Permutation Polynomials over Finite Fields

Daniele Bartoli (Università degli Studi di Perugia),
Ariane Masuda (New York City College of Technology, CUNY),
Qiang Wang (Carleton University)

June 9 – June 16, 2019

1 Overview of the Field

After the seminal works of Hermite [3] and Dickson [2] at the end of the 19^{th} century, many researchers have dedicated themselves to studying permutation polynomials over finite fields, not just because they are interesting in their own right, but also due to their connections with several applications.

Permutation polynomials over a finite field $\mathbb{F}_q$ are polynomials that induce bijections over $\mathbb{F}_q$ as mappings. For example, a monomial x^n permutes $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. Even though permutation monomials are well understood and simply described, the situation with binomials changes completely as not too many families of permutation binomials are known.

The problems in this area tend to fall into two categories: characterization and enumeration. The first category involves questions regarding criteria and tests for permutation polynomials, relationships between their coefficients, numbers and degrees of their terms, and finding families of permutation polynomials. The second one includes questions about the distribution and number of permutation polynomials of a given degree or special form, bounds and asymptotic formulas for these numbers, and the non-existence of permutation polynomials of certain shapes. In several situations these two kinds of problems are closely related. Applications in Coding Theory, Combinatorial Designs and Cryptography often require permutation polynomials having a particular structure or additional extraordinary properties. Permutation polynomials meeting these conditions are usually difficult to find.

The study of permutation polynomials has greatly benefited from a variety of tools in Algebraic Geometry, Combinatorics and Number Theory that involve algebraic curves, power sums, character sums, among others. Surveys like [6, 7, 4, 5] provide an excellent overview of the area.

2 Recent Developments and Open Problems

Over the past few decades the majority of papers in this area have been devoted to finding families of permutation polynomials. Many of them have built up on previous works by incorporating new ideas into known techniques. One of the goals of the workshop was to better understand the many existing families of permutation polynomials and see how they are related to each other under a more general framework.

The *index* of a polynomial was first introduced by Akbary, Ghioca, and Wang in 2009 to study the distribution of permutation polynomials over finite fields [1]. Given a non-constant polynomial g of degree less than $q-1$ over $\mathbb{F}_q$, the index ℓ of g is the unique integer for which g can be written as $a(x^r f(x)^{(q-1)/\ell}) + b$ for some $r \in \mathbb{N}_0$, $a, b \in \mathbb{F}_q$, and $f \in \mathbb{F}_q[x]$. They showed that the density of permutation polynomials in the

set of polynomials with prescribed index and exponents is higher when the index is smaller. The index of a polynomial has been also investigated in contexts that do not involve permutation polynomials. For instance, the index of a polynomial is closely related to the concept of the least index of a cyclotomic mapping polynomial. As a consequence, Wan and Wang obtained an index bound for character sums of polynomials over finite fields that is better than the Weil bound in some situations. This has potential applications related to the correlation of sequences, the minimum distance of trace codes, and the number of solutions of Artin-Schreier equations. Very recently Wang wrote a survey [8] on the index approach where a long section is dedicated to classifying permutation polynomials from over 60 papers based on their indices. We note that many results in these papers do not mention the index of the polynomial involved explicitly. So this survey is an important and major step in trying to organize the many existing permutation polynomials. It confirms that the index approach is very promising and provides a rich source of research directions.

In the workshop we aimed to pursue some of these directions. Dickson had already found all permutation polynomials of degree up to 6 back in 1896. More than 100 years passed, and only in 2010 permutation polynomials of degree 7 in finite fields of even characteristic were found. Wang's survey revealed that many known permutation polynomials were identified as having small indices. We thus propose the following.

Problem 1: Classify all permutation polynomials of small indices over $\mathbb{F}_q$ in terms of their coefficients.

Another interesting direction concerns the so-called *complete permutation polynomials*. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a complete permutation polynomial over $\mathbb{F}_q$ if both $f(x)$ and $f(x) + x$ are permutation polynomials over $\mathbb{F}_q$. Complete permutation polynomials are also related to bent and negabent functions that appear in a number of applications in Coding Theory, Combinatorial Designs and Cryptography. The most studied class of complete permutation polynomials is the monomial one.

Problem 2: Classify families of permutation polynomials or complete permutation polynomials like monomials $a^{-1}x^{\frac{q^n-1}{q-1}+1}$ and sparse permutation polynomials over $\mathbb{F}_{q^n}$ having indices $q-1$, $q+1$, or $c(q^{n-1}+\cdots+q+1)$ for some constant c.

3 Presentation Highlights

Motivated by the emerging emphasis on permutation rational functions, Bartoli presented a different viewpoint in classifying permutation rational functions of degree 3. He also showed several applications of algebraic curves in combinatorics. In a second talk Bartoli focused on techniques to prove irreducibility and to find irreducible components of curves over finite fields, and on their applications in the study of permutation polynomials, exceptional polynomials, complete mappings, planar polynomials, and APN functions.

Hou talked about a class of permutation trinomials of index $q + 1$. He discussed the main ingredients in the proof which involve number theoretic techniques, an application of the Hasse-Weil bound, and symbolic computations of resultants and factorizations.

Wang gave a survey talk on the index approach to study and classify permutation polynomials over finite fields. Permutation polynomials of intermediate indices are a recent focus in this area. They can be related to rational functions and complete mappings, depending on the choice of the index. For instance, Wang presented a construction of permutation polynomials with index $q + 1$ based on rational functions.

4 Scientific Progress Made

During the meeting, we mainly focused on the classification problem for permutation trinomials. We were able to obtain several non-existence results using the Hermite's criterion and algebraic curves. We expect to have a paper gathering our findings within the next few months.

Throughout the week we spent together, we had many opportunities to talk about the different directions that our area has been taking. The number of papers on permutation polynomials has greatly increased, and many new researchers have joined the area. While we currently have a rich source of results, many of them deal with particular shapes of polynomials. It is a challenge for the community to determine what is known, and whether or not certain results have already been obtained. The discussion led us to consider a long-term project that will involve digging through all papers on permutation polynomials, and classifying them, not just

in terms of natural parameters like their degrees, number of terms and finite field orders, but also through their indices. This will be a continuation of the work that Wang initiated in [8]. Our overarching goal is to have a better understanding of what is known, to organize the existing permutation polynomials in a systematic way, and to provide the research community access to the valuable data we will be collecting in the form of an online database and a survey book. The process will likely reveal many interesting interconnections. We greatly believe that this will open doors to further development of new mathematics, and prompt researchers to explore and investigate pertinent questions.

5 Outcome of the Meeting

The workshop gave a select group the unique opportunity to interact, concentrate efforts, and focus on problems. It was the first forum dedicated to discuss permutation polynomials over finite fields exclusively. Having participants with a diverse range of experience working with permutation polynomials and other related problems was highly important to promote expertise sharing. The group included two Ph.D. students and one postdoctoral fellow. We all greatly benefited from seeing how each one contributed to the discussion by exchanging research experiences. Our week was very productive and inspiring. We expect that our collaboration will give rise to one research article and, as a long-term objective, an online database of permutation polynomials and a book.

References

[1] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* **15** (2009), no. 2, 195–206.

[2] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, part I, *Ann. of Math.* **11** (1896–1897), 65–120.

[3] C. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris* **57** (1863), 750–757; Oeuvres, vol. 2, pp. 280–288, Gauthier-Villars, Paris, 1908.

[4] X. Hou, Permutation polynomials over finite fields – a survey of recent advances, *Finite Fields Appl.* **32** (2015), 82–119.

[5] X. Hou, A survey of permutation binomials and trinomials over finite fields, Proceedings of the 11th International Conference on Finite Fields and Their Applications, Magdeburg, Germany, 2013, *Contemporary Mathematics* **632** (2015), 177–191.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20**, second edition, Cambridge University Press, Cambridge, 1997.

[7] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, Taylor & Francis, Boca Raton, 2013.

[8] Q. Wang, Polynomials over finite fields: an index approach, in the Proceedings of Pseudo-Randomness and Finite Fields, Multivariate Algorithms and their Foundations in Number Theory, October 15-19, Linz, 2018, Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications, Degruyter, 2019, 319–348.