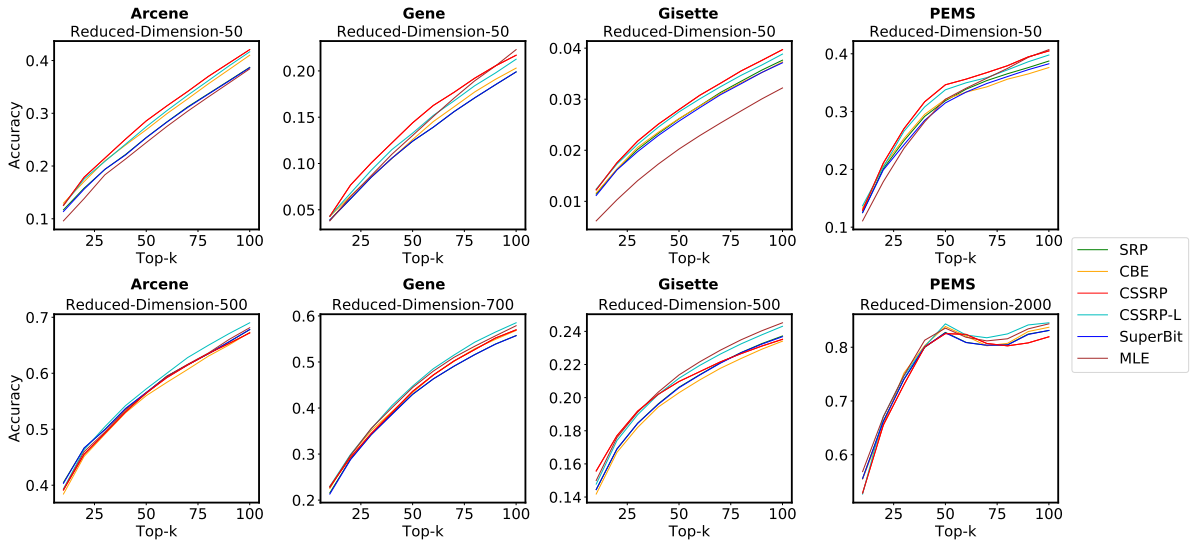

Figure 6: Comparison among the baselines on the task of Top-k similarity search. A higher value of accuracy indicates a better performance.

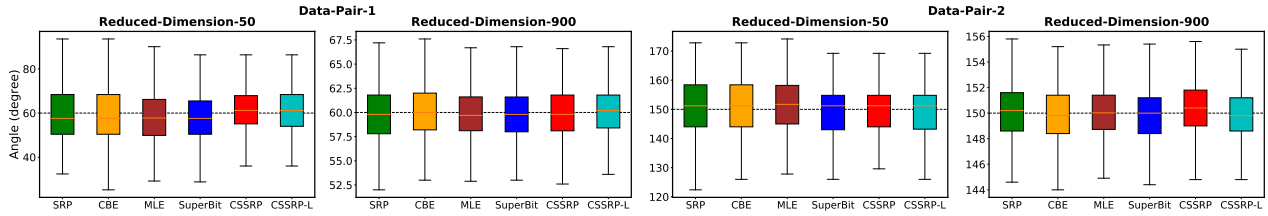

Figure 7: Comparison among baselines on the task of variance analysis via box plot. The sampled pairs are at angles $60°$ and $150°$, respectively. The smaller interquartile range is an indicator of lower variance. The dotted line represents the actual angle in degree.

(listed in first rows of the respective plots) for both accuracy and recall, our estimator CSSRP estimator performed significantly better than the baselines. However, with the increase of dimension CSSRP performance slightly decreases (listed in second rows of the respective plots), which was circumvented by our other proposal $\mathrm{CSSRP-L}$, whose performance remains at least in the top two.

5.4 VARIANCE ANALYSIS VIA BOX-PLOT:

Experimental setting: In this experiment, our aim is to compare the variances of the baselines via box-plot. To do so, we generate a synthetic dataset in 10000 dimension, and randomly sample a pair of points from it. We compress this pair and compute the estimated similarity using all the baselines. We repeat this step 500 times independently, and use the respective estimate to generate the box plot. We summarise our findings in Figures 7, 9 (in appendix).

Insight: We observe that at a small reduced dimension, the variance of our CSSRP estimator is lower than the variance of the other baselines. However, at higher reduced dimension variance of CSSRP is slightly worse than the remaining. This problem is tackled by our other proposal $\mathrm{CSSRP-L}$, which offers smaller variance than the baselines, even at higher values of the reduced dimension.

6 CONCLUSION

We consider dimensionality reduction for real-valued data that approximate cosine similarity. The classical algorithm for this task - SRP [Charikar, 2002] suffers from high variance, running time, and space complexity involved in the similarity computation. Popular improvements such as [Kang and Wong, 2018, Yu et al., 2014, Ji et al., 2012] address only one or two aspects of the above. We present algorithms (CSSRP and $\mathrm{CSSRP-L}$) that address all these limitations. When the sketch dimension $K = o(D)$, our proposal CSSRP offers a faster and space-efficient algorithm along with the smaller variance. However, for large K, the guarantee of CSSRP does not hold. Our other proposal $\mathrm{CSSRP-L}$, addresses this by offering a faster and space efficient algorithm with smaller variance, when K is large. We give a theoretical analysis of our proposals and complement it via empirical simulations. We notice the speedup of several orders (even with faster variants of SRP [Yu et al., 2014]) and simultaneously accurate performance on end tasks, *w.r.t.* baselines. Finally, we could only empirically show that our proposals have smaller variance *w.r.t.* the baselines. Giving its mathematical proof still remains an open question of the work.

References

Andrei Z. Broder, Moses Charikar, Alan M. Frieze, and Michael Mitzenmacher. Min-wise independent permutations (extended abstract). In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 327–336, New York, NY, USA, 1998. Association for Computing Machinery. ISBN 0897919629. doi: 10.1145/276698.276781. URL https://doi.org/10.1145/276698.276781.

Moses Charikar, Kevin Chen, and Martin Farach-Colton. Finding frequent items in data streams. *Theoretical Computer Science*, 312(1):3 – 15, 2004a. ISSN 0304-3975. doi: https://doi.org/10.1016/S0304-3975(03)00400-6. URL http://www.sciencedirect.com/science/article/pii/S0304397503004006. Automata, Languages and Programming.

Moses Charikar, Kevin C. Chen, and Martin Farach-Colton. Finding frequent items in data streams. *Theor. Comput. Sci.*, 312(1):3–15, 2004b. doi: 10.1016/S0304-3975(03)00400-6. URL https://doi.org/10.1016/S0304-3975(03)00400-6.

Moses S Charikar. Similarity estimation techniques from rounding algorithms. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 380–388, 2002.

Krzysztof M Choromanski, Mark Rowland, and Adrian Weller. The unreasonable effectiveness of structured random orthogonal embeddings. *Advances in neural information processing systems*, 30, 2017.

Kenneth L. Clarkson and David P. Woodruff. Low rank approximation and regression in input sparsity time. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 81–90. ACM, 2013. doi: 10.1145/2488608.2488620. URL https://doi.org/10.1145/2488608.2488620.

Kenneth L Clarkson and David P Woodruff. Low-rank approximation and regression in input sparsity time. *Journal of the ACM (JACM)*, 63(6):1–45, 2017.

Anirban Dasgupta, Ravi Kumar, and Tamás Sarlós. A sparse johnson: Lindenstrauss transform. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 341–350, 2010.

Dheeru Dua and Casey Graff. UCI machine learning repository, 2017. URL http://archive.ics.uci.edu/ml.

William Feller. *An introduction to probability theory and its applications. Vol. II.* Second edition. John Wiley & Sons Inc., New York, 1971.

F. Gotze. On the Rate of Convergence in the Multivariate CLT. *The Annals of Probability*, 19(2):724 – 739, 1991. doi: 10.1214/aop/1176990448. URL https://doi.org/10.1214/aop/1176990448.

Monika Henzinger. Finding near-duplicate web pages: A large-scale evaluation of algorithms. In *Proceedings of the 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '06, page 284–291, New York, NY, USA, 2006. Association for Computing Machinery. ISBN 1595933697. doi: 10.1145/1148170.1148222. URL https://doi.org/10.1145/1148170.1148222.

Phuc-Tran Ho, Hee Sun Kim, and Sung-Ryul Kim. Application of sim-hash algorithm and big data analysis in spam email detection system. In *RACS '14*, 2014.

Jianqiu Ji, Jianmin Li, Shuicheng Yan, Bo Zhang, and Qi Tian. Super-bit locality-sensitive hashing. In *Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1*, NIPS'12, page 108–116, Red Hook, NY, USA, 2012. Curran Associates Inc.

W. B. Johnson and J. Lindenstrauss. Extensions of lipschitz mappings into a hilbert space. *Conference in modern analysis and probability (New Haven, Conn., 1982), Amer. Math. Soc., Providence, R.I.*, pages 189–206, 1983. doi: 10.1016/S0022-0000(03)00025-4. URL http://dx.doi.org/10.1016/S0022-0000(03)00025-4.

Daniel M. Kane and Jelani Nelson. Sparser johnson-lindenstrauss transforms. *J. ACM*, 61(1), jan 2014. ISSN 0004-5411. doi: 10.1145/2559902. URL https://doi.org/10.1145/2559902.

Keegan Kang and Weipin Wong. Improving sign random projections with additional information. In Jennifer Dy and Andreas Krause, editors, *Proceedings of the 35th International Conference on Machine Learning*, volume 80 of *Proceedings of Machine Learning Research*, pages 2479–2487. PMLR, 10–15 Jul 2018. URL https://proceedings.mlr.press/v80/kang18b.html.

Ping Li, Trevor Hastie, and Kenneth Ward Church. Improving random projections using marginal information. In *Learning Theory, 19th Annual Conference on Learning Theory, COLT 2006, Pittsburgh, PA, USA, June 22-25, 2006, Proceedings* Li et al. [2006a], pages 635–649. doi: 10.1007/11776420_46. URL https://doi.org/10.1007/11776420_46.

Ping Li, Trevor Hastie, and Kenneth Ward Church. Very sparse random projections. In *Proceedings of the Twelfth ACM SIGKDD International Conference on Knowledge*

Discovery and Data Mining, Philadelphia, PA, USA, August 20-23, 2006 Li et al. [2006b], pages 287–296. doi: 10.1145/1150402.1150436. URL https://doi.org/10.1145/1150402.1150436.

M. Lichman. UCI machine learning repository, 2013. URL http://archive.ics.uci.edu/ml.

Gurmeet Singh Manku, Arvind Jain, and Anish Das Sarma. Detecting near-duplicates for web crawling. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, page 141–150, New York, NY, USA, 2007. Association for Computing Machinery. ISBN 9781595936547. doi: 10.1145/1242572.1242592. URL https://doi.org/10.1145/1242572.1242592.

I. S. Shiganov. Refinement of the upper bound of the constant in the central limit theorem. *Journal of Soviet Mathematics*, 35:2545–2550, 1986.

Kilian Q. Weinberger, Anirban Dasgupta, John Langford, Alexander J. Smola, and Josh Attenberg. Feature hashing for large scale multitask learning. In *Proceedings of the 26th Annual International Conference on Machine Learning, ICML 2009, Montreal, Quebec, Canada, June 14-18, 2009*, pages 1113–1120, 2009. doi: 10.1145/1553374.1553516. URL http://doi.acm.org/10.1145/1553374.1553516.

Felix X. Yu, Sanjiv Kumar, Yunchao Gong, and Shih-Fu Chang. Circulant binary embedding. In *Proceedings of the 31st International Conference on International Conference on Machine Learning - Volume 32*, ICML'14, pages II–946–II–954. JMLR.org, 2014. URL http://dl.acm.org/citation.cfm?id=3044805.3044998.

Felix X. Yu, Aditya Bhaskara, Sanjiv Kumar, Yunchao Gong, and Shih-Fu Chang. On binary embedding using circulant matrices. *Journal of Machine Learning Research*, 18(150):1–30, 2018. URL http://jmlr.org/papers/v18/15-619.html.

Improving Sign-Random-Projection via Count Sketch (Supplementary Materials)

A EXTENDED EXPERIMENTAL RESULTS:

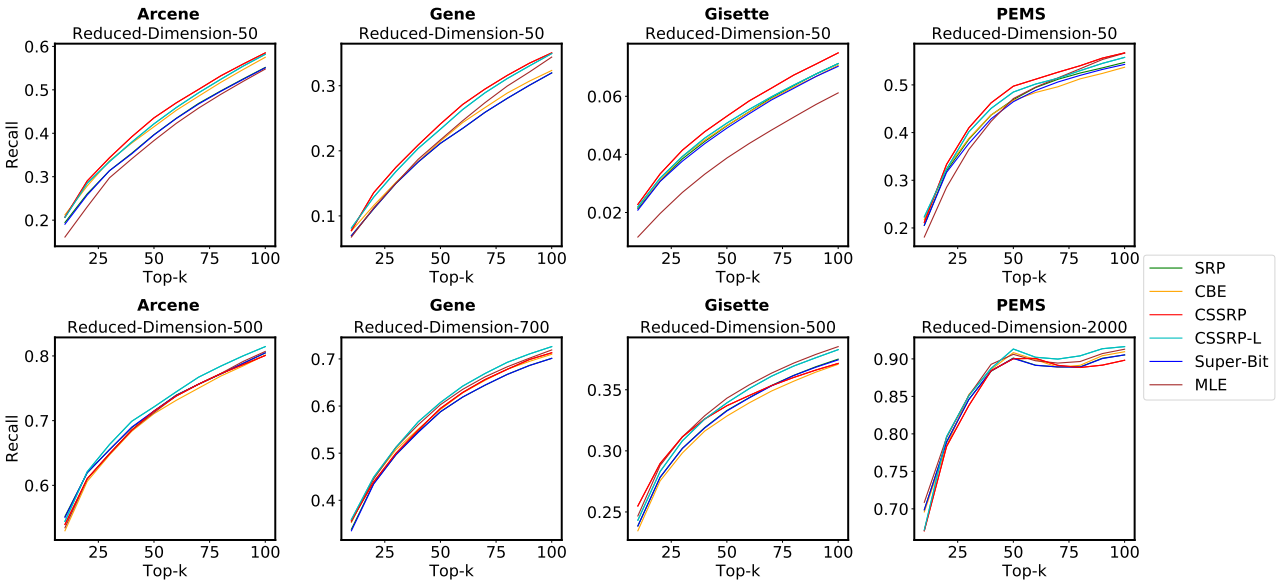

Figure 8: Comparison among the baselines on the task of top-k similarity search. A higher value of recall indicates a better performance.

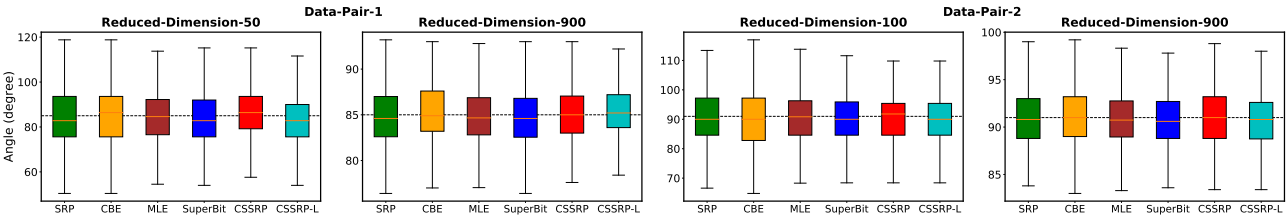

Figure 9: Comparison among baselines on the task of variance analysis via box plot. The sampled pairs are at angles $85°$ and $90°$, respectively. The smaller interquartile range is an indicator of lower variance. The dotted line represents the actual angle in degree.

B MISSING PROOFS:

In this section, we present the missing proofs from the main paper. For convenience, we also restate them here.

Proof of Lemma 3:

Lemma 3. *[Adapted from Lemma 4 of Li et al. [2006b]] Let* $\vec{r} = (r_1, \ldots, r_j, \ldots, r_D) \in \mathbb{R}^D$ *s.t.*

$$r_j \sim \begin{cases} 1 & \textit{with probability } \frac{1}{2K} \\ 0 & \textit{with probability } \frac{K-1}{K} \\ -1 & \textit{with probability } \frac{1}{2K} \end{cases} \tag{4}$$

and $\vec{a} \in \mathbb{R}^D$. Denote $\alpha = \sum_{j=1}^{D} r_j a_j = \langle \vec{r}, \vec{a} \rangle$. Then if $D \to \infty$ and $K = o(D)$, we have $\alpha \xRightarrow{\mathcal{L}} \mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$ with the rate of convergence

$$|F_\alpha(y) - \Phi(y)| \leq 0.8\sqrt{K}\frac{\sum_{i=1}^{D}|a_i|^3}{(\sum_{i=1}^{D} a_i^2)^{3/2}} = 0.8\sqrt{\frac{K}{D}}\frac{\mathbb{E}[|a_i|^3]}{(\mathbb{E}[a_i^2])^{3/2}} \to 0, \tag{5}$$

where $\xRightarrow{\mathcal{L}}$ denotes "convergence in distribution", $F_\alpha(y)$ is the empirical cumulative density function of α, and $\Phi(y)$ is the CDF of $\mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$.

Proof. We know that

$$\alpha = \sum_{j=1}^{D} r_j a_j,$$

where

$$r_j \sim \begin{cases} 1 & \text{with probability } \frac{1}{2K}, \\ 0 & \text{with probability } \frac{K-1}{K}, \\ -1 & \text{with probability } \frac{1}{2K}. \end{cases}$$

Let

$$z_j = r_j a_j.$$

Then

$$\mathbb{E}[z_j] = \mathbb{E}[r_j a_j] = a_j \mathbb{E}[r_j] = 0.$$
$$\mathrm{Var}[z_j] = \mathbb{E}[(z_j - \mathbb{E}[z_j])^2] = \mathbb{E}[z_j^2] = \mathbb{E}[r_j^2 a_j^2] = \frac{a_j^2}{K}.$$
$$\mathbb{E}[|z_j|^{2+\delta}] = |a_j|^{2+\delta}\mathbb{E}[|r_j|^{2+\delta}] = |a_j|^{2+\delta}\left(1 \times \frac{1}{K} + 0 \times \frac{K-1}{K}\right) = \frac{|a_j|^{2+\delta}}{K}.$$

Let

$$S_D^2 = \sum_{j=1}^{D} \mathrm{Var}[z_j] = \frac{\sum_{j=1}^{D} a_j^2}{K}.$$

To prove that $\frac{\sum_{j=1}^{D} z_j}{S_D} \xRightarrow{\mathcal{L}} \mathcal{N}(0,1)$, we need to show that following Lindeberg condition is satisfied.

$$\frac{1}{S_D^2}\sum_{j=1}^{D}\mathbb{E}\left[z_j^2; |z_j| > \epsilon S_D\right] \to 0 \quad \text{for any } \epsilon > 0. \tag{14}$$

$$\implies \frac{1}{S_D^2}\sum_{j=1}^{D}\mathbb{E}\left[z_j^2; |z_j| > \epsilon S_D\right] \leq \frac{1}{S_D^2}\sum_{j=1}^{D}\mathbb{E}\left[\frac{|z_j|^{2+\delta}}{(\epsilon S_D)^\delta}\right]. \tag{15}$$

$$= \frac{1}{\frac{\sum_{j=1}^{D} a_j^2}{K}} \cdot \frac{1}{\epsilon^\delta} \cdot \frac{\sum_{j=1}^{D}\frac{|a_j|^{2+\delta}}{K}}{\left(\frac{\sum_{j=1}^{D} a_j^2}{K}\right)^{\frac{\delta}{2}}}. \tag{16}$$

$$= \frac{1}{\epsilon^\delta} \cdot \frac{\sum_{j=1}^{D}\frac{|a_j|^{2+\delta}}{K}}{\left(\frac{\sum_{j=1}^{D} a_j^2}{K}\right)^{\frac{2+\delta}{2}}}. \tag{17}$$

$$= K^{\frac{\delta}{2}} \cdot \frac{1}{\epsilon^{\delta}} \cdot \frac{\sum_{j=1}^{D} \frac{|a_j|^{2+\delta}}{D}}{\left(\frac{\sum_{j=1}^{D} a_j^2}{D}\right)^{\frac{2+\delta}{2}}} \cdot \frac{1}{D^{\frac{\delta}{2}}}. \tag{18}$$

$$= \left(\frac{K}{D}\right)^{\frac{\delta}{2}} \cdot \frac{1}{\epsilon^{\delta}} \cdot \frac{\mathbb{E}\left[|a_j|^{2+\delta}\right]}{\left(\mathbb{E}[a_j^2]\right)^{\frac{2+\delta}{2}}}. \tag{19}$$

$$\to 0. \tag{20}$$

Equation (20) holds as $K = o(D)$. Therefore, for $K = o(D)$, due to Lindeberg Central Limit theorem Gotze [1991], Feller [1971], we have

$$\frac{\sum_{j=1}^{D} z_j}{S_D} = \frac{\sum_{j=1}^{D} r_j a_j}{\sqrt{\frac{\sum_{j=1}^{D} a_j^2}{K}}} = \frac{\alpha}{\sqrt{||\vec{a}||^2/K}} \overset{\mathcal{L}}{\Rightarrow} \mathcal{N}(0,1). \tag{21}$$

$$\alpha \overset{\mathcal{L}}{\Rightarrow} \mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right). \tag{22}$$

We remain to find the rate of convergence. For this we use Berry Esseen theorem Shiganov [1986], Feller [1971]. Let us denote

$$\rho_D = \sum_{j=1}^{D} \mathbb{E}\left[|z_j|^3\right]. \tag{23}$$

$$= \sum_{j=1}^{D} |a_j|^3 \mathbb{E}\left[|r_j|^3\right]. \tag{24}$$

$$= \frac{\sum_{j=1}^{D} |a_j|^3}{K}. \tag{25}$$

Then due to Berry Esseen theorem, we have

$$|F_\alpha(y) - \Phi(y)| \leq 0.8 \frac{\rho_D}{S_D^3}.$$

$$= 0.8 \frac{\frac{\sum_{j=1}^{D} |a_j|^3}{K}}{\left(\frac{\sum_{j=1}^{D} a_j^2}{K}\right)^{\frac{3}{2}}}.$$

$$= 0.8 \times \sqrt{\frac{K}{D}} \frac{\sum_{j=1}^{D} |a_j|^3/D}{\left(\sum_{j=1}^{D} a_j^2/D\right)^{\frac{3}{2}}}.$$

$$= 0.8 \times \sqrt{\frac{K}{D}} \frac{\mathbb{E}[|a_j|^3]}{\left(\mathbb{E}[a_j^2]\right)^{\frac{3}{2}}}.$$

$$\to 0 \qquad \text{as} \quad D \to \infty. \tag{26}$$

Equation (26) holds for $K = o(D)$. Equation (22) and (26) completes a proof of the Lemma 3. □

Proof of Theorem 6:

Theorem 6. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h(\vec{a})$ and $h(\vec{b})$ be their K-dimensional binary vector obtained via our proposal (Definition 2). If $K = o(D)$, then as $D \to \infty$ we have the following*

$$\text{Var}\left[\frac{\pi}{K}||h(\vec{a}) - h(\vec{b})||_1\right]$$

$$= \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\frac{\theta_{(\vec{a},\vec{b})}}{\pi} \times \eta\right) - \theta^2_{(\vec{a},\vec{b})}.$$

where, $k_1 \neq k_2$*,* $k_1, k_2 \in [K]$*, and*
$\eta = \Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \mid \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right]$.

Proof. We know that

$$\mathrm{Var}\left[\frac{\pi}{K}||h(\vec{a}) - h(\vec{b})||_1\right] = \frac{\pi^2}{K^2}\mathrm{Var}\left[||h(\vec{a}) - h(\vec{b})||_1\right]. \tag{27}$$

$$= \frac{\pi^2}{K^2}\mathrm{Var}\left[\sum_{k=1}^{K} Y_k\right]. \tag{28}$$

$$\text{where } Y_k := \mathbb{1}_{\{h^{(k)}(\vec{a}) \neq h^{(k)}(\vec{b})\}}. \tag{29}$$

We focus on the term

$$\mathrm{Var}\left[\sum_{k=1}^{K} Y_k\right] = \mathbb{E}\left[\left(\sum_{k=1}^{K} Y_k\right)^2\right] - \left(\mathbb{E}\left[\sum_{k=1}^{K} Y_k\right]\right)^2. \tag{30}$$

$$= \mathbb{E}\left[\sum_{k=1}^{K} Y_k^2 + \sum_{k_1 \neq k_2, k_1, k_2 \in [K]} Y_{k_1} Y_{k_2}\right] - \left(\mathbb{E}\left[\sum_{k=1}^{K} Y_k\right]\right)^2. \tag{31}$$

$$= \sum_{k=1}^{K} \mathbb{E}\left[Y_k\right] + \sum_{k_1 \neq k_2, k_1, k_2 \in [K]} \mathbb{E}\left[Y_{k_1} Y_{k_2}\right] - \left(\mathbb{E}\left[\sum_{k=1}^{K} Y_k\right]\right)^2. \tag{32}$$

We compute the value of each term one-by-one as follows:

$$\sum_{k=1}^{K} \mathbb{E}\left[Y_k\right] = \sum_{k=1}^{K} \Pr\left[h^{(k)}(\vec{a}) \neq h^{(k)}(\vec{b})\right]. \tag{33}$$

$$= \sum_{k=1}^{K} \frac{\theta_{(\vec{a},\vec{b})}}{\pi} = \frac{K\theta_{(\vec{a},\vec{b})}}{\pi}. \tag{34}$$

$$\sum_{k_1 \neq k_2, k_1, k_2 \in [K]} \mathbb{E}\left[Y_{k_1} Y_{k_2}\right] = \sum_{k_1 \neq k_2} \Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \cap \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right]. \tag{35}$$

$$= \sum_{k_1 \neq k_2, k_1, k_2 \in [K]} \Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \mid \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right] \times \Pr\left[\left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right]. \tag{36}$$

$$= \sum_{k_1 \neq k_2, k_1, k_2 \in [K]} \frac{\theta_{(\vec{a},\vec{b})}}{\pi} \cdot \Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \mid \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right]. \tag{37}$$

$$\left(\mathbb{E}\left[\sum_{k=1}^{K} Y_k\right]\right)^2 = \left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi}\right)^2. \tag{38}$$

We denote
$\Pr\left[\left(h^{(k_2)}(\vec{a}) \neq h^{(k_2)}(\vec{b})\right) \mid \left(h^{(k_1)}(\vec{a}) \neq h^{(k_1)}(\vec{b})\right)\right] := \eta$ in Equation (37), and $\eta \in \left[0, \frac{\theta}{\pi}\right]$. Therefore

$$\mathrm{Var}\left[\sum_{k=1}^{K} Y_k\right] = \frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1) \times \frac{\theta_{(\vec{a},\vec{b})}}{\pi} \times \eta - \left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi}\right)^2 \tag{39}$$

$$(40)$$

Thus the variance of our estimate is

$$\mathrm{Var}\left[\frac{\pi}{K}||h(\vec{a})-h(\vec{b})||_1\right] = \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\times\frac{\theta_{(\vec{a},\vec{b})}}{\pi}\times\eta - \left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi}\right)^2\right). \tag{41}$$

$$= \frac{\pi^2}{K^2}\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\times\frac{\theta_{(\vec{a},\vec{b})}}{\pi}\times\eta\right) - \theta^2_{(\vec{a},\vec{b})}. \tag{42}$$

The variance of SRP estimator is given as

$$\mathrm{Var}[X] = \frac{\pi^2}{K^2}\times\left(\frac{K\theta_{(\vec{a},\vec{b})}}{\pi} + K(K-1)\times\left(\frac{\theta_{(\vec{a},\vec{b})}}{\pi}\right)^2\right) - {\theta_{(\vec{a},\vec{b})}}^2. \tag{43}$$

□

Proof of Theorem 9:

In order to prove Theorem 9, we require the following lemma which is similar to Lemma 3. We first complete its proof and then conclude with the proof of Theorem 9.

Lemma 12. *[Adapted from Lemma 4 of Li et al. [2006b]] Let $\vec{r}' = (r'_1, \ldots, r'_j, \ldots, r'_D) \in \mathbb{R}^D$ s.t.*

$$r'_j \sim \begin{cases} 1 & \textit{with probability } \frac{l}{2K} \\ 0 & \textit{with probability } \frac{K-l}{K} \\ -1 & \textit{with probability } \frac{l}{2K} \end{cases} \tag{44}$$

and $\vec{a} \in \mathbb{R}^D$. Denote $\alpha' = \sum_{j=1}^D r'_j a_j = \langle \vec{r}', \vec{a}\rangle$. Then if $D \to \infty$ and $K = o(lD)$, we have $\alpha' \xRightarrow{\mathcal{L}} \mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$ with the rate of convergence

$$|F_{\alpha'}(y) - \Phi(y)| \leq 0.8\sqrt{\frac{K}{l}}\frac{\sum_{i=1}^D |a_i|^3}{(\sum_{i=1}^D a_i^2)^{3/2}} = 0.8\sqrt{\frac{K}{lD}}\frac{\mathbb{E}[|a_i|]^3}{(\mathbb{E}[a_i^2])^{3/2}} \to 0, \tag{45}$$

where $\xRightarrow{\mathcal{L}}$ denotes "convergence in distribution", $F_{\alpha'}(y)$ is the empirical cumulative density function of α', and $\Phi(y)$ is the CDF of $\mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$.

Proof. We know that

$$\alpha' = \sum_{j=1}^D r'_j a_j,$$

where

$$r'_j \sim \begin{cases} 1 & \text{with probability } \frac{l}{2K}, \\ 0 & \text{with probability } \frac{K-l}{K}, \\ -1 & \text{with probability } \frac{l}{2K}. \end{cases}$$

Let

$$z'_j = r'_j a_j.$$

Then

$$\mathbb{E}[z'_j] = \mathbb{E}[r'_j a_j] = a_j \mathbb{E}[r'_j] = 0.$$

$$\mathrm{Var}[z'_j] = \mathbb{E}[(z'_j - \mathbb{E}[z'_j])^2] = \mathbb{E}[z'^2_j] = \mathbb{E}[r'^2_j a_j^2] = \frac{l}{K} a_j^2.$$

$$\mathbb{E}[|z'_j|^{2+\delta}] = |a_j|^{2+\delta}\mathbb{E}[|r'_j|^{2+\delta}] = |a_j|^{2+\delta}\left(1 \times \frac{l}{K} + 0 \times \frac{K-l}{K}\right) = \frac{l}{K}|a_j|^{2+\delta}.$$

Let

$$S'^2_D = \sum_{j=1}^{D} \mathrm{Var}[z_j] = \frac{l}{K}\sum_{j=1}^{D} a_j^2.$$

To prove that $\frac{\sum_{j=1}^{D} z'_j}{S'_D} \overset{\mathcal{L}}{\Longrightarrow} \mathcal{N}(0,1)$, we need to show that following Lindeberg condition Gotze [1991], Feller [1971] is satisfied.

$$\frac{1}{S'^2_D}\sum_{j=1}^{D} \mathbb{E}\left[z'^2_j; |z'_j| > \epsilon S'_D\right] \to 0 \quad \text{for any } \epsilon > 0. \tag{46}$$

$$\implies \frac{1}{S'^2_D}\sum_{j=1}^{D} \mathbb{E}\left[z'^2_j; |z'_j| > \epsilon S'_D\right] \leq \frac{1}{S'^2_D}\sum_{j=1}^{D} \mathbb{E}\left[\frac{|z'_j|^{2+\delta}}{(\epsilon S'_D)^\delta}\right]. \tag{47}$$

$$= \frac{1}{\frac{l}{K}\sum_{j=1}^{D} a_j^2} \cdot \frac{1}{\epsilon^\delta} \cdot \frac{\frac{l}{K}\sum_{j=1}^{D} |a_j|^{2+\delta}}{\left(\frac{l}{K}\sum_{j=1}^{D} a_j^2\right)^{\frac{\delta}{2}}}. \tag{48}$$

$$= \frac{1}{\epsilon^\delta} \cdot \frac{\frac{l}{K}\sum_{j=1}^{D} |a_j|^{2+\delta}}{\left(\frac{l}{K}\sum_{j=1}^{D} a_j^2\right)^{\frac{2+\delta}{2}}}. \tag{49}$$

$$= \left(\frac{K}{l}\right)^{\frac{\delta}{2}} \cdot \frac{1}{\epsilon^\delta} \cdot \frac{\sum_{j=1}^{D} \frac{|a_j|^{2+\delta}}{D}}{\left(\frac{\sum_{j=1}^{D} a_j^2}{D}\right)^{\frac{2+\delta}{2}}} \cdot \frac{1}{D^{\frac{\delta}{2}}}. \tag{50}$$

$$= \left(\frac{K}{lD}\right)^{\frac{\delta}{2}} \cdot \frac{1}{\epsilon^\delta} \cdot \frac{\mathbb{E}\left[|a_j|^{2+\delta}\right]}{\left(\mathbb{E}[a_j^2]\right)^{\frac{2+\delta}{2}}}. \tag{51}$$

$$\to 0. \tag{52}$$

Equation (52) holds when $K = o(lD)$. Therefore, for $K = o(lD)$, due to Lindeberg Central Limit theorem Gotze [1991], Feller [1971], we have

$$\frac{\sum_{j=1}^{D} z'_j}{S'_D} = \frac{\sum_{j=1}^{D} r'_j a_j}{\sqrt{\frac{\sum_{j=1}^{D} a_j^2}{K}}} = \frac{\alpha'}{\sqrt{||\vec{a}||^2/K}} \overset{\mathcal{L}}{\Longrightarrow} \mathcal{N}(0,1). \tag{53}$$

$$\alpha' \overset{\mathcal{L}}{\Longrightarrow} \mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right). \tag{54}$$

We remain to find the rate of convergence. For this we use Berry Esseen theorem Shiganov [1986], Feller [1971]. Let us denote

$$\rho'_D = \sum_{j=1}^{D} \mathbb{E}\left[|z'_j|^3\right]. \tag{55}$$

$$= \sum_{j=1}^{D} |a_j|^3 \mathbb{E}\left[|r'_j|^3\right]. \tag{56}$$

$$= \frac{l}{K}\sum_{j=1}^{D} |a_j|^3. \tag{57}$$

From Berry Esseen theorem Shiganov [1986], Feller [1971], we have

$$
\begin{aligned}
&|F_{\alpha'}(y) - \Phi(y)| \leq 0.8 \frac{\rho'_D}{S'^3_D}. \\
&= 0.8 \frac{\frac{l}{K}\sum_{j=1}^{D} |a_j|^3}{\left(\frac{l}{K}\sum_{j=1}^{D} a_j^2\right)^{\frac{3}{2}}}. \\
&= 0.8 \times \sqrt{\frac{K}{lD}} \frac{\sum_{j=1}^{D} |a_j|^3/D}{\left(\sum_{j=1}^{D} a_j^2/D\right)^{\frac{3}{2}}}. \\
&= 0.8 \times \sqrt{\frac{K}{lD}} \frac{\mathbb{E}[|a_j|^3]}{\left(\mathbb{E}[a_j^2]\right)^{\frac{3}{2}}}. \\
&\to 0 \qquad \text{as} \quad D \to \infty. \qquad (58)
\end{aligned}
$$

Equation (58) holds for $K = o(lD)$. Equation (54) and (58) completes a proof of the Lemma 12. □

We now complete a proof of Theorem 9.

Theorem 9. *Let $\vec{a}, \vec{b} \in \mathbb{R}^D$, and let $h'(\vec{a})$ and $h'(\vec{b})$ be their K-dimensional binary vector obtained via our improved estimator proposal (stated in Definition 8). If $K = o(lD)$, then as $D \to \infty$ we have the following*

$$
\mathbb{E}\left[\frac{\pi}{K}||h'(\vec{a}) - h'(\vec{b})||_1\right] = \theta_{(\vec{a},\vec{b})}. \qquad (13)
$$

Proof. We first consider each row $\vec{r}'_k, 1 \leq k \leq K$ of the random matrix in Equation (12). The goal is to find the distribution of each $\vec{r}'_k$, and hence compute

$$
\mathbb{E}\left[\sum_{k=1}^{K} |h'^{(k)}(\vec{a}) - h'^{(k)}(\vec{b})|\right] = \sum_{k=1}^{K} \mathbb{E}\left[|h'^{(k)}(\vec{a}) - h'^{(k)}(\vec{b})|\right].
$$

Suppose we denote $Z'_k := |h'^{(k)}(\vec{a}) - h'^{(k)}(\vec{b})|$. While each Z'_k are not independent due to our construction of R', let us briefly consider how each $\vec{r}'_k$ is distributed.

When $k = 1$, we have that each entry in $\vec{r}'_1$ comes from a sparse Bernoulli distribution with

$$
r'_{1j} \sim \begin{cases} 1 & \text{with probability } \frac{l}{2K} \\ 0 & \text{with probability } \frac{K-l}{K} \\ -1 & \text{with probability } \frac{l}{2K}. \end{cases} \qquad (59)
$$

where $\mathbb{E}[r'_{1j}] = 0$, with $\text{Var}[r'_{1j}] = \frac{l}{K}$. Here, we note that each entry in $\vec{r}'_1$ is i.i.d.

We can also compute the moment generating function of each r'_{1j} and get

$$
\mathbb{E}\left[e^{sr'_{1j}}\right] = \frac{K-l}{K} + \frac{l \cdot (\exp\{s\} + \exp\{-s\})}{2K}. \qquad (60)
$$

Now let us consider the case $k = 2$, and compute the moment generating function for each r'_{2j}. By using the Law of Total Expectation, we have that

$$
\mathbb{E}\left[e^{sr'_{2j}}\right] = \mathbb{E}\left[e^{sr'_{2j}} \mid r'_{1j} = 0\right] \mathbb{P}\left[r'_{1j} = 0\right] + \mathbb{E}\left[e^{sr'_{2j}} \mid r'_{1j} = 1\right] \mathbb{P}\left[r'_{1j} = 1\right] + \mathbb{E}\left[e^{sr'_{2j}} \mid r'_{1j} = -1\right] \mathbb{P}\left[r'_{1j} = -1\right]. \qquad (61)
$$

$$
\begin{aligned}
&= \left(\frac{l(\exp\{s\} + \exp\{-s\})}{2(K-1)} + \frac{K-l-1}{K-1}\right)\frac{K-l}{K} + \left(\frac{(l-1)(\exp\{s\} + \exp\{-s\})}{2(K-1)} + \frac{K-l}{K-1}\right)\frac{l}{2K} \\
&\quad + \left(\frac{(l-1)(\exp\{s\} + \exp\{-s\})}{2(K-1)} + \frac{K-l}{K-1}\right)\frac{l}{2K}. \qquad (62)
\end{aligned}
$$

$$= l(K-1) \times \frac{(\exp\{s\} + \exp\{-s\})}{2K(K-1)} + \frac{(K-l)(K-1)}{(K-1)K}. \tag{63}$$

$$= \frac{l \cdot (\exp\{s\} + \exp\{-s\})}{2K} + \frac{(K-l)}{K}. \tag{64}$$

which is the same moment generating function as the Sparse Bernoulli distribution mentioned in Equation (59).

Now consider $\vec{r}_k, 2 < k \leq K-l$, and suppose we have seen l' non-zero entries so far. Denote $\lambda = \exp\{s\} + \exp\{-s\}$.

For ease of notation, if we have seen l' non-zero entries so far, then we have $\max(l-l', 0)$ non-zero entries to choose, out of the remaining $K-k+1$ terms, and the probability of drawing a non-zero for our k^{th} entry has to be given by $\frac{1}{2}p^{(l-l')}_{(K-k+1)} = \frac{\max(l-l',0)}{(K-k+1)}$.

Then we can write

$$\mathbb{E}\left[e^{sr'_{kj}}\right] = \sum_{i=0}^{l'} \left(\mathbb{E}\left[e^{sr'_{kj}} \mid i \text{ non-zeroes for } r'_{k'j}, k' < k\right] \times \mathbb{P}\left[i \text{ non-zeroes for } r'_{k'j}, k' < k\right]\right).$$

$$= \sum_{i=0}^{l'} \left[\left(\frac{1}{2}\lambda p^{(l-i)}_{(K-k+1)} + \left(1 - p^{(l-i)}_{(K-k+1)}\right)\right) \times \mathbb{P}\left[i \text{ non-zeroes for } r'_{k'j}, k' < k\right]\right].$$

Consider each term in the above summation. For the right term, we have

$$\begin{aligned}
&\sum_{i=1}^{l'} (1 - p^{(l-i)}_{(K-k+1)}) \mathbb{P}\left[i \text{ non-zeroes for } r'_{k'j}, k' < k\right] \\
&= \sum_{i=1}^{l'} p^{(K-l-(k-1-i))}_{(K-k+1)} \mathbb{P}\left[k-1-i \text{ zeroes for } r'_{k'j}, k' < k\right] \\
&= p_K^{K-l} \\
&= \frac{K-l}{K}.
\end{aligned} \tag{65}$$

The left term is more straightforward, and we have

$$\frac{1}{2}\sum_{i=0}^{l'} p^{(l-i)}_{(K-k+1)} \mathbb{P}\left[i \text{ non-zeroes for } r_{k'j}, k' < k\right] = \frac{1}{2}\frac{l}{K}\lambda.$$

Adding both terms together, we get the MGF of the Sparse Bernoulli distribution mentioned in Equation (59). Using Lemma 12, we can show that $\alpha'_k = \langle \vec{r'}_k, \vec{a} \rangle$ and $\beta'_k = \langle \vec{r'}_k, \vec{b} \rangle$ converge in distribution to $\mathcal{N}\left(0, \frac{||\vec{a}||^2}{K}\right)$ as D grows large. This fact and Lemma 4, concludes a proof of the theorem. □

C OTHER DETAILS:

GUARANTEE OF COUNT-SKETCH ALGORITHM:

The following theorem states that for a pair of real-valued vectors their sketches obtained via COUNT-SKETCH closely approximate the original pairwise inner product.

Theorem 13 (Weinberger et al. [2009], Charikar et al. [2004b])**.** *Given vectors $\vec{a} = [a_1, \ldots a_D]$, $\vec{b} = [b_1, \ldots b_D]$ get compressed into vectors $\vec{\alpha} = [\alpha_1, ..\alpha_k, ..\alpha_K]$ and $\vec{\beta} = [\beta_1, ..\beta_k, ..\beta_K]$, respectively, using the* COUNT-SKETCH *algorithm, where $k \in [K]$. Then, we have the following*

$$\mathbb{E}[\vec{\alpha}] = \mathbb{E}[\vec{\beta}] = \vec{0}. \tag{66}$$

$$\mathbb{E}[\langle \vec{\alpha}, \vec{\beta} \rangle] = \langle \vec{a}, \vec{b} \rangle. \tag{67}$$

$$\text{Var}[\langle \vec{\alpha}, \vec{\beta} \rangle] = \frac{1}{K} \sum_{i \neq j, i,j=1}^{D} \left(a_i^2 b_j^2 + a_i b_i a_j b_j\right). \tag{68}$$