Goldreich, Oded; **Wigderson, Avi**

On the circuit complexity of perfect hashing. (English) Zbl 1343.94057

Goldreich, Oded (ed.), Studies in complexity and cryptography. Miscellanea on the interplay between randomness and computation. In collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman. Berlin: Springer (ISBN 978-3-642-22669-4/pbk). Lecture Notes in Computer Science 6650, 26-29 (2011).

Summary: We consider the size of circuits that perfectly hash an arbitrary subset $S \subset \{0,1\}^n$ of cardinality 2^k into $\{0,1\}^m$. We observe that, in general, the size of such circuits is exponential in $2k-m$, and provide a matching upper bound.

For the entire collection see [Zbl 1220.68005].

MSC:

94A60 Cryptography
68R05 Combinatorics in computer science

Keywords:

perfect hashing; circuit complexity

Full Text: DOI

References:

[1] Alon, N., Babai, L., Itai, A.: A fast and Simple Randomized Algorithm for the Maximal Independent Set Problem. J. of Algorithms˜7, 567–583 (1986) · Zbl 0631.68063 · doi:10.1016/0196-6774(86)90019-2

[2] Carter, L., Wegman, M.: Universal Classes of Hash Functions. J. Computer and System Sciences˜18, 143–154 (1979) · Zbl 0412.68090 · doi:10.1016/0022-0000(79)90044-8

[3] Fredman, M., Komlós, J.: On the Size of Separating Systems and Perfect Hash Functions. SIAM J. Algebraic and Discrete Methods˜5, 61–68 (1984) · Zbl 0525.68037 · doi:10.1137/0605009

[4] Fredman, M., Komlós, J., Szemerédi, E.: Storing a Sparse Table with O(1) Worst Case Access Time. Journal of the ACM˜31, 538–544 (1984) · Zbl 0629.68068 · doi:10.1145/828.1884

[5] Korner, J., Marton, K.: New Bounds for Perfect Hashing via Information Theory. Europ. J. Combinatorics˜9, 523–530 (1988) · Zbl 0676.68007 · doi:10.1016/S0195-6698(88)80048-9

[6] Mehlhorn, K.: Data Structures and Algorithms. EATCS Monographs on Theoretical Computer Science, vol.˜1 (1984) · Zbl 0556.68002

[7] Nilli, A.: Perfect Hashing and Probability. Combinatorics, Probability and Computing˜3, 407–409 (1994) · Zbl 0820.68063 · doi:10.1017/S0963548300001280