Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Guadalajara

Programming of Data Structures and Fundamental Algorithms

Act 5.2 - Comprehensive activity on the use of hash codes

Santiago Vera Espinoza

A01641585

TC1031, Grupo 613

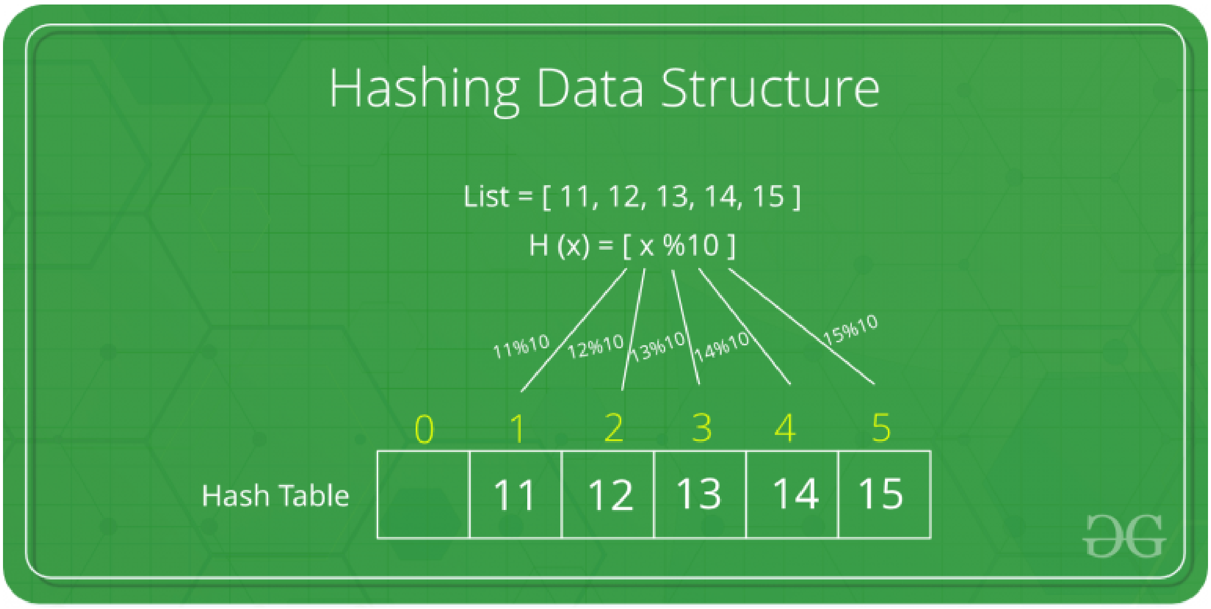
Jorge Enrique González Zapata

Noviembre 2022

Importance and efficiency of Hash Tables

The hash tables are used to store a large number of information or data so efficient search algorithms are required to have a good control of the data consists of sets of key pairs (unique in data storage) and set; these data are the hashes, the hashes are designed to solve the search problem efficiently so instead of making comparisons with a large number of values are stored in pairs to be introduced to the hash function, in this way could be found in a more efficient way and in the end we will have the two matrices, one of keys and the other for values. (Arquitectura de Sistemas UC3M, s.f.)

“Hashing is a technique or process of mapping keys, and values into the hash table by using a hash function. It is done for faster access to elements. The efficiency of mapping depends on the efficiency of the hash function used.” (GeeksforGeeks, 2022)



> Hashing means using some function or algorithm to map object data to some representative integer value. This so-called hash code (or simply hash) can be used as a way to delimit our search when looking for the element in the map. (Grupo Atico34, 2020)

Key functions according to "Grupo Atico34" (2020):

- Insert (key, value):Introduction to the function to be able to generate data storage.
- Get (key):Here we get the data from the hash table by means of the key.
- Delete (key): Deletes some data with its key if necessary.

They are used due to their benefits such as low cost, uniformity, variable range, collision resistance analysis, continuity, etc. (Grupo Atico34, 2020).

Hash tables have many applications, they can be used in any structure where a fast and efficient search is required, it could be applied in a dictionary where the same word is the key, the definition or translation could be the value or data of the hash table.

SHA 256

> SHA-2 (Secure Hash Algorithm 2), of which SHA-256 is a part, is one of the most popular hash algorithms around. A cryptographic hash, also often referred to as a “digest”, “fingerprint” or “signature”, is an almost perfectly unique string of characters that is generated from a separate piece of input text. SHA-256 generates a 256-bit (32-byte) signature. (Wagner, 2022)

Because the block cipher works on a fixed-size block of bits, the time complexity of running it is O(1). There are a total of Θ(n) applications of that block cipher (the input is split apart into fixed-sized blocks, so there are Θ(n) of those blocks), and the cost of computing the padding bit is probably O(1) but could potentially be O(n). Overall, this means that the runtime of computing these hash functions is Θ(n), which makes sense because each bit is visited at least once and the work done per bit is constant. (templatetypedef, 2017)

SHA-2 is known for its security (it hasn’t broken down like SHA-1) and its speed. In cases where keys are not generated, such as proof-of-work Bitcoin mining, a fast hash algorithm like SHA-2 often has the upper hand. In fact, SHA-256 is formally defined in the National Institute of Standards and Technology’s FIPS 180-4. (Wagner, 2022)

It is a proposal that in the case it is used is sufficient and greatly reduces the number of collisions. However, due to its complexity, we consider that its implementation would be an overkill for the resolution of the objective.

References

Arquitectura de Sistemas UC3M. (s.f.). *Tablas Hash*. Arquitectura de Sistemas UC3M. Retrieved November 23, 2022, from https://www.it.uc3m.es/pbasanta/asng/course_notes/ch07.html

GeeksforGeeks. (2022, 11 22). *Hashing Data Structure*. GeeksforGeeks. Retrieved November 23, 2022, from https://www.geeksforgeeks.org/hashing-data-structure/

Grupo Atico34. (2020, October 27). ▷ *¿Qué es y para qué sirve un hash?* Grupo Atico34. Retrieved November 23, 2022, from https://protecciondatos-lopd.com/empresas/hash/

templatetypedef. (2017, October 8). *What is the time complexity for cryptographic hash function?* Stack Overflow. Retrieved November 23, 2022, from https://stackoverflow.com/questions/46636078/what-is-the-time-complexity-for-cryptographic-hash-function

Wagner, L. (2022, October 12). *What Is SHA-256? | Boot.dev*. Boot.dev Blog. Retrieved November 23, 2022, from https://blog.boot.dev/cryptography/how-sha-2-works-step-by-step-sha-256/

/