Workshop on

Emerging Applications of Finite Fields

December 09-13, 2013

as part of the

Radon Special Semester 2013 on

Applications of Algebra and Number Theory

ÖAW
Austrian Academy
of Sciences

RICAM
JOHANN · RADON · INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

"*On the Goldbach conjecture in the function field case*"

Andreas Bender University of Pavia, Italy

Abstract

The result to be discussed shows that the analogon to the Goldbach conjecture is true in odd characteristic if the size of the finite coefficient field is larger than a bound depending on the degree of the polynomial which is to be represented as the sum of two irreducible polynomials. The method of proof involves a reduction to a previous result on the Schinzel hypothesis in the function field case by Olivier Wittenberg and the speaker.

"*Correlation-immune Boolean functions and counter-measures to side channel attacks*"

Claude Carlet University of Paris 8, France

Abstract

Correlation-immune Boolean functions (from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) and vectorial functions (from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$) have well-known applications in symmetric cryptography, since they can be used in the pseudo-random generators of stream ciphers to combine the outputs to several LFSR (in the so-called combiner model); their correlation immunity allows resisting the Siegenthaler attack. In this framework, they must be balanced, that is, have uniform output distribution (they are then called resilient). No construction of infinite classes of resilient functions allowing resistance to all main attacks on the combiner model is known yet.

New ways of having correlation immune functions playing a role in cryptography have appeared very recently. The implementation of cryptographic algorithms in devices like smart cards, FPGA or ASIC leaks information on the secret data, leading to very efficient *side channel attacks* allowing recovering the key with few plaintext-ciphertext pairs in a few seconds if no counter-measure is included in the algorithm and/or the device. Counter-measures are costly in terms of running time and of memory when they need to resist higher order side channel attacks. The most commonly used counter-measure is a secret-sharing method called *masking*. Correlation immune functions can play a role in this framework, at least in two ways:

- A method called *leakage squeezing* for reducing the overhead due to masking, by achieving with one mask the same protection as with several ones, has been introduced recently. This method uses bijective vectorial functions, which are applied to the mask, and whose graph indicators need to be correlation immune of highest possible order;
- Independently, a way of reducing the number of possible mask values needed for the counter-measure is to choose them within a set whose indicator is a correlation-immune function of low weight.

In both cases, this poses new questions on correlation-immune functions (note that most of the numerous studies made until now dealt with resilient functions). We shall explain the role played by these correlation immune functions in this new framework, study them and study constructions.

This is joint work with Sylvain Guilley.

"*The discrete logarithm problem with auxiliary inputs*"

Jung Hee Cheon Seoul National University, Korea

Abstract

The Discrete Logarithm Problem (DLP) is a classical hard problem in computational number theory on which the security of many cryptographic schemes is based. The DLP is required to solve α for given group elements g and g^α for cyclic group $G = \langle g \rangle$ of finite order n. Recently, many variants of the DLP have been used to assure the security of pairing-based cryptosystem such as ID-based encryption, broadcast encryption and short signatures. These cryptosystems give us more various functionalities, but their underlying problems are not well understood. A generalization of these variants of DLP called the Discrete Logarithm Problem with Auxiliary Inputs (DLPwAI), is asked to find α for given $g, g^\alpha, \cdots, g^{\alpha^d}$. This

survey talk first recalls several well-known solutions of the original DLP and mainly focuses on the recent trials to solve the DLPwAI. The research for the DLPwAI starts from Cheon's $p \pm 1$ algorithms which use the embedding of the discrete logarithm into the extension of the finite field. Later, Satoh and Kim et al. tried to generalize the Cheon's algorithm to $\Phi_k(p)$ cases for $k \geq 3$, where $\Phi_k(\cdot)$ is the k-th cyclotomic polynomial. However, the result of Kim et al. says that this generalization of Cheon's algorithm cannot be better than the usual square root complexity algorithms such as Pollard's rho algorithm when $k \geq 3$. Recently, Cheon and Kim observed that solving the DLPwAI reduces into the problem finding a polynomial of degree d with small value sets. And then, Cheon, Kim and Song introduced a generalized version of the DLPwAI and gave a heuristic algorithm to solve that problem.

"*On the discrete logarithm problem in finite fields*"
Pierrick Gaudry CNRS, Nancy, France

Abstract

There has been a lot of recent progress in the topic of computing discrete logarithms in finite fields, in particular (but not only) in fields of small characteristic. In this talk, we will present a survey of the current situation with best known complexities, depending on the size of the characteristic compared to the size of the finite field. Then, we will give a more detailed description of the (heuristic) quasi-polynomial algorithm for fields of small characteristic that we proposed with Barbulescu, Joux and Thom. Although there has been also many improvements on the practical side, we will take a pure complexity point of view.

"*Exponential sum estimate over subgroup in an arbitrary finite field*"
Alexey Glibichuk Moscow Institute of Physics and Technology, Russia

Abstract

Exponential sum estmates for multiplicative subgroups is an interesting and complicated problem. In fields of prime order $\mathbb{F}_p$ nontrivial estimates for exponential sums over multiplicative subgroups H is known if its cardinality is larger than $e^{\frac{c \ln p}{\ln \ln p}}$, where $c > 0$ is an absolute constant. Presence of nontrivial subfields is an obvious obstacle when one is trying to extend the above-mentioned result to the case of an arbitrary finite field $\mathbb{F}_q$, since there is a character which is concentrated in this subfield. The usual restriction on the cardinality of the multiplicative subgroup is not sufficient in finite fields, and we need to require more. More precisely, one can expect nontrivial results if the multiplicative subgroup is not largely contained in any multiplicative shift of an arbitrary subfield. We obtained a bound when the subgroup H is larger than $e^{\frac{c(\eta) \ln q}{\ln \ln q}}$, $c(\eta) > 0$ and $|H \cap dS| < |H|^{1-\eta}, \eta > 0$ for any $d \in \mathbb{F}_q \setminus \{0\}$ and subfield $S \subseteq \mathbb{F}_q$. In the talk the proof of this estimate will be sketched.

This is joint work with Jean Bourgain.

"*Nonlinear shift registers - A survey and challenges*"
Tor Helleseth University of Bergen, Norway

Abstract

Linear feedback shift registers (LFSRs) have many applications in coding theory, cryptography and modern communications systems. The theory of LFSRs has been thoroughly studied and is well understood. In particular, the periodic structure of sequences generated by an LFSR and the distribution of the elements during a period have been analyzed using methods from finite fields. Sequences generated by a nonlinear feedback shift registers (NLFSRs) is a much more challenging and difficult topic and its theory is far less developed and understood. There is a much richer selection of sequences that can be generated by NLFSRs compared with only using LFSRs of the same degree. In the 1960s Magelby and Golomb in their pioneering works gave a contribution to NLFSRs that significantly increased the interest in the topic and provided several basic results in the field. In the 1970s and 1980s Mykkeltveit, Fredricksen, Kjeldsen and many others developed several new fundamental ideas and results. During the last 30 years the progress has been more limited than expected and many interesting problems remain essentially unsolved. For example to determine the period and distribution of 0's and 1's in a sequence generated by an NLFSR is a very challenging problem. In this paper we will give a basic introduction and overview of NLFSRs and provide some known connections to combinatorics, algebra and finite fields and discuss the status of some of the open problems in this area.

"*The connections between the Erdős distance problem and the restriction problem for spheres in the finite field setting*"
Doowon Koh Chungbuk National University, South Korea

Abstract

In this talk we introduce the restriction problem for spheres and the Erdős distance problem in vector spaces over finite fields. The purpose of this talk is to address how one can deduce the Erdős distance results from the restriction theorems for spheres in the finite field setting. The L^2-restriction estimates play a crucial role in deriving the Erdős distance results.

"*Some pseudorandom phenomena in finite fields*"
Swastik Kopparty Rutgers University, USA

Abstract

I will talk about two recent results showing pseudorandom properties of some simple functions over finite fields of small characteristic (such as $\mathbb{F}_{2^n}$).

The first result shows that some functions over $\mathbb{F}_{2^n}$, such as the cubic residue character and Trace($x^{1/3}$), are uncorrelated with degree $n^{0.1}$ polynomials over $\mathbb{F}_2$. The theorems and proofs are related to the Razborov-Smolensky method for proving lower bounds on arithmetic circuits over $\mathbb{F}_2$.

The second result (joint with Eli Ben-Sasson) shows that some other functions, such as Trace(x^7), are nonconstant on subspaces of small dimension, provided $\mathbb{F}_{2^n}$ has no large subfields. The proof uses an algebraic expression of the sum-product phenomenon involving properties of ”subspace polynomials”.

"*Ramanujan graphs, Ramanujan hypergraphs and zeta functions*"
Wen-Ching Winnie Li Pennsylvania State University, USA

Abstract

Ramanujan graphs are spectrally extremal k-regular graphs. Using number theory, Margulis and independently Lubotzky-Phillips-Sarnak constructed infinite families of Ramanujan graphs for $k = q + 1$, where q is a prime power. Recently Marcus-Spielman-Srivastava proved the existence of an infinite family of Ramanujan graphs for any $k > 1$ using analysis and combinatorics. Regarding graphs as 1-dimensional simplicial complexes, the higher dimensional analogue of Ramanujan graphs, called Ramanujan complexes, for finite quotients of the building attached to $PGL(n)$ has been studied, and infinite families of Ramanujan complexes were explicitly constructed by Li, Lubotzky-Samuels-Vishne, and Sarveniazi, respectively, using deep results in number theory. Another way to characterize these Ramanujan graphs and complexes is in terms of their attached zeta functions. More precisely, a graph or complex is Ramanujan if and only if its zeta function satisfies the Riemann Hypothesis. In this survey talk we shall review these developments.

"*Uniqueness of $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ and existence of non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$*"

Ferruh Özbudak Middle East Technical University, Ankara, Turkey

Abstract

Let q be a power of an odd prime. We prove that all $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ are equivalent. We also give a geometric method to find the corresponding equivalence explicitly.

The results above imply that any $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ is obtained by restriction of an $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^3$. We also show that there exist $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$ which cannot be obtained by restriction of any $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^4$. We call such maps *non-extendable* $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$.

This is joint work with Alexander Pott.

"*Semifields, relative difference sets, and bent functions*"

Alexander Pott Otto-von-Guericke-University Magdeburg, Germany

Abstract

Recently, the interest in semifields has increased due to the discovery of several new families and progress in the classification problem. Commutative semifields play an important role since they are equivalent to certain planar functions (in the case of odd characteristic) and to modified planar functions in even characteristic. Similarly, commutative semifields are equivalent to relative difference sets. The goal of this survey is to describe the connection between these concepts. Moreover, we shall discuss power mappings that are planar and consider component functions of planar mappings, which may be also viewed as projections of relative difference sets. It turns out that the component functions in the even characteristic case are related to negabent functions.

This is joint work with Kai-Uwe Schmidt and Yue Zhou.

"*Sum-product estimates in finite fields*"

Oliver Roche-Newton University of Reading, UK

Abstract

For a given set A, we can define its sum set to be the set

$$A + A := \{a + b : a, b \in A\}$$

of all pairwise sums determined by A. Similarly, the product set of A is defined by

$$AA := \{ab : a, b \in A\}.$$

It is believed that at least one of these sets should always be "large". To be more precise, it was conjectured by Erdős and Szemerédi that for any finite set $A \subset \mathbb{Z}$, and any $\varepsilon > 0$,

$$\max\{|A + A|, |AA|\} \gg A^{2-\varepsilon}.$$

This talk concerns the problem in the setting where A is a subset of the finite field $\mathbb{F}_q$. Although the problem is morally similar to the Erdős-Szemerédi conjecture, there are also stark differences, in terms of both what has been achieved and what we might hope to achieve, as well as the techniques used. The intention here is to give some insight into these differences, explain a little about the methods which have been effective so far, and finally to discuss some existing and potential applications.

“*Testing algebraic independence over finite fields*”

Nitin Saxena Department of CSE, IIT Kanpur, India

Abstract

The problem of algebraic independence is to test whether for given polynomials $f_1, \ldots, f_m$ (over a field k), there is a nontrivial annihilating polynomial $A(y_1, \ldots, y_m)$ such that $A(f_1, \ldots, f_m) = 0$. This is a fundamental problem with several known computational applications. There is an efficient randomized algorithm to solve this when k has characteristic zero. This is based on the *Jacobian criterion*.

There is no efficient algorithm known when k is a general finite field. We will describe in this talk a new criterion to handle these cases – the *Witt-Jacobian* criterion. This criterion is not yet efficient but is theoretically better than the brute-force method. We will sketch the proof, with the de Rham-Witt complex being the main tool.

Based on: *Algebraic Independence in Positive Characteristic – A p-adic Calculus*, with Johannes Mittmann and Peter Scheiblechner. **Trans. Amer. Math. Soc.**, 2013

“*The eigenvalues method in combinatorial number theory*”

Ilya Shkredov Steklov Mathematical Institute, Moscow, Russia

Abstract

In the talk a family of operators (finite matrices) with interesting properties will be discussed. These operators appeared during attempts to give a simple proof of Chang’s theorem from Combinatorial Number Theory. At the moment our operators have found several applications in the area connected with Chang’s result as well as other problems of Number Theory such as: bounds for the additive energy of some families of sets, new structural results for sets with small higher energy, estimates of Heilbronn’s exponential sums and others.

“*NTRU cryptosystem: recent developments*”

Ron Steinfeld Monash University, Australia

Abstract

The NTRU public-key cryptosystem, proposed in 1996 by Hoffstein, Pipher and Silverman, is a fast and practical alternative to classical schemes based on factorization or discrete logarithms. In contrast to the latter schemes, it offers quasi-optimal asymptotic efficiency and conjectured security against quantum computing attacks. The scheme is defined over finite polynomial rings, and its security analysis involves the study of natural statistical and computational problems defined over these rings.

We survey several recent developments in both the security analysis and in the applications of NTRU and its variants, within the broader field of lattice-based cryptography. These developments include a provable relation between the security of NTRU and the computational hardness of worst-case instances of certain lattice problems, and the construction of cryptosystems with powerful extra functionality. In the process, we identify the underlying statistical and computational problems in finite rings.

Part of this talk is based on joint work with Damien Stehlé.

“*On the linear complexity of Legendre-Sidelnikov sequences*”

Ming Su Nankai University, Tianjin, China

Abstract

Linear complexity is an important cryptographic quality measure of sequences. We study the linear complexity of $p(q-1)$-periodic Legendre-Sidelnikov sequences, which combine the concepts of Legendre sequences and Sidelnikov sequences. We get lower and upper bounds on the linear complexity in different cases, and experiments show that the upper bounds can be attained. Remarkably, we associate the linear complexity of Legendre-Sidelnikov sequences with some famous primes including safe prime and Fermat prime. If 2 is a primitive root modulo $\frac{q-1}{2}$, and q is a safe prime greater than 7, the linear complexity is the period if $p \equiv 3 \bmod 8$; $p(q-1)-p+1$ if $p \equiv q \equiv 7 \bmod 8$, and $p(q-1)-\frac{p-1}{2}$ if $p \equiv 7 \bmod 8$, $q \equiv 3 \bmod 8$. If q is a Fermat prime, the linear complexity is the period if $p \equiv 3 \bmod 8$, and $p(q-1)-q+2$ if $p \equiv 5 \bmod 8$. It is very interesting that the Legendre-Sidelnikov sequence has maximal linear complexity and is balanced if we choose $p = q$ to be some safe prime.

"*Finite field models in additive combinatorics*"

Julia Wolf University of Bristol, UK

Abstract

The use of a finite-dimensional vector space over a prime field as a setting in which to model additive problems concerning subsets of the integers was strongly advocated by Green in an excellent article of the same name. Almost a decade later, we shall survey the model's successes to date as well as its limitations, and try to capture a glimpse of what may be to come.