Muratović-Ribić, Amela; Pasalic, Enes

**A note on complete polynomials over finite fields and their applications in cryptography.** (English) Zbl 1302.11096

Finite Fields Appl. 25, 306-315 (2014).

Summary: A recursive construction of complete mappings over finite fields is provided in this work. These permutation polynomials, characterized by the property that both $f(x) \in \mathbb{F}_q[x]$ and its associated mapping $f(x) + x$ are permutations, have an important application in cryptography in the construction of bent-negabent functions which actually leads to some new classes of these functions. Furthermore, we also provide a recursive construction of mappings over finite fields of odd characteristic, having an interesting property that both $f(x)$ and $f(x + c) + f(x)$ are permutations for every $c \in \mathbb{F}_q$. Both the multivariate and univariate representations are treated and some results concerning fixed points and the cycle structure of these permutations are given. Finally, we utilize our main result for the construction of so-called negabent functions and bent functions over finite fields.

**MSC:**

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



**Keywords:**

finite fields; complete permutation polynomials; bent-negabent functions; planar mappings

**Full Text:** DOI

**References:**

[1] Ambrosimov, A. C., Properties of the bent functions of \textit{q}-ary logic over finite fields, Discrete Math., 6, 3, 50-60, (1994)

[2] Biham, E.; Shamir, A., Differential cryptanalysis of DES-like cryptosystems, J. Cryptol., 4, 1, 3-72, (1991) · Zbl 0729.68017

[3] Dembowski, P.; Ostrom, T. G., Planes of order \textit{n} with collineation groups of order $n^2$, Math. Z., 103, 239-258, (1968) · Zbl 0163.42402

[4] Laigle-Chapuy, Y., Permutation polynomials and applications to coding theory, Finite Fields Appl., 13, 1, (2007) · Zbl 1107.11048

[5] Leander, N. G., Monomial bent functions, IEEE Trans. Inf. Theory, 52, 2, 738-743, (2006) · Zbl 1161.94414

[6] Mann, H. B., The construction of orthogonal Latin squares, Ann. Math. Stat., 13, 418-423, (1942) · Zbl 0060.02706

[7] Mullen, G. L.; Niederreiter, H., Dickson polynomials over finite fields and complete mappings, Can. Math. Bull., 30, 1, 19-27, (1987) · Zbl 0576.12020

[8] Muratović-Ribić, A., A note on the coefficients of inverse polynomials, Finite Fields Appl., 13, 4, 977-980, (2007) · Zbl 1167.11044

[9] Niederreiter, H.; Robinson, K. H., Complete mappings of finite fields, J. Aust. Math. Soc., 33, 197-212, (1982) · Zbl 0495.12018

[10] Nyberg, K., Differentially uniform mappings for cryptography, (Advances in Cryptology—EUROCRYPT'93, Lect. Notes Comput. Sci., vol. 765, (1993), Springer-Verlag), 55-64 · Zbl 0951.94510

[11] Stănică, P.; Gangopadhyay, S.; Chaturvedi, A.; Gangopadhyay, A. K.; Maitra, S., Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inf. Theory, 58, 6, 4064-4072, (2012) · Zbl 1365.94684

[12] Su, W.; Pott, A.; Tang, X., Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree, (2012), CoRR · Zbl 1364.94806

[13] Tokareva, N., Generalizations of bent functions, a survey, J. Appl. Ind. Math., 5, 1, (2011) · Zbl 1249.94057

[14] Yuan, Y.; Tong, Y.; Zhang, H., Complete mapping polynomials over finite field $\mathbb{F}_{16}$, (Proceedings of the 1st International Workshop on Arithmetic of Finite Fields, WAIFI'07, (2007)), 147-158 · Zbl 1213.11193

[15] Wang, Q., On inverse permutation polynomials, Finite Fields Appl., 15, 2, 207-213, (2009) · Zbl 1183.11075

paper as accurately as possible without claiming the completeness or perfect precision of the matching.