Mesnager, Sihem; **Kim, Kwang Ho**; **Jo, Myong Song**

On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic Boolean functions. (English) Zbl 1453.94172

Cryptogr. Commun. 12, No. 4, 659-674 (2020).

Summary: Determine the number of the rational zeros of any given linearized polynomial is one of the vital problems in finite field theory, with applications in modern symmetric cryptosystems. But, the known general theory for this task is much far from giving the exact number when applied to a specific linearized polynomial. The first contribution of this paper is a better general method to get a more precise upper bound on the number of rational zeros of any given linearized polynomial over arbitrary finite field. We anticipate this method would be applied as a useful tool in many research branches of finite field and cryptography. Really we apply this result to get tighter estimations of the lower bounds on the second-order nonlinearities of general cubic Boolean functions, which has been an active research problem during the past decade. Furthermore, this paper shows that by studying the distribution of radicals of derivatives of a given Boolean function one can get a better lower bound of the second-order nonlinearity, through an example of the monomial Boolean functions $g_\mu = \mathrm{Tr}(\mu x^{2^{2r}+2^r+1})$ defined over the finite field $\mathbb{F}_{2^n}$.

MSC:

94D10 Boolean functions
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
94A60 Cryptography
11T06 Polynomials over finite fields

Keywords:

Boolean functions; nonlinearity; linearized polynomial; root number

Full Text: DOI

References:

[1] Berlekamp, ER; Welch, LR, Weight distributions of the cosets of the (32; 6) Reed-Muller code, IEEE Trans. Inf. Theory, 18, 1, 203-207 (1972) · Zbl 0228.94003 · doi:10.1109/TIT.1972.1054732

[2] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G., Determining the nonlinearity of a new family of APN functions. AAECC 2007, LNCS, 4851, 72-79 (2007) · Zbl 1195.94048

[3] Bracken, C.; Leander, G., A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields Applic., 16, 231-242 (2010) · Zbl 1194.94182 · doi:10.1016/j.ffa.2010.03.001

[4] Canteaut, A.; Charpin, P.; Kyureghyan, GM, A new class of monomial bent functions, Finite Fields Applic., 14, 221-241 (2008) · Zbl 1162.94004 · doi:10.1016/j.ffa.2007.02.004

[5] Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. ChapterinBoolean Models and Methods in Mathematics, Computer Science, and Engineering. In: Crama, Y., Hammer, P.L. (eds.) , pp 257-397. Cambridge University Press (2010) · Zbl 1209.94035

[6] Carlet, C., On the higher order nonlinearities of algebraic immune functions. CRYPTO 2006, LNCS, 4117, 584-601 (2006) · Zbl 1129.94015

[7] Carlet, C.: On the nonlinearity profile of the Dillon function. http://eprint.iacr.org/2009/577.pdf (2009)

[8] Carlet, C., Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inf. Theory, 54, 3, 1262-1272 (2008) · Zbl 1192.94145 · doi:10.1109/TIT.2007.915704

[9] Carlet, C., On the nonlinearity of monotone Boolean functions, Cryptogr. Commun., 10, 6, 1051-1061 (2018) · Zbl 1419.94032 · doi:10.1007/s12095-017-0262-5

[10] Carlet, C.; Mesnager, S., Improving the upper bounds on the covering radii of binary Reed-Muller codes, IEEE Trans. Inf. Theory, 53, 1, 162-173 (2007) · Zbl 1192.94139 · doi:10.1109/TIT.2006.887494

[11] Carlet, C., On the higher order nonlinearities of algebraic immune Boolean functions, CRYPTO 2006, ser, Lect. Notes Comput. Sci., 4117, 2006, 584-601 (2006) · Zbl 1129.94015 · doi:10.1007/11818175$_3$5

[12] Carlet, C.; Dalai, DK; Gupta, KC; Maitra, S., Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction, IEEE Trans. Inf. Theory, 52, 7, 3105-3121 (2006) · Zbl 1192.94091 · doi:10.1109/TIT.2006.876253

[13] Dobbertin, H., One-to-one highly nonlinear power functions on GF(2n), Applic. Algebra Eng. Commun. Comput., 9, 2, 139-152 (1998) · Zbl 0924.94026 · doi:10.1007/s002000050099

[14] Fu, S., Feng, X., Wu, B.: Differentially 4-uniform permutations with the best known nonlinearity from butterflies. http://eprint.iacr.org/2017/449.pd (2017)

[15] Gangopadhyay, S., Garg, M.: The good lower bound of second-order nonlinearity of a class of Boolean function. http://eprint.iacr.org/2011/452.pdf (2011) · Zbl 1241.94024

[16] Gangopadhyay, S.; Sarkar, S.; Telang, R., On the lower bounds of the second order nonlinearity of some Boolean functions, Inform. Sci., 180, 2, 266-273 (2010) · Zbl 1184.94236 · doi:10.1016/j.ins.2009.09.006

[17] Garg, M., Gangopadhyay, S.: Good second-order nonlinearity of a bent function via Niho power function. http://eprint.iacr.org/2011/171.pdf (2011)

[18] Gode, R., Gangopadhyay, S.: On second-order nonlinearities of cubic monomial Boolean functions. http://eprint.iacr.org/2009/502.pdf (2009) · Zbl 1252.94066

[19] Gow, R.; Quinlan, R., Galois extensions and subspaces of alternating bilinear forms with special rank properties, Linear Algebra Appl.s, 430, 8, 2212-2224 (2009) · Zbl 1211.15030 · doi:10.1016/j.laa.2008.11.021

[20] Hou, X., GL(m, 2) acting on R(r,m)/R(r − 1,m), Discret. Math., 149, 99-122 (1996) · Zbl 0852.94020 · doi:10.1016/0012-365X(94)00342-G

[21] Iwata, T., Kurosawa, K.: Probabilistic higher order differential attack and higher order bent functions. ASIACRYPT 1999, pp. 62-74. Springer. LNCS 1716 (1999) · Zbl 0977.94033

[22] Kolokotronis, N., Limniotis, K.: Maiorana-McFarland functions with high second-order nonlinearity. http://eprint.iacr.org/2011/212.pdf (2011)

[23] Li, X.; Hu, Y.; Gao, J., The lower bounds on the second-order nonlinearity of cubic Boolean functions. Lower bounds on the second order nonlinearity of Boolean functions, Int. J. Found. Comput. Sci., 22, 6, 1331-1349 (2011) · Zbl 1252.94083 · doi:10.1142/S012905411100874X

[24] Lobanov, M., Exact relation between nonlinearity and algebraic immunity, Discret. Math. Appl., 16, 5, 453-460 (2006) · Zbl 1121.94020 · doi:10.1515/156939206779238418

[25] McEliece, R.J.: Finite Fields for Computer Scientists and Engineers. Kluwer Academic Publishers (1987) · Zbl 0662.94014

[26] Mesnager, S., Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, IEEE Trans. Inf. Theory, 54, 8, 3656-3662 (2008) · Zbl 1247.94028 · doi:10.1109/TIT.2008.926360

[27] Pless, VS; Huffman, WC, Handbook of Coding Theory (1998), Amsterdam: Elsevier, Amsterdam

[28] Schatz, J., The second-order Reed-Muller code of length 64 has covering radius 18, IEEE Trans. Inf. Theory, 27, 529-530 (1981) · Zbl 0459.94024 · doi:10.1109/TIT.1981.1056364

[29] Singh, D., Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions, Int. J. Comput. Sci. Inf. Secur., 2, 2, 786-791 (2011)

[30] Schmidt, KU, Nonlinearity measures of random Boolean functions, Cryptogr. Commun., 8, 4, 637-645 (2016) · Zbl 1386.94121 · doi:10.1007/s12095-015-0164-3

[31] Sun, G.; Wu, C., The lower bounds on the second-order nonlinearity of three classes of Boolean functions with high nonlinearity, Inform. Sci., 179, 3, 267-278 (2010) · Zbl 1156.94382 · doi:10.1016/j.ins.2008.10.002

[32] Sun, G.; Wu, C., The lower bound on the second-order nonlinearity of a class of Boolean functions with high nonlinearity, Applic. Algebra Eng. Commun. Comput., 22, 37-45 (2011) · Zbl 1254.94045 · doi:10.1007/s00200-010-0136-y

[33] Wang, Q.; Johansson, T., A note on fast algebraic attacks and higher order nonlinearities, INSCRYPT 2010, Lect. Notes Comput. Sci, 6584, 84-98 (2010) · Zbl 1285.68115 · doi:10.1007/978-3-642-13675-7$_7$