Fast Locality-Sensitive Hashing for Approximate Near Neighbor Search*

Tobias Christiani

Abstract

The Indyk-Motwani Locality-Sensitive Hashing (LSH) framework (STOC 1998) is a general technique for constructing a data structure to answer approximate near neighbor queries by using a distribution $H$ over locality-sensitive hash functions that partition space. For a collection of $n$ points, after preprocessing, the query time is dominated by $O(n^\rho \log n)$ evaluations of hash functions from $H$ and $O(n^\rho)$ hash table lookups and distance computations where $\rho \in (0, 1)$ is determined by the locality-sensitivity properties of $H$. It follows from a recent result by Dahlgaard et al. (FOCS 2017) that the number of locality-sensitive hash functions can be reduced to $O(\log^2 n)$, leaving the query time to be dominated by $O(n^\rho)$ distance computations and $O(n^\rho \log n)$ additional word-RAM operations. We state this result as a general framework and provide a simpler analysis showing that the number of lookups and distance computations closely match the Indyk-Motwani framework, making it a viable replacement in practice. Using ideas from another locality-sensitive hashing framework by Andoni and Indyk (SODA 2006) we are able to reduce the number of additional word-RAM operations to $O(n^\rho)$.

1998 ACM Subject Classification E.1 Data Structures, H.3.3 Information Search and Retrieval

Keywords and phrases locality-sensitive hashing, approximate near neighbors, similarity search

Digital Object Identifier 10.4230/OASIcs...

1 Introduction

The approximate near neighbor problem is the problem of preprocessing a collection $P$ of $n$ points in a space $(X, \text{dist})$ into a data structure such that, for parameters $r_1 < r_2$ and given a query point $q \in X$, if there exists a point $x \in P$ with $\text{dist}(q, x) \leq r_1$, then the data structure is guaranteed to return a point $x' \in P$ such that $\text{dist}(q, x') < r_2$.

Indyk and Motwani [23] introduced a general framework for constructing solutions to the approximate near neighbor problem using a technique known as locality-sensitive hashing (LSH). The framework takes a distribution over hash functions $H$ that partition space with the property that near points are more likely to collide under a random $h \sim H$.

The locality-sensitive hashing framework of Indyk and Motwani has had a large impact in both theory and practice (see surveys [3] and [32] for an introduction), and many of the best known solutions to the approximate near neighbor problem in high-dimensional spaces, such as Euclidean space [2], the unit sphere under inner product similarity [4], and sets under Jaccard similarity [7] come in the form of families of locality-sensitive hash functions that can be plugged into the Indyk-Motwani LSH framework.

* The research leading to these results has received funding from the European Research Council under the European Union’s 7th Framework Programme (FP7/2007-2013) / ERC grant agreement no. 614331.
Fast Locality-Sensitive Hashing for Approximate Near Neighbor Search

**Definition 1** (Locality-sensitive hashing [23]). Let \((X, \text{dist})\) be a distance space and let \(\mathcal{H}\) be a distribution over functions \(h: X \rightarrow R\). We say that \(\mathcal{H}\) is \((r_1, r_2, p_1, p_2)\)-sensitive if for \(x, y \in X\) and \(h \sim \mathcal{H}\) we have that:

- If \(\text{dist}(x, y) \leq r_1\) then \(\Pr[h(x) = h(y)] \geq p_1\).
- If \(\text{dist}(x, y) \geq r_2\) then \(\Pr[h(x) = h(y)] \leq p_2\).

The Indyk-Motwani framework takes a \((r_1, r_2, p_1, p_2)\)-sensitive family \(\mathcal{H}\) and constructs a data structure that solves the approximate near neighbor problem for parameters \(r_1 < r_2\) with some positive constant probability of success. We will refer to this randomized approximate version of the near neighbor problem as the \((r_1, r_2)\)-near neighbor problem, where we require queries to succeed with probability at least 1/2 (Definition 7). To simplify the exposition we will assume throughout the introduction that \(0 < p_1 < p_2 < 1\) are constant, that a hash function \(h \in \mathcal{H}\) can be stored in \(n/\log n\) words of space, and for \(\rho = \log(1/p_1)/\log(1/p_2) \in (0, 1)\) that a point \(x \in X\) can be stored in \(O(n^\rho)\) words of space. Note that the assumption of a constant gap between \(p_1\) and \(p_2\) allows us to avoid performing distance computations by instead using the 1-bit sketching scheme of Li and König [25] together with the family \(\mathcal{H}\) to approximate distances (see Section 4 for details). In the remaining part of the paper we will state our results without any such assumptions to ensure, for example, that our results hold in the important case where \(p_1\) and \(p_2\) may depend on \(n\) or the dimensionality of the space [2, 4].

**Theorem 2** (Indyk-Motwani [23, 21], simplified). Let \(\mathcal{H}\) be \((r_1, r_2, p_1, p_2)\)-sensitive and let \(\rho = \log(1/p_1)/\log(1/p_2)\), then there exists a solution to the \((r_1, r_2)\)-near neighbor problem using \(O(n^{1+\rho})\) words of space and with query time dominated by \(O(n^\rho \log n)\) evaluations of functions from \(\mathcal{H}\).

The query time of the Indyk-Motwani framework is dominated by the number of evaluations of locality-sensitive hash functions. To make matters worse, almost all of the best known and most widely used locality-sensitive families have an evaluation time that is at least linear in the dimensionality of the underlying space [7, 11, 15, 2, 4]. Perhaps surprisingly, significant effort has been devoted to the problem of reducing the evaluation complexity of locality-sensitive hash families [31, 17, 24, 28, 29, 14], while the question of how many independent locality-sensitive hash functions are actually needed to solve the \((r_1, r_2)\)-near neighbor problem has received relatively little attention [1, 14].

This paper aims to bring attention to, strengthen, generalize, and simplify results that reduce the number of locality-sensitive hash functions used to solve the \((r_1, r_2)\)-near neighbor problem. In particular, we will extract an improved framework from a technique introduced by Dahlgaard et al. [12] in the context of set similarity search under Jaccard similarity, showing that the number of locality-sensitive hash functions can be reduced to \(O(\log^2 n)\).

### 1.1 Related work

**Indyk-Motwani.** The Indyk-Motwani framework uses \(L = O(n^\rho)\) independent partitions of space, each formed by overlaying \(k = O(\log n)\) random partitions induced by \(k\) random hash functions from a locality-sensitive family \(\mathcal{H}\). The parameter \(k\) is chosen such that a random partition has the property that a pair of points \(x, y \in X\) with \(\text{dist}(x, y) \leq r_1\) has probability \(n^{-\rho}\) of ending up in the same part of the partition, while a pair of points with \(\text{dist}(x, y) \geq r_2\) has probability \(n^{-1}\) of colliding. By randomly sampling \(L = O(n^\rho)\) such partitions we are able to guarantee that a pair of near points will collide with constant probability in at least one of them. Applying these \(L\) partitions to our collection of data points \(P\) and storing the result of each partition of \(P\) in a hash table we obtain a data structure that solves the \((r_1, r_2)\)-near neighbor problem as outlined in Theorem 2 above. Section 3 and 3.1 contains a more complete description of LSH-based frameworks and the Indyk-Motwani framework.
Andoni-Indyk. As previously mentioned, many locality-sensitive hash functions happen to have a super-constant evaluation time. This motivated Andoni and Indyk to introduce a replacement to the Indyk-Motwani framework in a paper on substring near neighbor search [1]. The key idea is to re-use hash functions from a small collection of size \( m \ll L \) by forming all combinations of \( \binom{m}{t} \) hash functions. This technique is also known as tensoring and has seen some use in the work on alternative solutions to the approximate near neighbor problem, in particular the work on locality-sensitive filtering [15, 6, 12]. By applying the tensoring technique the Andoni-Indyk framework reduces the number of hash functions to \( O(\exp(\sqrt{\rho \log n \log \log n})) = n^{o(1)} \) as stated in Theorem 3.

▶ Theorem 3 (Andoni-Indyk [1], simplified). Let \( \mathcal{H} \) be \((r_1, r_2, p_1, p_2)\)-sensitive and let \( \rho = \frac{\log(1/p_1)}{\log(1/p_2)} \), then there exists a solution to the \((r_1, r_2)\)-near neighbor problem using \( O(n^{1+\rho}) \) words of space and with query time dominated by \( O(\exp(\sqrt{\rho \log n \log \log n})) \) evaluations of functions from \( \mathcal{H} \) and \( O(n^\rho) \) other word-RAM operations.

The paper by Andoni and Indyk did not state this result explicitly as a theorem in the same form as the Indyk-Motwani framework and the analysis made some implicit restrictive assumptions on \( p_1, p_2 \) and ignored integer constraints. Perhaps for these reasons the result does not appear to have received much attention, although it has seen some limited use in practice [33]. In Section 3.2 we present a slightly different version of the Andoni-Indyk framework together with an analysis that satisfies integer constrains, providing a more accurate assessment of the performance of the framework in the general, unrestricted case.

Dahlgaard-Knudsen-Thorup. The paper by Dahlgaard et al. [14] introduced a different technique for constructing the \( L \) hash functions/partitions from a smaller collection of \( m \) hash functions from \( \mathcal{H} \). Here the idea is quite simply, instead of forming all combinations of subsets of size \( t \), to sample \( k \) hash functions from the collection to form each of the \( L \) partitions. The paper focused on a particular application to set similarity search under Jaccard similarity, and stated the result in terms of a solution to this problem. In Section 3.3 we provide a simplified and tighter analysis to yield a general framework:

▶ Theorem 4 (Dahlgaard-Knudsen-Thorup [14], simplified). Let \( \mathcal{H} \) be \((r_1, r_2, p_1, p_2)\)-sensitive and let \( \rho = \frac{\log(1/p_1)}{\log(1/p_2)} \), then there exists a solution to the \((r_1, r_2)\)-near neighbor problem using \( O(n^{1+\rho}) \) words of space and with query time dominated by \( O(\log^2 n) \) evaluations of functions from \( \mathcal{H} \) and \( O(n^\rho \log n) \) other word-RAM operations.

The analysis of [14] indicates that the Dahlgaard-Knudsen-Thorup framework, when compared to the Indyk-Motwani framework, would use at least 50 times as many partitions (and a corresponding increase in the number of hash table lookups and distance computations) to solve the \((r_1, r_2)\)-near neighbor problem with success probability at least \( 1/2 \). Using elementary tools, the analysis in this paper shows that we only have to use twice as many partitions as the Indyk-Motwani framework to obtain the same guarantee of success.

Comparison in practice. To provide some idea of what the number of hash functions \( H \) used by the different frameworks would be in practice, Figure 1 shows the value of \( \log_2 H \) that is obtained by actual implementations of the Indyk-Motwani (IM), Andoni-Indyk (AI), and Dahlgaard-Knudsen-Thorup (DKT) frameworks as described in Section 3 for \( p_1 = 1/2 \) and every value of \( 0 < p_2 < 1/2 \) for a solution to the \((r_1, r_2)\)-near neighbor problem on a collection of \( n = 2^{30} \) points. Figure 1 reveals that the number of hash functions used by the Indyk-Motwani framework exceeds \( 2^{30} \), the size of the collection of points \( P \), as
$p_2$ approaches $p_1$. In addition, locality-sensitive hash functions used in practice such as Charikar’s SimHash [11] and $p$-stable LSH [15] have evaluation time $O(d)$ for points in $\mathbb{R}^d$. These two factors might help explain why a linear scan over sketches of the entire collection of points is a popular approach in practice [33, 19]. The Andoni-Indyk framework reduces the number of hash functions by several orders of magnitude, and the Dahlgaard-Knudsen-Thorup framework presents another improvement of several orders of magnitude. Since the word-RAM complexity of the DKT framework matches the number of hash function used by the IM framework, the gap between the solid line (DKT) and the dotted line (IM) gives some indication of the time we can spend on evaluating a single hash function in the DKT framework without suffering a noticeable increase in the query time.

### 1.2 Contribution

**Improved word-RAM complexity.** In addition to our work on the Andoni-Indyk and Dahlgaard-Knudsen-Thorup frameworks as mentioned above, we show how the word-RAM complexity of the DKT framework can be reduced by a logarithmic factor. The solution is a simple combination of the DKT sampling technique and the AI tensoring technique: First we use the DKT sampling technique twice to construct two collections of $\sqrt{L}$ partitions. Then we use the AI tensoring technique to form $L = \sqrt{L} \times \sqrt{L}$ pairs of partitions from the two collections. Below we state our main Theorem 5 in its general form where we make no implicit assumptions about $H$ or about the complexity of storing a point or computing the distance between pairs of points in the space $(X, \text{dist})$.

▶ **Theorem 5.** Let $H$ be $(r_1, r_2, p_1, p_2)$-sensitive and let $\rho = \log(1/p_1)/\log(1/p_2)$, then there exists a solution to the $(r_1, r_2)$-near neighbor with the following properties:

- The complexity of the query operation is dominated by $O(\log^2(n)/p_1 \log^2(1/p_2))$ evaluations of functions from $H$ and $O(n^\rho/p_1)$ distance computations.

- The solution uses $O(n^{1+\rho}/p_1)$ words of space in addition to the space required to store the data and $O(\log^2(n)/p_1 \log^2(1/p_2))$ functions from $H$. 

![Figure 1](image-url) The number of locality-sensitive hash functions from a $(r_1, r_2, 0.5, p_2)$-sensitive family used by different frameworks to solve the $(r_1, r_2)$-near neighbor problem on a collection of $2^{30}$ points.
Under the same simplifying assumptions used in the statements of Theorem 2, 3, and 4, our main Theorem 5 can be stated as Theorem 4 with the word-RAM complexity reduced by a logarithmic factor to \(O(n^\rho)\). This improvement in the word-RAM complexity comes at the cost of a (rather small) constant factor increase in the number of hash functions, lookups, and distance computations compared to the DKT framework. By varying the size \(m\) of the collection of hash functions from \(H\) and performing independent repetitions we can obtain a tradeoff between the number of hash functions and the number of lookups. In Section 3.3 we remark on some possible improvements in the case where \(p_1\) is large.

Distance sketching using LSH. Finally, we combine Theorem 5 with the 1-bit sketching scheme of Li and König [25] where we use the locality-sensitive hash family to create sketches that allow us to leverage word-level parallelism and avoid direct distance computations. This sketching technique is well known and has been used before in combination with LSH-based approximate similarity search [13], but we believe there is some value in the simplicity of the analysis and in a clear statement of the combination of the two results as given in Theorem 6, for example in the important case where \(0 < p_2 < p_1 < 1\) are constant.

**Theorem 6.** Let \(H\) be \((r_1, r_2, p_1, p_2)\)-sensitive and let \(\rho = \log(1/p_1)/\log(1/p_2)\), then there exists a solution to the \((r_1, r_2)\)-near neighbor with the following properties:

- The complexity of the query operation is dominated by \(O(\log^2(n)/(p_1 - p_2)^2)\) evaluations of hash functions from \(H\) and \(O(n^\rho/(p_1 - p_2)^2)\) other word-RAM operations.
- The solution uses \(O(n^{1+\rho}/p_1 + n/(p_1 - p_2)^2)\) words of space in addition to the space required to store the data and \(O(\log^2(n)/(p_1 - p_2)^2)\) hash functions from \(H\).

## Preliminaries

### Problem and dynamization.
We begin by defining the version of the approximate near neighbor problem that the frameworks presented in this paper will be solving:

**Definition 7.** Let \(P \subseteq X\) be a collection of \(|P| = n\) points in a distance space \((X, \text{dist})\). A solution to the \((r_1, r_2)\)-near neighbor problem is a data structure that supports the following query operation: Given a query point \(q \in X\), if there exists a point \(x \in P\) with \(\text{dist}(q, x) \leq r_1\), then, with probability at least \(1/2\), return a point \(x' \in P\) such that \(\text{dist}(q, x') < r_2\).

We aim for solutions with a failure probability that is upper bounded by \(1/2\). The standard trick of using \(\eta\) independent repetitions of the data structure allows us to reduce the probability of failure to \(1/2^\eta\). For the sake of simplicity we restrict our attention to static solutions, meaning that we do not concern ourselves with the complexity of updates to the underlying set \(P\), although it is simple to modify the static solutions presented in this paper to dynamic solutions where the update complexity essentially matches the query complexity [27, 21].

### LSH powering.
The Indyk-Motwani framework and the Andoni-Indyk framework will make use of the following standard powering technique described in the introduction as “overlaying partitions”. Let \(k \geq 1\) be an integer and let \(H\) denote a locality-sensitive family of hash functions as in Definition 1. We will use the notation \(H^k\) to denote the distribution over functions \(h': X \rightarrow \mathbb{R}^k\) where

\[
h'(x) = (h_1(x), \ldots, h_k(x))
\]
and $h_1, \ldots, h_k$ are sampled independently at random from $\mathcal{H}$. It is easy to see that $\mathcal{H}^k$ is $(r_1, r_2, p_1^k, p_2^k)$-sensitive. To deal with some special cases we define $\mathcal{H}^0$ to be the family consisting of a single constant function.

**Model of computation.** We will work in the standard word-RAM model of computation [20] with a word length of $\Theta(\log n)$ bits where $n$ denotes the size of the collection $P$ to be searched in the $(r_1, r_2)$-near neighbor problem. During the preprocessing stage of our solutions we will assume access to a source of randomness that allows us to sample independently from a family $\mathcal{H}$ and to seed pairwise independent hash functions [9, 10]. The latter can easily be accomplished by augmenting the model with an instruction that generates a uniformly random word in constant time and using that to seed the tables of a Zobrist hash function [34].

### 3 Frameworks

**Overview.** We will describe frameworks that take as input a $(r_1, r_2, p_1, p_2)$-sensitive family $\mathcal{H}$ and a collection $P$ of $n$ points and constructs a data structure that solves the $(r_1, r_2)$-near neighbor problem. The frameworks described in this paper all use the same high-level technique of constructing $L$ hash functions $g_1, \ldots, g_L$ that are used to partition space such that a pair of points $x, y$ with $\text{dist}(x, y) \leq r_1$ will end up in the same part of one of the $L$ partitions with probability at least $1/2$. That is, for $x, y$ with $\text{dist}(x, y) \leq r_1$ we have that $\Pr[\exists l \in [L]: g_l(x) = g_l(y)] \geq 1/2$ where $[L]$ is used to denote the set $\{1, 2, \ldots, L\}$. At the same time we ensure that the expected number of collisions between pairs of points $x, y$ with $\text{dist}(x, y) \geq r_2$ is at most one in each partition.

**Preprocessing and queries.** During the preprocessing phase, for each of the $L$ hash functions $g_1, \ldots, g_L$ we compute the partition of the collection of points $P$ induced by $g_l$ and store it in a hash table in the form of key-value pairs $(z, \{x \in P \mid g_l(x) = z\})$. To reduce space usage we store only a single copy of the collection $P$ and store references to $P$ in our $L$ hash tables. To guarantee lookups in constant time we can use the perfect hashing scheme by Fredman et al. [18] to construct our hash tables. We will assume that hash values $z = g_l(x)$ fit into $O(1)$ words. If this is not the case we can use universal hashing [8] to operate on fingerprints of the hash values.

We perform a query for a point $q$ as follows: for $l = 1, \ldots, L$ we compute $g_l(q)$, retrieve the set of points $\{x \in P \mid g_l(x) = g_l(q)\}$, and compute the distance between $q$ and each point in the set. If we encounter a point $x'$ with $\text{dist}(q, x') < r_2$ then we return $x'$ and terminate. If after querying the $L$ sets no such point is encountered we return a special symbol $\emptyset$ and terminate.

We will proceed by describing and analyzing the solutions to the $(r_1, r_2)$-near neighbor problem for different approaches to sampling, storing, and computing the $L$ hash functions $g_1, \ldots, g_L$, resulting in the different frameworks as mentioned in the introduction.

#### 3.1 Indyk-Motwani

To solve the $(r_1, r_2)$-near neighbor problem using the Indyk-Motwani framework we sample $L$ hash functions $g_1, \ldots, g_L$ independently at random from the family $\mathcal{H}^k$ where we set $k = [\log(n)/\log(1/p_2)]$ and $L = [\ln 2]/p_1^k$. Correctness of the data structure follows from the observation that the probability that a pair of points $x, y$ with $\text{dist}(x, y) \leq r_1$ does not collide under a randomly sampled $g_l \sim \mathcal{H}^k$ is at most $1 - p_1^k$. We can therefore upper bound...
the probability that a near pair of points does not collide under any of the hash functions by 
\((1 - p_1^k)^L \leq \exp(-Lp_1^k) \leq 1/2\) using a standard bound stated as Lemma 13 in Appendix A.

In the worst case, the query operation computes \(L\) hash functions from \(H^k\) corresponding to \(Lk\) hash functions from \(H\). For a query point \(q\) the expected number of points \(x' \in P\) with \(\text{dist}(q, x') \geq r_2\) that collide with \(q\) under a randomly sampled \(g_i \sim H^k\) is at most 
\[np_2^k \leq np_2^{\log(n)/\log(1/p_2)} = 1.\]
It follows from linearity of expectation that the total expected number of distance computations during a query is at most \(L\). The result is summarized in Theorem 8 from which the simplified Theorem 2 follows.

\[\textbf{Theorem 8} \text{(Indyk-Motwani [23, 21]). Given a} (r_1, r_2, p_1, p_2)\)-sensitive family \(H\) we can construct a data structure that solves the \((r_1, r_2)\)-near neighbor problem such that for 
\(k = \lceil \log(n)/\log(1/p_2) \rceil\) the data structure has the following properties:

- The query operation uses at most \(Lk\) evaluations of hash functions from \(H\), expected \(L\) distance computations, and \(O(Lk)\) other word-RAM operations.
- The data structure uses \(O(nL)\) words of space in addition to the space required to store the \(H\) and \(Lk\) hash functions from \(H\).

Theorem 8 gives a bound on the expected number of distance computations while the simplified version stated in Theorem 2 uses Markov’s inequality and independent repetitions to remove the expectation from the bound by treating an excessive number of distance computations as a failure.

### 3.2 Andoni-Indyk

In 2006 Andoni and Indyk, as part of a paper on the substring near neighbor problem, introduced an improvement to the Indyk-Motwani framework that reduces the number of locality-sensitive hash functions [1]. Their improvement comes from the use of a technique that we will refer to as tensoring: setting the hash functions \(g_1, \ldots, g_L\) to be all \(t\)-tuples from a collection of \(m\) functions sampled from \(H^{k1}\) where \(m \ll L\). The analysis in [1] shows that by setting \(m = n^{o(t)}\) and repeating the entire scheme \(t\) times, the total number of hash functions can be reduced to \(O(\exp(\sqrt{\log n \log \log n}))\) when setting \(t = \sqrt{n \log n / \log \log n}\). This analysis ignores integer constraints on \(t, k, m\), and implicitly place restrictions on \(p_1\) and \(p_2\) in relation to \(n\) (e.g. \(0 < p_2 < p_1 < 1\) are constant). We will introduce a slightly different scheme that takes into account integer constraints and analyze it without restrictions on the properties of \(H\).

Assume that we are given a \((r_1, r_2, p_1, p_2)\)-sensitive family \(H\). Let \(\eta, t, k_1, k_2, m_1, m_2\) be non-negative integer parameters. Each of the \(L\) hash functions \(g_1, \ldots, g_L\) will be formed by concatenating one hash function from each of \(t\) collections of \(m_1\) hash functions from \(H^{k_1}\) and concatenating a last hash function from a collection of \(m_2\) hash functions from \(H^{k_2}\). We take all \(m_1 m_2\) hash functions of the above form and repeat \(\eta\) times for a total of \(L = \eta m_1 m_2\) hash functions constructed from a total of \(H = \eta (m_1 k_1 t + m_2 k_2)\) hash functions from \(H\). In Appendix 3 we set parameters, leaving \(t\) variable, and provide an analysis of this scheme, showing that \(L\) matches the Indyk-Motwani framework bound of \(O(1/p_2^k)\) up to a constant where \(k = \lceil \log(n)/\log(1/p_2) \rceil\) as in Theorem 8.

**Setting \(t\).** It remains to show how to set \(t\) to obtain a good bound on the number of hash functions \(H\). Note that in practice we can simply set \(t = \arg \min_H L\) by trying \(t = 1, \ldots, k\). If we ignore integer constraints and place certain restrictions of \(H\) as in the original tensoring scheme by Andoni and Indyk we want to set \(t\) to minimize the expression \(t^2 \log t = \rho \log n\). This minimum is obtained when setting \(t\) such that \(t^2 \log t = \rho \log n\). We therefore cannot do much better...
than setting \( t = \sqrt{\rho \log(n)/\log m} \) which gives the bound \( H = O(\exp(\sqrt{\rho \log(n) \log \log n})) \) as shown in [11]. To allow for easy comparison with the Indyk-Motwani framework without placing restrictions on \( H \) we set \( t = \sqrt{\log k} \), resulting in Theorem 9.

**Theorem 9.** Given a \((r_1, r_2, p_1, p_2)\)-sensitive family \( H \) we can construct a data structure that solves the \((r_1, r_2)\)-near neighbor problem such that for \( k = \lceil \log(n) / \log(1/p_2) \rceil \), \( H = k(\sqrt{r_1} / p_1)^{\sqrt{r}} \), and \( L = \lceil 1/p_1 \rceil \) the data structure has the following properties:

- The query operation uses \( O(H) \) evaluations of functions from \( H \), \( O(L) \) distance computations, and \( O(L + H) \) other word-RAM operations.
- The data structure uses \( O(nL) \) words of space in addition to the space required to store the data and \( O(H) \) hash functions from \( H \).

Thus, compared to the Indyk-Motwani framework we have gone from using \( O(k(1/p_1)^k) \) locality-sensitive hash functions to \( O(k(\sqrt{r_1} / p_1)^{\sqrt{r}}) \) locality-sensitive hash functions. Figure 1 shows the actual number of hash functions of the revised version of the Andoni-Indyk scheme as analyzed in Appendix B when \( t \) is set to minimize \( H \).

### 3.3 Dahlgaard-Knudsen-Thorup

In a recent paper Dahlgaard et al. [14] introduce a different technique for reducing the number of locality-sensitive hash functions. The idea is to construct each hash value by sampling and concatenating \( k \) hash values from a collection of \( km \) pre-computed hash functions from \( H \). In what follows we will use the notation \([n]\) to denote the set of integers \( \{1, 2, \ldots, n\} \). For \( i \in [k] \) and \( j \in [m] \) let \( h_{i,j} \sim H \) denote a hash function in our collection. To sample from the collection we use \( k \) pairwise independent [10] hash functions of the form \( f_i : [L] \to [m] \) and set

\[
g_i(x) = (h_{i, f_i(1)}(x), \ldots, h_{i, f_i(l)}(x)).
\]

For two points \( x \) and \( y \) let \( Z_i = 1 \{ g_i(x) = g_i(y) \} \) so that \( Z = \sum_{i=1}^L Z_i \) denotes the sum of collisions under the \( L \) hash functions. To show correctness of this scheme we will use make use of an elementary one-sided version of Chebyshev’s inequality stating that for a random variable \( Z \) with mean \( \mu > 0 \) and variance \( \sigma^2 < \infty \) we have that \( \Pr[Z \leq 0] \leq \sigma^2/(\mu^2 + \sigma^2) \). For completeness we have included the proof of this inequality in Lemma 15. Let \( p = \Pr_{h \sim H}[h(x) = h(y)] \) then by linearity of expectation we have that \( \mu = E[Z] = Lp^k \). To bound \( \sigma^2 = E[Z^2] - \mu^2 \) we proceed by bounding \( E[Z^2] \) where we note that \( Z_i = \Pi_{i=1}^k Y_{i,i} \) for \( Y_{i,i} = 1(h_{i,i}(x) = h_{i,i}(y)) \) and make use of the independence between \( Y_{i,i} \) and \( Y_{i,i'} \) for \( i \neq i' \).

\[
E[Z^2] = \sum_{i,i' \in [L]} E[Z_i Z_{i'}] + \sum_{i=1}^L E[Z_i] \\
= (L^2 - L)E[Z Z'] + \mu \\
\leq L^2 E[[\Pi_{i=1}^k Y_{i,i} Y_{i'}]] + \mu \\
= L^2 (E[Y_{i,i} Y_{i,i'}])^k + \mu.
\]

We have that \( E[Y_{i,i} Y_{i,i'}] = \Pr[f_i(l) = f_i(l')] + \Pr[f_i(l) \neq f_i(l')]p^2 = (1/m)p + (1 - 1/m)p^2 \) which follows from the pairwise independence of \( f_i \). Let \( \varepsilon > 0 \) and set \( m = \lceil \frac{1-p_1}{p_1} \ln(1+\varepsilon) \rceil \) then for \( p \geq p_1 \) we have that \( (E[Y_{i,i} Y_{i,i'}])^k \leq (1+\varepsilon)^{2k} \). This allows us to bound the variance of \( Z \) by \( \sigma^2 \leq \varepsilon \mu^2 + \mu \) resulting in the following lower bound on the probability of collision between similar points.
Lemma 10. For \( \varepsilon > 0 \) let \( m \geq \lceil \frac{1-p_1}{p_1} \frac{k}{\ln(1+\varepsilon)} \rceil \), then for every pair of points \( x, y \) with \( \text{dist}(x,y) \leq r_1 \) we have that
\[
\Pr[\exists \in [L]: g_1(x) = g_1(y)] \geq \frac{1 + \varepsilon \mu}{1 + (1 + \varepsilon )\mu}.
\]

By setting \( \varepsilon = 1/4 \) and \( L = \lceil (2\ln(2))/p_1^k \rceil \) we obtain an upper bound on the failure probability of 1/2. Setting the size of each of the \( k \) collections of pre-computed hash values to \( m = \lceil 5k/p_1 \rceil \) is sufficient to yield the following solution to the \((r_1, r_2)\)-near neighbor problem where provide exact bounds on the number of lookups \( L \) and hash functions \( H \):

**Theorem 11 (Dahlgaard-Knudsen-Thorup [14]).** Given a \((r_1, r_2, p_1, p_2)\)-sensitive family \( \mathcal{H} \) we can construct a data structure that solves the \((r_1, r_2)\)-near neighbor problem such that for \( k = \lceil \log(n)/\log(1/p_2) \rceil \), \( H = k[5k/p_1] \), and \( L = \lceil (2\ln(2))/p_1^k \rceil \) the data structure has the following properties:
- The query operation uses at most \( H \) evaluations of hash functions from \( \mathcal{H} \), expected \( L \) distance computations, and \( O(Lk) \) other word-RAM operations.
- The data structure uses \( O(nL) \) words of space in addition to the space required to store the data and \( H \) hash functions from \( \mathcal{H} \).

Compared to the Indyk-Motwani framework we have reduced the number of locality-sensitive hash functions \( H \) from \( O(k(1/p_1)^k) \) to \( O(k^2/p_1) \) at the cost of using twice as many lookups. To reduce the number of lookups further we can decrease \( \varepsilon \) and perform several independent repetitions. This reduces to the cost of an increase in the number of hash functions \( H \).

### 3.4 Reducing the word-RAM complexity

One drawback of the DKT framework is that each hash value \( g_1(x) \) still takes \( O(k) \) word-RAM operations to compute, even after the underlying locality-sensitive hash functions are known. This results in a bound on the total number of additional word-RAM operations of \( O(Lk) \). We show how to combine the DKT universal hashing technique with the AI tensoring technique to ensure that the running time is dominated by \( O(Lk) \) distance computations and \( O(Hk) \) hash function evaluations. The idea is simply to use the DKT scheme to construct two collections of respectively \( L_1 \) and \( L_2 \) hash functions, and then to use the AI tensoring approach to form \( g_1, \ldots, g_L \) as the \( L = L_1 \times L_2 \) combinations of functions from the two collections. The number of lookups can be reduced by applying tensoring several times in independent repetitions, but for the sake of simplicity we use a single repetition. For the usual setting of \( k = \lceil \log(n)/\log(1/p_2) \rceil \) let \( k_1 = \lceil k/2 \rceil \) and \( k_2 = \lfloor k/2 \rfloor \). Set \( L_1 = \lceil 6(1/p_1)^{k_1} \rceil \) and \( L_2 = \lceil 6(1/p_1)^{k_2} \rceil \). According to Lemma 10 if we set \( \varepsilon = 1/6 \) the success probability of each collection is at least 3/4 and by a union bound the probability that either collection fails to contain a colliding hash function is at most 1/2. This concludes the proof of our main Theorem 5.

### 3.5 Corner cases

When the collision probabilities of the \((r_1, r_2, p_1, p_2)\)-sensitive family \( \mathcal{H} \) are close to one we get the behavior displayed in Figure 2 where we have set \( p_1 = 0.9 \). Here it may be possible to reduce the number of hash functions by applying the DKT framework to the family \( \mathcal{H}^\tau \) for some positive integer \( \tau \). The number of locality-sensitive hash functions from \( \mathcal{H} \) used by the DKT framework is given by \( H = O((\log(n)/\log(1/p_2))^2/p_1) \). If we instead use the family \( \mathcal{H}^\tau \) the expression becomes \( H = O(\tau(\log(n)/\log(1/p_2))^2/p_1^\tau) = O((\log(n)/\log(1/p_2))^2/\tau p_1^\tau) \). Ignoring integer constraints, we set \( \tau = 1/\ln(1/p_1) \) to maximize \( \tau p_1^\tau \) thereby minimizing \( H \).
The resulting number of hash functions when we set $\tau = \lceil \frac{1}{\ln(1/p_1)} \rceil$ is given by
$$H = O(\rho (\log n)^2 / p_1 \log(1/p_2))$$
When $p_1$ is below $e^{-1/2} \approx 0.6$ the optimal value of $\tau$ is less than 2.

The behavior for small values of $p_1$ is displayed in Figure 3 where we have set $p_1 = 0.1$.

### 4 Sketching

The theorems of the previous section made no assumptions on the word-RAM complexity of distance computations and instead stated the number of distance computations as part of the query complexity. We can use a $(r_1, r_2, p_1, p_2)$-sensitive family $H$ to create sketches that allows us to efficiently approximate the distance between pairs of points, provided that the gap between $p_1$ and $p_2$ is sufficiently large. In this section we will re-state the results of Theorem 5 when applying the family $H$ to create sketches using the 1-bit sketching scheme of Li and König [25]. Let $b$ be a positive integer denoting the length of the sketches in bits.

For $i = 1, \ldots, b$ let $h_i: X \to R$ denote a randomly sampled locality-sensitive hash function from $H$ and let $f_i: R \to \{0, 1\}$ denote a randomly sampled universal hash function. We let $s(x) \in \{0, 1\}^b$ denote the sketch of a point $x \in X$ where we set the $i$th bit of the sketch $s(x)_i = f_i(h(x))$. For two points $x, y \in X$ the probability that they agree on the $i$th bit is $1$ if the points collide under $h_i$ and $1/2$ otherwise.

$$\Pr[s(x)_i = s(y)_i] = \Pr[h_i(x) = h_i(y)] + (1 - \Pr[h_i(x) = h_i(y)])/2 = (1 + \Pr[h_i(x) = h_i(y)])/2.$$  

We will apply these sketches during our query procedure instead of direct distance computations when searching through the points in the $L$ buckets, comparing them to our query point $q$. Let $\lambda \in (0, 1)$ be a parameter that will determine whether we report a point or not. For sketches of length $b$ we will return a point $x$ if $\|s(q) - s(x)\|_1 > \lambda b$. An application of Hoeffding’s inequality gives us the following properties of the sketch:
Figure 3. The number of locality-sensitive hash functions from a \((r_1, r_2, 0.1, p_2)\)-sensitive family used by different frameworks to solve the \((r_1, r_2)\)-near neighbor problem on a collection of \(2^{30}\) points.

Lemma 12. Let \(\mathcal{H}\) be a \((r_1, r_2, p_1, p_2)\)-sensitive family and let \(\lambda = (1 + p_2)/2 + (p_1 - p_2)/4\), then for sketches of length \(b \geq 1\) and for every pair points \(x, y \in X\):

- If \(\text{dist}(x, y) \leq r_1\) then \(\Pr[\|s(x) - s(y)\|_1 \leq \lambda b] \leq e^{b(p_1 - p_2)^2}/8\).
- If \(\text{dist}(x, y) \geq r_2\) then \(\Pr[\|s(x) - s(y)\|_1 > \lambda b] \leq e^{b(p_1 - p_2)^2}/8\).

If we replace the exact distance computations with sketches we want to avoid two events: Failing to report a point with \(\text{dist}(q, x) \leq r_1\) and reporting a point \(x\) with \(\text{dist}(q, x) \geq r_2\). By setting \(b = O(\ln(n)/(p_1 - p_2)^2)\) and applying a union bound over the \(n\) events that the sketch fails for a point in our collection \(P\) we obtain Theorem 6.

5 Conclusion and open problems

We have shown that there exists a simple and general framework for solving the \((r_1, r_2)\)-near neighbor problem using only few locality-sensitive hash functions and with a word-RAM complexity matching the number of distance computations. The analysis in this paper indicates that the performance of the Dahlgaard-Knudsen-Thorup is highly competitive compared to the Indyk-Motwani framework in practice, especially when locality-sensitive hash functions are expensive to evaluate, as is often the case.

An obvious open problem is the question of whether the number of locality-sensitive hash functions can be reduced even below \(O(k^2/p_1)\). Another possible direction for future research would be to obtain similar framework results in the context of solutions to the \((r_1, r_2)\)-near neighbor problem that allow for space-time tradeoffs [5, 12].

Acknowledgements. I want to thank Rasmus Pagh for making me aware of the application of the tensoring technique in [30] that led me to the Andoni-Indyk framework [1].
A Inequalities

We make use of the following standard inequalities for the exponential function. See [26, Chapter 3.6.2] for more details.

- **Lemma 13.** Let \( n, t \in \mathbb{R} \) such that \( n \geq 1 \) and \( |t| \leq n \) then \( e^{-t}(1-t^2/n) \leq (1-t/n)^n \leq e^{-t} \).

- **Lemma 14.** For \( t \geq 0 \) we have that \( e^{-t} \leq 1 - t + t^2/2 \).

We make use of a one-sided version of Chebyshev’s inequality to show correctness of the Dahlgaard-Knudsen-Thorup LSH framework.

- **Lemma 15 (Cantelli’s inequality).** Let \( Z \) be a random variable with \( \mathbb{E}[Z] = \mu > 0 \) and \( \text{Var}[Z] = \sigma^2 < \infty \) then \( \Pr[Z \leq 0] \leq \sigma^2/(\mu^2 + \sigma^2) \).

**Proof.** For every \( s \in \mathbb{R} \) we have that

\[
\Pr[Z \leq 0] = \Pr[-(Z - \mu) + s \geq \mu + s] \leq \Pr[(Z - \mu) + s \geq (\mu + s)^2].
\]

Next we apply Markov’s inequality

\[
\Pr[(Z - \mu) + s] \geq (\mu + s)^2 \leq \mathbb{E}[(Z - \mu) + s]/(\mu + s) = (\sigma^2 + s^2)/(\mu + s)^2
\]

Set \( s = \sigma^2/\mu \) and use that \( \sigma^2 = s\mu \) to simplify

\[
(\sigma^2 + s^2)/(\mu + s)^2 = (s\mu + s^2)/(\mu + s)^2 = \sigma^2/(\mu^2 + \sigma^2).
\]

To analyze the 1-bit sketching scheme by Li and König we make use of Hoeffding’s inequality:

- **Lemma 16 (Hoeffding [22, Theorem 1]).** Let \( X_1, X_2, \ldots, X_n \) be independent random variables satisfying \( 0 \leq X_i \leq 1 \) for \( i \in [n] \). Define \( \bar{X} = (X_1 + X_2 + \cdots + X_n)/n \) and \( \mu = \mathbb{E}[\bar{X}] \), then:
  - For \( 0 < \varepsilon < 1 - \mu \) we have that \( \Pr[\bar{X} - \mu \geq \varepsilon] \leq e^{-2n\varepsilon^2} \).
  - For \( 0 < \varepsilon < \mu \) we have that \( \Pr[\bar{X} - \mu \leq -\varepsilon] \leq e^{-2n\varepsilon^2} \).

B Analysis of the Andoni-Indyk framework

Let \( \varphi \) denote the probability that a pair of points \( x, y \) with \( \text{dist}(x, y) \leq r_1 \) collide in a single repetition of the scheme. A collision occurs if and only if there exists at least one hash function in each of the underlying \( t + 1 \) collections where the points collide. It follows that

\[
\varphi = (1 - (1 - p_1^{k_1})^{m_1})(1 - (1 - p_1^{k_2})^{m_2}).
\]

To guarantee a collision with probability at least \( 1/2 \) it suffices to set \( \eta = \lfloor \ln(2)/\varphi \rfloor \).

We will proceed by analyzing this scheme where we let \( t \geq 1 \) be variable and set parameters as follows:

\[
\begin{align*}
  k &= \lceil \log(n)/\log(1/p_2) \rceil \\
  k_1 &= \lceil k/t \rceil \\
  k_2 &= k - tk_1 \\
  m_1 &= \lceil 1/t^p_1^{k_1} \rceil \\
  m_2 &= \lceil 1/p_1^{k_2} \rceil \\
  \eta &= \lfloor \ln(2)/\varphi \rfloor.
\end{align*}
\]
To upper bound $L$ we begin by lower bounding $\varphi$. The second part of $\varphi$ can be lower bounded using Lemma 13 to yield $(1 - (1 - p^{k_1}_{i})^{m_2}) \geq 1 - 1/e$. To lower bound $(1 - (1 - p^{k_1}_{i})^{m_1})$ we first note that in the case where $p^{k_1}_{i} > 1/t$ we have $m_1 = 1$ and the expression can be lower bounded by $p^{k_1}_{i} = (p^{k_1}_{i}m_1)^{t} \geq (p^{k_1}_{i}m_1)^{t}/2e$. The same lower bound holds in the case there $t = 1$. In the case where $p^{k_1}_{i} \leq 1/t$ and $t \geq 2$ we make use of Lemma 13 and 14 to derive the lower bound.

$$1 - (1 - p^{k_1}_{i})^{m_1} \geq 1 - (1 - p^{k_1}_{i}m_1 + (p^{k_1}_{i}m_1)^{t}/2)$$

$$\geq p^{k_1}_{i}m_1(1 - p^{k_1}_{i}(1/tp^{k_1}_{i} + 1)/2)$$

$$\geq p^{k_1}_{i}m_1(1 - 1/t).$$

Using the bound $(p^{k_1}_{i}m_1(1 - 1/t))^{t} \geq (p^{k_1}_{i}m_1)^{t}/2e$ we have that

$$\varphi \geq (p^{k_1}_{i}m_1)^{t}/4e \geq (1/t)^{t}/4e.$$ 

We can then bound the number of lookups and the expected number of distance computations

$$L = \eta m_1^{t}m_2 \leq (4e/(p^{k_1}_{i}m_1)^{t} + 1)m_1^{t}(1/p^{k_2}_{i} + 1) \leq 16e(1/p^{k}_{i}).$$

Note that this matches the upper bound of the Indyk-Motwani LSH framework up to a constant factor.

To bound the number of hash functions from $\mathcal{H}$ we use that $k_1 \leq k/t \leq k$ and $k_2 < t$.

$$H = \eta(m_1k_1t + m_2k_2) \leq 8e^{t}\left(\frac{k}{tp^{k_1}_{i}/t} + \frac{t - 1}{p^{k_1}_{i}1}\right).$$

References

1. A. Andoni and P. Indyk. Efficient algorithms for substring near neighbor problem. In Proc. SODA ’06, pages 1203–1212, 2006.
2. A. Andoni and P. Indyk. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions. In Proc. FOCS ’06, pages 459–468, 2006.
3. A. Andoni and P. Indyk. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions. Commun. ACM, 51(1):117–122, 2008.
4. A. Andoni, P. Indyk, T. Laarhoven, I. Razenshteyn, and L. Schmidt. Practical and optimal lsh for angular distance. In Proc. NIPS ’15, pages 1225–1233, 2015.
5. A. Andoni, T. Laarhoven, I. P. Razenshteyn, and E. Waingarten. Optimal hashing-based time-space trade-offs for approximate near neighbors. In Proc. SODA ’17, pages 47–66, 2017.
6. A. Becker, L. Ducas, N. Gama, and T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Proc. SODA ’16, pages 10–24, 2016.
7. Andrei Z. Broder, Moses Charikar, Alan M. Frieze, and Michael Mitzenmacher. Min-wise independent permutations. J. Comput. Syst. Sci., 60(3):630–659, 2000.
8. J. L. Carter and M. N. Wegman. Universal classes of hash functions. In Proc. STOC ’77, pages 106–112, 1977.
9. J. L. Carter and M. N. Wegman. Universal classes of hash functions. J. Comput. Syst. Sci., 18(2):143–154, 1979.
10. J. L. Carter and M. N. Wegman. New hash functions and their use in authentication and set equality. J. Comput. System Sci., 22(3):265–279, 1981.
11 M. Charikar. Similarity estimation techniques from rounding algorithms. In Proc. STOC '02, pages 380–388, 2002.
12 T. Christiani. A framework for similarity search with space-time tradeoffs using locality-sensitive filtering. In Proc. SODA '17, pages 31–46, 2017.
13 T. Christiani, R. Pagh, and J. Sivertsen. Scalable and robust set similarity join. CoRR, abs/1707.06814, 2017.
14 S. Dahlgaard, M. B. T. Knudsen, and M. Thorup. Fast similarity sketching. CoRR, abs/1704.04370, 2017. URL: http://arxiv.org/abs/1704.04370.
15 M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni. Locality-sensitive hashing scheme based on p-stable distributions. In Proc. SOCG ’04, pages 253–262, 2004.
16 M. Dubiner. Bucketing coding and information theory for the statistical high-dimensional nearest-neighbor problem. IEEE Trans. Information Theory, 56(8):4166–4179, 2010.
17 K. Eshghi and S. Rajaram. Locality sensitive hash functions based on concomitant rank order statistics. In Proc. KDD ’08, pages 221–229, 2008.
18 M. L. Fredman, J. Komlós, and E. Szemerédi. Storing a sparse table with 0(1) worst case access time. J. ACM, 31(3):538–544, 1984.
19 Y. Gong, S. Kumar, V. Verma, and S. Lazebnik. Angular quantization-based binary codes for fast similarity search. In NIPS, pages 1205–1213, 2012.
20 T. Hagerup. Sorting and searching on the word RAM. In Proc. STACS ’98, pages 366–398, 1998.
21 S. Har-Peled, P. Indyk, and R. Motwani. Approximate nearest neighbor: Towards removing the curse of dimensionality. Theory of computing, 8(1):321–350, 2012.
22 W. Hoeffding. Probability inequalities for sums of bounded random variables. Jour. Am. Stat. Assoc., 58(301):13–30, 1963.
23 P. Indyk and R. Motwani. Approximate nearest neighbors: towards removing the curse of dimensionality. In Proc. STOC ’98, pages 604–613, 1998.
24 C. Kennedy and R. Ward. Fast cross-polytope locality-sensitive hashing. CoRR, abs/1602.06922, 2016. URL: http://arxiv.org/abs/1602.06922.
25 Ping Li and Arnd Christian König. Theory and applications of b-bit minwise hashing. Communications of the ACM, 54(8):101–109, 2011.
26 Dragoslav S Mitriović. Analytic inequalities. Springer-Verlag, Berlin, New York, 1970.
27 M. H. Overmars and J. van Leeuwen. Worst-case optimal insertion and deletion methods for decomposable searching problems. Information Processing Letters, 12(4):168–173, 1981.
28 A. Shrivastava. Simple and efficient weighted minwise hashing. In NIPS, pages 1498–1506, 2016.
29 A. Shrivastava. Optimal densification for fast and accurate minwise hashing. In ICML, volume 70 of Proceedings of Machine Learning Research, pages 3154–3163. PMLR, 2017.
30 N. Sundaram, A. Turmukhametova, N. Satish, T. Mostak, P. Indyk, S. Madden, and P. Dubey. Streaming similarity search over one billion tweets using parallel locality-sensitive hashing. PVLDB, 6(14):1930–1941, 2013.
31 K. Terasawa and Y. Tanaka. Spherical LSH for approximate nearest neighbor search on unit hypersphere. In Proc. WADS ’07, pages 27–38, 2007.
32 J. Wang, H. T. Shen, J. Song, and J. Ji. Hashing for similarity search: A survey. CoRR, abs/1408.2927, 2014. URL: http://arxiv.org/abs/1408.2927.
33 Y. Weiss, A. Torralba, and R. Fergus. Spectral hashing. In NIPS, pages 1753–1760. Curran Associates, Inc., 2008.
34 Albert L Zobrist. A new hashing method with application for game playing. ICCA journal, 13(2):69–73, 1970.