Colloquium

on

Finite Geometry, Coding Theory and Cryptography

November 7, 2014

Abstracts

Partial permutation decoding for binary Hadamard codes

Roland D. Barrolleta

Universitat Autònoma de Barcelona

(Joint work with Mercè Villanueva)

Permutation decoding is a technique which involves finding a subset S, called PD-set, of the permutation automorphism group $\mathrm{PAut}(C)$ of a code C in order to assist in decoding. A method to obtain s-PD-sets of size $s+1$ for partial permutation decoding for the binary linear Hadamard codes H_m of length 2^m, for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{1+m} \right\rfloor$, is described. Moreover, a recursive construction to obtain s-PD-sets of size $s+1$ for H_{m+1} of length 2^{m+1}, from a given s-PD-set of the same size for the Hadamard code of half length H_m is also established. It is known that some nonlinear Hadamard codes can be constructed as binary images under the Gray map of codes over $\mathbb{Z}_4$. In this talk, we provide examples of small s-PD-sets for this family of nonlinear Hadamard codes.

Universitat Autònoma de Barcelona, Departament d'Enginyeria de la Informació i de les Comunicacions. Edifici Q, 08193, Bellaterra, Cerdanyola del Vallès (Barcelona)
rolanddavid.barrolleta@uab.cat, merce.villanueva@uab.cat

Codes for Synchronization Error Correction

Johann A. Briffa

University of Malta

(Joint work with Hans Georg Schaathun, Stephan Wesemeyer, and Victor Buttigieg)

Channels subject to synchronization errors have been known for a long time in coding theory. Interest was rekindled when Davey and MacKay [1] proposed a concatenated scheme combining an outer q-ary LDPC code with a sparse inner code for synchronization correction. Alternative approaches have also been tried, including the insertion of short marker sequences in binary LDPC codewords [2], and extending the state space of convolutional codes to allow correction of synchronization errors. More recently, the latter approach has been applied successfully to turbo codes [3]. This increase in interest is mainly due to new applications requiring such codes. However, synchronization error channels introduce a number of difficulties, and much remains unknown.

In this presentation, we introduce the problem of correcting synchronization errors, reviewing common channel models. This is followed by an overview of existing codes for insertion/deletion correction, focusing on our Time-Varying Block (TVB) codes [4], which generalize a number of previous synchronization error-correcting codes. We discuss our main contributions to this topic, including an expression for the expected distribution of drift on a common channel model, an optimal decoder for TVB codes, and practical recommendations based on probabilistic arguments. We also review practical contributions, including an optimized massively parallel implementation of a flexible decoder [5]. In closing, we consider what problems remain open.

References

[1] M. C. Davey and D. J. C. MacKay, "Reliable communication over channels with insertions, deletions, and substitutions," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 687–698, 2001.

[2] F. Wang, D. Fertonani, and T. M. Duman, "Symbol-level synchronization and LDPC code design for insertion/deletion channels," *IEEE Trans. Commun.*, vol. 59, no. 5, pp. 1287–1297, May 2011.

[3] M. F. Mansour and H. T. Ahmed, "A turbo coding scheme for channels with synchronization errors," *IEEE Trans. Commun.*, vol. 60, no. 8, pp. 2091–2100, Aug. 2012.

[4] J. A. Briffa, V. Buttigieg, and S. Wesemeyer, "Time-varying block codes for synchronization errors: MAP decoder and practical issues," *IET Journal of Engineering*, Jun. 30th 2014.

[5] J. A. Briffa, "Graphics processing unit implementation and optimization of a flexible maximum a-posteriori decoder for synchronisation correction," *IET Journal of Engineering*, Jun. 11th 2014.

Department of Communications & Computer Engineering, Faculty of ICT, University of Malta, Msida MSD 2080, Malta
johann.briffa@um.edu.mt

Some two-torsion issues for curves in characteristic two

Wouter Castryck

Universiteit Gent

(Joint work with Marco Streng and Damiano Testa)

Consider a smooth plane curve of odd degree d over GF(2^r) with defining equation

$$\sum_{i+j+k=d} c_{ijk} X^i Y^j Z^k = 0$$

and suppose that $c_{ijk} = 0$ as soon as i, j, k are all odd. At first sight, the latter condition seems equation-specific, but an easy calculation shows that it is actually invariant under projective transformations. So something more geometric is going on, but what? In this talk we will provide an answer, generalize it to a broader class of curves, and relate it to two-torsion phenomena of the following kind: if one takes a random smooth plane curve over GF(2^r) of a given odd degree d, then the probability that its Jacobian has an even number of points converges to 1 as r and/or d tend to infinity (a fact first observed and proved by Cais, Ellenberg and Zureick-Brown [2]).

[1] B. Cais, J. Ellenberg, D. Zureick-Brown, *Random Dieudonné modules, random p-divisible groups, and random curves over finite fields*, Journal of the Institute of Mathematics of Jussieu **12**(3), pp. 651-676 (2013)
[2] W. Castryck, M. Streng, D. Testa, *Curves in characteristic 2 with non-trivial 2-torsion*, to appear in Advances in Mathematics of Communications

Universiteit Gent, Vakgroep Wiskunde, Krijgslaan 281, 9000 Gent (Belgium)
wouter.castryck@ugent.be

Fingerprinting codes and their limits

Gábor Fodor

Vrije Universiteit Brussel, Belgium

(Joint work with Adriaan Barri)

Fingerprinting is the task of identifying re-distributors of digital content. Given a set of N users, we want to generate a unique code X_i for each user so that under certain distortion assumptions, the probability of accusing an innocent user is lower than ϵ_1 and the probability of missing the guilty user(s) is lower than ϵ_2, with $0 \leq \epsilon_1, \epsilon_2 \leq 1$ being fixed constants.

We are particulary interested in collusion attacks, a form of attack when a set of users combine their codes in order to generate a new, forged one, subject to certain strict limitations, like the Boneh-Shaw marking assumption [1] or its relaxed version, suggested by Guth and Pfitzmann [2]. Given the maximum number of colluders to be c, we are then interested in generating fingerprinting codes that satisfy the error constraints for arbitrary $(c, \epsilon_1, \epsilon_2)$ value. This presentation will deal with optimal code lengths, capacity of such codes, alphabet sizes and different aspects of the collusion attack channel.

Vrije Universiteit Brussel, Boulevard de la Plaine 2, 1050 Ixelles, Belgium
gfodor@etro.vub.ac.be

References

[1] D. Boneh, M. Naor, *Traitor Tracing with Constant Size Ciphertext*, Proceedings of the 15th ACM conference on Computer and Communications Security (CCS), p 455-470, 2008.

[2] J. Guth and B. Pfitzmann, *Error- and collusion-secure fingerprinting for digital data*, Information Hiding (IH99) LNCS 1768, Springer-Verlag, Berlin, p 134-145, 2000.

About a class of Hadamard Propelinear Codes

E. Suárez-Canedo

Universitat Autònoma de Barcelona

(Joint work with J. Rifà)

This article aims to explore the algebraic structure of Hadamard propelinear codes, which are not abelian in general but they have good algebraic and combinatorial properties. Concretely, we construct a subclass of Hadamard propelinear codes which enlarges the Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.Several papers have been devoted to the relations between difference sets, t-designs, cocyclic-matrices and Hadamard groups, and we present a link between them and a class of Hadamard propelinear codes, which will be called full propelinear. Finally, as an exemplification, we go over Hadamard codes of length sixteen giving a propelinear structure for all of them.

Universitat Autónoma de Barcelona, Departament d'Enginyeria de la Informació i de les Comunicacions
josep.rifa@deic.uab.cat, emilio.suarez@deic.uab.cat

On some transitive combinatorial structures and codes constructed from the symplectic group $S(6,2)$

Andrea Švob

University of Rijeka, Croatia

(Joint work with Dean Crnković and Vedrana Mikulić Crnković)

The main topic of this talk will be the construction of transitive combinatorial structures from finite groups. The method will be applied on the construction of 2-designs and strongly regular graphs. The structures will be defined on the conjugacy classes of the maximal and second maximal subgroups under the action of the symplectic group $S(6,2)$. Furthermore, using this method linear codes invariant under the action of the group $S(6,2)$ as the codes of the constructed designs were constructed. In this talk, the constructed structures will be described.

University of Rijeka, Department of Mathematics, Radmile Matejcic 2, 51000 Rijeka, Croatia
asvob@math.uniri.hr