Ordinances of the vectors of the n-dimensional Boolean cube in accordance with their weights

Valentin Bakoev[1]

[1]Department of Algebra and Geometry, Faculty of Mathematics and Informatics, "St. Cyril and St. Methodius" University of Veliko Tarnovo, Bulgaria, v.bakoev@uni-vt.bg

The problem "Given a Boolean function f of n variables by its Truth Table vector, denoted by $TT(f)$. Find (if exists) a vector $\alpha \in \{0,1\}^n$ of minimal (or maximal) weight, such that $f(\alpha) = 1$." arises in computing the algebraic degree of Boolean functions or vectorial Boolean functions called S-boxes. The solutions to this problem have useful generalizations and applications (for example, in generating all subsets of a given set in accordance with their cardinalities, or in generating combinations etc.). To find effective solutions we examine the ways of ordering the vectors of the Boolean cube in accordance with their weights. The notion "k-th layer" of the n-dimensional Boolean cube is involved in the definition and examination of the "weight order" relation. It is compared with the known relation "precedes". We enumerate the maximum chains for both relations. An algorithm that generates the vectors of the n-dimensional Boolean cube in accordance with their weights is developed. The lexicographic order is chosen as a second criterion for an ordinance of the vectors of equal weights. The algorithm arranges the vectors in a unique way called a weight-lexicographic order. It is represented by the (serial) numbers of the vectors, instead of the vectors itself. Its time and space complexities are $\Theta(2^n)$, i.e., of linear type with respect to the size of the output. The obtained results are summarized and added as a new sequence (A294648) in the OEIS.

References

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley Publishing Company, 1974.

[2] A. V. Aho, J. E. Hopcroft and J. D. Ullman, Data Structures and Algorithms, Addison-Wesley Publishing Company, 1983.

[3] V. Bakoev, Discrete mathematics: Sets, Relations, Combinatorics, Sofia: KLMN 2014. (in Bulgarian).

[4] I. Bouyukliev and V. Bakoev, Efficient Computing of Some Vector Operations over GF(3) and GF(4), Serdica Journal of Computing **2** (2008), 137–144.

[5] C. Carlet, Boolean functions for cryptography and error correcting codes, in: Y. Crama and P. L. Hammer (Eds.) Boolean Models and Methods in Mathematics, Computer Science and Engineering, Cambridge Univ. Press, 2010, 257–397.

[6] C. Carlet, Vectorial boolean functions for cryptography, in: Y. Crama and P. L. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science and Engineering, Cambridge Univ. Press, 2010, 398–469.

[7] T. Cormen, Ch. Leiserson, R. Rivest and Cl. Stein, Introduction to Algorithms, Third Edition, The MIT Press, 2009.

[8] R. Garnier and J. Taylor, Discrete Mathematics for New Technology, Second Edition, IOP Publishing Ltd. 2002.

[9] R. Grimaldi, Discrete and Combinatorial Mathematics. An Applied Introduction, Fifth Edition, Addison-Wesley, 2004.

[10] D. Knuth, The Art of Computer Programming, Combinatorial Algorithms, **4A**, Part 1, Addison-Wesley, 2011.

[11] T. Koshy, Discrete Mathematics with Applications, Academic Press, 2003.

[12] D. Kreher and D. Stinson, Combinatorial Algorithms: Generation, Enumeration and Search, CRC Press LLC, 1999.

[13] O. Kuznetsov, Discrete Mathamatics for Engineers, Sixth Edition, St. Peterburg-Moskow-Krasnodar: Lan, 2006 (in Russian).

[14] K. N. Manev, Introduction to Discrete Mathematics, Fourth Edition, Sofia: KLMN, 2007, (in Bulgarian).

[15] A. Nijenhuis and H. Wilf, Combinatorial Algorithms for Computers and Calculators, Second Ed. Academic Press, 1978.

[16] S. Pemmaraju and S. Skiena, Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica, Cambridge Univ. Press, 2003.

[17] E. Reingold, J. Nievergelt and N. Deo, Combinatorial algorithms, Theory and Practice, New Jersey, Prentice-Hall, 1977.

[18] K. H. Rosen, Discrete Mathematics and its Applications, Seventh Edition, McGraw-Hill, 2012.

[19] K. Rosen (ed. in Chief), J. Michaels, J. Gross, J. Grossman and D. Shier, Handbook of Discrete and Combinatorial Mathematics, CRC Press, 2000.

[20] F. Ruskey, Combinatorial Generation, working Version (1j-CSC 425/ 520), 2003, accessible on line at http://www.1stworks.com/ref/ruskeycombgen.pdf

[21] C. Savage, A Survey of Combinatorial Gray Codes, SIAM Review **39**(4), (1997), 605–629.

[22] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences (OEIS), 2009, published electronically at http://oeis.org/

[23] S. Skiena, The Algorithm Design Manual, Second Edition, Springer, 2008.