A Survey on Efficient Hashing Techniques in Software Configuration Management

Bernhard Grill
Vienna University of Technology
Vienna, Austria
Email: e1028282@student.tuwien.ac.at

Abstract—This paper presents a survey on efficient hashing techniques in software configuration management (CM) settings. Therefore it introduces in the most important hashing techniques as open hashing, separate chaining and minimal perfect hashing. Furthermore we evaluate those hashing techniques utilizing large data sets. Therefore we compare the hash functions in terms of time to build the data structure, performing only successful lookups and performing only unsuccessful lookups. The results indicate that minimal perfect hashing clearly outperforms the other presented hashing techniques.

I. INTRODUCTION & OVERVIEW

This paper presents an overview on efficient hashing techniques in software configuration management (CM) settings. Software configuration management tools store the configuration for an executable, e.g. configuration file and command line parameters. Therefore such systems typically utilize key-value stores. An example for such a CM is Elektra [19]. It’s widely known that hashing techniques represent an efficient way to handle key-value pairs in relation to lookup times. Therefore this paper focus on different hashing techniques applicable in CM settings.

First the paper introduces the most important hashing techniques as open hashing, separate chaining and minimal perfect hashing. Section II has a detailed look into open hashing techniques like linear probing, quadratic probing, double and Cuckoo hashing. Section III outlines separate chaining techniques, in particular we tackle exact fit and move to front technique. Perfect hashing and especially minimal perfect hashing are discussed in Section IV. Section V compares the presented hashing techniques in terms of storing large data sets, while Section VI concludes the paper.

The most important aspect of hash functions is their behavior in terms of collisions i.e. when two keys both try to occupy the same hash table location. In general there are two techniques how to deal with collisions. The first one is to handle the occurring conflicts while the second technique is to completely avoid collisions. Figure 1 outlines the most important hashing data structures and surveys their behavior. Open hashing utilizes a probing function for collision resolution which is invoked until an empty position in the table is found. The basic idea of separate chaining techniques is to apply linked lists for collision management, so in case of a conflict the new key is appended to the linked list. The idea of minimal perfect hashing is to always map distinct elements to distinct hash table positions without any collisions by creating a custom hashing function perfectly fitting the used key set.

II. OPEN HASHING

This section outlines a survey on the most effective open hashing techniques. Open hashing (also known as open addressing) is a technique utilizing an additional probing function for collision resolution. Whenever a hash collision occurs the probing function is invoked until either the target key is located or an empty record is found i.e. indicating the requested key is not existent. In the following we will discuss the most important probing functions:

• Linear probing [15] - Section II-A
• Quadratic probing [15] - Section II-B
• Double hashing [15] - Section II-C
• Cuckoo hashing [18] - Section II-D

A. Linear Probing

The principle of linear probing is accomplished by utilizing a start index, determined by \( h(k) \), and a stepping value \( i \), where \( h \) is the hashing function and \( k \) is the new key to insert. The starting index is determined by the hash function \( h(k) \), whereas \( i \) contains the stepping interval which is continuously added, until a free key is found in the hash table or the whole table is passed through: \( i \) is typically a relative prime number to the hash table’s size \( m \), in order to ensure the whole table is traversed. The position for a key utilizing linear probing is computed by: \( h(k, i) = (h(k) + i) \mod m \)

When the stepping value \( i \) is equals one, the probing function selects consecutive positions in the hash table. Double hashing is a type of linear probing utilizing a hash function to determine \( i \).

The performance for linear probing depends on the amount of probes fired during a key search, which depends on the hash table’s load factor \( \alpha = n/m \), where \( n \) is the number of occupied entries and \( m \) the hash table’s size. The higher the hash table’s load factor \( \alpha \) the higher is the amount of probes performed. According to Knuth [15] the estimated average number of probes operated by linear probing is given by \( \frac{1}{2} (1 + \frac{1}{1 - \alpha}) \).

Typically hardware architecture dependent parameters, like the cache size, have significant performance impacts on hashing techniques. Several contributions [2], [7], [13], [21], [23]
show the impact of caching on open hashing and separate chaining techniques.

B. Quadratic Probing

Quadratic probing is highly related to linear probing. The position for a key is computed by: \( h(k, i) = (h(k) + c_1 i + c_2 i^2) \mod m \). The hash function \( h(k) \) determines the position for key \( k \). The hash table’s size is given by \( m \), whereas \( i \) is the probe position for the key \( k \) and \( c_1 \) and \( c_2 \) are constant values [15].

Heileman et al. showed that linear probing has a better performance than quadratic probing in settings where the entire hash table does not fit into the cache memory [13]. On the other hand quadratic probing has a better performance in scenarios with high hash table load factors \( \alpha \). This characteristic is based on the improved clustering nature of linear probing compared to quadratic probing. Though linear probing typically produces more probing attempts than quadratic probing, those attempts feature a very high cache hit rate resulting in a better overall performance in practice when the whole hash table doesn’t fit in the cache memory. In settings where most of the hash table resides in cache memory, quadratic probing techniques like [15] or [16] outperform linear hashing procedures. The outperformance is based on the fact that most of the probes are cache hits and quadratic probing produces less probing attempts than linear probing. On the other hand quadratic probing shares some drawbacks with linear probing, e.g. the high search costs for tables with hash table load factors \( \alpha \) close to 1 [14]. According to Knuth [15] the following equation calculates the estimated average number of probes for a key search utilizing quadratic probing:

\[
1 - \ln(1 - \alpha) - \frac{\alpha}{2}
\]

C. Double Hashing

Double hashing utilizes two hash functions \( h_1 \) and \( h_2 \). While \( h_1 \) calculates the start index for the key, \( h_2 \) determines the step value in case of a collision. Using double hashing a key’s position is computed as follows: \( h(k, i) = (h_1(k) + i * h_2(k)) \mod m \) [15]. The other parameters are defined as before.

Double hashing effectively tackles clustering problems occurring in linear and quadratic probing, as the second hashing function \( h_2 \) provides varying step values for each key. Furthermore multi-collision settings produce a more homogeneous key distribution than linear or quadratic probing. Double hashing still shares some problems with the afore mentioned techniques as increased search costs for hash tables with a high load factor \( \alpha \). According to Knuth [15] the estimated average number of probes for a key search using double hashing is given by \(-\frac{2}{\alpha}\ln(1 - \alpha)\).

D. Cuckoo Hashing

The name Cuckoo hashing refers the cuckoo bird, where baby cuckoos push other chicks out of their nest after hatching. In terms of hashing a new key may push an existing key to a different position in the hash table. It utilizes two hash functions \( h_1(k) \) and \( h_2(k) \). Whenever a new key \( k \) is inserted, either the position computed by \( h_1(k) \) or \( h_2(k) \) is chosen. When the chosen position is already occupied by key \( k_2 \), the key \( k_2 \) will be replaced by \( k \). Then the replaced key \( k_2 \) has two possible new locations as well, defined by \( h_1(k) \) and \( h_2(k) \). One of those two possible locations will be used as new position for \( k_2 \). If both locations for \( k_2 \) are occupied the procedure is repeated until each pushed key is inserted or the key can not be inserted anymore [10], [18].

The replacement behavior may result in an infinite loop as cycles may appear during insertion. Infinite loops can be prevented by permitting only a certain amount of iteration cycles. Nevertheless, in this case the hashing technique won’t be able to insert the key, before the entire hash table is rebuilt with two different hash functions \( h_1(k) \) and \( h_2(k) \).

Figure 2 outlines the functionality of Cuckoo hashing by an example. The arrows indicate the alternative positions of each key. Consider a new item would be inserted in the location of key "A". Therefore the existing key "A" is moved to its alternative position, at the moment taken by key "B". Now key "B" has to be pushed to its alternative position which is currently unoccupied. Inserting a new item currently occupied by "H" would not succeed, as key "H" and "W" build a cycle, kicking each other endlessly.

Pagh et al. showed that insertions succeed in constant time,
though considering the scenario to rebuild the entire hash table as long as the table’s load $\alpha$ es kept below 50% [18].

Erlingsson et al. proposed a generalized Cuckoo hashing technique which can handle hash table’s load up to 99% [10]. The idea is to utilize not only two hash functions but an arbitrary amount of different hashing functions. The more different hashing functions are applied, the higher is the resulting maximum load factor $\alpha$ of the hash table.

Ross et al. proposed performance improvements for the generalized Cuckoo hashing technique by applying single-instruction-multiple-datastream (SIMD) instructions to exploit parallelisms and eliminate branch instructions within the probing functions [21].

III. SEPARATE CHAINING

The basic idea of separate chaining techniques is to utilize additional data structures, e.g. linked lists, for collision resolution. Each hash table key has its own list for collision resolution. The advantage of chaining techniques relies in the ability to easily resolve conflicts and the permanent possibility to insert new keys without resizing the hash table. Hence, applying separate chaining techniques may result in drastic performance penalties when the hash table degenerates, e.g. to a linked list. Such a degeneration may also increase the cache miss rates dramatically [7]. In the following we will discuss the two most important chaining techniques:

• Move to front [22] - Section III-A
• Exact fit [15] - Section III-B

A. Move to Front

The move to front technique consists of the hash table and a linked list for each key to handle the collisions. Whenever a conflict in a hash table key occurs, the new key is appended to the list’s end. The core idea of this technique is whenever a key is accessed it is moved to the beginning of the linked list.

In case of searching a key in the hash table’s conflict resolution list, the same parts of memory are accessed repeatedly. The move to front technique exploits the locality by moving recently used keys to the front of the list. This technique speeds up the future search for the same key. Hence, frequently accessed keys tend to occupy positions at the beginning of the list, while rarely used ones are typically stored at the list’s end. This behavior reduces the average lookup time for keys.

B. Exact Fit

The exact fit technique provides a cache-aware option for separate chaining technique. It keeps an array of neighboring entries instead of a linked list for per hash table item. Therefore this method is able to exploit higher memory locality than techniques applying linked lists, where items are typically stored in random memory locations. Hence, the array entries for conflict resolution are stored in a contiguous way in memory, resulting in less cache misses and decreased lookup time. Figure 3 outlines a hash table exploiting the exact fit technique.

![Fig. 3. Hash table applying exact fit technique](image)

The benefit of the exact fit technique is simultaneously a drawback as the technique requires storing colliding hash table entries in a contiguous way. Thus inserting a new value can results in allocating memory and copying the old array’s content to the new contiguous location.

Askitis et al. have shown that applying the exact fit technique in settings with variable length keys can result in heavy performance impacts [2].

IV. PERFECT HASHING

The basic idea of perfect hashing is to avoid collisions at all. Perfect hash functions map a static key set of $n$ entries to a set of $m$ numbers without any collision. In other words they map distinct elements to distinct hash table positions without collisions at all times for static key sets. Therefore such techniques do not have to implement collision resolutions techniques. In mathematical terms, perfect hashing techniques apply total injective functions. In the following we will discuss minimal and order preserving perfect hash functions.
Minimal perfect hash functions (MPH) map different keys exclusive of any collisions and without leaving any position inbetween unoccupied. In other words if \( n \) (the number of entries for the static key set) is equal to \( m \) (the number of hash table entries) the function is called a minimal perfect hashing function. Figure 4 outlines the difference between perfect hash functions and minimal perfect hash functions. Whereas perfect hash functions map keys to hash table positions without any collisions, minimal perfect hash functions additionally produce consecutive entries in the hash table without leaving any location vacant.

Minimal perfect hash functions are often used for fast lookup and memory efficient storage of static key sets. Examples for such static key sets are URLs in online web search engines, words for languages (both natural and programming languages) or configuration parameters for software programs. Furthermore MPH functions are highly relevant as indexing structure in database applications as shown by Botelho in [8]. Typically B+ trees are used for indexing in database systems. B+ trees are beneficial in highly dynamic scenarios with numerous insert and remove operations on the data structure. However B+ trees are not suitable in scenarios with little change and a massive amount of entries, as those data structures perform poorly and are highly complex to administer in large key set scenarios. In areas like database systems, big data or business intelligence working with huge data structures is daily business. For example assigning ids to a collection of URLs might be challenging, as database systems utilizing traditional data structures might collapse once the working set for the URLs does not fit into the main memory anymore. On the other hand minimal perfect hashing functions can easily handle up to hundred of million entries in memory using standard commodity hardware, due to their dense data structure. [20]

Order preserving minimal perfect hash functions additionally preserve the order of keys in subject to a function \( f \). E.g. consider the following keys \( a_1, a_2, \ldots, a_n \); given any keys \( a_j \) and \( a_k \) \((j < k)\) implies \( f(a_j) < f(a_k) \). Such hashing techniques require necessarily \( \Omega(n \log n) \) bits to be represented [11].

As perfect hash functions do not suffer from collisions or unoccupied positions within their data structures, such hashing functions have to be generated individually to fit the desired key set. Therefore hash function generators are utilized to create the proper fitting perfect hash function for the favored key set. Those generators use the desired key set as input to construct the fitting hash function.

Fredman et al. and Melhorn et al. introduced perfect hash functions in their publications in 1984 [12], [17]. In the same year Fredman et al. proved that minimal perfect hash functions require at least \( n \log e + \log u - O(\log n) \) bits [12]. Also in 1984 Melhorn et al. provided a minimal perfect hashing function [17] nearly satisfying the lower bound proposed by Fredman et al. [12]. His hashing function requires at most \( n \log e + \log u + O(\log n) \) bits. Belazzougui et al. proposed methods to create monotone minimal perfect hash functions [4], [5]. The minimal perfect hash functions proposed by Botelho et al. are the best in term of lookup time and storage space [9]. Those require about 2.62 bits per key [3], [9]. In 2009 Belazzougui et al. discovered a fundamental lower bound for minimal perfect hashing functions which require minimum 1.44 bits per key [6].

V. HASH PERFORMANCE COMPARISON

In 2011 Botelho et al. evaluated the performance of different hash function types [8]. In this section we present an aggregation and discussion on those results.

The experiments were performed on Linux 2.6, with an Intel Core 2 processor @1.86 GHz, 4 GB of main memory and 4 MB L2 cache. The results are averages on 50 repetitions and were statistically validated with a confidence level of 95%.

They used three different key sets for evaluation. The first consists of 5,424,923 unique queries from a online search engine, subsequent referred as WebQ. The second and third key set contain 10 million respectively 37,294,116 unique URLs, henceforth called URLs-10 and URLs-37.

In the following we will compare the performance of open hashing techniques in Section V-A and Cuckoo hashing, separate chaining and perfect hashing techniques in Section V-B.

A. Comparing Open Hashing Techniques

This section compares the performance of open hashing techniques except of Cuckoo hashing because the number of probing attempts were not measured for Cuckoo. Cuckoo’s performance is evaluated in Section V-B.

Table I gives a survey on the hash table’s load factor \( \alpha \) (in percent of the hash table’s size) impact on the times (in seconds) to successfully \( T_{\text{suc}} \) respectively unsuccessfully \( T_{\text{not}} \) lookup keys. The evaluation utilizes linear probing (LP), quadratic probing (QP) and double hashing (DH) techniques. It looks up 10, 20 respectively 250 million keys in the WebQ, URLs-10 respectively URLs-37 key set applying load factors ranging from 20% to 90%. The evaluation considers both successful \( T_{\text{suc}} \) and unsuccessful \( T_{\text{not}} \) lookup times for all queries. \( P_{\text{suc}} \) indicates the average number of probes per key for the scenario only processing successful lookups, whereas \( P_{\text{not}} \) traces the average number of probes for the unsuccessful
lookups only scenario. Furthermore the table outlines the time $T_b$ in seconds to build the hash structure. The bold items mark the best values per category.

In general, linear probing performs pretty well in terms of average probing attempts per key access ($P_{\text{suc}}$, $P_{\text{not}}$) and time for a successful or unsuccessful search ($T_{\text{suc}}$, $T_{\text{not}}$) in case of low and medium load factors ($\alpha = 20$, $\alpha = 50$). But its performance declines sharply when applying high load factors. Furthermore the amount of probing attempts per key access (both $P_{\text{suc}}$ and $P_{\text{not}}$) increases dramatically for linear probing in high load settings. This behavior indicates massive troubles for the technique to deal with clustering in the hash table’s data structure.

Double hashing clearly outperforms linear and quadratic probing in terms of probing attempts per key access (both $P_{\text{suc}}$ and $P_{\text{not}}$). On the other hand double hashing is slower in case of average time spent for successfully looking up the keys ($T_{\text{suc}}$) compared to quadratic probing.

Linear probing shows the best performance in terms of time to build the hash data structure $T_b$ in case of low or medium load factors ($\alpha = 20$, $\alpha = 50$). Whereas quadratic probing has the best performance with high load factors.

The average number of probing attempts ($P_{\text{suc}}$ and $P_{\text{not}}$) are close to the expected numbers according to the presented equations in Section II. Table II compares the calculated and observed average number of probing attempts. The calculation for the observed average number of probes is based on the results from Table I.

<table>
<thead>
<tr>
<th>Probing technique</th>
<th>$\alpha$</th>
<th>Observed avg. probes</th>
<th>Calculated avg. probes</th>
<th>Deviation (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LP</td>
<td>20</td>
<td>1.13</td>
<td>1.13</td>
<td>0.00</td>
</tr>
<tr>
<td>LP</td>
<td>50</td>
<td>1.49</td>
<td>1.50</td>
<td>0.66</td>
</tr>
<tr>
<td>LP</td>
<td>90</td>
<td>5.20</td>
<td>5.30</td>
<td>5.45</td>
</tr>
<tr>
<td>QP</td>
<td>20</td>
<td>1.12</td>
<td>1.12</td>
<td>0.00</td>
</tr>
<tr>
<td>QP</td>
<td>50</td>
<td>1.43</td>
<td>1.44</td>
<td>0.69</td>
</tr>
<tr>
<td>QP</td>
<td>90</td>
<td>2.71</td>
<td>2.85</td>
<td>4.91</td>
</tr>
<tr>
<td>DH</td>
<td>20</td>
<td>1.31</td>
<td>1.32</td>
<td>0.89</td>
</tr>
<tr>
<td>DH</td>
<td>50</td>
<td>1.38</td>
<td>1.39</td>
<td>0.72</td>
</tr>
<tr>
<td>DH</td>
<td>90</td>
<td>2.51</td>
<td>2.56</td>
<td>1.95</td>
</tr>
</tbody>
</table>

TABLE II
COMPARING THE OBSERVED AND CALCULATED AVERAGE NUMBER OF PROBING ATTEMPTS

Interestingly the observed average amount of probing attempts is always lower or equal than the calculated one. In general it differs the most when applying high load factors $\alpha$.

B. Comparing Cuckoo Hashing, Separate Chaining and Perfect Hashing Techniques

This section compares the performance of the remaining hashing techniques as Cuckoo hashing (CuH), separate chaining with move to front (SCMTF), separate chaining with exact fit (SCEF), separate chaining with exact fit and move to front (SCEFMTF) and minimal perfect hashing (MPH) which are outlined in Table III. The parameters have the same meaning as in Table I.

As Cuckoo hashing can not operate on load factors > 50%, the evaluation outlines the results for load factors between 20% and 50% (indicating maximum possible load).

Table III shows very interesting results. The bold items mark the best and the worst values per column. The hash table’s build time $T_b$ for minimal perfect hashing (MPH) is extraordinary fast compared to the other techniques, as it does not need to handle any collisions. When the data structure MPH fits into the L2 cache, which applies in case of WebQ and URLS-10 key set, it significantly outperforms other hashing techniques. This observation applies for both successful and unsuccessful scenarios ($T_{\text{suc}}$ and $T_{\text{not}}$). In the contrary situation, where the hashing data structure doesn’t fit into the L2 cache, the performance is pretty similar among the investigated hashing techniques in both successful and unsuccessful lookup settings. Altogether MPH either outperforms or in worst case has similar performance results as the other hashing techniques have.

In case of low hash table load factors Cuckoo hashing has related performance characteristics as the other hashing techniques. But in high load factor scenarios Cuckoo’s performance significantly declines in both settings. Notably, the chaining techniques don’t suffer as much performance impact in high load factor scenarios as open hashing techniques do (compare Table I and III). Interestingly the performance of separate chaining with exact fit and move to front (SCEFMTF) does not decline on high load factors, on the contrary it has the lowest minimum lookup time (except of MPH) for the URLS-37 key set. The reason is the dense hashing data structure caused by the high load factor which additionally benefits from caching effects compared to sparse data structures. This observation does not hold for successful lookup times $T_{\text{suc}}$.  

<table>
<thead>
<tr>
<th>Hash</th>
<th>$\alpha$</th>
<th>$P_{\text{suc}}$</th>
<th>$P_{\text{not}}$</th>
<th>$T_{\text{suc}}$</th>
<th>$T_{\text{not}}$</th>
<th>$T_b$</th>
<th>$P_{\text{suc}}$</th>
<th>$P_{\text{not}}$</th>
<th>$T_{\text{suc}}$</th>
<th>$T_{\text{not}}$</th>
<th>$T_b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>LP</td>
<td>20</td>
<td>1.13</td>
<td>1.28</td>
<td>3.38</td>
<td>3.92</td>
<td>2.86</td>
<td>1.14</td>
<td>1.30</td>
<td>12.65</td>
<td>13.98</td>
<td>9.35</td>
</tr>
<tr>
<td>QP</td>
<td>20</td>
<td>1.11</td>
<td>1.25</td>
<td>3.41</td>
<td>3.79</td>
<td>2.92</td>
<td>1.13</td>
<td>1.27</td>
<td>12.43</td>
<td>13.89</td>
<td>9.58</td>
</tr>
<tr>
<td>DH</td>
<td>20</td>
<td>1.10</td>
<td>1.24</td>
<td>3.46</td>
<td>3.85</td>
<td>2.89</td>
<td>1.11</td>
<td>1.25</td>
<td>12.68</td>
<td>13.99</td>
<td>9.65</td>
</tr>
<tr>
<td>LP</td>
<td>50</td>
<td>1.48</td>
<td>2.50</td>
<td>3.74</td>
<td>4.74</td>
<td>2.99</td>
<td>1.49</td>
<td>2.50</td>
<td>14.32</td>
<td>15.30</td>
<td>9.68</td>
</tr>
<tr>
<td>QP</td>
<td>50</td>
<td>1.42</td>
<td>2.13</td>
<td>3.80</td>
<td>4.68</td>
<td>3.04</td>
<td>1.42</td>
<td>2.13</td>
<td>14.45</td>
<td>15.15</td>
<td>9.76</td>
</tr>
<tr>
<td>DH</td>
<td>50</td>
<td>1.38</td>
<td>2.00</td>
<td>3.89</td>
<td>4.85</td>
<td>3.04</td>
<td>1.37</td>
<td>2.00</td>
<td>14.69</td>
<td>15.32</td>
<td>10.01</td>
</tr>
<tr>
<td>LP</td>
<td>90</td>
<td>5.18</td>
<td>50.54</td>
<td>5.21</td>
<td>17.85</td>
<td>4.05</td>
<td>5.17</td>
<td>50.53</td>
<td>17.20</td>
<td>48.19</td>
<td>11.76</td>
</tr>
<tr>
<td>QP</td>
<td>90</td>
<td>2.71</td>
<td>11.52</td>
<td>4.80</td>
<td>9.05</td>
<td>3.60</td>
<td>2.66</td>
<td>11.52</td>
<td>16.52</td>
<td>23.48</td>
<td>10.94</td>
</tr>
<tr>
<td>DH</td>
<td>90</td>
<td>2.51</td>
<td>10.00</td>
<td>5.01</td>
<td>9.46</td>
<td>3.66</td>
<td>2.48</td>
<td>10.00</td>
<td>16.95</td>
<td>24.70</td>
<td>11.15</td>
</tr>
</tbody>
</table>

TABLE I
PERFORMANCE COMPARISON BETWEEN LINEAR PROBING, QUADRATIC PROBING AND DOUBLE HASHING UTILIZING DIFFERENT HASH TABLE LOAD FACTORS $\alpha$, DATA FROM [8]
of separate chaining with exact fit (SCMTF) since it can’t exploit caching so well, due to the random memory accesses performed during linked list traversal.

Although MPH functions show a clear outperformance compared to other hashing techniques, it has the drawback of being only able to handle static key sets which results in recreating the MPH function on each configuration parameter change. Generating the MPH function to utilize the WebQ, URLs-10 and URLs-37 key set took 9.57, 21.81 respectively 95.48 seconds. This observation shows a nearly linear scale in terms of the key size for the MPH function’s generation time. The performance gain is based on the MPH function’s ability to find any key in the table via one single probe and its great cache memory exploitation behavior due to extremely dense hash data structures.

VI. CONCLUSION

In general linear probing (LP) performs pretty well in scenarios with low hash table loads α. While quadratic probing (QP) outperforms LP when applying high load to the hash table, double hashing (DH) has the lowest amount of probing attempts throughout the evaluation of open hashing techniques. Cuckoo hashing, Separate Chaining with Exact Fit (SCF) and Separate Chaining with Exact Fit and Move to Front (SCFMFT) performed rather poor compared to the other techniques.

Minimal perfect hashing (MPH) clearly outperforms all the other presented techniques. The performance gain is based on MPH’s ability to find any key via one single probe and its great cache memory exploitation behavior due to extremely dense hash data structures. Therefore MPH clearly outperforms the other techniques in scenarios where the whole data structure fits into the CPU cache. Furthermore MPH has by far the lowest build time \( T_b \) for the hash data structure during the evaluation. Although MPH functions are only able to handle static key sets, which results in recreating the MPH function on each configuration parameter update, they clearly beat the other hashing techniques presented in this paper and are therefore the best hashing technique in software configuration scenarios.

REFERENCES


