BULLETIN OF THE ICA
Article in press.

CCZ-invariants for APN functions based on the Weisfeiler-Lehman algorithm

Xiaohuan Jiang, Yue Zhou

Abstract. In this paper we apply the WL-algorithm to study the topological features of codes, especially the linear codes associated with APN functions. By using the WL-algorithm, we propose new CCZ-invariants for APN functions, which effectively distinguish CCZ-inequivalent APN functions including x^3 and x^9 over $\mathbb{F}_{2^7}$ that traditional methods struggle to separate, providing a graph-theoretic tool for the classification problem of APN functions.

References

[1] L. Babai, Graph isomorphism in quasipolynomial time, in *Proc. 48th ACM Symp. Theory Comput.*, ACM, New York, NY, USA, (2016), 684–697.

[2] C. Beierle and G. Leander, New instances of quadratic APN functions, *IEEE Trans. Inf. Theory* **68** (1) (2022), 670–678.

[3] C. Beierle, P. Langevin, G. Leander, A. Polujan, and S. Rasoolzadeh, Millions of inequivalent quadratic APN functions in eight variables, *arXiv preprint* (2025), arXiv:2508.04644.

[4] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inf. Theory* **52** (3) (2006), 1141–1152.

[5] M. Brinkmann and G. Leander, On the classification of APN functions up to dimension five, *Des. Codes Cryptogr.* **49** (2008), 273–288.

Key words and phrases: almost perfect nonlinear functions, CCZ-equivalence, Weisfeiler-Lehman algorithm, linear codes
Mathematics Subject Classifications: 05B10, 05C60, 94A60, 94B05
Corresponding author: Yue Zhou <yue.zhou.ovgu@gmail.com>

Received: 3 December 2025
Accepted: 12 February 2026

[6] K. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan, APN polynomials and related codes, *J. Combin. Inform. System Sci.* **34** (Special Issue) (2009), 135–159.

[7] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15** (2) (1998), 125–156.

[8] C. Carlet, Vectorial Boolean functions for cryptography, *Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer (eds.), Cambridge University Press, pp. 398–469, 2010.

[9] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge Univ. Press, Cambridge, UK, 2021.

[10] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, *Lecture Notes in Comput. Sci.* **950** (1995), 356–365.

[11] Y. Edel, Quadratic APN functions as subspaces of alternating bilinear forms, in *Proc. Contact Forum Coding Theory and Cryptography III* (*Brussel*), The Royal Flemish Academy of Belgium for Science and the Arts, 2011, 11–24.

[12] F. Fuhlbrück, J. Köbler, I. Ponomarenko, and O. Verbitsky, The Weisfeiler-Leman algorithm and recognition of graph properties, *Theoret. Comput. Sci.* **895** (2021), 96–114.

[13] N. S. Kaleyski, Invariants for EA- and CCZ-equivalence of APN and AB functions, *Cryptogr. Commun.* **13** (6) (2021), 995–1023.

[14] C. Morris, M. Ritzert, M. Fey, W. L. Hamilton, J. E. Lenssen, G. Rattan, and M. Grohe, Weisfeiler and Leman go neural: Higher-order graph neural networks, *Proc. AAAI Conf. Artif. Intell.* **33** (01) (2019), 4602–4609.

[15] K. Nyberg and L. R. Knudsen, Provable security against differential cryptanalysis, in *Ann. Int. Cryptol. Conf.*, Springer Berlin Heidelberg, Berlin, Heidelberg, (1992), 566–574.

[16] A. Pott, Y. Tan, T. Feng, and S. Ling, Association schemes arising from bent functions, *Des. Codes Cryptogr.* **59** (1) (2011), 319–331.

[17] N. Shervashidze, P. Schweitzer, E. J. Van Leeuwen, K. Mehlhorn, and K. M. Borgwardt, Weisfeiler-Lehman graph kernels, *J. Mach. Learn. Res.* **12** (9) (2011), 2539–2561.

[18] B. Weisfeiler and A. Leman, The reduction of a graph to canonical form and the algebra which appears therein, *NTI, Ser. 2* **9** (1968), 12–16.

[19] Z. Zhou, K. Li, and Y. Zhou, Topological invariants for linear codes and APN functions, *IEEE Trans. Inf. Theory* **71** (9) (2025), 6771–6784.