JOURNÉES ESTIVALES DE LA MÉTHODE POLYNOMIALE

LILLE, 24-27 JUIN, 2013

Length Multiset-Complete Krull Monoids

Paul Baginski

Let H be a Krull monoid or Krull domain, let G be its divisor class group, and let $G_0 \subset G$ be the classes containing prime divisors. It is well known that each nonunit $x \in H$ has only finitely many factorizations into irreducibles. If $x = a_1 \cdots a_n$ is a factorization $\mathbf{z}$ of x into irreducibles, the length of this factorization is $n = |\mathbf{z}|$. We elaborate upon the well-studied set $\mathcal{L}(x)$ of factorization lengths of x to account for the number of factorizations of a given length. If $Z(x)$ is the set of factorizations of x (a subset of the free monoid over the irreducibles of H), then the length multiset of x, denote $\mathcal{LM}(x)$, is the multiset $\{\{\ |\mathbf{z}|\ :\ \mathbf{z} \in Z(x)\ \}\}$.

Kainrath has shown that if the Krull monoid H has infinite class group G and $G_0 = G$, then for any finite multiset S on $\mathbb{N}\backslash\{1\}$, there is an $x \in H$ with $\mathcal{LM}(x) = S$. Kainrath's proof was nonconstructive. In this talk we will give the background on Kainrath's result and illustrate a constructive proof for $G = \mathbb{Z}$. We will also discuss recent work to extending Kainrath's result to Krull monoids with $G = \mathbb{Z}$ but G_0 a proper subset of $\mathbb{Z}$. Given time, we shall also discuss the analogous problem over finite class groups, where the polynomial method may be of more immediate use.

– –

Additive combinatorics in $\mathbb{F}_p$ and the polynomial method

Eric Balandraud

In this talk, we will present two additive problems, whose proofs rely on the polynomial method. Both are additive combinatorics problems, the first concerns sets (of subsums) and the second sequences (whose sums are zero) in $\mathbb{F}_p$.

A basic result in additive combinatorics is Cauchy-Davenport Theorem, it gives the minimal size of the sumset of two subsets in $\mathbb{F}_p$ (p prime). One of the first result proved thanks to the polynomial method by Alon, Nathanson and Rusza was a generalization for restricted addition (The Erdös-Heilbronn conjecture, proved earlier by Dias da Silva and Hamidoune). The Dias da Silva-Hamidoune generalization gives the minimal number of subsums of prescribed size of a set. The total number of subsums (of all sizes from 1 to $|A|$) was bounded only with additional conditions by Olson, using analytic methods. Thanks to the polynomial method, we give an unconditionnal minimal size of the total number of subsums of a set.

Another result of Olson proves that given any sequence of p non-zero elements (not all equal) in $\mathbb{F}_p$, there are at least p zero-sum subsequences. In a joint work with B. Girard, considering these zero-sum subsequences in a geometrical way, as 0-1 vectors, that are orthogonal to the initial sequence, we will show that the set of these sequences characterize the initial sequence. This result can also be understood in the following geometrical statement: In $\mathbb{F}_p^p$ every oblique hyperplane is fully characterized by its intersection with the p-cube $\{0,1\}^p$.

– –

Number of irreducible and indecomposable polynomials over finite fields

Arnaud Bodin

We first give a naive formula and an estimation for the number of irreducible polynomials in two (or more) variables over a finite field. We secondly recover these numbers in a more efficient way by using generating series. We also consider the case of indecomposable polynomials.

– –

Segre's lemma of tangents and linear MDS codes

Jan De Beule

A linear $[n,k,d]$-code C over the finite field $\mathbb{F}_q$ is the set of vectors of a k-dimensional subspace of the n-dimensional vector space $V(n,q)$ over $\mathbb{F}_q$. The Hamming distance between two codewords is the number of positions in which they differ. The minimum distance $d(C)$ is the minimum of the distances between all pairs of codewords of C. The Singleton bound for linear codes is the following relation between the parameters k, n and d of a linear code:

$$k \leq n - d + 1 \,.$$

If C reaches the Singleton bound, then $n-k = d-1$. By the fundamental theorem of linear codes, every $d-1$ columns of the parity check matrix of C are linearly independent. Hence, its columns represent a *set of vectors in $V(n-k,q)$ with the property that every subset of size $n-k$ is a basis*, and vice versa. The following statement is known as the MDS-conjecture.

> An arc S of a vector space $V(r,q)$, $r<q$, has size at most $q+1$, except when q is even and $r=3$ or $r=q-1$, in which case it has size at most $q+2$.

Recently, two results towards the MDS conjecture have been proven. The first important ingredient is a coordinate free version of the *lemma of tangents of Segre.* The second ingredient is the exploitation of this lemma through interpolation. In the talk we will focus on several algebraic aspects of these recent results.

References

[1] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc. (JEMS)*, 14(3):733–748, 2012.

[2] S. Ball and J. De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, 65(1-2):5–14, 2012.

– –

Zero-sums in F_p^3

Satwik Mukherjee

The Kemnitz Conjecture states that if we take a sequence of length $4p-3$ in $\mathbb{F}_p^2$, where p a prime number, then it has a subsequence of length p, whose sum is zero modulo p. For this we use the notation $s(\mathbb{F}_p^2) = 4p-3$. It is known that $s(F_p^3)$ is atleast $9p-8$. In this talk we will give analogous results on the constant $s_I(\mathbb{F}_p^3)$ for certain sets I in $\mathbb{F}_p^3$.

This is in line with the work of Kubertin and Geroldinger-Grynkewicz-Schmid.

– –

Barycentric-sum problems over cyclic groups

Alain Plagne

La k-ème (k est un entier positif) constante d'Olson barycentrique d'un groupe abélien (noté additivement) $(G,+)$ est définie comme le plus petit entier ℓ tel que tout sous-ensemble A de G contenant au moins ℓ éléments contient un sous-ensemble à k éléments $g_1,\dots,g_k$ satisfaisant $g_1+\cdots+g_k = k\ g_j$ pour un certain $1 \le j \le k$. Nous expliquerons comment obtenir de nouveaux résultats sur la k-ème constante d'Olson barycentrique d'un groupe abélien (principalement cyclique).

The k-th (k a positive integer) barycentric Olson constant of an abelian (additive) group $(G,+)$, is defined as the smallest integer ℓ such that each subset A of G with at least ℓ elements contains a subset with k elements $g_1,\dots,g_k$ satisfying $g_1+\cdots+g_k = k\ g_j$ for some $1 \le j \le k$. We shall explain how to derive some new results on the k-th barycentric Olson constants of abelian groups (mainly cyclic).

– –

Inverse additive results in $\mathbb{F}_p$

Christian Reiher

– –

The Quantitative Combinatorial Nullstellensatz and Integer-Valued Polynomials

Uwe Schauz

In the first part of our talk, we start with a corollary to the Combinatorial Nullstellensatz. It says that problems of "low complexity" with precisely one trivial solution posses non-trivial solutions. For example, any 4-regular graph possess a nontrivial 3-regular subgraph, as the empty subgraph is a 3-regular subgraph. Similarity, certain sequences of numbers or group elements posses nontrivial zero-sum subsequences, as empty subsequences may be seen as trivial solutions here. We then describe and proof the Quantitative Combinatorial Nullstellensatz and its numerous special cases, as, for example, Ryser's Permanent Formula or Scheim's expression for the number of edge n-colorings of planar n-regular graphs.

In the second part of our talk, we introduce periodic integer-valued polynomials, as, for example, the polynomial

$$P := -\tfrac{1}{8}X^4 + \tfrac{3}{4}X^3 - \tfrac{7}{8}X^2 - \tfrac{3}{4}X + 1\,,$$

which induces a map $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_9$ in a canonical way. At first, it gives rise to a map $\mathbb{Z} \longrightarrow \mathbb{Q}$ which actually is integer valued, as one can show. Second, this map $\mathbb{Z} \longrightarrow \mathbb{Z}$ induces the map $\mathbb{Z}l$ to $\mathbb{Z}_9$, $x \longmapsto P(x) + 9\mathbb{Z}$. Finally, it turns out that our new map is even 3-periodic, $P(x+3) \equiv P(x) \pmod 9$. So, we obtain a well defined map

$$P\colon \mathbb{Z}_3 \longrightarrow \mathbb{Z}_9\ , \qquad x = \hat{x} + 3\mathbb{Z} \longmapsto P(x) := P(\hat{x}) + 9\mathbb{Z}\ .$$

Of course, not every polynomial over $\mathbb{Q}$ gives rice to a well defined map $\mathbb{Z}_3 lto \mathbb{Z}_9$, but we have enough polynomials to obtain all maps $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_9$. This is not true for maps $\mathbb{Z}_q \longrightarrow \mathbb{Z}_r$ in general, it holds only if $q = p^\alpha$ and $r = p^\beta$, with a common prime p. More generally, we examine which maps between finite commutative groups can be described by multivariate polynomials with tuples of rational numbers as coefficients. As application, we formulate a Combinatorial Nullstellensatz for our polynomial maps, and deduce Olson's Theorem from it. This can be done in the exactly same way as Warning's Theorem is deduced from the classical Combinatorial Nullstellensatz. We also describe the connection between Olson's Theorem and Alon, Friedland and Kalai's conjectures about zero-sum subsequences and regular subgraphs of graphs.

_ _

Polynomial methods, group-ring methods, and 'ad-hoc approaches' in zero-sum theory, an incomplete comparison

Wolfgang A. Schmid

One of the classical results in zero-sum theory over finite abelian groups is the determination of the exact value of the Davenport constant for p-groups.

There are several – some well-known, some lesser known – proofs of this result. We survey some of these proofs, and proofs of related results, using different methods.

The aim of this talk is to high-light similarities and differences between various existing methods, in the hope that such a comparison can lead to a better understanding of the respective strengths and current limitations of each of them.

– –

The polynomial method in Galois geometries

Leo Storme

In Galois geometries, the study of substructures in finite projective spaces, polynomial techniques can be used.

With some substructures, it is possible to associate a polynomial. The geometrical properties of the substructure translate into properties of the polynomial, and vice versa, the properties of the polynomial translate into geometrical properties of the substructure.

This nice interaction has to led to fundamental results on blocking sets, maximal arcs in projective planes, blocking sets on the Hermitian curve, ovoids of the parabolic quadric $Q(4, q)$, and on other substructures in finite projective spaces.

In this talk, I will present a number of these links between substructures and polynomials, explain the results obtained and the techniques used for obtaining these results.

References

[1] S. Ball, The polynomial method in Galois geometries. Chapter in *Current research topics in Galois geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers (2012), 105-130.

– –

Lacunary polynomials and finite geometry

Tamás Szőnyi

The polynomial method has many applications in finite geometry, for example for (multiple) blocking sets, arcs, caps, (k, n)-arcs, and other substructures of finite affine or projective spaces. In this talk a small part of the applications is selected: applications of fully reducible lacunary polynomials over finite fields. Such polynomials were introduced by László Rédei in [1, 2], and he applied them to the problem of directions determined by a set of q points in a Desarguesian affine plane. In this talk we briefly survey the main theorems of Rédei's book and some more recent applications of fully reducible lacunary polynomials in finite geometry. These results are mostly related to generalizations of the above mentioned direction problem and blocking sets. Some of the results from the nineties can be found in [3].

References

[1] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser, Basel, 1970.

[2] L. Rédei, *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, and North-Holland, Amsterdam, 1973

[3] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* **208/209** (1999), 557-575.

– –