Colloquium on Galois Geometry

May 4, 2012

Abstracts

Finite Spreads in Random Network Coding

Anna-Lena Trautmann

University of Zurich, Switzerland

(Joint work with Thomas Feulner, Felice Manganiello)

Constant dimension codes are defined to be subsets of the Grassmannian $\mathcal{G}_q(k,n)$ over a finite field $\mathbb{F}_q$, and are of great interest since Kötter and Kschischang developed a theory of subspace codes for application in random network coding [1].

A spread of a vector space $\mathbb{F}^n$ is a set of k-subspaces of $\mathbb{F}^n$ that covers the whole space and whose elements intersect only trivially. It is a well-known geometrical object. A spread over a finite field is called a finite spread.

Naturally finite spreads can be seen as constant dimension codes. They are very interesting from a coding point of view since they are the only known optimal constant dimension codes, i.e. their cardinality fulfills the Singleton-like bound for given error correction capability.

In this talk we will explain the random network coding model and show how the structure of Desarguesian spreads can be used for various coding theoretic aspects. Among others we will present a decoding algorithm and show how to compute the linear and semilinear automorphism groups of these codes.

References

[1] R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *Information Theory, IEEE Transactions on*, 54(8):3579–3591, August 2008.

Anna-Lena Trautmann, Institute of Mathematics, University of Zurich
Winterthurerstrasse 190, 8057 Zürich, Switzerland
anna-lena.trautmann@math.uzh.ch

Ring-linear codes from projective Hjelmslev geometries

Michael Kiermaier

Universität Bayreuth

In 1967, the *Nordstrom-Robinson-Code* was discovered, which is a binary block code of length 16, size 2^8 and minimum Hamming distance 6. It is famous for the fact that it has higher minimum distance than all *linear* binary codes of the same length and size. We say that it is a BTL-Code (better-than-linear). In 1994 the striking discovery was made that all these codes can be represented linearly over the ring $\mathbb{Z}_4$ of the integers modulo 4 [1]. Since then, a lot of research has been done on $\mathbb{Z}_4$-linear codes and on linear codes over more general finite rings. However, the examples of strong ring-linear codes found since then are comparatively sparse.

In this talk, we will discuss the connection between ring-linear codes and point sets in certain projective Hjelmslev geometries [2]. For example, the Nordstrom-Robinson-Code is related to a hyperoval in the projective Hjelmslev plane over $\mathbb{Z}_4$. The geometric point of view allows us the construction of several new series of good ring-linear codes. These codes include non-linear binary block codes of the BTL parameters $(58, 2^7, 28)$ and $(114, 2^8, 56)$ [3,4].

References

[1] J. A. Roger Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[2] T. Honold and I. Landjev, "Linear codes over finite chain rings," *Electron. J. Combin.*, vol. 7, #R11, 2000.

[3] M. Kiermaier and J. Zwanzger, "A $\mathbb{Z}_4$-linear code of high minimum Lee distance derived from a hyperoval," *Adv. Math. Commun.*, vol. 5, no. 2, pp. 275–286, 2011.

[4] M. Kiermaier and J. Zwanzger, "New ring-linear codes from dualization in projective Hjelmslev geometries," *Des. Codes Cryptogr.*, 2012, to appear.

Michael Kiermaier, Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany
michael.kiermaier@uni-bayreuth.de

Relations between invariant polynomials

Relinde Jurrius

Eindhoven University of Technology, The Netherlands

Linear codes can be associated to many other objects in discrete mathematics, such as matroids and geometric lattices. For all these objects, several invariant polynomials are defined. For example, a well-known invariant polynomial of a linear code is its weight enumerator. There is a lot to ask about the relations between invariant polynomials. Does one polynomial determine another? Do two polynomials determine each other? Can a set of polynomials determine another polynomial? Does a polynomial determine the same polynomial for the dual object, like the MacWilliams relations for the weight enumerator?

In this talk I will discuss the relation between two polynomials that are associated to geometric lattices: the coboundary and the Möbius polynomial. The motivation for much of the theory comes from coding theory, so in this talk I will only address those geometric lattices that are associated to linear codes. In general, the coboundary and Möbius polynomial do not determine each other. But in some cases, the Möbius polynomial of a code, together with the Möbius polynomial of the dual code, do determine the coboundary polynomial.

The coboundary polynomial is closely related to the extended weight enumerator of a linear code, therefore we can formulate a MacWilliams-type property for duality. The Möbius polynomial determines the dual minimum distance of the code. This makes it possible to use techniques for weight enumeration to give us more information about the relations between the coboundary and Möbius polynomial.

References

[1] R. P. M. J. Jurrius. Relations between Möbius and coboundary polynomial. arXiv:1202.3303, 2012. Submitted.

Relinde Jurrius, Eindhoven University of Technology, Department of Mathematics and Computer Science, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
r.p.m.j.jurrius@tue.nl

The probability that an $\mathbb{F}_q$-hypersurface is smooth

Jeroen Demeyer

Ghent University

Consider the n-dimensional projective space $\mathbb{P}^n$ over a finite field $\mathbb{F}_q$. A *hypersurface* is defined by one homogeneous equation, say of degree d, with coefficients in $\mathbb{F}_q$. For d going to infinity, we show that the probability that a hypersurface of degree d is non-singular tends to $1/\zeta_{\mathbb{P}^n}(n+1)$. In the particular case of $n = 2$, this gives a probability of $(q^3-1)(q^2-1)/q^5$.

This is a special case of the results in Bjorn Poonen's paper "Bertini Theorems over Finite Fields", where he computes the probability that the intersection of a given variety and a random hypersurface is smooth. Poonen uses the full power of algebraic geometry, whereas the special case of the projective space can be proven using elementary linear algebra and properties of finite fields.

Jeroen Demeyer, Department of Mathematics, Ghent University, Krijgslaan 281, S22, B-9000 Ghent, Belgium
jdemeyer@cage.ugent.be

Selected results on APN functions and DHOs

Yves Edel

Ghent University

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be almost perfect nonlinear (APN) if the equation $\beta(x,a) := f(x) + f(x+a) + f(a) + f(0) = b$ has at most two solutions, for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$. We say f is quadratic if its algebraic degree is 2, i.e. if $\beta(x,a)$ is an alternating bilinear map.

A set $\mathcal{S}$, of cardinality $\frac{q^n-1}{q-1}+1$, of n-dimensional vector spaces over $\mathbb{F}_q$ is said to be a dimensional dual hyperoval (DHO) if any 1-dimensional subspace of an element of $\mathcal{S}$ equals the intersection of two different elements in $\mathcal{S}$.

We present an extended introduction to (quadratic) APN functions and DHOs over $\mathbb{F}_2$, introduce their connections to other structures such as semibiplanes, rank metric codes and spaces external to the line Grassmanian and point out some analogies to semifields, spreads and projective planes. In the second part an overview on the results of [1] will be given. We give a characterization of quadratic APNs and bilinear DHOs as APNs and DHOs admitting a translation group, and present results on the structure of the normal closure of the translation groups, in the automorphism group, and on equivalences of such APNs and DHOs.

References

[1] U. Dempwolff and Y. Edel. Dimensional Dual Hyperovals and APN Functions with Translation Groups. 2012, submitted.

Yves Edel, Department of Mathematics, Ghent University, Krijgslaan 281, S22, B-9000 Ghent, Belgium
yedel@cage.ugent.be

Enumeration of designs with subdesigns

Petteri Kaski

Aalto University, Helsinki

(Joint work with Patric R. J. Östergård and Alexandru Popa)

This talk will review approaches to enumerate, up to isomorphism, a family of designs with the restriction that each design must admit at least one subdesign of a fixed type. While most such results to date are *constructive*, that is, enumeration means that one explicitly constructs exactly one design from each isomorphism class, it turns out that *nonconstructive* techniques can in some cases be deployed to extend the reach of enumeration, for example, by reducing to the study of double cosets of the automorphism group of the subdesign and the automorphism group of the residual. Two recent examples will be considered in the context of Steiner triple systems (STSs), namely a constructive enumeration of the 12,661,527,336 nonisomorphic STS(21)s with a sub-STS(9), and a nonconstructive enumeration of the 1,356,574,942,538,935,943,268,083,236 nonisomorphic STS(27)s with a sub-STS(13).

Petteri Kaski, Aalto University, Department of Information and Computer Science, P.O. Box 15400, FI-00076 Aalto, Finland
petteri.kaski(atsymbol)aalto.fi