OPORP: One Permutation + One Random Projection

Ping Li, Xiaoyun Li
LinkedIn Ads
700 Bellevue Way NE, Bellevue, WA, 98004, USA
{pinli,xiaoyli}@linkedin.com

ABSTRACT

OPORP is a variant of the count-sketch data structure by using a **fixed-length binning** scheme and a **normalization** step for the estimation. In our experience, we find engineers like the name "one permutation + one random projection" as it tells the exact steps.

Consider two vectors (e.g., embeddings): $u, v \in \mathbb{R}^D$ with $\rho = \cos(u, v)$. In embedding-based applications (e.g., EBR), $D = 256 \sim 4096$ are common. With OPORP, we first apply a permutation on the data vectors. A vector $r \in \mathbb{R}^D$ is generated i.i.d. with $E(r_i) = 0, E(r_i^2) = 1, E(r_i^3) = 0, E(r_i^4) = s$, where $s \geq 1$. We multiply (as Hadamard product) r with all permuted data vectors. Then we break the D columns into k equal-length bins and aggregate (i.e., sum) the values in each bin to obtain k samples from each data vector. One crucial step is to normalize the k samples to the unit l_2 norm. We show that the estimation variance equals:

$$(s-1)A + \frac{D-k}{D-1}\frac{1}{k}\left[(1-\rho^2)^2 - 2A\right], \qquad A \geq 0, \quad s \geq 1,$$

which reveals several key properties of the proposed scheme:

- We need $s = 1$, otherwise the variance would have a term which does not decrease with increasing sample size k.
- The factor $\frac{D-k}{D-1}$ is beneficial in reducing variances, especially for short vectors which are common in embeddings.
- The term $(1-\rho^2)^2$ is a drastic variance reduction compared to $(1+\rho^2)$ which is the variance term without normalization.

Moreover, the technique in our work also substantially improves the "very sparse random projections" (VSRP) in KDD'06. Another major use of OPORP will be in differential privacy (DP).

CCS CONCEPTS

• **Mathematics of computing → Probabilistic algorithms**.

KEYWORDS

Compression, Random projection, Hashing, Count Sketch

ACM Reference Format:
Ping Li, Xiaoyun Li. 2023. OPORP: One Permutation + One Random Projection. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23), August 6–10, 2023, Long Beach, CA, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3580305.3599457

KDD '23, August 6–10, 2023, Long Beach, CA, USA

ACM ISBN 979-8-4007-0103-0/23/08…$15.00
https://doi.org/10.1145/3580305.3599457

1 INTRODUCTION

OPORP ("one permutation + one random projection") is a vector compression scheme based on a variant of the count-sketch data structure [15]. The work has been adopted by research in differential privacy (DP) to develop "DP-OPORP", "DP-SignOPORP", etc [42].

Given two D-dimensional vectors (e.g., embeddings) $u, v \in \mathbb{R}^D$, a routine task is to compute the cosine similarity between u and v:

$$\rho = \frac{\sum_{i=1}^D u_i v_i}{\sqrt{\sum_{i=1}^D u_i^2}\sqrt{\sum_{i=1}^D v_i^2}}. \tag{1}$$

Often times applications also need to compute the (un-normalized) inner product (denoted by a) and the l_2 distance (denoted by d):

$$a = \sum_{i=1}^D u_i v_i, \qquad d = \sum_{i=1}^D |u_i - v_i|^2. \tag{2}$$

The data vectors can be the "embeddings" learned from deep learning models such as the celebrated "two-tower" model [32]. They can also be data vectors processed without training, for example, the n-grams (shingles), which can have million or billion or even higher dimensions [7, 8, 19, 20, 41, 47, 52, 54, 65, 68].

Embedding vectors generated from deep learning models are typically relatively short (e.g., $D = 256$ or $D = 1024$), often dense and normalized, i.e., $\sum_{i=1}^D u_i^2 = \sum_{i=1}^D v_i^2 = 1$. (In this study, we will not assume data vectors are normalized.) For example, for BERT-type of embeddings [24], the embedding size D is typically 768 or 1024; and Applications with BERT models may also use higher embedding dimensions, e.g., $D = 4096$ [29]. For GLOVE word embeddings [56], $D = 300$ is often the default choice. In recent EBR (embedding based retrieval) applications [14, 73, 74], using $D = 256$ or $D = 512$ appears common. For knowledge graph embeddings, we see the use of embedding size $D = 256 \sim 768$ [33, 64]. In many computer vision applications, the embedding sizes are often larger, e.g., 4096, 8192 or even larger [36, 38, 72]. The recent advances in GPT-3 models [10] for NLP tasks (text classification, semantic search, etc.) learn word embeddings with $D = 1024 \sim 12288$ [55].

Even with merely $D = 256$, the storage cost for the embeddings can be prohibitive in practical applications. Suppose an app has 100 million (active) users and each user is represented by a $D = 256$ embedding vector. Then just storing the embeddings (assuming each dimension is a 4-byte real number) would cost 100GB.

1.1 Count-Sketch and Variants

We briefly review the count-sketch data structure [15]. It first uses a hash function $h : [D] \mapsto [k]$ to uniformly map each data coordinate to one of k bins, and aggregates the coordinate values within the bin. Each coordinate $i \in [1, D]$ is multiplied by a Rademacher variable r_i with $P(r_i = -1) = P(r_i = 1) = 1/2$ before the aggregation. The binning procedure of count-sketch can be interpreted,

in a probabilistically equivalent manner, as the "variable-length binning scheme". That is, we first apply a random permutation on the data vector and splits the coordinates into k bins whose lengths follow a multinomial distribution. Also, in the original count-sketch, the above procedure is repeated m times (for identifying heavy hitters, another term for "compressed sensing"). The count-sketch data structure and variants have been widely used in applications. Recent examples include graph embedding [70], word & image embedding [2, 17, 62, 75, 76], model & communication compression [18, 31, 46, 60, 69], privacy [42], etc. Note that in many applications, only $m = 1$ repetition is used. Our analysis extends to $m > 1$. In fact, we can recover "very sparse random projections" (VSRP) [45] if we let $m > 1$ (and $k = 1$, i.e., using just one bin).

1.2 (Very Sparse) Random Projection

The work of OPORP is closely related to random projections (RP), especially "sparse" or "very sparse" random projections [1, 45]. The basic idea of random projections is to multiply the original data vectors, e.g., $u \in \mathbb{R}^D$ with a random matrix $R \in \mathbb{R}^{D\times k}$ to generate new vectors, e.g., $x \in \mathbb{R}^k$, as samples from which we can recover the original similarities (e.g., the inner products or cosines). The entries of the random matrix R are typically sampled i.i.d. from the standard Gaussian distribution or the Rademacher distribution. The projection matrix can also be made (very) sparse to facilitate computations. For instance, the entries in R take values in $\{-1, 0, 1\}$ with probabilities $\{1/(2s), 1 - 1/s, 1/(2s)\}$, and we can control the sparsity by altering s. In many cases, R can be considerably sparse while maintaining good learning capacity/utility. For example, in our experiments (Section 4), the performance does not drop much when the projection matrix contains around 90% zeros (i.e., $s = 10$).

As an effective tool for dimensionality reduction and geometry preservation, the methods of (very sparse) random projections have been widely adopted by numerous applications in data mining, learning, computational biology, databases, compressed sensing, etc. [1, 5, 11, 12, 16, 21–23, 26, 28, 30, 35, 45, 48–51, 57, 58, 67].

1.3 Our Contributions

OPORP differs from the standard count-sketch [15] in that: (i) we use a **fixed-length binning** scheme; (ii) we adopt a **normalization** step in the estimation stage. Compared with the previous works [43, 46, 69] which used count-sketch type data structures for building large-scale machine learning models, the normalization step significantly reduces the estimation variance, as shown by our theoretical analysis. In addition, the fixed-binning scheme brings in a multiplicative term $\frac{D-k}{D-1}$ in the variance (k is the number of bins in OPORP) which also substantially reduces the estimation error when (e.g.,) $k = D/4$. Experiments on retrieval and classification are provided in Section 4 to validate the advantage of OPORP.

In general, OPORP and VSRP (very sparser random projections) are two examples of the general family of sparse random projections. We can utilize OPORP to recover VSRP. Basically, by using m repetitions for OPORP and letting the k (number of bins) to be $k = 1$, we exactly recover VSRP with m projections. This means that the theory we develop for OPORP directly applies to VSRP. In particular, we immediately obtain the normalized estimator for VSRP and its theoretical variance. The normalized estimator of VSRP again substantially improves the un-normalized estimator.

2 THE PROPOSED ALGORITHM OF OPORP

As the name "OPORP" suggests, the proposed algorithm mainly consists of applying "one permutation" then "one random projection" on the data vectors $\in \mathbb{R}^D$, for the purpose of reducing the dimensionality, the memory/disk space, and the computational cost. The dimensionality D varies significantly, depending on applications. As discussed in Section 1, for embedding vectors generated from learning models, using $D = 256 \sim 1024$ is fairly common, although some applications use $D = 8192$ or even larger. As long as the embedding size D is not too large, it is affordable (and convenient) to simply generate and store the permutation vector and the random projection vector. In fact, even when D is as large as a billion ($D = 10^9$), storing two D-dimensional dense vectors is often affordable. On the other hand, for applications which need $D \gg 10^9$, we might have to resort to various approximations to generate/store the permutation/projection vectors such as the standard "universal hashing" [13]. In particular, in the literature of minwise hashing [7–9, 16, 34, 41, 46, 47], there are abundance of discussions about generating permutations in extremely high-dimensional space.

2.1 The Procedure of OPORP

In summary, the procedure of OPORP has the following steps:

- Generate a permutation $\pi : [D] \longrightarrow [D]$.
- Apply the same permutation to all vectors, e.g., $u, v \in \mathbb{R}^D$.
- Generate a random vector r of size D, with i.i.d. entries r_i of the following first four moments:

$$E(r_i) = 0, \quad E(r_i^2) = 1, \quad E(r_i^3) = 0, \quad E(r_i^4) = s. \tag{3}$$

  We show that $s = 1$ leads to the smallest variance. We carry out the calculations for general s, for the convenience of comparing with "very sparse random projections" [45].

- Divide the D columns into k bins. We will study the following two binning strategies:
  1) Fixed-length binning scheme: every bin has a length of D/k. We assume D is divisible by k, if not, we can always pad zeros. Our analysis will show that using this fixed-length scheme results in a variance reduction by a factor of $\frac{D-k}{D-1}$, which is quite significant for typical EBR applications, compared to the commonly-analyzed variable-length binning scheme of count-sketch.
  2) Variable-length binning scheme: the bin lengths follow a multinomial distribution $multinomial(D, 1/k, 1/k, ..., 1/k)$ with k bins. Note that k can be larger than D, i.e., some bins will be empty. The variable-length binning scheme is the strategy in the previous literature [15, 43, 46, 69].
- For each bin, we generate a sample as follows:

$$x_j = \sum_{i=1}^{D} u_i r_i I_{ij}, \qquad y_j = \sum_{i=1}^{D} v_i r_i I_{ij}, \quad j = 1, 2, ..., k, \tag{4}$$

  where I_{ij} is an indicator: $I_{ij} = 1$ if the original coordinate i is mapped to bin j, and $I_{ij} = 0$ otherwise. As there are two binning schemes, wherever necessary, we will use $I_{1,ij}$ (fixed-length) and $I_{2,ij}$ (variable-length) to differentiate them.

After obtaining the samples (x_j, y_j), we estimate the inner product a, l_2 distance d, and cosine ρ of the original data vectors as:

$$\hat{a} = \sum_{j=1}^{k} x_j y_j, \quad \hat{d} = \sum_{j=1}^{k} |x_j - y_j|^2, \quad \hat{\rho} = \frac{\sum_{j=1}^{k} x_j y_j}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}. \quad (5)$$

Note that, for $\hat{\rho}$, the normalization step is not needed at the estimation time if we pre-normalize the samples, e.g., $x'_j = \frac{x_j}{\sqrt{\sum_{t=1}^{k} x_t^2}}$.

Again, wherever necessary, we will use $\hat{a}_1$, $\hat{a}_2$, $\hat{d}_1$, $\hat{d}_2$, $\hat{\rho}_1$, $\hat{\rho}_2$, to differentiate two binning schemes. If the original data vectors (u, v) are normalized, then $\hat{a}$ also provides an estimate of the cosine because the original inner product is identical to the cosine in normalized data. One major contribution in this paper is to show that using $\hat{\rho}$ would be substantially more accurate than using $\hat{a}$ even when the original data are already normalized. Basically, the variance of $\hat{\rho}$ is proportional to $(1-\rho^2)^2$ while the variance of $\hat{a}$ (in normalized data) is proportional to $1+\rho^2$. The difference between $(1-\rho^2)^2$ and $1+\rho^2$ can be highly substantial, especially for $|\rho|$ close to 1.

2.2 The Choice of r

For the random projection vector $r \in \mathbb{R}^D$, we have only specified that its entries are i.i.d. and obey the following moment conditions:

$$E(r_i) = 0, \qquad E(r_i^2) = 1, \qquad E(r_i^3) = 0, \qquad E(r_i^4) = s, \quad s \geq 1.$$

Note that $s \geq 1$ is needed because $E(r_i^4) \geq E^2(r_i^2) = 1$. Readers who are familiar with random projections might attempt to sample r from the Gaussian distribution. Our analysis, however, will show that the Gaussian should not be used for OPORP. This is quite different from the standard random projections for which using either the Gaussian distribution or the Rademacher distribution (i.e., $r_i \in \{-1, +1\}$ with equal probabilities) would not make an essential difference. For OPORP, our analysis will show that we need $s = 1$ (i.e., the Rademacher distribution) to achieve a small estimation variance, by carrying out the calculations for general $s \geq 1$.

Here, we list some common distributions as follows:

- The standard Gaussian distribution $N(0, 1)$. This is the popular choice in the literature of random projections. The fourth moment of the standard Gaussian is 3, i.e., $s = 3$.
- The uniform distribution, $\sqrt{3} \times unif[-1, 1]$. We need the $\sqrt{3}$ factor in order to have $E(r_i^2) = 1$. For this choice of distribution, we have $E(r_i^4) = s = 9/5$.
- The "very sparse" distribution, as used in Li et al. [45]:

$$r_i = \sqrt{s} \times \begin{cases} -1 & \text{with prob.} \quad 1/(2s), \\ 0 & \text{with prob.} \quad 1 - 1/s, \\ +1 & \text{with prob.} \quad 1/(2s), \end{cases} \quad (6)$$

  which generalizes Achlioptas [1] (for $s = 1$ and $s = 3$).

2.3 Comparison: OPORP versus VSRP

Even though OPORP only effectively uses one random projection, we can still view that as a random projection "matrix" $\in \mathbb{R}^{D \times k}$ with exactly one 1 on each row. In comparison, the "very sparse random projections" (VSRP) [45] uses a random projection matrix $\in \mathbb{R}^{D \times k}$ with entries sampled i.i.d. from the "very sparse" distribution (6). Interestingly, for VSRP, if we let its "s" parameter to be $s = k$, then OPORP (with its $s = 1$) and VSRP will have the same sparsity on average in the projection "matrix". In terms of implementation, suppose we store the projection matrix, then it would be more convenient to store the one projection vector for OPORP because it is really just a vector of length D. In comparison, storing the sparse random projection matrix would incur an overhead because we have to store the locations (coordinates) of each non-zero entries.

In terms of the estimation variance, OPORP (with $s = 1$) would be more accurate than VSRP. Firstly, OPORP with the fixed-length binning scheme has the $\frac{D-k}{D-1}$ variance reduction term. Secondly, if we do not consider the $\frac{D-k}{D-1}$ term and we choose $s = 1$ for both OPORP and VSRP, then their theoretical variances are identical. As long as $s > 1$ for VSRP, the theoretical variance is larger than that of OPORP (for $s = 1$). If we choose $s = k$ for VSRP (to achieve the same average sparsity as OPORP), then its variance might be significantly larger, depending on the original data (e.g., u and v).

As mentioned, we can actually recover VSRP if we just use one bin for OPORP and repeat the procedure k times. This means that theory and estimators we develop for OPORP can be directly utilized to develop new theory and new estimator for VSRP. In particular, the normalized estimator for VSRP is developed whose variance can be directly inferred from the variance of OPORP.

3 THEORETICAL ANALYSIS OF OPORP AND NUMERICAL VERIFICATION

In this section, we conduct the theoretical analysis to derive the estimation variances for OPORP. Recall that, we generate k samples

$$x_j = \sum_{i=1}^{D} u_i r_i I_{ij}, \qquad y_j = \sum_{i=1}^{D} v_i r_i I_{ij}, \qquad j = 1, 2, ..., k$$

where I_{ij} is a random variable determined by one of the following two binning schemes:

(1) (*First binning scheme*) The fixed-length binning scheme: every bin has a length of D/k. We assume that D is divisible by k, if not, we can pad zeros. This is convenient in practice.

(2) (*Second binning scheme*) The variable-length binning scheme: as in the literature [15, 43, 46, 69], the bin lengths follow a multinomial distribution $multinomial(D, 1/k, 1/k, ..., 1/k)$.

Specifically, $I_{ij} = 1$ if the original coordinate $i \in [1, D]$ is mapped to bin $j \in [1, k]$; $I_{ij} = 0$ otherwise. Wherever necessary, we will use $I_{1,ij}$ and $I_{2,ij}$ to differentiate the two binning schemes. We have the following Lemma regarding the useful proprieties of I_{ij}.

LEMMA 3.1. *For $\forall i \in [1, D]$, $j \in [1, k]$, $i \neq i'$, $j \neq j'$, we have*

$$E(I_{1,ij}) = E(I_{1,ij}^n) = E(I_{2,ij}) = E(I_{2,ij}^n) = \frac{1}{k}, n = 1, 2, 3, ...,$$
$$E(I_{1,ij} I_{1,ij'}) = 0, \quad E(I_{2,ij} I_{2,ij'}) = 0,$$
$$E(I_{1,ij} I_{1,i'j'}) = \frac{D}{D-1}\frac{1}{k^2}, \quad E(I_{2,ij} I_{2,i'j'}) = \frac{1}{k^2},$$
$$E(I_{1,ij} I_{1,i'j}) = \frac{D-k}{D-1}\frac{1}{k^2}, \quad E(I_{2,ij} I_{2,i'j}) = \frac{1}{k^2},$$
$$kE\left(I_{ij} I_{i'j}\right) + k(k-1)E\left(I_{ij} I_{i'j'}\right) = 1.$$

Proof of Lemma 3.1: Consider the first binning scheme, where all k bins have the same length D/k. Thus, $E(I^n_{1,ij}) = E(I_{1,ij}) = \frac{D/k}{D} = \frac{1}{k}$. Each coordinate i can only be mapped to one bin, hence $E(I_{1,ij}I_{1,ij'}) = 0, \forall j \neq j'$. To understand $E(I_{1,ij}I_{1,i'j'}) = \frac{1}{k}\frac{D/k}{D-1} = \frac{D}{D-1}\frac{1}{k^2}$, we first assign i to j which occurs with probability $1/k$; then assign i' to j', which occurs with probability $\frac{D/k}{D-1}$ because the bin length is D/k and there are $D-1$ locations left (as one is taken). Finally, to understand $E(I_{1,ij}I_{1,i'j}) = \frac{1}{k}\frac{D/k-1}{D-1} = \frac{D-k}{D-1}\frac{1}{k^2}$, we only have $D/k-1$ (instead of D/k) choices because one location in bin j is already taken. For the second binning scheme, as the k bin lengths follow the multinomial distribution, the results follow using properties of multinomial moments after some algebra. □

3.1 The Un-normalized Estimators

Once we have samples x_j, y_j, we can estimate the original inner product a by $\hat{a} = \sum_{j=1}^k x_j y_j$. The results in Lemma 3.1 can assist us to derive the variances of the inner product estimators, $\hat{a}_1$ and $\hat{a}_2$ for two binning schemes, respectively.

Theorem 3.2.

$$E(\hat{a}) = a,$$

$$Var(\hat{a}_1) = (s-1)\sum_{i=1}^D u_i^2 v_i^2 + \frac{1}{k}\left(a^2 + \sum_{i=1}^D u_i^2 \sum_{i=1}^D v_i^2 - 2\sum_{i=1}^D u_i^2 v_i^2\right)\frac{D-k}{D-1},$$

$$Var(\hat{a}_2) = (s-1)\sum_{i=1}^D u_i^2 v_i^2 + \frac{1}{k}\left(a^2 + \sum_{i=1}^D u_i^2 \sum_{i=1}^D v_i^2 - 2\sum_{i=1}^D u_i^2 v_i^2\right).$$

Proof of Theorem 3.2: See Appendix A. □

Compared to $Var(\hat{a}_2)$ for the variable-bin-length scheme (which appeared in the prior work [46]), the additional factor $\frac{D-k}{D-1}$ in $Var(\hat{a}_1)$ demonstrates the benefit of the proposed fixed-bin-length strategy. Also, it is clear that we should choose $s = 1$. What if we only use one bin, i.e., $k = 1$? In this case $\frac{D-k}{D-1} = 1$, i.e., two binning scheme becomes identical. This is of course expected and also explains why in $\frac{D-k}{D-1}$ we have $D-1$ instead of just D.

What will happen if we repeat OPORP m times? In that case, the variances will be reduced by a factor of $\frac{1}{m}$, i.e.,

$$Var(\hat{a}_1; m \text{ repetitions})$$
$$= \frac{1}{m}\left[(s-1)\sum_{i=1}^D u_i^2 v_i^2 + \frac{1}{k}\left(a^2 + \sum_{i=1}^D u_i^2 \sum_{i=1}^D v_i^2 - 2\sum_{i=1}^D u_i^2 v_i^2\right)\frac{D-k}{D-1}\right],$$

$$Var(\hat{a}_2; m \text{ repetitions})$$
$$= \frac{1}{m}\left[(s-1)\sum_{i=1}^D u_i^2 v_i^2 + \frac{1}{k}\left(a^2 + \sum_{i=1}^D u_i^2 \sum_{i=1}^D v_i^2 - 2\sum_{i=1}^D u_i^2 v_i^2\right)\right].$$

Furthermore, if we let $k = 1$ and still repeat m times, then the two estimators become the same one and the variance would be

$$Var(\hat{a}; m \text{ repetitions and } k = 1)$$
$$= \frac{1}{m}\left(a^2 + \sum_{i=1}^D u_i^2 \sum_{i=1}^D v_i^2 + (s-3)\sum_{i=1}^D u_i^2 v_i^2\right),$$

which is exactly the variance formula for the inner product estimator of "very sparse random projections" (VSRP) [45]. This is expected because with $k = 1$ for OPORP and m repetitions, we recover the regular random projections with a projection matrix of size $D \times m$. We can also change the notation from $D \times m$ to $D \times k$.

Once we have the variances for the inner products, it is straightforward to derive the variances for the distance estimators:

$$\hat{d} = \sum_{j=1}^k |x_j - y_j|^2 = \sum_{j=1}^k \left|\sum_{i=1}^D u_i r_i I_{ij} - \sum_{i=1}^D v_i r_i I_{ij}\right|^2 = \sum_{j=1}^k \left|\sum_{i=1}^D (u_i - v_i) r_i I_{ij}\right|^2.$$

Clearly, we just need to replace, in Theorem 3.2, both u_i and v_i by $u_i - v_i$, in order to derive Theorem 3.3.

Theorem 3.3.

$$E(\hat{d}) = d,$$

$$Var(\hat{d}_1) = (s-1)\sum_{i=1}^D |u_i - v_i|^4 + \frac{1}{k}\left(2d^2 - 2\sum_{i=1}^D |u_i - v_i|^4\right)\frac{D-k}{D-1},$$

$$Var(\hat{d}_2) = (s-1)\sum_{i=1}^D |u_i - v_i|^4 + \frac{1}{k}\left(2d^2 - 2\sum_{i=1}^D |u_i - v_i|^4\right).$$

In the variance formulas, the term $\frac{D-k}{D-1}$ of the fixed-length binning scheme, would be beneficial if k is a considerable fraction of D. This is possible in EBR (embedding-based retrieval) applications. For example, when $D = 512$ and $k = 128$, we have $\frac{D-k}{D} = 0.75$. A variance reduction by 25% would be quite considerable. Also the fixed-length binning scheme is actually easier to implement than the variable-length binning scheme. Note that, with the fixed-length scheme, we cannot choose a k value between $D/2$ and D.

Here, we provide a simulation study to verify Theorem 3.2 and present the simulation results in Figure 1. For each panel (for a specific target ρ) of Figure 1, we first generate two vectors from the standard bivariate Gaussian distribution with the target correlation ρ. To avoid ambiguity, we generate the vectors many times until we have two vectors whose cosine value is very close to the target ρ before we store the vectors. Otherwise the empirical cosine value can be quite different from the target ρ. After we generate the two vectors, we normalize them to simplify the presentation of the results because otherwise the results would be related to the norms too. Then we conduct OPORP 10^5 times for each k in $\{2, 4, 8, 16, 32, ..., D/2\}$. For convenience, we choose D to be powers of 2. We only present results for $D = 1024$ and $D = 64$ because the other plots are pretty similar. Note that for the variable-length binning scheme, we also add simulations for $D/2 < k < D$.

We report the simulations for both $s = 1$ and $s = 3$. In each panel, we plot four curves: the empirical mean square errors (MSE = variance + bias^2) for both binning schemes, and the theoretical variance curves (in dashed lines) for both binning schemes. The dashed lines are not visible because they overlap with the empirical MSEs, which verify that the correctness of the variance formulas. We can also see that, with the fixed-length binning scheme (Bin#1), the variance is noticeably smaller than the variance of the variable-length scheme at the same k, confirming the benefits due to the $\frac{D-k}{D-1}$ term. Note that for $s = 3$, the difference between the two binning scheme becomes smaller, because in the formulas the $\frac{D-k}{D-1}$ term does not apply to the term involving $(s-1)$.

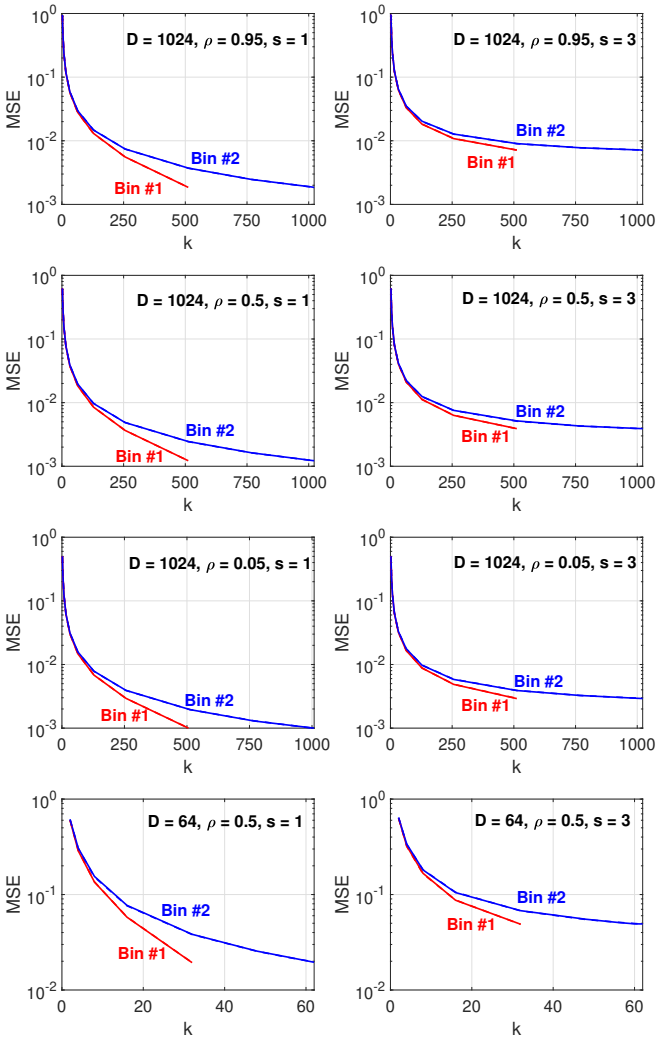

Figure 1: In each panel, we simulated two (normalized) vectors with the target ρ value. Then we conduct OPORP 10^5 times for each k, and both binning schemes. In each panel, the two solid curves represent the empirical mean square errors (MSE) and the two dashed curves for the theoretical variances. The dashed curves are not visible because they overlap with the solid curves. For the fixed-length binning scheme ("Bin #1"), we cannot choose a k between $D/2$ and D.

3.2 The Normalized Estimators

One can (substantially) improve the estimation accuracy via the "normalization" trick. That is, once we have the samples (x_j, y_j), $j = 1, 2, ..., k$, we can use the following normalized estimator:

$$\hat{\rho} = \frac{\sum_{j=1}^{k} x_j y_j}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}.$$

Again, we use $\hat{\rho}_1$ and $\hat{\rho}_2$ to denote the estimates for the fixed-length binning and variable-length binning, respectively. As explained earlier, the normalization step will not be needed at the estimation time if we pre-normalize the samples, a recommended practice.

Theorem 3.4. *For large k, $\hat{\rho}$ converges to ρ, almost surely, with*

$$Var(\hat{\rho}_1) = (s-1)A + \left\{\frac{1}{k}\left[(1-\rho^2)^2 - 2A\right] + O\left(\frac{1}{k^2}\right)\right\}\frac{D-k}{D-1},$$

$$Var(\hat{\rho}_2) = (s-1)A + \left\{\frac{1}{k}\left[(1-\rho^2)^2 - 2A\right] + O\left(\frac{1}{k^2}\right)\right\}.$$

where

$$A = \sum_{i=1}^{D}\left(u_i' v_i' - \rho/2(u_i'^2 + v_i'^2)\right)^2, u_i' = \frac{u_i}{\sqrt{\sum_{t=1}^{D} u_t^2}}, v_i' = \frac{v_i}{\sqrt{\sum_{t=1}^{D} v_t^2}}.$$

Proof of Theorem 3.4: See Appendix B. □

The variances in Theorem 3.4 hold for large k (i.e., $k \to D$ for the fixed-length binning and $k \to \infty$ for the variable-length binning). Note that the term $\frac{1}{k}\left(1-\rho^2\right)^2$ inside the variances of $\hat{\rho}$ is exactly the classical asymptotic variance of the correlation estimator for the bivariate Gaussian distribution [3]. Because $A \geq 0$, we know that OPORP achieves smaller (asymptotic) variance than the classical estimator in statistics, even without considering the $\frac{D-k}{D-1}$ factor.

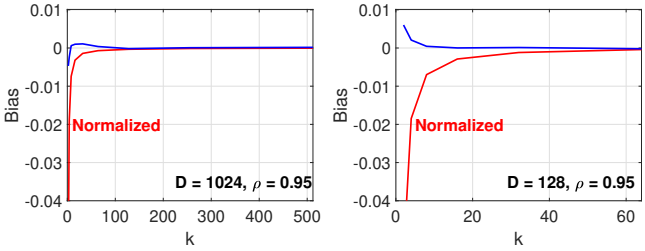

Figure 2: Empirical biases ($E(\hat{\rho}) - \rho$) of the normalized estimator $\hat{\rho}$ as well as the un-normalized estimator $\hat{a}$, evaluated on the same normalized data vectors in Figure 1, for $s = 1$ and the fixed-length binning scheme. The empirical biases are very small (and bias^2 would be much smaller).

A simulation study presented in Figure 2 and Figure 3 shows that k does not need to be large in order for these variance formulas to be sufficiently accurate.

In Figure 2 and Figure 3, we use the same data vectors as in Figure 1, for $s = 1$ and only the fixed-length binning scheme. Recall that those generated vectors are already normalized, and hence the inner product is the same as the cosine. This makes it convenient to present both the un-normalized and normalized estimators on the same plot. Recall MSE = variance + bias^2. Figure 2 illustrates that the variance formula in Theorem 3.4 is accurate, as long as k is not too small. The biases are very small (and bias^2 would be much smaller). The empirical MSE plots in Figure 3 confirm the significant variance reduction due to the normalization step.

3.3 The Normalized Estimator for VSRP

We have explained how to recover "very sparse random projections" (VSRP) [45] from OPORP by using $k = 1$ and repeating OPORP m times. We can also take advantage of this finding to develop the normalized estimator for VSRP and obtain its variance. To present the estimator and its theory for VSRP, instead of introducing new notation, we borrow the existing notation. Also, we still use k for

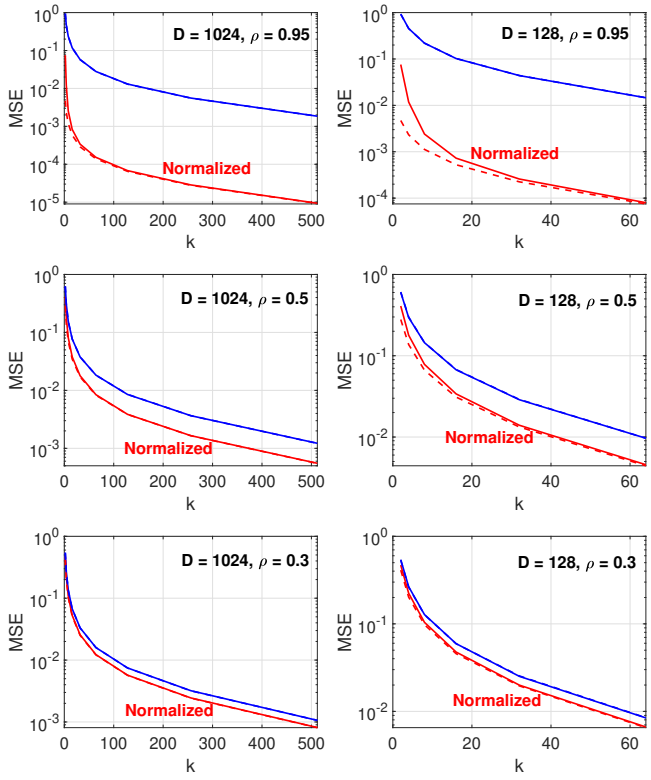

Figure 3: Empirical MSEs for both un-normalized and normalized estimators of OPORP, for $s = 1$ and the fixed-length binning scheme, using the same data vectors as in Figure 1. The normalization reduces the MSEs considerably especially for large ρ (i.e., higher similarity). The dashed curves for the theoretical (asymptotic) variance of $\hat{\rho}$ in Theorem 3.4 differ slightly from the empirical MSEs (solid curves) if k is small.

the sample size of VSRP instead of m. That is, we have

$$x_j = \sum_{i=1}^{D} u_i r_{ij}, \qquad y_j = \sum_{i=1}^{D} v_i r_{ij}, \qquad j = 1, 2, ..., k.$$

where r_{ij} follows the sparse distribution parameterized by s:

$$r_{ij} = \sqrt{s} \times \begin{cases} -1 & \text{with prob.} \quad 1/(2s) \\ 0 & \text{with prob.} \quad 1 - 1/s \\ +1 & \text{with prob.} \quad 1/(2s) \end{cases}$$

We have the un-normalized estimator for a and the normalized for ρ:

$$\hat{a}_{vsrp} = \frac{1}{k} \sum_{j=1}^{k} x_j y_j, \qquad \hat{\rho}_{vsrp} = \frac{\sum_{j=1}^{k} x_j y_j}{\sqrt{\sum_{j=1}^{k} x_j^2} \sqrt{\sum_{j=1}^{k} y_j^2}},$$

We have shown how to use the OPORP variance of $\hat{a}$ to recover the variance of $\hat{a}_{vsrp}$, to be

$$Var(\hat{a}_{vsrp}) = \frac{1}{k} \left(a^2 + \sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 + (s-3) \sum_{i=1}^{D} u_i^2 v_i^2 \right).$$

Since the normalized estimator and its variance for VSRP are new results, we present the result as a theorem.

Theorem 3.5. *As $k \to \infty$, $\hat{\rho}_{vsrp} \to \rho$ almost surely, with*

$$Var(\hat{\rho}_{vsrp}) = \frac{1}{k} \left((1-\rho^2)^2 + (s-3)A \right) + O\left(\frac{1}{k^2}\right),$$

where

$$A = \sum_{i=1}^{D} \left(u_i' v_i' - \rho/2 (u_i'^2 + v_i'^2) \right)^2, u_i' = \frac{u_i}{\sqrt{\sum_{t=1}^{D} u_t^2}}, v_i' = \frac{v_i}{\sqrt{\sum_{t=1}^{D} v_t^2}}.$$

One way to compare VSRP (for general s) with OPORP (for $s = 1$ and $m = 1$ repetition), is to evaluate the ratios of variances:

$$\frac{Var(\hat{a}_{vsrp,s})}{Var(\hat{a})} \approx \frac{\sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 + a^2 + (s-3) \sum_{i=1}^{D} u_i^2 v_i^2}{\sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 + a^2 - 2 \sum_{i=1}^{D} u_i^2 v_i^2}, \quad (7)$$

$$\frac{Var(\hat{\rho}_{vsrp,s})}{Var(\hat{\rho})} \approx \frac{(1-\rho^2)^2 + (s-3)A}{(1-\rho^2)^2 - 2A}, \quad (8)$$

where we use $\approx$ as we neglect the beneficial factor of $\frac{D-k}{D-1}$. Obviously, when $s = 1$, both ratios equal 1. The ratio increases with increasing s for VSRP. As the ratio is data-dependent, it is better that we compute it using real data.

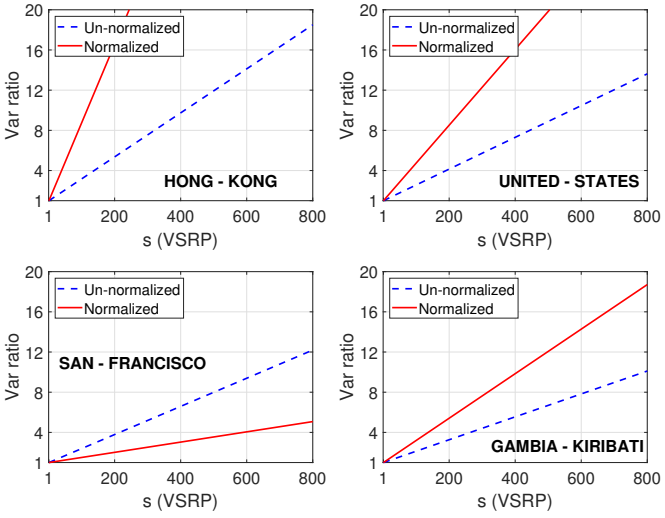

Figure 4: Ratio of variances in (7) and (8) to compare VSRP (parameterized by s) with OPORP (for its $s = 1$), for both the un-normalized (dashed) and normalized (solid) estimators, on four word pairs from the "Words" dataset (see Table 1).

Figure 4 presents the variance ratios in (7) and (8) on four selected word (vector) pairs from the "Words" dataset; see Table 1 for the description of the data. In general, if the s is not too large for VSRP (e.g., $s < 10$), then VSRP works pretty well. For larger s, then the performance of VSRP largely depends on data. For example, on "SAN-FRANCISCO", VSRP with the normalized estimator still works well (the variance ratio is smaller than 2) if with $s = 200$. On "HONG-KONG", however, VSRP does not perform well: for the normalized estimator, the variance ratio > 4 when $s > 40$; and for the un-normalized estimator, the variance ratio > 4 when $s > 150$.

The variance ratio = 4 means that we need to increase the sample size of VSRP by a factor of 4 in order to maintain the same accuracy. For VSRP with a the projection matrix size of size $D \times k$, it will need

Table 1: Summary statistics of word-pairs from the "Words" dataset [41]. For example, "HONG" represents a vector of length 2^{16} with each entry being the number of times that "HONG" appears in the collection of 2^{16} documents.

word 1	word 2	ρ	$a = \sum_{i=1}^{D} u_i v_i$	$\sum_{i=1}^{D} u_i^2$	$\sum_{i=1}^{D} v_i^2$
HONG	KONG	0.9623	12967	13556	13395
WEEK	MONTH	0.8954	281297	323073	305468
OF	AND	0.8788	57219161	69006071	61437886
UNITED	STATES	0.6693	69201	85934	124415
BEFORE	AFTER	0.6633	59136	65541	121284
SAN	FRANCISCO	0.5623	29386	125109	21832
GAMBIA	KIRIBATI	0.5250	228	360	524
RIGHTS	RESERVED	0.3949	14710	79527	17449
HUMAN	NATURE	0.2992	14896	87356	28367

$s = k$ if we hope to achieve the same level of sparsity as OPORP. Depending on applications, we typically observe that $k = 100 \sim 500$ might be sufficient for the standard (dense) random projections.

In summary, VSRP should work well in general if we use a sparsity parameter s around 10. VSRP may still perform well with a much larger s but then that will be data-dependent. In Section 4, the experimental results on VSRP will also confirm the same finding.

3.4 The Inner Product Estimators

The simulations in Figure 1, Figure 2, and Figure 3 have used data vectors which are normalized to the unit l_2 norm, in part for the convenience of presenting the plots. In many EBR applications, the embedding vectors from learning models are indeed already normalized. On the other hand, there are also numerous applications which use un-normalized data. In fact, the entire literature about "maximum inner product search" (MIPS) [4, 59, 61, 66, 78] is built on the fact that in many applications the norms are different and the goal is to find the maximum inner products (instead of the cosines). Also see Fan et al. [27] for the use of MIPS on advertisement retrievals in a commercial search engine.

Recall that, with samples (x_j, y_j), $j = 1, ..., k$, we can estimate the inner product a by $\hat{a} = \sum_{j=1}^{k} x_j y_j$. To improve the estimation accuracy, we can utilize the normalized cosine estimator $\hat{\rho} = \frac{\sum_{j=1}^{k} x_j y_j}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}$ to have a "normalized inner product estimator" $\hat{a}_n$:

$$\hat{a}_n = \hat{\rho}\sqrt{\sum_{i=1}^{D} u_i^2}\sqrt{\sum_{i=1}^{D} v_i^2},$$

whose variance is the scaled version of the variance of $\hat{\rho}$:

$$Var\left(\hat{a}_n\right) = Var\left(\hat{\rho}\right)\sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2.$$

Table 1 lists 9 word-pairs from the "Words" dataset [41]. Each word represents a vector of length 2^{16} and each entry records the number of times that word appears in a collection of 2^{16} documents. The selected 9 pairs cover a wide range of sparsity and similarity.

Next, we compare the two inner product estimators $\hat{a}$ and $\hat{a}_n$ for these 9 pairs of words. In order to provide a more complete picture, we also add another estimator based on the (approximate) maximum likelihood estimation (MLE). Because characterizing the exact joint distribution of (x_j, y_j), $j = 1, 2, ..., k$ would be too complicated, we resort to the MLE for the standard Gaussian random projections, as studied in Li et al. [44]. Basically, they show that the MLE estimator $\hat{a}_m$ is the solution to the following cubic equation:

$$\hat{a}_m^3 - \hat{a}_m^2 \sum_{j=1}^{k} x_j y_j - \sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 \sum_{j=1}^{k} x_j y_j + \hat{a}_m \left(- \sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 + \sum_{i=1}^{D} u_i^2 \sum_{j=1}^{k} y_j^2 + \sum_{i=1}^{D} v_i^2 \sum_{j=1}^{k} x_j^2 \right) = 0.$$

The MLE has the smallest variance if $\sum_{i=1}^{D} u_i^2$ and $\sum_{i=1}^{D} v_i^2$ are known. Obviously, the estimator $\hat{a}_m$ can no longer be written as an inner product (i.e., $\hat{a}_m$ is not a valid kernel for machine learning), unlike $\hat{a}$ or $\hat{\rho}$ or $\hat{a}_n$. Nevertheless, we can still use the MLE to assess the accuracy of estimators to see how close they are to be optimal.

Although we do not have the exact MLE for OPORP, we still use the above cubic equation as the "surrogate" for the MLE of OPORP and plot the empirical MSEs together with the MSEs of $\hat{a}$ and $\hat{a}_n$ in Figure 5, for estimating the inner products of the 9 word-pairs in Table 1. Each panel of Figure 5 presents 5 curves: the empirical MSEs for $\hat{a}$, $\hat{a}_n$, and $\hat{a}_m$, and the theoretical variances for $\hat{a}$ and $\hat{a}_n$. As expected, for $\hat{a}$ (the un-normalized estimator), the empirical MSEs overlap with the theoretical variances. The normalized estimator $\hat{a}_n$ is considerably more accurate than the un-normalized estimator $\hat{a}$, especially for word pairs with higher similarities. Also, for $\hat{a}_n$, the

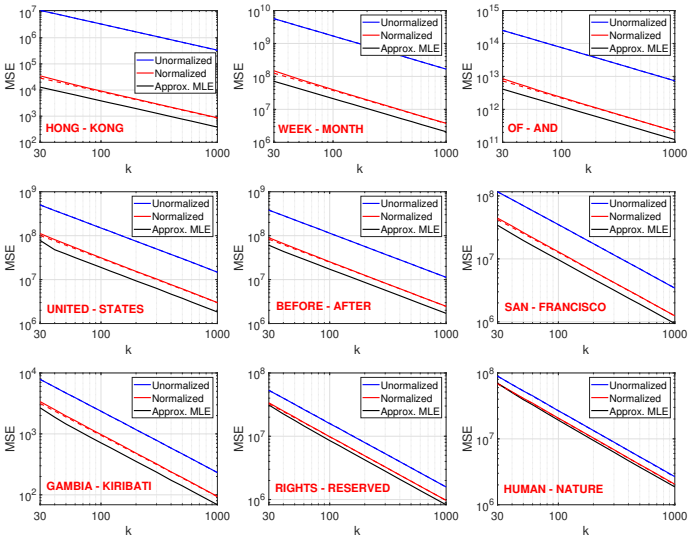

Figure 5: We estimate the inner products of the 9 pairs of words in Table 1, using the un-normalized estimator $\hat{a}$, the normalized estimator $\hat{a}_n$, as well as the approximate MLE estimator $\hat{a}_m$. We also plot, as dashed curves, the theoretical variances for $\hat{a}$ and $\hat{a}_n$. As expected, for $\hat{a}$, the empirical MSEs overlap with the theoretical variances. The normalized estimator $\hat{a}_n$ is considerably more accurate than $\hat{a}$, especially for word pairs with higher similarities. Also, for $\hat{a}_n$, the empirical MSEs do not differ much from the theoretical asymptotic variances. The "approximate MLE" $\hat{a}_m$ is still more accurate than $\hat{a}_n$, although the differences are quite small.

empirical MSEs do not differ much from the theoretical asymptotic variances, although they do not fully overlap. Interestingly, the "approximate MLE" $\hat{a}_m$ is still more accurate than the normalized estimator $\hat{a}_n$, although the differences are quite small.

Finally, Figure 6 compares VSRP (for its $s \in \{1, 10, 30, 100, 200\}$) with OPORP, for both the normalized and un-normalize estimator, using the "HONG-KONG" word pair. The plots confirm the theoretical result in Theorem 3.5. In this example, VSRP with $s = 1$ has essentially the same MSEs as OPORP, as the theory predicts. Note that in this case $\frac{D-k}{D-1}$ is too small to be able to help OPORP to reduce the variance. As we increase s for VSRP, the accuracy degrades quite substantially, again as predicted by the theory. We will observe the similar pattern in the experimental study in Section 4.

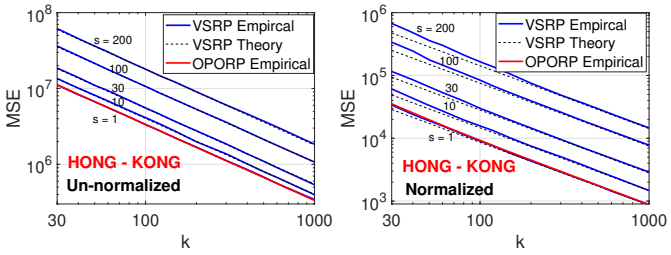

Figure 6: Comparing VSRP (with $s \in \{1, 10, 30, 100, 200\}$) with OPORP, in terms of their empirical MSEs, for both the un-normalized (left) and normalized (right) estimators, for the "HONG-KONG" word pair. As predicted by the theory, VSRP with $s = 1$ essentially has the same accuracy as OPORP. Clearly, the normalized estimators are substantially more accurate than the un-normalized estimators. For the un-normalized VSRP estimator, the theoretical variance curves (dashed) overlap the solid MSE curves (solid). For the normalized VSRP estimator, the empirical MSEs slightly deviate from the theoretical variances (in Theorem 3.5) for small k.

4 EXPERIMENTS

For the sake of repeatability, we conduct experiments on two standard (small) datasets: the MNIST dataset with 60000 training samples and 10000 testing samples, and the ZIP dataset (zipcode) with 7291 training samples and 2007 testing samples. The data vectors are normalized to have the unit l_2 norm. The MNIST dataset has 784 features and the ZIP dataset has 256 features. These dimensions well correspond with typical EBR embedding vector sizes.

4.1 Retrieval

We treat the test data as query vectors. For each query vector, we compute/estimate the cosine similarities with all the data vectors in the training set. For each estimation method, we rank the retrieved data vectors according to the estimated cosine similarities. In other words, there will be two ranked lists, one using the true cosines and the other using estimated cosines. By walking down the lists, we can compute the precision and recall curves. This allows us to compare OPORP with VSRP and their various estimators.

Figure 7 presents the precision-recall curves for retrieving the top-50 candidates on MNIST. The curves for top-10 are pretty similar. As expected, the OPORP normalized estimator performs much

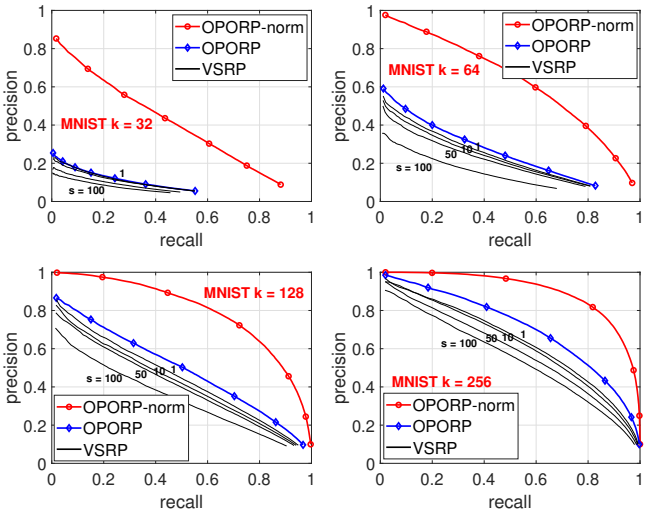

Figure 7: Precision-recall curves for MNIST (top-50) retrieval, using estimated cosines from the OPORP normalized estimator $\hat{\rho}$, the OPORP un-normalized estimator $\hat{a}$ (note that the original data are normalized), and the VSRP (parameterized by s) inner product estimator for $s \in \{1, 10, 50, 100\}$.

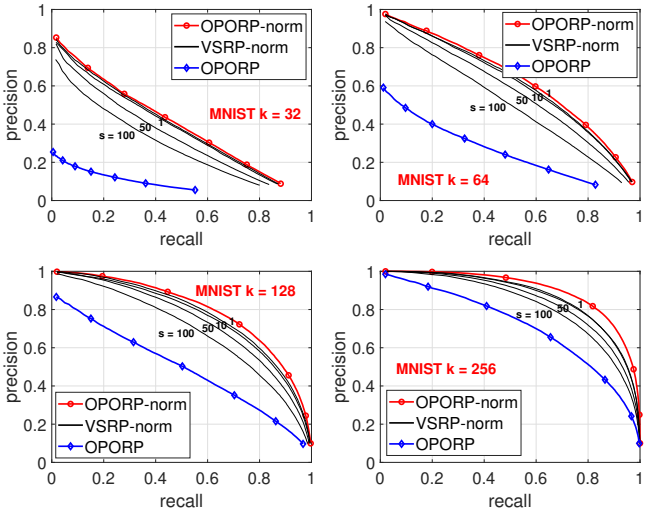

Figure 8: The content is similar to Figure 7, but this time we normalize the estimator of VSRP with $s \in \{1, 10, 50, 100\}$.

better than the un-normalized inner product estimator of OPORP, for all $k \in \{32, 64, 128, 256\}$. The comparisons with VSRP (parameterized by s) are very interesting. Recall that VSRP with $s = 1$ has the same variance as the un-normalized estimator of OPORP except for the $\frac{D-k}{D-1}$ term. In Figure 7, it is clear that the un-normalized OPORP estimator performs better than VSRP, which is due to the $\frac{D-k}{D-1}$ term. This effect is especially obvious for $k = 256$ and $k = 128$. By increasing s for VSRP, we can observe deteriorating performances. In particular, when $s = 100$ (i.e., the projection matrix of VSRP is extremely sparse), the loss of accuracy might be unacceptable.

Figure 8 is quite similar to Figure 7 except that Figure 8 presents the normalized inner product estimator of VSRP, again for $s \in$

$\{1, 10, 50, 100\}$. Indeed, as already shown by theory, the normalized estimator of VSRP improves the accuracy considerably. On the other hand, we still observe that, when $s = 1$ for VSRP, its accuracy is slightly worse than OPORP (due to the $\frac{D-k}{D-1}$ factor); and when $s = 100$, there is a severe deterioration of performance. Figure 8 once again confirms that the normalization trick is an excellent tool, which ought to be taken advantage of.

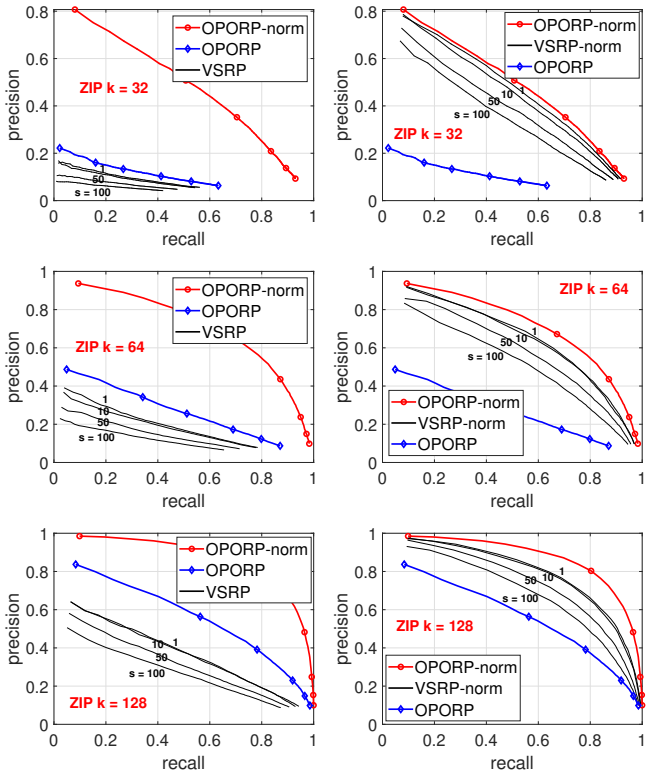

Figure 9: Precision-recall curves for ZIP (top-10) retrieval. The left panels are analogous to Figure 7 and the right panels are analogous to Figure 8 for MNIST retrieval.

Figure 9 presents the (top-10) retrieval experiments on the ZIP dataset. The plots are analogous to the plots in Figure 7 and Figure 8, with essentially the same conclusion. The normalized estimators considerably improve their un-normalized counterparts, for both VSRP and OPORP. There is more obvious gap between OPORP and VSRP with $s = 1$ because $\frac{D-k}{D-1}$ is quite small in for this dataset.

4.2 KNN classification

Figure 10 presents the experiments on KNN (K nearest neighbors) classification, in particular 1-NN and 10-NN, for both MNIST and ZIP datasets. We need the class labels for this set of experiments. In each panel, the vertical axis represents the test classification accuracy (in %). The original classification accuracy (the dashed horizontal curve) is pretty high, but we can approach the same accuracy with OPORP using the normalized estimator (with e.g., $k \geq 128$ for MNIST and $k \geq 64$ for ZIP). The performance of the un-normalized estimator of OPORP is considerably worse. Also, OPORP improves VSRP with $s = 1$ owing to the $\frac{D-k}{D-1}$ factor. Again, using VSRP with large s values leads to poor performance.

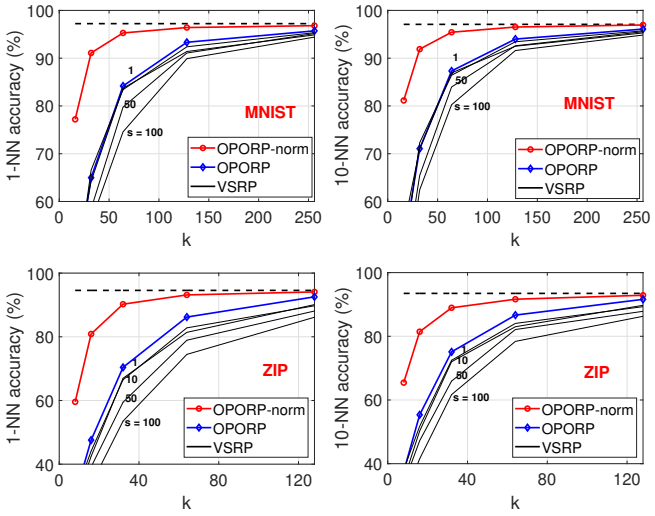

Figure 10: 1-NN and 10-NN classification results using cosines. The horizontal dashed lines represent the results using the true cosines. The general trends are pretty much the same as observed in the retrieval experiments in Figure 7. The vertical axis is the test classification accuracy.

5 CONCLUSION

Computing or estimating the inner products (or cosines) is the routine operation in numerous applications, not limited to machine learning. Reducing the storage/memory cost and speeding up the computations for computing/estimating the inner products or cosines can be crucial especially in many industrial applications such as embedding-based retrieval (EBR) for search and advertising.

The "one permutation + one random projection" (OPORP) is a variant of count-sketch and is closely related to "very sparse random projections" (VSRP). Compared to the standard random projections, OPORP is substantially more efficient (as it involves only one projection) and also more accurate. It differs from the standard count-sketch in that OPORP utilizes **(i) the fixed-length binning** scheme; **(ii) the normalized estimator** of cosine and inner product. We have conducted thorough variance analysis for OPORP (as well as VSRP) for both un-normalized and normalized estimators.

Among many applications (e.g., AI model compression), this work can be used as a key component in modern ANN (approximate near neighbor search) systems. For example, Zhao et al. [77] developed the GPU graph-based ANN and used random projections to reduce memory cost when data do not fit in the memory. For large-scale graph-based ANN methods [53, 78], the main cost is to compute similarities on the fly. We can effectively compress the vectors using OPORP to facilitate the distance computations at reduced storage.

OPORP and VSRP ("very sparse random projections") [45] are two examples of the family of sparse random projections. Our work on OPORP naturally recovers the estimator and theory of VSRP. As a "by-product", we also develop the normalized estimator for VSRP.

OPORP can be further quantized just like quantized random projections [6, 16, 23, 25, 30, 37, 39, 40, 48, 50, 51, 63, 71, 79]. Another major use of OPORP would be for the differential privacy (DP) [42].

REFERENCES

[1] Dimitris Achlioptas. Database-friendly random projections: Johnson-lindenstrauss with binary coins. *J. Comput. Syst. Sci.*, 66(4):671–687, 2003.

[2] Eman Abdullah AlOmar, Wajdi Aljedaani, Murtaza Tamjeed, Mohamed Wiem Mkaouer, and Yasmine N. El-Glaly. Finding the needle in a haystack: On the automatic identification of accessibility user reviews. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 387:1–387:15, Virtual Event / Yokohama, Japan, 2021.

[3] Theodore W. Anderson. *An Introduction to Multivariate Statistical Analysis*. John Wiley & Sons, third edition, 2003.

[4] Yoram Bachrach, Yehuda Finkelstein, Ran Gilad-Bachrach, Liran Katzir, Noam Koenigstein, Nir Nice, and Ulrich Paquet. Speeding up the Xbox recommender system using a euclidean transformation for inner-product spaces. In *Proceedings of the Eighth ACM Conference on Recommender Systems (RecSys)*, pages 257–264, Foster City, CA, 2014.

[5] Ella Bingham and Heikki Mannila. Random projection in dimensionality reduction: Applications to image and text data. In *Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 245–250, San Francisco, CA, 2001.

[6] Petros Boufounos and Richard G. Baraniuk. 1-bit compressive sensing. In *Proceedings of the 42nd Annual Conference on Information Sciences and Systems (CISS)*, pages 16–21, Princeton, NJ, 2008.

[7] Andrei Z Broder. On the resemblance and containment of documents. In *Proceedings of the Compression and Complexity of Sequences (SEQUENCES)*, pages 21–29, Salerno, Italy, 1997.

[8] Andrei Z. Broder, Steven C. Glassman, Mark S. Manasse, and Geoffrey Zweig. Syntactic clustering of the web. *Comput. Networks*, 29(8-13):1157–1166, 1997.

[9] Andrei Z. Broder, Moses Charikar, Alan M. Frieze, and Michael Mitzenmacher. Min-wise independent permutations. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing (STOC)*, pages 327–336, Dallas, TX, 1998.

[10] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel Ziegler, Jeffrey Wu, Clemens Winter, Chris Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. Language models are few-shot learners. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 1877–1901, virtual, 2020.

[11] Jeremy Buhler. Efficient large-scale sequence comparison by locality-sensitive hashing. *Bioinformatics*, 17(5):419–428, 2001.

[12] Emmanuel J. Candès, Justin K. Romberg, and Terence Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inf. Theory*, 52(2):489–509, 2006.

[13] Larry Carter and Mark N. Wegman. Universal classes of hash functions (extended abstract). In *Proceedings of the 9th Annual ACM Symposium on Theory of Computing (STOC)*, pages 106–112, Boulder, CO, 1977.

[14] Wei-Cheng Chang, Felix X. Yu, Yin-Wen Chang, Yiming Yang, and Sanjiv Kumar. Pre-training tasks for embedding-based large-scale retrieval. In *Proceedings of the 8th International Conference on Learning Representations (ICLR)*, Addis Ababa, Ethiopia, 2020.

[15] Moses Charikar, Kevin Chen, and Martin Farach-Colton. Finding frequent items in data streams. *Theor. Comput. Sci.*, 312(1):3–15, 2004.

[16] Moses S Charikar. Similarity estimation techniques from rounding algorithms. In *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing (STOC)*, pages 380–388, Montreal, Canada, 2002.

[17] Danqi Chen, Adam Fisch, Jason Weston, and Antoine Bordes. Reading wikipedia to answer open-domain questions. In *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (ACL)*, pages 1870–1879, Vancouver, Canada, 2017.

[18] Wenlin Chen, James Wilson, Stephen Tyree, Kilian Weinberger, and Yixin Chen. Compressing Neural Networks with the Hashing Trick. In *Proceedings of the 32nd International Conference on Machine Learning (ICML)*, pages 2285–2294, Lille, France, 2015.

[19] Flavio Chierichetti, Ravi Kumar, Silvio Lattanzi, Michael Mitzenmacher, Alessandro Panconesi, and Prabhakar Raghavan. On compressing social networks. In *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 219–228, Paris, France, 2009.

[20] Abhinandan Das, Mayur Datar, Ashutosh Garg, and Shyamsundar Rajaram. Google news personalization: scalable online collaborative filtering. In *Proceedings of the 16th International Conference on World Wide Web (WWW)*, pages 271–280, Banff, Alberta, Canada, 2007.

[21] Sanjoy Dasgupta. Experiments with random projection. In *Proceedings of the 16th Conference in Uncertainty in Artificial Intelligence (UAI)*, pages 143–151, Stanford, CA, 2000.

[22] Sanjoy Dasgupta and Yoav Freund. Random projection trees and low dimensional manifolds. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC)*, pages 537–546, Victoria, Canada, 2008.

[23] Mayur Datar, Nicole Immorlica, Piotr Indyk, and Vahab S Mirrokni. Locality-sensitive hashing scheme based on p-stable distributions. In *Proceedings of the Twentieth Annual Symposium on Computational Geometry (SCG)*, pages 253–262, Brooklyn, NY, 2004.

[24] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT)*, pages 4171–4186, Minneapolis, MN, 2019.

[25] Wei Dong, Moses Charikar, and Kai Li. Asymmetric distance estimation with sketches for similarity search in high-dimensional spaces. In *Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)*, pages 123–130, 2008.

[26] David L. Donoho. Compressed sensing. *IEEE Trans. Inf. Theory*, 52(4):1289–1306, 2006.

[27] Miao Fan, Jiacheng Guo, Shuai Zhu, Shuo Miao, Mingming Sun, and Ping Li. MOBIUS: towards the next generation of query-ad matching in baidu's sponsored search. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD)*, pages 2509–2517, Anchorage, AK, 2019.

[28] Xiaoli Zhang Fern and Carla E. Brodley. Random projection for high dimensional data clustering: A cluster ensemble approach. In *Proceedings of the Twentieth International Conference (ICML)*, pages 186–193, Washington, DC, 2003.

[29] John M. Giorgi, Osvald Nitski, Bo Wang, and Gary D. Bader. Declutr: Deep contrastive learning for unsupervised textual representations. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing, ACL/IJCNLP*, pages 879–895, Virtual Event, 2021.

[30] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. ACM*, 42(6):1115–1145, 1995.

[31] Farzin Haddadpour, Belhal Karimi, Ping Li, and Xiaoyun Li. Fedsketch: Communication-efficient and private federated learning via sketching. *arXiv preprint arXiv:2008.04975*, 2020.

[32] Po-Sen Huang, Xiaodong He, Jianfeng Gao, Li Deng, Alex Acero, and Larry P. Heck. Learning deep structured semantic models for web search using clickthrough data. In *Proceedings of the 22nd ACM International Conference on Information and Knowledge Management (CIKM)*, pages 2333–2338, San Francisco, CA, 2013.

[33] Xiao Huang, Jingyuan Zhang, Dingcheng Li, and Ping Li. Knowledge graph embedding based question answering. In *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining (WSDM)*, pages 105–113, Melbourne, Australia, 2019.

[34] Piotr Indyk. Sublinear time algorithms for metric space problems. In Jeffrey Scott Vitter, Lawrence L. Larmore, and Frank Thomson Leighton, editors, *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing (STOC)*, pages 428–434, Atlanta, GA, 1999.

[35] William B. Johnson and Joram Lindenstrauss. Extensions of Lipschitz mapping into Hilbert space. *Contemporary Mathematics*, 26:189–206, 1984.

[36] Andrej Karpathy, Armand Joulin, and Li Fei-Fei. Deep fragment embeddings for bidirectional image sentence mapping. In *Advances in Neural Information Processing Systems (NIPS)*, pages 1889–1897, Montreal, Canada, 2014.

[37] Karin Knudson, Rayan Saab, and Rachel Ward. One-bit compressive sensing with norm estimation. *IEEE Trans. Inf. Theory*, 62(5):2748–2758, 2016.

[38] Jack Lanchantin, Tianlu Wang, Vicente Ordonez, and Yanjun Qi. General multi-label image classification with transformers. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 16478–16488, virtual, 2021.

[39] Cong Leng, Jian Cheng, and Hanqing Lu. Random subspace for binary codes learning in large scale image retrieval. In *Proceedings of the 37th International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)*, pages 1031–1034, Gold Coast, Australia, 2014.

[40] Ping Li. Sign-full random projections. In *Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence (AAAI)*, pages 4205–4212, Honolulu, HI, 2019.

[41] Ping Li and Kenneth Ward Church. Using sketches to estimate associations. In *Proceedings of the Human Language Technology Conference and the Conference on Empirical Methods in Natural Language Processing (HLT/EMNLP)*, pages 708–715, Vancouver, Canada, https://github.com/pltrees/Smallest-K-Sketch, 2005.

[42] Ping Li and Xiaoyun Li. Differential privacy with random projections and sign random projections. *arXiv preprint*, 2023.

[43] Ping Li and Weijie Zhao. GCWSNet: Generalized consistent weighted sampling for scalable and accurate training of neural networks. In *Proceedings of the 31st ACM International Conference on Information and Knowledge Management (CIKM)*, Atlanta, GA, 2022.

[44] Ping Li, Trevor Hastie, and Kenneth Ward Church. Improving random projections using marginal information. In *Proceedings of the 19th Annual Conference on Learning Theory (COLT)*, pages 635–649, Pittsburgh, PA, 2006.

[45] Ping Li, Trevor J Hastie, and Kenneth W Church. Very sparse random projections. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge*

discovery and data mining (KDD), pages 287–296, Philadelphia, PA, 2006.

[46] Ping Li, Anshumali Shrivastava, Joshua L. Moore, and Arnd Christian König. Hashing algorithms for large-scale learning. In *Advances in Neural Information Processing Systems (NIPS)*, pages 2672–2680, Granada, Spain, 2011.

[47] Ping Li, Art B Owen, and Cun-Hui Zhang. One permutation hashing. In *Advances in Neural Information Processing Systems (NIPS)*, pages 3122–3130, Lake Tahoe, NV, 2012.

[48] Ping Li, Michael Mitzenmacher, and Anshumali Shrivastava. Coding for random projections. In *Proceedings of the 31th International Conference on Machine Learning (ICML)*, pages 676–684, Beijing, China, 2014.

[49] Xiaoyun Li and Ping Li. Generalization error analysis of quantized compressive learning. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 15124–15134, Vancouver, Canada, 2019.

[50] Xiaoyun Li and Ping Li. Random projections with asymmetric quantization. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 10857–10866, Vancouver, Canada, 2019.

[51] Xiaoyun Li and Ping Li. One-sketch-for-all: Non-linear random features from compressed linear measurements. In *Proceedings of the 24th International Conference on Artificial Intelligence and Statistics (AISTATS)*, pages 2647–2655, Virtual Event, 2021.

[52] Xiaoyun Li and Ping Li. C-MinHash: Improving minwise hashing with circulant permutation. In *Proceedings of the International Conference on Machine Learning (ICML)*, pages 12857–12887, Baltimore, MD, 2022.

[53] Yury A. Malkov and Dmitry A. Yashunin. Efficient and robust approximate nearest neighbor search using hierarchical navigable small world graphs. *IEEE Trans. Pattern Anal. Mach. Intell.*, 42(4):824–836, 2020.

[54] Fatemeh Nargesian, Erkang Zhu, Ken Q. Pu, and Renée J. Miller. Table union search on open data. *Proc. VLDB Endow.*, 11(7):813–825, 2018.

[55] Arvind Neelakantan, Tao Xu, Raul Puri, Alec Radford, Jesse Michael Han, Jerry Tworek, Qiming Yuan, Nikolas Tezak, Jong Wook Kim, and Chris Hallacy. Text and code embeddings by contrastive pre-training. *arXiv preprint arXiv:2201.10005*, 2022.

[56] Jeffrey Pennington, Richard Socher, and Christopher D. Manning. Glove: Global vectors for word representation. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 1532–1543, Doha, Qatar, 2014.

[57] Stephan Rabanser, Stephan Günnemann, and Zachary C. Lipton. Failing loudly: An empirical study of methods for detecting dataset shift. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 1394–1406, Vancouver, Canada, 2019.

[58] Ali Rahimi and Benjamin Recht. Random features for large-scale kernel machines. In *Advances in Neural Information Processing Systems (NIPS)*, pages 1177–1184, Vancouver, Canada, 2007.

[59] Parikshit Ram and Alexander G Gray. Maximum inner-product search using cone trees. In *Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 931–939, Beijing, China, 2012.

[60] Daniel Rothchild, Ashwinee Panda, Enayat Ullah, Nikita Ivkin, Ion Stoica, Vladimir Braverman, Joseph Gonzalez, and Raman Arora. FetchSGD: Communication-efficient federated learning with sketching. In *Proceedings of the 37th International Conference on Machine Learning (ICML)*, pages 8253–8265, Virtual Event, 2020.

[61] Anshumali Shrivastava and Ping Li. Asymmetric LSH (ALSH) for sublinear time maximum inner product search (MIPS). In *Advances in Neural Information Processing Systems (NIPS)*, pages 2321–2329, Montreal, Canada, 2014.

[62] Karan Singhal, Hakim Sidahmed, Zachary Garrett, Shanshan Wu, John Rush, and Sushant Prakash. Federated reconstruction: Partially local federated learning. In *Advances in Neural Information Processing Systems (NeurIPS)*, virtual, 2021.

[63] Martin Slawski and Ping Li. On the trade-off between bit depth and number of samples for a basic approach to structured signal recovery from b-bit quantized linear measurements. *IEEE Trans. Inf. Theory*, 64(6):4159–4178, 2018.

[64] Giuseppe Spillo, Cataldo Musto, Marco de Gemmis, Pasquale Lops, and Giovanni Semeraro. Knowledge-aware recommendations based on neuro-symbolic graph embeddings and first-order logical rules. In *Proceedings of the Sixteenth ACM Conference on Recommender Systems (RecSys)*, pages 616–621, Seattle, WA, 2022.

[65] Acar Tamersoy, Kevin A. Roundy, and Duen Horng Chau. Guilt by association: large scale malware detection by mining file-relation graphs. In *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 1524–1533, New York, NY, 2014.

[66] Shulong Tan, Zhaozhuo Xu, Weijie Zhao, Hongliang Fei, Zhixin Zhou, and Ping Li. Norm adjusted proximity graph for fast inner product retrieval. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*, pages 1552–1560, Virtual Event, Singapore, 2021.

[67] Tyler M. Tomita, James Browne, Cencheng Shen, Jaewon Chung, Jesse Patsolic, Benjamin Falk, Carey E. Priebe, Jason Yim, Randal C. Burns, Mauro Maggioni, and Joshua T. Vogelstein. Sparse projection oblique randomer forests. *J. Mach. Learn. Res.*, 21:104:1–104:39, 2020.

[68] Pinghui Wang, Yiyan Qi, Yuanming Zhang, Qiaozhu Zhai, Chenxu Wang, John C. S. Lui, and Xiaohong Guan. A memory-efficient sketch method for estimating high similarities in streaming sets. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD)*, pages 25–33, Anchorage, AK, 2019.

[69] 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)*, pages 1113–1120, Montreal, Canada, 2009.

[70] Jun Wu, Jingrui He, and Jiejun Xu. DEMO-Net: Degree-specific graph neural networks for node and graph classification. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD)*, pages 406–415, Anchorage, AK, 2019.

[71] Zhaozhuo Xu, Beidi Chen, Chaojian Li, Weiyang Liu, Le Song, Yingyan Lin, and Anshumali Shrivastava. Locality sensitive teaching. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 18049–18062, virtual, 2021.

[72] Chaojian Yu, Xinyi Zhao, Qi Zheng, Peng Zhang, and Xinge You. Hierarchical bilinear pooling for fine-grained visual recognition. In *Proceedings of the 15th European Conference on Computer Vision (ECCV), Part XVI*, pages 595–610, Munich, Germany, 2018.

[73] Tan Yu, Zhipeng Jin, Jie Liu, Yi Yang, Hongliang Fei, and Ping Li. Boost CTR prediction for new advertisements via modeling visual content. In *Proceedings of the IEEE International Conference on Big Data (IEEE BigData)*, Osaka, Japan, 2022.

[74] Tan Yu, Jie Liu, Yi Yang, Yi Li, Hongliang Fei, and Ping Li. EGM: enhanced graph-based model for large-scale video advertisement search. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*, pages 4443–4451, Washington, DC, 2022.

[75] Shan Zhang, Lei Wang, Naila Murray, and Piotr Koniusz. Kernelized few-shot object detection with efficient integral aggregation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 19185–19194, New Orleans, LA, 2022.

[76] Zhaoqi Zhang, Panpan Qi, and Wei Wang. Dynamic malware analysis with feature engineering and feature learning. In *Proceedings of the Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI)*, pages 1210–1217, New York, NY, 2020.

[77] Weijie Zhao, Shulong Tan, and Ping Li. SONG: approximate nearest neighbor search on GPU. In *Proceedings of the 36th IEEE International Conference on Data Engineering (ICDE)*, pages 1033–1044, Dallas, TX, 2020.

[78] Zhixin Zhou, Shulong Tan, Zhaozhuo Xu, and Ping Li. Möbius transformation for fast inner product search on graph. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 8216–8227, Vancouver, Canada, 2019.

[79] Argyrios Zymnis, Stephen P. Boyd, and Emmanuel J. Candès. Compressed sensing with quantized measurements. *IEEE Signal Process. Lett.*, 17(2):149–152, 2010.

A PROOF OF THEOREM 3.2

For two data vectors $u, v \in \mathbb{R}^D$, recall the notations of OPORP:

$$\hat{a} = \sum_{j=1}^{k} x_j y_j, \qquad x_j = \sum_{i=1}^{D} u_i r_i I_{ij}, \qquad y_j = \sum_{i=1}^{D} v_i r_i I_{ij}.$$

Assume the random variable r admits $E(r_i) = 0, E(r_i^2) = 1, E(r_i^3) = 0, E(r_i^4) = s$. Firstly, for the mean, we have

$$E(\hat{a}) = E(\sum_{j=1}^{k} x_j y_j) = E(\sum_{j=1}^{k}\sum_{i=1}^{D} u_i r_i I_{ij} \sum_{i=1}^{D} v_i r_i I_{ij})$$

$$= E(\sum_{j=1}^{k}\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j}) = E(\sum_{j=1}^{k}\sum_{i=1}^{D} u_i v_i \frac{1}{k}) = a.$$

We can compute the second moment of $\hat{a}$ as

$$E(\hat{a}^2) = E(\sum_{j=1}^{k} x_j y_j)^2 = E(\sum_{j=1}^{k}\sum_{i=1}^{D} u_i r_i I_{ij} \sum_{i=1}^{D} v_i r_i I_{ij})^2$$

$$= E(\sum_{j=1}^{k}\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})^2$$

$$= \sum_{j=1}^{k} E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})^2 + \sum_{j\neq j'} E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2$$

$$+ \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij'}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij'} I_{i'j'}). \quad (9)$$

For the first term, $E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})^2 = \frac{s\sum_{i=1}^{D} u_i^2 v_i^2}{k} + \sum_{i\neq i'}(u_i^2 v_{i'}^2 + 2u_i v_i u_{i'} v_{i'}) E(I_{ij} I_{i'j})$. To see this calculation, we can calculate three terms:

$$E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2)^2 = E(\sum_{i=1}^{D} u_i^2 v_i^2 r_i^4 I_{ij}^4) + E(\sum_{i\neq i'} u_i v_i r_i^2 I_{ij}^2 u_{i'} v_{i'} r_{i'}^2 I_{i'j}^2)$$

$$= s\frac{1}{k}\sum_{i=1}^{D} u_i^2 v_i^2 + \sum_{i\neq i'} u_i v_i u_{i'} v_{i'} E(I_{ij} I_{i'j}),$$

$$E(\sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})^2 = E(\sum_{i<i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j} + \sum_{i>i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})^2$$

$$= E[\sum_{i\neq i'} u_i^2 v_{i'}^2 r_i^2 r_{i'}^2 I_{ij}^2 I_{i'j}^2 + \sum_{i<i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j} \sum_{i<i'} u_{i'} v_i r_i r_{i'} I_{ij} I_{i'j}]$$

$$= \sum_{i\neq i'} u_i^2 v_{i'}^2 E(I_{ij} I_{i'j}) + \sum_{i\neq i'} u_i u_{i'} v_i v_{i'} E(I_{ij} I_{i'j}),$$

and $E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2)(\sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j}) = 0$, by noting that r_i's are i.i.d. and $E(r_i) = E(r_i^3) = 0$. Next, we compute

$$E(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij'}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij'} I_{i'j'})$$

$$= E[\sum_{i=1}^{D} u_i v_i r_i^2 I_{ij}^2 \sum_{i=1}^{D} u_i v_i r_i^2 I_{ij'}^2 + \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j} \sum_{i\neq i'} u_i v_{i'} r_i r_{i'} I_{ij'} I_{i'j'}]$$

$$= s\sum_{i=1}^{D} u_i^2 v_i^2 E(I_{ij} I_{ij'}) + \sum_{i\neq i'} u_i v_i u_{i'} v_{i'} E(I_{ij} I_{i'j'}) + \sum_{i\neq i'} u_i^2 v_{i'}^2 E(I_{ij} I_{i'j} I_{ij'} I_{i'j'})$$
$$+ \sum_{i\neq i'} u_i u_{i'} v_i v_{i'} E(I_{ij} I_{i'j} I_{ij'} I_{i'j'}) = \sum_{i\neq i'} u_i v_i u_{i'} v_{i'} E(I_{ij} I_{i'j'}),$$

where we have used the fact that $I_{ij} I_{ij'} = 0$ always. Now turning back to (9), we obtain $E(\hat{a}^2) = s\sum_{i=1}^{D} u_i^2 v_i^2 + kE(I_{ij} I_{i'j})\sum_{i\neq i'}(u_i^2 v_{i'}^2 + 2u_i v_i u_{i'} v_{i'}) + k(k-1)E(I_{ij} I_{i'j'})\sum_{i\neq i'} u_i v_i u_{i'} v_{i'}$. Therefore, the variance can be expressed as (after some algebra)

$$Var(\hat{a}) = E(\hat{a}^2) - a^2$$

$$= (s-1)\sum_{i=1}^{D} u_i^2 v_i^2 + kE(I_{ij} I_{i'j})\sum_{i\neq i'} u_i^2 v_{i'}^2 + kE(I_{ij} I_{i'j})\sum_{i\neq i'} u_i v_i u_{i'} v_{i'}$$

$$= (s-1)\sum_{i=1}^{D} u_i^2 v_i^2 + kE(I_{ij} I_{i'j})[a^2 + \sum_{i=1}^{D} u_i^2 \sum_{i=1}^{D} v_i^2 - 2\sum_{i=1}^{D} u_i^2 v_i^2].$$

The remaining part is to compute $E(I_{ij} I_{i'j})$ for the two binning schemes respectively using Lemma 3.1. □

B PROOF OF THEOREM 3.4

Recall the notations in OPORP:

$$x_j = \sum_{i=1}^{D} u_i r_i I_{ij}, \qquad y_j = \sum_{i=1}^{D} v_i r_i I_{ij}, \qquad j = 1, 2, ..., k.$$

To analyze the normalized cosine estimator $\hat{\rho} = \frac{\sum_{j=1}^{k} x_j y_j}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}$, it suffices to assume the original data are normalized to unit l_2 norms, i.e., $\sum_{i=1}^{D} u_i^2 = \sum_{i=1}^{D} v_i^2 = 1$. When the data are normalized, the inner product and the cosine are the same, i.e., $a = \rho$. Thus,

$$E(\sum_{j=1}^{k} x_j y_j) = \rho, \qquad E(\sum_{j=1}^{k} x_j^2) = E(\sum_{j=1}^{k} x_j^2) = 1,$$

We express the "deviation" as

$$\hat{\rho} - \rho = \frac{\sum_{j=1}^{k} x_j y_j - \rho}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}} + \rho\frac{1 - \sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}{\sqrt{\sum_{j=1}^{k} x_j^2}\sqrt{\sum_{j=1}^{k} y_j^2}}$$

$$= \sum_{j=1}^{k} x_j y_j - \rho/2\sum_{j=1}^{k} x_j^2 - \rho/2\sum_{j=1}^{k} y_j^2 + O_P(1/k),$$

where we use the approximation that $1 - ab = (1-a) + (1-b) - (1-a)(1-b)$ for $a, b \approx 1$. Hence, it suffices to analyze the term:

$$(\sum_{j=1}^{k} x_j y_j - \rho/2\sum_{j=1}^{k} x_j^2 - \rho/2\sum_{j=1}^{k} y_j^2)^2 \quad (10)$$

$$= (\sum_{j=1}^{k} x_j y_j)^2 + \frac{\rho^2}{4}(\sum_{j=1}^{k} x_j^2 + \sum_{j=1}^{k} y_j^2)^2 - \rho(\sum_{j=1}^{k} x_j y_j)(\sum_{j=1}^{k} x_j^2 + \sum_{j=1}^{k} y_j^2).$$

By Theorem 3.2, we know that $E(\sum_{j=1}^{k} x_j y_j)^2$ equals

$$= (s-1)\sum_{i=1}^{D} u_i^2 v_i^2 + kE(I_{ij} I_{i'j})[1 + \rho^2 - 2\sum_{i=1}^{D} u_i^2 v_i^2] + \rho^2, \quad (11)$$

and we can write $E(\sum_{j=1}^{k} x_j^2 \sum_{j=1}^{k} y_j^2) = E(\sum_{j=1}^{k} x_j^2 y_j^2 + \sum_{j\neq j'} x_j^2 y_{j'}^2)$. We now calculate each term. First, we have for $j = 1, ..., k$,

$$E(x_j^2 y_j^2) = s\frac{1}{k}\sum_{i=1}^{D} u_i^2 v_i^2 + E(I_{ij} I_{i'j})\sum_{i\neq i'}(u_i^2 v_{i'}^2 + 2u_i v_i u_{i'} v_{i'}).$$

Also, for $j \neq j'$, $E(x_j^2 y_{j'}^2) = E(\sum_{i=1}^D u_i r_i I_{ij})^2 (\sum_{i=1}^D v_i r_i I_{ij'})^2 = E(I_{ij} I_{i'j'}) \sum_{i \neq i'} u_i^2 v_{i'}^2$. Therefore, we obtain that

$$E(\sum_{j=1}^k x_j^2 \sum_{j=1}^k y_j^2) = s \sum_{i=1}^D u_i^2 v_i^2 + kE(I_{ij} I_{i'j}) \sum_{i \neq i'} (u_i^2 v_{i'}^2 + 2u_i v_i u_{i'} v_{i'}) + k(k-1) E(I_{ij} I_{i'j'}) \sum_{i \neq i'} u_i^2 v_{i'}^2.$$

Hence, $E(\sum_{j=1}^k x_j^2 + \sum_{j=1}^k y_j^2)^2$ equals

$$= (s-1) \sum_{i=1}^D (u_i^4 + v_i^4) + 2kE(I_{ij} I_{i'j})[4 - \sum_{i=1}^D (u_i^4 + v_i^4)] + 2s \sum_{i=1}^D u_i^2 v_i^2 + 2kE(I_{ij} I_{i'j}) \sum_{i \neq i'} (u_i^2 v_{i'}^2 + 2u_i v_i u_{i'} v_{i'}) + 2k(k-1) E(I_{ij} I_{i'j'}) \sum_{i \neq i'} u_i^2 v_{i'}^2. \quad (12)$$

We now analyze the third term in (10). It holds that

$$E(\sum_{j=1}^k x_j y_j)(\sum_{j=1}^k x_j^2 + \sum_{j=1}^k y_j^2) = E(\sum_{j=1}^k x_j^3 y_j + \sum_{j \neq j} x_j y_j x_{j'}^2) + E(\sum_{j=1}^k x_j y_j^3 + \sum_{j \neq j} x_j y_j y_{j'}^2).$$

We have

$$E(x_j y_j^3) = E(\sum_{i=1}^D u_i r_i I_{ij})(\sum_{i=1}^D v_i r_i I_{ij})^3$$

$$= E(\sum_{i=1}^D u_i v_i r_i^2 I_{ij} + \sum_{i \neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i=1}^D v_i^2 r_i^2 I_{ij} + \sum_{i \neq i'} v_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})$$

$$= E[\sum_{i=1}^D u_i v_i r_i^2 I_{ij} \sum_{i=1}^D v_i^2 r_i^2 I_{ij} + \sum_{i \neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j} \sum_{i \neq i'} v_i v_{i'} r_i r_{i'} I_{ij} I_{i'j}]$$

$$= \frac{s}{k} \sum_{i=1}^D u_i v_i^3 + \sum_{i \neq i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j}) + 2 \sum_{i \neq i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j})$$

$$= \frac{s}{k} \sum_{i=1}^D u_i v_i^3 + 3E(I_{ij} I_{i'j}) \sum_{i \neq i'} u_i v_i v_{i'}^2,$$

where we use the following computation:

$$E(\sum_{i \neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i \neq i'} v_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})$$

$$= \sum_{i \neq i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j}) + E(\sum_{i<i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i>i'} v_i v_{i'} r_i r_{i'} I_{ij} I_{i'j}) + E(\sum_{i>i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i<i'} v_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})$$

$$= \sum_{i \neq i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j}) + \sum_{i<i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j}) + \sum_{i<i'} u_{i'} v_i^2 v_{i'} E(I_{ij} I_{i'j})$$

$$= 2 \sum_{i \neq i'} u_i v_i v_{i'}^2 E(I_{ij} I_{i'j}).$$

Furthermore, we have

$$E(x_j y_j x_{j'}^2) = E(\sum_{i=1}^D u_i r_i I_{ij})(\sum_{i=1}^D v_i r_i I_{ij})(\sum_{i=1}^D u_i r_i I_{ij'})^2$$

$$= E(\sum_{i=1}^D u_i v_i r_i^2 I_{ij} + \sum_{i \neq i'} u_i v_{i'} r_i r_{i'} I_{ij} I_{i'j})(\sum_{i=1}^D u_i^2 r_i^2 I_{ij'} + \sum_{i \neq i} u_i u_{i'} r_i r_{i'} I_{ij'} I_{i'j'})$$

$$= E(I_{ij} I_{i'j'}) \sum_{i \neq i} u_i u_{i'}^2 v_i.$$

Thus, by symmetry we have

$$E(\sum_{j=1}^k x_j y_j)(\sum_{j=1}^k x_j^2 + \sum_{j=1}^k y_j^2) \quad (13)$$

$$= E(\sum_{j=1}^k x_j^3 y_j + \sum_{j \neq j} x_j y_j x_{j'}^2) + E(\sum_{j=1}^k x_j y_j^3 + \sum_{j \neq j} x_j y_j y_{j'}^2)$$

$$= s \sum_{i=1}^D (u_i v_i^3 + u_i^3 v_i) + 3kE(I_{ij} I_{i'j}) \sum_{i \neq i'} (u_i v_i v_{i'}^2 + u_i v_i u_{i'}^2) + k(k-1) E(I_{ij} I_{i'j'}) \sum_{i \neq i} (u_i u_{i'}^2 v_i + u_i v_{i'}^2 v_i).$$

Now we combine (11), (12) and (13) with (10) to obtain

$$(\sum_{j=1}^k x_j y_j - \rho/2 \sum_{j=1}^k x_j^2 - \rho/2 \sum_{j=1}^k y_j^2)^2$$

$$= (s-1) \sum_{i=1}^D ((1+\rho^2/2) u_i^2 v_i^2 + \rho^2 u_i^4/4 + \rho^2 v_i^4/4 - \rho u_i v_i^3 - \rho u_i^3 v_i) + kE(I_{ij} I_{i'j})[1 + \rho^2 - 2 \sum_{i=1}^D u_i^2 v_i^2] + \rho^2 kE(I_{ij} I_{i'j})[1 - \sum_{i=1}^D \frac{(u_i^4 + v_i^4)}{2}] + \rho^2 [4 + 2kE(I_{ij} I_{i'j})(\rho^2 - \sum_{i=1}^D u_i^2 v_i^2)]/2 - \rho[2\rho + 2kE(I_{ij} I_{i'j})(2\rho - \sum_{i=1}^D (u_i^3 v_i + u_i v_i^3))]$$

$$= (s-1) \sum_{i=1}^D ((1+\rho^2/2) u_i^2 v_i^2 + \rho^2 u_i^4/4 + \rho^2 v_i^4/4 - \rho u_i v_i^3 - \rho u_i^3 v_i) + kE(I_{ij} I_{i'j})[1 + \rho^2 - 2 \sum_{i=1}^D u_i^2 v_i^2 + \rho^2 - \rho^2/2 \sum_{i=1}^D (u_i^4 + v_i^4) + \rho^4 - \rho^2 \sum_{i=1}^D u_i^2 v_i^2 - 4\rho^2 + 2\rho \sum_{i=1}^D (u_i^3 v_i + u_i v_i^3)]$$

$$= (s-1)A + kE(I_{ij} I_{i'j})[(1-\rho^2)^2 - 2A],$$

where $A = \sum_{i=1}^D ((1+\rho^2/2) u_i^2 v_i^2 + \rho^2 u_i^4/4 + \rho^2 v_i^4/4 - \rho u_i v_i^3 - \rho u_i^3 v_i)$. This gives the general expression of the variance term. Applying Lemma 3.1 leads to the variance formula for the two binning schemes respectively. Lastly, we may simplify A as

$$A = \sum_{i=1}^D u_i^2 v_i^2 + \rho^2/4 \sum_{i=1}^D (u_i^2 + v_i^2)^2 - \rho \sum_{i=1}^D (u_i^3 v_i + u_i v_i^3)$$

$$= \sum_{i=1}^D (u_i v_i - \frac{\rho}{2}(u_i^2 + v_i^2))^2 + \rho(u_i v_i)(u_i^2 + v_i^2) - \rho(u_i^3 v_i + u_i v_i^3)$$

$$= \sum_{i=1}^D (u_i v_i - \frac{\rho}{2}(u_i^2 + v_i^2))^2.$$

This completes the proof for normalized data. Otherwise, we need to replace u_i and v_i by $u_i' = \frac{u_i}{\sqrt{\sum_{t=1}^D u_t^2}}$, and $v_i' = \frac{v_i}{\sqrt{\sum_{t=1}^D v_t^2}}$. □