Opponent´s opinion

on the habilitation thesis

Projective polynomials over finite fields and their applications in cryptography and combinatorics

by

Faruk Göloğlu

Faruk Göloğlu received the Ph.D. degree from Otto-von-Guericke University Magdeburg in 2009. His habilitation thesis summarizes the original results of 10 papers, 3 of them are one-author papers, and 7 are written with co-authors. These papers appeared in the period 2013-2023, in journals or lecture notes which doubtlessly count to the best and most prestigious in their field, but also in the wider area of discrete mathematics. I only mention the IEEE Transactions of Information Theory, Transactions of AMS, and Finite Fields and Their Applications. Article [K] is given in the thesis as "submitted", but it has already been published on the home page of Designs, Codes, and Cryptography.

8 of the papers deal with concepts that are strongly related: planar functions, perfect nonlinear (PN) and almost perfect nonlinear (APN) functions, permutation polynomials, and finite semifields. The notion of highly nonlinear maps between finite vector spaces (also called vectorial Boolean functions, substitution boxes, or S-boxes) plays an important role in secret key (symmetric) cryptosystems: by being the only nonlinear components of the ciphers, they provide *confusion.* Since the beginning of the 20th century, one studied semifields in the context of finite geometry and non-associative algebras. From the start of the 21st century, finite semifields gained new importance by delivering examples of rank-metric codes with good parameters; many old ideas of semifield constructions were used to construct new classes of rank-metric codes. The connection between semifields and planar, PN, and APN function is somewhat surprising. In odd characteristic, every commutative pre-semifield can be written as the polarization of a planar Dembowski-Ostrom polynomial. In even characteristic, there is no straightforward link between nonlinear functions and semifields, but the general impression is that tricks and methods that are efficient for constructing APN functions often help the construction of APN functions, and vice versa.

The topic of the remaining 2 papers is the hardness of the Discrete Logarithm Problem (DLP) in the multiplicative group of finite fields. Many recently used public key (asymmetric) cryptosystems, such as ElGamal, base their security on the assumption that the DLP is computationally intractable. A mini-revolution began with Joux's 2012 paper in which he introduced a new approach to the index calculus algorithm for fields of large prime order. The two papers extend Joux's results to the context of binary fields. The power of this approach was demonstrated via the solution of a DLP in the field GF(2^{1971}) and the field GF(2^{6120}).

At this point, the reader of this report may have the impression that Faruk Göloğlu's habilitation thesis is simply the disjoint union of 10 high-profile papers. I would say that the exact opposite of this is the case: the notion of q-projective polynomials connects the different topics. This notion was introduced by Abhyankar in 1997, but Hughes, Kleinfeld, and Knuth had already used polynomials of this class in the 1960s to construct finite semifields. The notion is simple with a very rich and nontrivial structure in the background. One can say that many results of the thesis followed from understanding the role of projective q-polynomials in previous constructions of planar functions, perfect nonlinear (PN) and almost perfect nonlinear (APN) functions, permutation polynomials, and finite semifields. The DLP algorithm results rely on the fact that a projective q-polynomial of the form $X^{q+1}+aX^q+bX+c$ has either 0,1,2 or q+1 roots in a field containing the coefficients a,b,c.

The thesis consists of three parts. In the *Preface*, the candidate gives a brief overview of the publications, his contributions, context, and organization of the thesis. The second part is called *Part 1: Commentary*, the most important and valuable piece of the dissertation. It intends to tell us the story of projective q-polynomials and to guide us through the 10 selected publications. It does this by elegantly presenting all the necessary concepts in such a way, that a non-expert like myself can follow. Together with 2 students of mine, we spent quite a time in the last 2 years learning the APN function and semifield constructions of Taniguchi and Zhou-Pott. The survey given in this chapter could have saved many efforts of us. As a side remark: I came across projective q-polynomial recently by studying the (k,n)-arc property of the hermitian curve $X^{q+1}+Y^q+Y=0$ in the Galois plane over $GF(q^{2r})$, r>3. I only mention these facts to emphasize the high didactical value of the *Commentary.*

The last (and longest) section of the thesis is *Part 2: Publications.* This is the concatenation of the 10 papers.

As I said above, the thesis survey results are original, they were published in top mathematical journals. This implies that listing all significant achievements would be a long and meaningless act. Therefore, I select three theorems that attract the most my personal attention.

1. Theorem 6.2 of [A] proves strong isotopy conditions within the family S of semifields. These conditions lead to an exponential lower bound on the number of non-isotopic commutative semifield of order p^n, with fixed odd prime p. Such bounds are crucial for dealing with an old problem by Kantor on the asymptotic number of semifield of a given order. The core element of the method is that the problem of determining the conjugacy of two *unknown* groups of autotopisms is converted to the problem of determining the conjugacy of two *known* nice subgroups.
2. Theorems V.1, V.3, and V.4 of [B] give three new classes of APN functions of the form F(x,y) = (f(x,y), g(x,y)) where f(x,y), g(x,y) are projective q-polynomials and q^3-polynomials, respectively. To prove the APN property, one needs a delicate computation with partial differentials. The real difficulty is to show that the new classes are not CCZ-equivalent to previously known classes of APN functions. Here, the proof uses properties of the Walsh-Hadamard transform and the bent property of the component Boolean functions of F.
3. Theorem 3 of [G] improves the result by Granger, Kleinjung, and Zumbrägel saying that for every prime p, there exist infinitely many explicit extension fields $GF(p^n)$ for which the discrete logarithm problem can be solved in expected quasi-polynomial time. The new result deals with the DLP in field extensions of small fields. The proof transfers the computation of the factor base into problems of finding points on algebraic curves over certain finite fields.

I resume my opinion by stating clearly that the thesis presented by Faruk Göloğlu meets the highest standards for a habilitation. The work contains excellent original scientific results.

I have passed the Turnitin originality check and it is clear that this is original work that only overlaps with existing literature. Automatic plagiarism check (Turnitin system report) showed no scientific error related to copying. **I warmly recommend to progress further in the habilitation procedure.**

Szeged, December 5, 2023

Prof. Dr. Gábor P. Nagy
Bolyai Institute
University of Szeged (Hungary)