To appear in proceedings of ESA 2001. © Springer Verlag.
Available on-line at http://www.brics.dk/ pagh/papers/

Lossy Dictionaries

Rasmus Pagh[1] and Flemming Friche Rodler

BRICS[2], Department of Computer Science
University of Aarhus, Denmark
{pagh,ffr}@brics.dk

Abstract. Bloom filtering is an important technique for space efficient storage of a conservative approximation of a set S. The set stored may have up to some specified number of "false positive" members, but all elements of S are included. In this paper we consider *lossy dictionaries* that are also allowed to have "false negatives". The aim is to maximize the weight of included keys within a given space constraint. This relaxation allows a very fast and simple data structure making almost optimal use of memory. Being more time efficient than Bloom filters, we believe our data structure to be well suited for replacing Bloom filters in some applications. Also, the fact that our data structure supports information associated to keys paves the way for new uses, as illustrated by an application in lossy image compression.

1 Introduction

Dictionaries are part of many algorithms and data structures. A dictionary provides access to information indexed by a set S of *keys*: Given a key, it returns the associated information or reports that the key is not in the set. In this paper we will not be concerned with updates, i.e., we consider the *static* dictionary problem. The main parameters of interest are of course the space used by the dictionary and the time for looking up information. We will assume keys as well as the information associated with keys to have a fixed size.

A large literature has grown around the problem of constructing efficient dictionaries, and theoretically satisfying solutions have been found. Often a slightly easier problem has been considered, namely the *membership* problem, which is the dictionary problem without associated information. It is usually easy to derive a dictionary from a solution to the membership problem, using extra space corresponding to the associated information. In this paper we are particularly interested in dictionary and membership schemes using little memory. Let n denote the size of the key set S. It has been shown that when keys are w-bit

[1] Partially supported by the IST Programme of the EU under contract number IST-1999-14186 (ALCOM-FT).
[2] Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

machine words, lookups can be performed in constant time in a membership data structure occupying $B + o(B)$ bits of memory, where $B = \log \binom{2^w}{n}$ is the minimum amount of memory needed to be able to represent any subset of size n [2] (logarithms in this paper are base 2). However, constant factors in the lower order term and lookup time make this and similar schemes less than one could hope for from an applied point of view. Also, difficulty of implementation is an obstacle to practical use. In total, current schemes with asymptotically optimal space usage appear to be mainly of theoretical interest.

If one relaxes the requirements to the membership data structure, allowing it to store a slightly different key set than intended, new possibilities arise. A technique finding many applications in practice is *Bloom filtering* [1]. This technique allows space-efficient storage of a superset S' of the key set S, such that $S' \setminus S$ is no more than an ϵ fraction of $\{0,1\}^w$. For $n \ll 2^w$, about $\log(1/\epsilon)$ bits per key in S are necessary and sufficient for this [4]. This is a significant savings compared to a membership data structure using $B \approx n \log(\frac{2^w e}{n})$ bits. Lookup of a key using Bloom filtering requires $O(\log(1/\epsilon))$ memory accesses and is thus relatively slow compared to other hashing schemes when ϵ is small. Bloom filtering has applications in, for example, cooperative caching and differential files, where one wants no more than a small chance that an expensive operation is performed in vain. Bloom filtering differs from most other hashing techniques in that is does *not* yield a solution to the dictionary problem.

1.1 This Paper

In this paper we introduce the concept of *lossy dictionaries* that can have not only false positives (like Bloom filters), but also false negatives. That is, some keys in S (with associated information) are thrown away when constructing the dictionary. For false positives there is no guarantee on the associated information returned. We let each key in S have a weight, and try to maximize the sum of weights of keys in the dictionary under a given space constraint. This problem, with no false positives allowed, arises naturally in lossy image compression, and is potentially interesting for caching applications. Also, a dictionary with two-sided errors could take the place of Bloom filters in cooperative caching.

We study this problem on a unit cost RAM, in the case where keys are machine words of w bits. We examine a very simple and efficient data structure from a theoretical as well as an experimental point of view. Experimentally we find that our data structure has surprisingly good behavior with respect to keeping the keys of largest weight. The experimental results are partially explained by our theoretical considerations, under strong assumptions on the hash functions involved. Specifically, we assume in our RAM model that for a number of random functions, arbitrary function values can be returned in constant time by an oracle.

1.2 Related Work

Most previous work related to static dictionaries has considered the membership problem on a unit cost RAM with word size w. The first membership data structure with worst case constant lookup time using $O(n)$ words of space was constructed by Fredman et al. [7]. For constant $\delta > 0$, the space usage is $O(B)$ when $2^w > n^{1+\delta}$, but in general the data structure may use space $\Omega(Bw)$. The space usage has been lowered to $B + o(B)$ bits by Brodnik and Munro [2]. The lower order term was subsequently improved to $o(n) + O(\log w)$ bits by the first author [11]. The main concept used in the latter paper is that of a *quotient function* q of a hash function h, defined simply to be a function such that the mapping $k \mapsto (h(k), q(k))$ is injective.

The membership problem with false positives was first considered by Bloom [1]. Apart from Bloom filtering the paper presents a less space efficient data structure that is readily turned into a lossy dictionary with only false positives. However, the space usage of the derived lossy dictionary is not optimal. Carter et al. [4] provided a lower bound of $n \log(1/\epsilon)$ bits on the space needed to solve membership with an ϵ fraction false positives, for $n \ll 2^w$, and gave data structures with various lookup times matching or nearly matching this bound. Though none of the membership data structures have constant lookup time, such a data structure follows by plugging the abovementioned results on space optimal membership data structures [2, 11] into a general reduction provided in [4]. In fact, the dictionary of [11] can be easily modified to a lossy dictionary with false positives, thus also supporting associated information, using $O(n + \log w)$ bits more than the lower bound.

Another relaxation of the membership problem was recently considered by Buhrman et al. [3]. They store the set S exactly, but allow the lookup procedure to use randomization and to have some probability of error. For two-sided error ϵ they show that there exists a data structure of $O(nw/\epsilon^2)$ bits in which lookups can be done using just *one* bit probe. To do the same without false negatives it is shown that $O(n^2 w/\epsilon^2)$ bits suffice and that this is essentially optimal. Schemes using more bit probes and less space are also investigated. If one fixes the random bits of the lookup procedure appropriately, the result is a lossy dictionary with error ϵ. However, it is not clear how to fix the parameters in a reasonable model of computation.

2 Lossy Dictionaries

Consider a set S containing keys $k_1, \ldots, k_n$ with associated information $a_1, \ldots, a_n$ and positive weights $v_1, \ldots, v_n$. Suppose we are given an upper bound m on available space and an error parameter ϵ. The *lossy dictionary problem* for $\epsilon = 0$ is to store a subset of the keys in S and corresponding associated information in a data structure of m bits, trying to optimize the sum of weights of included keys, referred to as the *value*. For general ϵ we allow the dictionary to contain also $2^w \epsilon$ keys from the complement of S. In this section we show the following theorem.

Theorem 1. *Let a sequence of keys $k_1, \ldots, k_n \in \{0,1\}^w$, associated information $a_1, \ldots, a_n \in \{0,1\}^l$, and weights $v_1 \geq \cdots \geq v_n > 0$ be given. Let $r > 0$ be an even integer, and $b \geq 0$ an integer. Suppose we have oracle access to random functions $h_1, h_2 : \{0,1\}^w \to \{1, \ldots, r/2\}$ and corresponding quotient functions $q_1, q_2 : \{0,1\}^w \to \{0,1\}^s \setminus 0^s$. There is a lossy dictionary with the following properties:*

1. *The space usage is $r(s-b+l)$ bits (two tables with $r/2$ cells of $s-b+l$ bits).*
2. *The fraction of false positives is bounded by $\epsilon \leq (2^b - 1)r/2^w$.*
3. *The expected weight of the keys in the set stored is $\sum_{i=1}^{n} p_{r,i}\, v_i$ where*

$$p_{r,i} \geq \begin{cases} 1 - 52\, r^{-1}/(\frac{r/2}{i} - 1), & \text{for } i < r/2 \\ 2\,(1-2/r)^{i-1} - (1-2/r)^{2(i-1)}, & \text{for } i \geq r/2 \end{cases}$$

   is the probability that k_i is included in the set.
4. *Lookups are done using at most two (independent) accesses to the tables.*
5. *It can be constructed in time $O(n \log^* n + rl/w)$.*

As discussed in Sect. 2.1 there exist quotient functions for $s = w - \log r + O(1)$ if the hash functions map approximately the same number of elements to each value in $\{1, \ldots, r/2\}$. The inequality in item 2 is satisfied for $b = \lfloor \log(2^w \epsilon / r + 1) \rfloor$, so for $s = w - \log r + O(1)$ an ϵ fraction of false positives can be achieved using space $r\,(\log(\frac{1}{\epsilon + r/2^w}) + l + O(1))$. As can be seen from item 3, almost all of the keys $\{k_1, \ldots, k_{r/2}\}$ are expected to be included in the set represented by the lossy dictionary. For $i \geq r/2$ our bound on $p_{i,r}$ is shown in Fig. 1 of Sect. 3, together with experimentally observed probabilities. If $n \geq r$ and r is large enough it can be shown by integration that, in the expected sense, more than 70% of the keys from $\{k_1, \ldots, k_r\}$ are included in the set (our experiments indicate 84%). We show in Sect. 2.5 that the amount of space we use to achieve this is within a small constant factor of optimal.

Note that by setting $b = 0$ we obtain a lossy dictionary with no false positives. Another point is that given a desired maximum space usage m and false positive fraction ϵ, the largest possible size r of the tables can be chosen efficiently.

2.1 Preliminaries

The starting point for the design of our data structure is a static dictionary recently described in [12]. In this dictionary, two hash tables T_1 and T_2 are used together with two hash functions $h_1, h_2 : \{0,1\}^w \to \{1, \ldots, r/2\}$, where r denotes the combined size of the hash tables, assumed to be even. A key $x \in S$ is stored in either cell $h_1(x)$ of T_1 or cell $h_2(x)$ of T_2. It was shown that if $r \geq (2+\delta)\, n$, for $\delta > 0$, and h_1, h_2 are random functions, there exists a way of arranging the keys in the tables according to the hash functions with probability at least $1 - \frac{52}{\delta r}$. For small δ this gives a dictionary utilizing about 50% of the hash table cells. The arrangement of keys was shown to be computable in expected linear time.

Another central concept is that of *quotient functions*. Recall that a quotient function q of a hash function h is a function such that the mapping

$k \mapsto (h(k), q(k))$ is injective [11]. When storing a key k in cell $h(k)$ of a hash table, it is sufficient to store $q(k)$ to uniquely identify k among all other elements hashing to $h(k)$. To mark empty cells one needs a bit string not mapped to by the quotient function, e.g., 0^s for the quotient functions of Theorem 1. The idea of using quotient functions is, of course, that storing $q(k)$ may require fewer bits than storing k itself. If a fraction $O(1/r)$ of all possible keys hashes to each of r hash table cells, there is a quotient function whose function values can be stored in $w - \log r + O(1)$ bits. This approach was used in [11] to construct a dictionary using space close to the information theoretical minimum. As an example, we look at a hash function family from [6] mapping from $\{0,1\}^w$ to $\{0,1\}^t$. It contains functions of the form $h_a(k) = (ak \mod 2^w) \operatorname{div} 2^{w-t}$ for a odd and $0 \leq a < 2^w$. Letting bit masks and shifts replace modulo and division these hash functions can be evaluated very efficiently. A corresponding family of quotient functions is given by $q_a(k) = (ak \mod 2^w) \bmod 2^{w-t}$, whose function values can be stored in $w - \log r$ bits.

2.2 Our Data Structure

The idea behind our lossy dictionary, compared to the static dictionary of [12] described above, is to try to fill the hash tables almost completely, working with key sets of size similar to or larger than r. Each key has two hash table cells to which it can be matched. Thus, given a pair of hash functions, the problem of finding a maximum value subset of S that can be arranged into the hash tables is a maximum weight matching problem that can be solved in polynomial time, see e.g. [5]. In Sect. 2.3 we will present an algorithm that finds such an optimal solution in time $O(n \log^* n)$, exploiting structural properties. The term $O(rl/w)$ in the time bound of Theorem 1 is the time needed to copy associated information to the tables. Assume for now that we know which keys are to be represented in which hash table cells.

For $b = 0$ we simply store quotient function values in nonempty hash table cells and 0^s in empty hash table cells, using s bits per cell. For general b we store only the first $s - b$ bits. Observe that no more than 2^b keys with the same hash function value can share the first $s - b$ bits of the quotient function value. This means that there are at most $2^b - 1$ false positives for each nonempty cell. Since 0^s is not in the range, this is also true for empty cells. In addition to the $s - b$ bits, we use l bits per cell to store associated information.

We now proceed to fill in the remaining details on items 3 and 5 of Theorem 1.

2.3 Construction Algorithm

First note that it may be assumed without loss of generality that weights are distinct. If there are consecutive equal weights $v_j = \cdots = v_k$, we can imagine making them distinct by adding positive integer multiples of some quantity δ much smaller than the difference between any pair of achievable values. For sufficiently small δ, the relative ordering of the values of any two solutions with distinct values will not change.

When weights are distinct, the set of keys in an optimal solution is unique, as shown in the following lemma:

Lemma 2. *Suppose that weights are distinct. For $1 \leq i \leq n$, an optimal solution includes key k_i if and only if there is an optimal solution for the set $\{k_1, \ldots, k_{i-1}\}$ such that cell $h_1(k_i)$ of T_1 or cell $h_2(k_i)$ of T_2 is empty. In particular, the set of keys included in an optimal solution is unique.*

Proof. We proceed by induction on n. For $n = 1$ the claim is obvious. In general, the claim follows for $i < n$ by using the induction hypothesis on the set $\{k_1, \ldots, k_i\}$. For $i = n$ consider the unique set K of keys included in an optimal solution for $\{k_1, \ldots, k_{n-1}\}$. If there is an arrangement of K not occupying both cell $h_1(k_n)$ of T_1 and cell $h_2(k_n)$ of T_2, we may add the key k_n to the arrangement which must yield an optimal arrangement. On the other hand, if all arrangements of K occupy both cell $h_1(k_n)$ of T_1 and cell $h_2(k_n)$ of T_2, there is no way of including k_n without discarding a key in K. However, this would yield a lower value and hence cannot be optimal. □

Given hash functions h_1 and h_2 and a key set K, we define the bipartite graph $G(K)$ with vertex set $\{1, 2\} \times \{1, \ldots, r/2\}$, corresponding in a natural way to hash table cells, and the multiset of edges $\{\{(1, h_1(k)), (2, h_2(k))\} \mid k \in K\}$, corresponding to keys. Note that there may be parallel edges if several keys have the same pair of hash function values. We will use the terms keys/edges and cells/vertices synonymously. Define a connected component of $G(K)$ to be *saturated* if the number of edges is greater than or equal to the number of vertices, i.e., if it is not a tree. We have the following characterization of the key set of the optimal solution:

Lemma 3. *Suppose that weights are distinct. The optimal solution includes key k_i if and only if at least one of $(1, h_1(k_i))$ and $(2, h_2(k_i))$ is in a non-saturated connected component of $G(\{k_1, \ldots, k_{i-1}\})$.*

Proof. By Lemma 2 it is enough to show that the keys included in an optimal solution for a set of keys K can be arranged such that cell z is empty if and only if the connected component of z in $G(K)$ is not saturated. Consider the key set K' in an optimal solution for K. For every subset $H \subseteq K'$ it must hold that $|h_1(H)| + |h_2(H)| \geq |H|$ since otherwise not all keys could have been placed. Thus, a connected component with key set C is saturated if and only if $|h_1(C \cap K')| + |h_2(C \cap K')| = |C \cap K'|$. In particular, when arranging the keys of $C \cap K'$, where C is the set of keys of a saturated component, every cell in the connected component must be occupied. On the other hand, suppose there is no arrangement of K' such that z, say cell number i of T_1, is empty. Hall's theorem says that there must be a set $H \subseteq K'$ such that $|h_1(H) \backslash \{i\}| + |h_2(H)| < |H|$. In fact, as no other connected components are affected by blocking z, we may chose H as a subset of the keys in the connected component of z. But then the graph of edges in H must contain a cycle, meaning that the connected component is saturated. The case of z being in T_2 is symmetrical. □

The lemma implies that the following algorithm finds the key set S' of the optimal solution, given keys sorted according to decreasing weight.

1. Initialize a union-find data structure for the cells of the hash tables.
2. For each equivalence class, set a "saturated" flag to `false`.
3. For $i = 1, \ldots, n$:
   (a) Find the equivalence class c_b of cell $h_b(k_i)$ in T_b, for $b = 1, 2$.
   (b) If c_1 or c_2 is not saturated:
      i. Include k_i in the solution.
      ii. Join c_1 and c_2 to form an equivalence class c.
      iii. Set the saturated flag of c if $c_1 = c_2$ or if the flag is set for c_1 or c_2.

In the loop, equivalence classes correspond to the connected components of the graph $G(\{k_1, \ldots, k_{i-1}\})$. There is a simple implementation of a union-find data structure for which operations take $O(\log^* n)$ amortized time; see [16] which actually gives an even better time bound.

What remains is arranging the optimal key set S' in the tables. Consider a vertex in $G(S')$ of degree one. It is clear that there must be an arrangement such that the corresponding cell contains the key of the incident edge. Thus, one can iteratively handle edges incident to vertices of degree one and delete them. As we remove the same number of edges and vertices from each connected component, the remaining graph consists of connected components with no more edges than vertices and no vertices of degree one, i.e., cycles. The arrangement of edges in a cycle follows as soon as one key has been put (arbitrarily) into one of the tables. The above steps are easily implemented to run in linear time. This establishes item 5 of Theorem 1.

2.4 Quality of Solution

We now turn to the problem of estimating the quality of the solution. Again we will use the fact that weights can be assumed to be unique. A consequence of Lemma 2 is that the set of keys in an optimal solution does not depend on the actual weights, but only on the sequence of hash function values. Thus, the expected value of the optimal solution is $\sum_{i=1}^{n} p_{r,i}\, v_i$, where $p_{r,i}$ is the probability that the ith key is included in the optimal set of keys.

Lemma 2 says that if $\{k_1, \ldots, k_i\}$ can be accommodated under the given hash functions, they are included in an optimal solution. Using the earlier mentioned result of [12] on $\{k_1, \ldots, k_i\}$ with $\delta = \frac{r/2}{i} - 1$, we have that for $i < r/2$ this happens with probability at least $1 - 52\, r^{-1}/(\frac{r/2}{i} - 1)$. In particular, $p_{r,i}$ is at least this big.

For $i \geq r/2$ we derive a lower bound on $p_{r,i}$ as follows. If one of the vertices $(1, h_1(k_i))$ and $(2, h_2(k_i))$ in $G(\{k_1, \ldots, k_{i-1}\})$ is isolated, it follows by Lemma 3 that k_i is in the optimal solution. Under the assumption that hash function values are truly random, $G(\{k_1, \ldots, k_{i-1}\})$ has $i-1$ randomly and independently chosen edges. Thus, we have the bound $p_{r,i} \geq 1 - (1 - (1 - 2/r)^{i-1}))^2 = 2(1 - 2/r)^{i-1} - (1 - 2/r)^{2(i-1)} \approx 2e^{-i/r} - e^{-2i/r}$. This concludes the proof of Theorem 1.

2.5 A Lower Bound

This section gives a lower bound on the amount of memory needed by a lossy dictionary with an ϵ fraction of false positives and γn false negatives. Our proof technique is similar to that used for the lower bound in [4] for the case $\gamma = 0$.

Proposition 4. *For $0 < \epsilon < 1/2$ and $0 < \gamma < 1$, a lossy dictionary representing a set $S \subseteq \{0,1\}^w$ of $n \leq 2^{w-1}$ keys with at most $2^w\epsilon$ false positives and at most γn false negatives must use space at least*

$$(1-\gamma)\, n \log\left(\frac{1}{\epsilon + n/2^w}\right) - O(n) \text{ bits.}$$

Proof. We can assume without loss of generality that γn is integer. Consider the set of all data structures used for the various subsets of n elements from $\{0,1\}^w$. Any of these data structures must represent a set of at most $2^w\epsilon + n$ keys, in order to meet the requirement on the number of false positives. Thus, the number of n-element sets having up to γn keys not in the set represented by a given data structure is at most $\sum_{i=0}^{\gamma n} \binom{2^w\epsilon+n}{n-i}\binom{2^w}{i} \leq n\binom{2^w\epsilon+n}{n-\gamma n}\binom{2^w}{\gamma n}$. To represent all $\binom{2^w}{n}$ key sets one therefore needs space at least

$$\begin{aligned}
&\log\binom{2^w}{n} - \log\left(n\binom{2^w\epsilon+n}{(1-\gamma)n}\binom{2^w}{\gamma n}\right) \\
&\qquad \geq \log\left(\frac{2^w}{n}\right)^n - \log\left(n\left(\frac{(2^w\epsilon+n)e}{(1-\gamma)n}\right)^{(1-\gamma)n}\left(\frac{2^w e}{\gamma n}\right)^{\gamma n}\right) \\
&\qquad = n\log\left(\frac{(1-\gamma)/e}{\epsilon + n/2^w}\right) - \gamma n \log\left(\frac{(1-\epsilon)(1-\gamma)}{\gamma(\epsilon+n/2^w)}\right) - \log n \ .
\end{aligned}$$

The argument is concluded by first using $\gamma n \log(1/\gamma) = O(n)$, then merging the two first terms, and finally using $(1-\gamma)n\log(1-\gamma) = O(n)$. □

In the discussion following Theorem 1 we noted that if there are quotient functions with optimal range, the space usage of our scheme is $n\log(\frac{1}{\epsilon+n/2^w}) + O(n)$ when tables of combined size n are used. The expected fraction γ of false negatives is less than $3/10$ by Theorem 1. This means that our data structure uses within $O(n)$ bits of $10/7$ times the lower bound. The experiments described in Sect. 3 indicate that the true factor is less than $6/5$.

2.6 Using More Tables

We now briefly look at a generalization of the two table scheme to schemes with more tables. Unfortunately the algorithm described in Sect. 2.3 does not seem to generalize to more than two tables. An optimal solution can again be found using maximum weight matching, but the time complexity of this solution is not attractive. Instead we can use a variant of the *cuckoo* scheme described by the authors in [13], attempting to insert keys in order $k_1, \ldots, k_n$. For two tables

an insertion attempt for k_i works as follows: We store k_i in cell $h_1(k_i)$ of T_1 pushing the previous occupant, if any, away and thus making it *nestless*. If cell $h_1(k_i)$ was free we are done. Otherwise we insert the new nestless element in T_2, possibly pushing out another element. This continues until we either find a free cell or loop around unable to find a free cell, in which case k_i is discarded. It follows from [13] and the analysis in Sect. 2.3 that this algorithm finds an optimal solution, though not as efficiently as the algorithm given in Sect. 2.2. When using three or more tables it is not obvious in which of the tables one should attempt placing the "nestless" key. One heuristic that works well is to simply pick one of the two possible tables at random. It is interesting to compare this heuristic to a random walk on an expander graph, which will provably cross any large subset of the vertices with high probability.

The main drawback of using three tables is, of course, that another memory probe is needed for lookups. Furthermore, as the range of the hash functions must be smaller than when using two tables, the smallest possible range of quotient functions is larger, so more space may be needed for each cell.

3 Experiments

An important performance parameter of our lossy dictionaries is the ability to store many keys with high weight. Our first experiment tests this ability for lossy dictionaries using two and three tables. For comparison, we also test the simple one table scheme that stores in each cell the key of greatest weight hashing to it. The tests were done using truly random hash function values, obtained from a high quality collection of random bits freely available on the Internet [10]. Figure 1 shows experimentally determined values of $p_{r,\alpha r}$, the probability that key with index $i = \alpha r$ is stored in the dictionary, determined from 10^4 trials. For the experiments with one and two tables we used table size $r = 2048$ while for the experiment with three tables we used $r = 1536$. We also tried various other table sizes, but the graphs were almost indistinguishable from the ones shown. From the figure we see the significant improvement of moving from one to more tables. As predicted, nearly all of the $r/2$ heaviest keys are stored when using two tables. For three tables this number increases to about $.88r$. Of the r heaviest keys, about 84% are stored when using two tables, and 95% are stored when using three tables.

Apart from asymptotically vanishing differences around the point where the curves start falling from 1, the graphs of Fig. 1 seem independent of r. For two tables the observed value of $p_{r,\alpha r}$ for $\alpha > 1/2$ is approximately $3.5/9.6^{\alpha}$.

3.1 Application

To examine the practicality of our dictionaries we turn to the real world example of lossy image compression using wavelets. Today most state-of-the-art image coders, such as JPEG2000, are based on wavelets. The wavelet transform has the

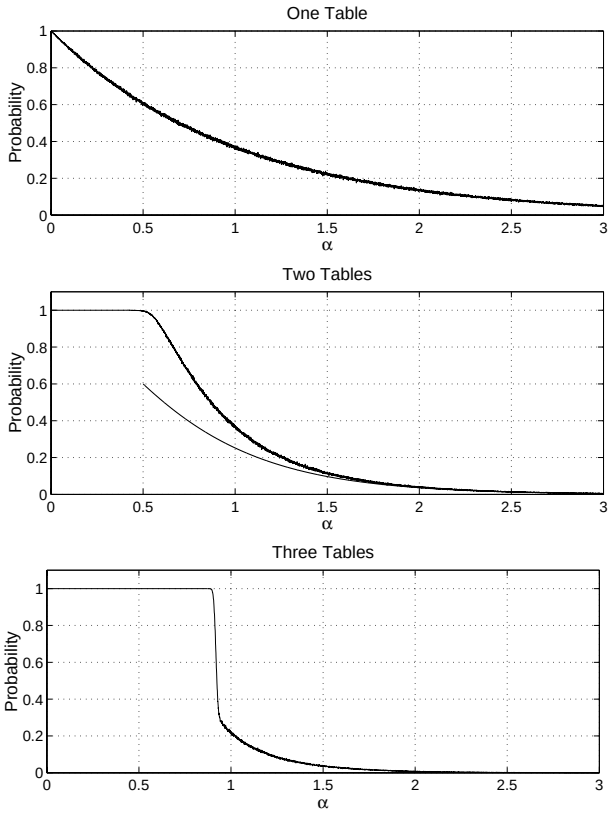

Fig. 1: The observed probability that the element with (αr)th highest weight is stored. For two tables our lower bound is shown.

ability to efficiently approximate nonlinear and nonstationary signals with coefficients whose magnitudes, in sorted order, decay rapidly towards zero. This is illustrated in Fig. 2. The figure shows the sorted magnitudes of the wavelet coefficients for the Lena image, a standard benchmark in image processing, computed using Daubechies second order wavelets. Thresholding the wavelet coefficients by a small threshold, i.e., setting small valued coefficients to zero, introduces only a small *mean squared error* (MSE) while leading to a sparse representation that can be exploited for compression purposes. The main idea of most wavelet based compression schemes is to keep the value and position of the r coefficients of largest magnitude. To this end many advanced schemes, such as zero-tree coding, have been developed. None of these schemes support access to a single pixel without decoding significant portions of the image.

Recently, interest in fast random access to decoded data, accessing only a few wavelet coefficients, has arisen [8, 9, 14, 15]. In [15] we show that lossy dictionaries are well suited for this purpose. Based on our data structure for lossy dictionaries, we present a new approach to lossy storage of the coefficients of wavelet transformed data. The approach supports fast random access

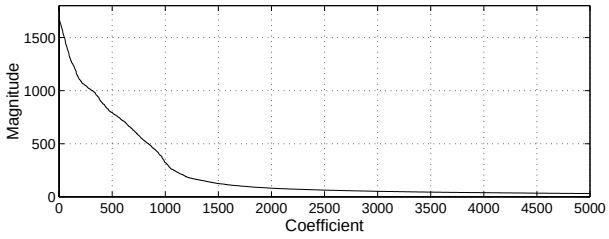

Fig. 2: Largest 5000 magnitudes of 67615 wavelet coefficients of the Lena image.

to individual data elements within the compressed representation. Compared to the previously best methods in the literature [8, 14] our lossy dictionary based scheme performs about 50%-80% better in terms of compression ratio, while reducing the random access time by more than 60%. A detailed description of the method is outside the scope of this paper. Instead we use the Lena image to give a flavor of the usefulness of lossy dictionaries on real world data. We store the coefficients of Fig. 2 in a two table lossy dictionary of total table size $r = 2^{11}$, using a simple family of hash functions. Specifically, we use hash functions of the form

$$h(k) = ((a_2k^2 + a_1a_2k + a_0) \bmod p) \bmod r/2,$$

where p is a prime larger than any key, $0 < a_0, a_1, a_2 < p$ and a_1 is even. A corresponding quotient function is

$$q(k) = 2(((a_2k^2 + a_1a_2k + a_0) \bmod p) \operatorname{div} r/2) + k \bmod 2 \ .$$

Again, 10^4 iterations were made, selecting random functions from the above family using C's `rand` function. The graph of $p_{r,\alpha r}$ is indistinguishable from that in Fig. 1. For our application, we obtain an MSE of 200, which is 27% more than the MSE when storing the r coefficients of largest magnitude. This difference would be difficult at best to detect in the reconstructed image. The previously mentioned family of [6] had somewhat worse performance. Using three tables reduces the MSE increase to a mere 1%.

4 Conclusion

We have introduced the concept of lossy dictionaries and presented a simple and efficient data structure implementing a lossy dictionary. Our data structure combines very efficient lookups and near-optimal space utilization, and thus seems a promising alternative to previously known data structures when a small percentage of false negatives is tolerable.

Though simple and efficient hash functions seem to work well in practice with our data structure, the challenge of finding such families that provably work well remains. Furthermore, the last two graphs in Fig. 1 are not completely understood. The same is true for the insertion heuristic for three or more tables.

Acknowledgment We thank Stephen Alstrup and Theis Rauhe for helpful discussions on the construction of our two table data structure.

References

[1] Burton H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, July 1970.

[2] Andrej Brodnik and J. Ian Munro. Membership in constant time and almost-minimum space. *SIAM J. Comput.*, 28(5):1627–1640 (electronic), 1999.

[3] Harry Buhrman, Peter Bro Miltersen, Jaikumar Radhakrishnan, and S. Venkatesh. Are bitvectors optimal? In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC '00)*, pages 449–458. ACM Press, New York, 2000.

[4] Larry Carter, Robert Floyd, John Gill, George Markowsky, and Mark Wegman. Exact and approximate membership testers. In *Proceedings of the 10th Annual ACM Symposium on Theory of Computing (STOC '78)*, pages 59–65. ACM Press, New York, 1978.

[5] William J. Cook, William H. Cunningham, William R. Pulleyblank, and Alexander Schrijver. *Combinatorial optimization*. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[6] Martin Dietzfelbinger, Torben Hagerup, Jyrki Katajainen, and Martti Penttonen. A reliable randomized algorithm for the closest-pair problem. *Journal of Algorithms*, 25(1):19–51, 1997. doi:10.1006/jagm.1997.0873.

[7] Michael L. Fredman, János Komlós, and Endre Szemerédi. Storing a sparse table with $O(1)$ worst case access time. *J. Assoc. Comput. Mach.*, 31(3):538–544, 1984.

[8] Insung Ihm and Sanghun Park. Wavelet-based 3D compression scheme for very large volume data. *Graphics Interface*, pages 107–116, 1998.

[9] Tae-Young Kim and Yeong Gil Shin. An efficient wavelet-based compression method for volume rendering. In *Seventh Pacific Conference on Computer Graphics and Applications*, pages 147–156, 1999.

[10] George Marsaglia. The Marsaglia random number CDROM including the diehard battery of tests of randomness. http://stat.fsu.edu/pub/diehard/.

[11] Rasmus Pagh. Low Redundancy in Static Dictionaries with $O(1)$ Lookup Time. In *Proceedings of the 26th International Colloquium on Automata, Languages and Programming (ICALP '99)*, volume 1644 of *Lecture Notes in Computer Science*, pages 595–604. Springer-Verlag, Berlin, 1999.

[12] Rasmus Pagh. On the Cell Probe Complexity of Membership and Perfect Hashing. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC '01)*. ACM Press, New York, 2001.

[13] Rasmus Pagh and Flemming Friche Rodler. Cuckoo hashing. To appear in Proceedings of ESA 2001, 2001.

[14] Flemming Friche Rodler. Wavelet based 3D compression with fast random access for very large volume data. In *Seventh Pacific Conference on Computer Graphics and Applications*, pages 108–117, Seoul, Korea, 1999.

[15] Flemming Friche Rodler and Rasmus Pagh. Fast random access to wavelet compressed volumetric data using hashing. Manuscript.

[16] Robert Endre Tarjan. Efficiency of a good but not linear set union algorithm. *J. Assoc. Comput. Mach.*, 22:215–225, 1975.