# Workshop on Finite Fields, Function Fields and Their Applications

*Karaköy Minerva Palas, İstanbul*
*April 26-27, 2018*

*In Honor of Alev Topuzoğlu and Henning Stichtenoth*

# 1 Program

### Thursday, April 26

**09:30-10:30:** Arnaldo Garcia (IMPA)
***"Explicit towers over finite fields"***

**10:30-11:30:** Eli Ben-Sasson (Technion - Israel Institute of Technology)
***"From Algebraic Geometry to improving Bitcoin Scalability and Privacy"***

**11:30-12:00:** *Coffee Break*

**12:00-13:00:** Alexander Pott (Otto von Guericke University Magdeburg)
***"On the isomorphism problem of combinatorial structures"***

**13:00-14:30:** *Lunch Break*

**14:30-15:30:** Ferruh Özbudak (Middle East Technical University)
***"Bent functions, MRD codes, plateaued functions and Alltop functions"***

**15:30-16:00:** *Coffee Break*

**16:00-17:00:** Alp Bassa (Boğaziçi University)
***"Function fields and the iterative construction of irreducible polynomials over finite fields"***

**17:00-18:00:** Domingo Gomez-Perez (University of Cantabria)
***"On the Carlitz Rank, some history and recent developments"***

**Friday, April 27**

**10:00-11:00:** Florian Pausinger (Queen's University Belfast)
***"Uniform distribution and the intriguing search for good permutations"***

**11:00-11:30:** *Coffee Break*

**11:30-12:30:** Ayça Çeşmelioğlu (Altınbaş University)
***"(Vectorial) Bent Functions and Partial Difference Sets"***

**12:30-14:30:** *Lunch Break*

**14:30-15:30:** Peter Beelen (Technical University of Denmark)
***"Weierstrass semigroups on, and a generalization of the Giulietti-Korchmáros curve"***

**15:30-16:00:** *Coffee Break*

**16:00-17:00:** Anna Somoza Henares (Universitat Politecnica de Catalunya, Universiteit Leiden)
***"From the difference of permutation polynomials to the construction of algebraic curves with Complex Multiplication"***

**17:00-18:00:** Daniel Panario (Carleton University)
***"Ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields"***

**18:00-18:30:** Closing Remarks

# 2 Abstracts

### Function fields and the iterative construction of irreducible polynomials over finite fields

Alp Bassa
*Boğaziçi University*

There are a variety of iterative constructions of irreducible polynomials over finite fields, the constructions using the $Q$-transform and the $R$-transform being the most prominent among these. Starting from a “suitable” irreducible polynomial, by iterative application of a transformation irreducible polynomials of arbitrary high degree can be constructed. We show how these constructions can be explained and unified by studying function field extensions corresponding to a given transformation and the use of Galois theory. We obtain a better understanding of the iterative constructions and various generalisations.

### Weierstrass semigroups on, and a generalization of the Giulietti-Korchmáros curve

Peter Beelen
*Technical University of Denmark*

The Giulietti-Korchmáros (GK) curve $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^6}$ that was discovered in 2009. The first topic that is addressed in this talk, concerns the structure of the Weierstrass semigroups of points on this curve. It turns out that there are three different possibilities for these semigroups and that the Weierstrass points of the GK curve are exactly the $\mathbb{F}_{q^6}$-rational points. A description of these three possible Weierstrass semigroups will be presented.

The GK curve was generalized to the family of Garcia-Güneri-Stichtenoth (GGS) curves in 2010. More precisely they found for each odd $n \geq 3$ a curve $\mathcal{C}_n$, maximal over $\mathbb{F}_{q^{2n}}$. The curve $\mathcal{C}_3$ equals the GK curve $\mathcal{C}$. In the second part of this talk a different generalization of the GK curve will be presented. If time allows, similarities and differences with the GGS curves will be discussed, especially their genera and automorphism groups.

These results were obtained together with Maria Montanucci.

### From Algebraic Geometry to improving Bitcoin Scalability and Privacy

Eli Ben-Sasson
*Technion - Israel Institute of Technology*

Scalable zero knowledge (ZK) proofs are constructed using techniques from algebraic geometry. This talk will discuss some of these techniques as well as research questions whose resolution will further improve the scalability and privacy of crypto-currencies like Bitcoin and Zcash.

## (Vectorial) Bent Functions and Partial Difference Sets

Ayça Çeşmelioğlu
*Altınbaş University*

Let $p$ be a prime and $V_n$ denote an $n$-dimensional vector space over the finite field $\mathbb{F}_p$. The Walsh transform of a function $f : V_n \to \mathbb{F}_p$ is defined as

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x)-b.x}$$

for each $b \in V_n$, where $\epsilon_p = e^{2\pi i/p}$ and $b.x$ is a nondegenerate inner product of $V_n$.
The function $f$ is called bent if for each $b \in V_n$ the absolute value of $\widehat{f}(b)$ is $p^{n/2}$. For a bent function the nonzero elements in the set $D_0^f = \{x \in V_n : f(x) = 0\}$ form a partial difference set under certain conditions.

A function $F : V_n \to V_m$ is a vectorial bent function if for each $\alpha \in V_n \setminus \{0\}$, the function $F_\alpha : V_n \to \mathbb{F}_p$ defined as $F_\alpha(x) = \alpha.F(x)$ is bent. A vectorial bent function is vectorial dual-bent if the set of its duals is a vector space of bent functions. We recently considered the relation between vectorial bent functions and partial difference sets. It turns out that being a vectorial dual-bent function is important for having a partial difference set.

In this talk I will introduce vectorial dual-bent functions and give the relation between such functions and partial difference sets.
This talk is based on the papers

- A. Çeşmelioğlu, W. Meidl and A. Pott , "Vectorial bent functions and their duals" Linear Algebra and its Applications Volume 548, 1 July 2018, Pages 305 − 320,
- A. Çeşmelioğlu, W. Meidl, "Bent and vectorial bent functions, partial difference sets and strongly regular graphs".

## Explicit towers over finite fields

Arnaldo Garcia
*IMPA*

Towers of function fields or of curves over finite fields play a central role in the asymptotic theory.

Ihara was the first to realize that the Hasse-Weil bound was weak when the genus grows to infinity and he introduced towers over fields of square cardinalities arising from modular curves. Over prime fields, Serre introduced towers arising from Class Field Theory. Both modular and class field towers are very hard to be made explicit; i.e., all function fields or curves are given by explicit polynomial equations.

This is a survey talk on the explicit towers we have worked out, specially with H. Stichtenoth.

### On the Carlitz Rank, some history and recent developments

Domingo Gomez-Perez
*University of Cantabria*

In 1953, Carlitz proved that all permutations over a finite field are compositions of linear polynomials and inversions. The Carlitz rank of a permutation $P$ measures how many inversions are necessary to represent $P$. Since it was introduced by Alev Topuzoğlu et al. in 2009, there has been a lot of movement in this field, because of its application to cryptography. Also recently, Federico Guidi and Giacomo Micheli have presented a new general theory to produce permutations of full length. In this talk, we review results regarding the Carlitz rank as well as connections with this new result.

### Bent functions, MRD codes, plateaued functions and Alltop functions

Ferruh Özbudak
*Middle East Technical University*

We recall some definitions and basic facts on bent functions, plateaued functions and Alltop functions over arbitrary finite fields. We give some new characterizations. We present some facts on MRD (maximum rank distance) codes. We also explain some applications related to cryptography, coding theory and communications briefly.

### Ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields

Daniel Panario
*Carleton University*

Let $\mathbb{F}_q$ be the finite field of $q$ elements, $q$ a prime power. If $f : \mathbb{F}_q \to \mathbb{F}_q$ induces a bijection, $f$ is a *permutation polynomial*; if $f$ is monic, $f(0) = 0$, and, when the degree $n$ of $f$ is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of $x^{n-1}$ is zero, $f$ is in *normalized* form. Normalized permutation polynomials are known exhaustively up to degree six.

For $a \in \mathbb{F}_q^*$, the *difference map* of $f$ is defined as $\Delta_{f,a}(x) = f(x+a) - f(x)$. This map plays a central role in differential cryptanalysis. To resist linear and differential cryptanalysis, we want permutation functions $f$ such that $|\Delta_{f,a}^{-1}(b)|$ is low for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We define $n_k(f)$ as the number of pairs $(a, b)$ such that $f(x+a) - f(x) = b$ has exactly $k$ solutions. The vector $[n_0(f), \ldots, n_q(f)]$ is the *spectrum* vector of the difference map of $f$. The *deficiency* of $f$ is $D(f) = n_0(f)$; it measures how close the $\Delta_{f,a}$'s are to be surjective. The *(weighted) ambiguity* of $f$ is $A(f) = \sum_{0 \le k \le n} n_k(f) \binom{k}{2}$; it measures how close the $\Delta_{f,a}$'s are to be injective.

We give exact formulas for the differential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

Joint work with Daniel Santana (Federal University of Santa Catarina, Brazil) and Qiang Wang (Carleton University, Canada).

### Uniform distribution and the intriguing search for good permutations

Florian Pausinger
*Queen's University Belfast*

A permuted van der Corput sequence in base $b$ is a one dimensional infinite sequence of real numbers in the unit interval generation of which involves a permutation of the set $\{0, 1, \ldots, b-1\}$. Such sequences are known to have low discrepancy and are, therefore, well studied in the theory of uniform distribution modulo 1.

The intriguing search for *good* generating permutations, i.e., permutations that generate permuted van der Corput sequences with exceptionally small discrepancy, was initiated by Henri Faure almost 40 years ago. Recently, it was shown that this search can be linked to the study of permutation polynomials over finite fields. The aim of this talk is to recall the basic notions of uniform distribution theory and to show how certain permutation polynomials contribute to a systematic study of van der Corput sequences.

This talk is based on my joint work with Alev Topuzoğlu:

F. Pausinger, A. Topuzoğlu, *On the discrepancy of two families of permuted van der Corput sequences.* Unif. Distrib. Theory **13** (2018), no 1, 47–64.

### On the isomorphism problem of combinatorial structures

Alexander Pott
*Otto von Guericke University Magdeburg*

Many combinatorial structures like designs are constructed via difference methods. In my talk, I will review some constructions and discuss the problem how to distinguish them, in particular I will answer a question recently posed by Davis, Huczynska and Mullen. This is joint work with my Ph.D. student Christian Kaspers.

### From the difference of permutation polynomials to the construction of algebraic curves with Complex Multiplication

Anna Somoza Henares
*Universitat Politecnica de Catalunya, Universiteit Leiden*

The Chowla-Zassenhaus conjecture states that there is no polynomial $f \in \mathbb{F}_p[x]$ of degree $d \geq 2$ such that both $f$ and $f + x$ are permutation polynomials if $p > (d^2 - 3d + 4)^2$.

This result was significantly generalized by Cohen, Mullen, and Shiue in 1995. They show that given $f$ and $f + g$ two permutation polynomials of degree $d \geq 3$ over $\mathbb{F}_p$, $p > (d^2 - 3d + 4)^2$, the difference $g$ is either constant or has degree $k \geq 3d/5$.

In this talk I introduce a recent generalization of this result in terms of the Carlitz rank and sketch the idea of the proof. In particular, given $f$ and $f + g$ permutation polynomials over an arbitrary finite field $\mathbb{F}_q$, we give a lower bound for the degree of $g$ in terms of the Carlitz rank of $f$ and $g$.

This is joint work with Nurdagül Anbar (RICAM), Almasa Odžak (University of Sarajevo), Vandita Patel (University of Toronto), Luciane Quoos (Universidade Federal do Rio de Janeiro) and Alev Topuzoğlu (Sabancı University).

On the second part of this talk I introduce my main research field: the construction of algebraic curves with Complex Multiplication (CM). I explain what is a curve with CM, how to construct such curves with the CM method and its application in cryptography based on curves.

## 3 Organizers

- Nurdagül Anbar, RICAM, Linz
- Cem Güneri, Sabancı University
- Canan Kaşıkcı, Sabancı University
- Wilfried Meidl, RICAM, Linz
- Seher Tutdere, Gebze Technical University

**This workshop is supported by Sabancı University.**