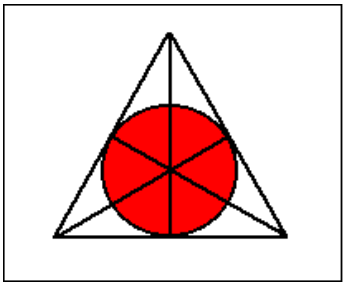


# JCCA-2014

## Japanese Conference on Combinatorics and its Applications 2014

**Tsukuba, Aug. 25 – Aug. 29, 2014**

## Invited Speakers

**Eiichi Bannai (Shanghai Jiao Tong University)**
**Genghua Fan (Fuzhou University)**
**James W. P. Hirschfeld (University of Sussex)**
**Ken-ichi Kawarabayashi (National Institute of Informatics)**
**Akira Saito (Nihon University)**
**Tran van Trung (Universität Duisburg-Essen)**
**Richard M. Wilson (California Institute of Technology)**
**Qing Xiang (University of Delaware)**

## Organizing Committee

**Ryoh Fuji-Hara (University of Tsukuba), Chair**
**Futaba Fujie (Nagoya University)**
**Masahiro Hachimori (University of Tsukuba)**
**Ying Miao (University of Tsukuba)**
**Yoshio Sano (University of Tsukuba)**
**Masanori Sawa (Kobe University)**

The map from The Tsukuba train station to The Tsukuba Center for Institutes


The Tsukuba Center for Institutes

The Tsukuba Center for Institutes was established in 1978 as a facility for common uses in the heart of Tsukuba Science City. Its purpose is to provide a place where researchers and other personnel meet together and exchange information and opinions, and to provide information on science and technology from all over the world to researchers in the city, thus promoting research exchange and enabling the best use of the opportunities offered by the concentration of research institutes and universities at Tsukuba. The facilities of the Center include an international conference hall, other conference rooms and exhibition rooms.

# JCCA2014 Time Table

| | Aug. 25 (Mon) | Aug. 26 (Tue) | Aug. 27 (Wed) | Aug. 28 (Thu) | Aug. 29 (Fri) |
|---|---|---|---|---|---|
| 9:00 | | Registration | Registration | Registration | Registration |
| 9:30 | Registration and Coffee Time | Invited Talk 3<br>E. Bannai | Invited Talk 5<br>A. Saito | Invited Talk 6<br>G. Fan | Invited Talk 8<br>T. van Trung |
| 10:30 | | Coffeee Break | Coffeee Break | Coffeee Break | Coffeee Break |
| 10:45 | Welcome Address | | | | |
| 11:00 | Invited Talk 1<br>J. W. P. Hirschfeld | F. Szollosi | | A. Schaefer | W. Moczurad |
| | | M. Hirao | | I. Sato | M. Homma |
| | | G. Greaves | | T. Adachi | S. Chisaki |
| | | K. Ozeki | | T. Rahim | K. Takeuchi |
| 12:00 | | | | | Closing Remark |
| 13:00 | Lunch | Lunch | **Excursion including Lunch** | Lunch | |
| 14:00 | Invited Talk 2<br>Q. Xiang | Invited Talk 4<br>R. M. Wilson | | Invited Talk 7<br>K. Kawarabayashi | |
| 15:00 | Drink Service | Drink Service | | Drink Service | |
| 15:30 | A. L. Gavrilyuk | T. Wong | | U. Schauz | |
| | K. Yamada | T. Okazaki | | P. Selin | |
| | X. Lu | K. Kumegawa | | M. Hachimori | |
| | H. Fu | H. Kanda | | S. M. Hosamani | |
| 16:30 | | | | | |
| | 17:00 – 21:00<br>**Welcome Party** | | 19:00 – 21:00<br>**Banquet** | | |

# Program

# Day 1 (August 25, 2014)

9:00-10:45 Registration and Coffee Time

10:45-11:00 Welcome Address

11:00-12:00 **James W. P. Hirschfeld** (Invited Talk 1)
*Open Problems in Finite Projective Spaces*

12:00-14:00 Lunch

14:00-15:00 **Qing Xiang** (Invited Talk 2)
*Cameron-Liebler line classes with parameter* $x = \frac{q^2-1}{2}$

15:00-15:30 Drink Service

15:30-15:45 **Alexander L. Gavrilyuk**
*A modular equality for Cameron-Liebler line classes*

15:45-16:00 **Kohei Yamada**
*Group divisible designs on the complement of a Baer subplane*

16:00-16:15 **Xiao-Nan Lu**
*Affine-invariant simple two-fold Steiner quadruple systems*

16:15-16:30 **Hung-Lin Fu**
*Optimal equi-difference conflict-avoiding codes of prime length and weight 4*

17:00-21:00 Welcome Party

# Day 2 (August 26, 2014)

9:00-9:30 (Registration)

9:30-10:30 **Eiichi Bannai** (Invited Talk 3)
*Tight relative t-designs in certain association schemes*

10:30-11:00 Coffee Break

11:00-11:15 **Ferenc Szöllősi**
*Families of complex Hadamard matrices in the Bose–Mesner algebra of association schemes*

11:15-11:30 **Masatake Hirao**
*Some remarks on operator-type cubature formulas*

11:30-11:45 **Gary Greaves**
*Graphs with precisely three distinct eigenvalues*

11:45-12:00 **Kenta Ozeki**
*Decomposition of cubic graphs*

12:00-14:00 Lunch

14:00-15:00 **Richard M. Wilson** (Invited Talk 4)
*Improving bounds on set-systems and codes with restricted distances*

15:00-15:30 Drink Service

15:30-15:45 **Tsai-Lien Wong**
*Hankel Determinants of Sums of Consecutive Schröder Numbers*

15:45-16:00 **Tsukasa Okazaki**
*Construction of new codes over the field of* 9 *elements*

16:00-16:15 **Kazuki Kumegawa**
*Nonexistence of some Griesmer codes of dimension 4 over finite fields*

16:15-16:30 **Hitoshi Kanda**
*New extension theorems for linear codes over finite fields*

# Day 3 (August 27, 2014)

| | |
|---|---|
| 9:00-9:30 | (Registration) |
| 9:30-10:30 | **Akira Saito** (Invited Talk 5)<br>*Precoloring Extension Involving Pairs of Vertices of Small Distance* |
| 10:30-11:00 | Coffee Break |
| 11:00-18:00 | Excursion including Lunch |
| 19:00-21:00 | Banquet |

# Day 4 (August 28, 2014)

9:00-9:30 (Registration)

9:30-10:30 **Genhua Fan** (Invited Talk 6)
*Integer 4-flows and Short Cycle Covers*

10:30-11:00 Coffee Break

11:00-11:15 **Artur Schaefer**
*Latin Squares Become Graph Endomorphisms*

11:15-11:30 **Iwao Sato**
*The weighted complexity of the line digraph of a digraph*

11:30-11:45 **Tomoko Adachi**
*Cyclic constructions for cluttered orderings of the complete bipartite graph*

11:45-12:00 **Tariq Rahim**

12:00-14:00 Lunch

14:00-15:00 **Ken-ichi Kawarabayashi** (Invited Talk 7)
*Towards the graph minor theorem for directed graphs*

15:00-15:30 Drink Service

15:30-15:45 **Uwe Schauz**
*The List Coloring Conjecture for Complete Graphs*

15:45-16:00 **Pavel Selin**
*On Constraints in Networks with Fixed Degrees of Nodes*

16:00-16:15 **Masahiro Hachimori**
*Hereditary-shellable simplicial complexes and extendability of shellings*

16:15-16:30 **Sunilkumar M. Hosamani**
*DERD-Domination in Graphs*

# Day 5 (August 29, 2014)

9:00-9:30 (Registration)

9:30-10:30 **Tran van Trung** (Invited Talk 8)
*Group factorization and cryptography*

10:30-11:00 Coffee Break

11:00-11:15 **Włodzimierz Moczurad**
*Defect property of $\mathbb{Z}^2$ figure codes*

11:15-11:30 **Masaaki Homma**
*Numbers of lines on surfaces in the projective* 3*-space over finite fields*

11:30-11:45 **Shoko Chisaki**
*The existence of perfect $(p, 3, f, \rho)$-difference systems of sets with $p = 3f + 1, 4f + 1$*

11:45-12:00 **Kota Takeuchi**
*Generalized VC dimension and Sauer lemma for classes of subsets of product sets*

12:00-12:15 Closing Remark

# Abstracts

# Day 1 (August 25, 2014)

# Open Problems in Finite Projective Spaces

J.W.P. Hirschfeld
Department of Mathematics, University of Sussex
Brighton BN1 9QH, United Kingdom
jwph@sussex.ac.uk

(joint work with J.A. Thas)

## 1 Background

Apart from being an interesting and exciting area in combinatorics with beautiful results, finite projective spaces or Galois geometries have many applications to coding theory, algebraic geometry, design theory, graph theory, cryptology and group theory. As an example, the theory of linear maximum distance separable codes (MDS codes) is equivalent to the theory of arcs in $\mathrm{PG}(n, q)$.

Finite projective geometry is essential for finite algebraic geometry, and finite algebraic curves are used to construct interesting classes of codes, the Goppa codes, now also known as algebraic geometry codes. Many interesting designs and graphs are constructed from finite Hermitian varieties, finite quadrics, finite Grassmannians and finite normal rational curves. Further, most such structures have an interesting group; the classical groups and other finite simple groups appear in this way.

For more history, see the preface of [3]. For more details, see [3], [2], [5], [4]. For a collection of current topics of interest, see [1] and [6].

## 2 Topics

(1) $k$-arcs
(2) $k$-caps
(3) Hermitian curves and unitals
(4) Maximal arcs
(5) Blocking sets
(6) Flocks
(7) Ovoids and spreads
(8) $m$-systems and BLT-sets
(9) Algebraic curves over a finite field

## 3 The plane $\mathrm{PG}(2, q)$

**Definition 3.1.** (1) A *$k$-arc* in $\mathrm{PG}(2, q)$ is a set of $k$ points, with $k \geq 3$, such that no 3 of its points lie on a line.

(2) An arc $\mathcal{K}$ is *complete* it it is not properly contained in a larger arc.
(3) The integer $m(2,q)$ is the size of the largest arc in the plane, and $m'(2,q)$ is the size of the second-largest complete arc.
(4) A $(k,r)$-*arc* is a set of $k$ points such that no $r+1$ of its points lie on a line, but with some line containing $r$ of its points.
(5) The integer $m_r(2,q)$ is the size of the largest $(k,r)$-arc in the plane.
(6) The integer $t_r(2,q)$ is the size of the smallest complete $(k,r)$-arc in the plane.

**Problem 3.2.** I. What is the value of $m'(2,q)$ and why is it not known for all $q$?
II. What is the value of $m_r(2,q)$ for $r>2$?
III. What is the value of $t_r(2,q)$ for $r>2$?
IV. Classify $m(2,q)$-arcs for $q$ even.

# 4 The space $\mathrm{PG}(3,q)$

**Definition 4.1.** (1) In $\mathrm{PG}(3,q)$, a set $\mathcal{K}$ of $k$ points no three of which are collinear is a $k$-*cap*.
(2) A $k$-cap is *complete* if it is not contained in a $(k+1)$-cap.
(3) The integer $m(3,q)$ is the size of the largest cap in $\mathrm{PG}(3,q)$.

**Problem 4.2.** I. Classify $m(3,q)$-caps for $q$ even.
II. Find $m'(3,q)$, the size of the second-largest, complete cap in $\mathrm{PG}(3,q)$.

# 5 The space $\mathrm{PG}(n,q),\ n>3$

**Definition 5.1.** (1) In $\mathrm{PG}(n,q)$, a set $\mathcal{K}$ of $k$ points no three of which are collinear is a $k$-*cap*.
(2) A $k$-*arc* in $\mathrm{PG}(n,q)$ is a set of $k$ points, with $k \geq n+1 \geq 3$, such that no $n+1$ of its points lie in a hyperplane.

**Problem 5.2.** I. Find $m_2(n,q)$, the size of the largest $k$-cap.
II. Show, for $q>n+1$, that the size $m(n,q)$ of the largest arc is $q+1$ or $q+2$.

# 6 Hermitian curves and unitals

**Definition 6.1.** (1) In $\mathrm{PG}(2,q)$, with $q$ square, any non-singular Hermitian curve is projectively equivalent to the algebraic curve $\mathcal{H}$ with equation

$$X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} = 0.$$

(2) The rational points of $\mathcal{H}$ form a *Hermitian arc*; that is, it consists of $q\sqrt{q}+1$ points such that any line meets it in 1 or $\sqrt{q}+1$ points.

**Problem 6.2.** I. Find all non-equivalent Hermitian arcs.

# 7 Finite classical polar spaces

There are five types of finite *classical polar spaces* $\mathcal{S} = (\mathcal{P}, \mathcal{B})$.

(1) $\mathcal{W}_n(q)$: the elements of $\mathcal{P}$ are the points of $\mathrm{PG}(n, q)$, with $n$ odd and $n \geq 3$; the elements of $\mathcal{B}$ are the subspaces of the self-polar $\frac{1}{2}(n-1)$-dimensional spaces of a symplectic polarity of $\mathrm{PG}(n, q)$; the rank $r = \frac{1}{2}(n+1)$.

(2) $\mathcal{P}(2n, q)$: the elements of $\mathcal{P}$ are the points of a non-singular quadric $\mathcal{P}_{2n}$ of $\mathrm{PG}(2n, q)$, with $n \geq 2$; the elements of $\mathcal{B}$ are the subspaces of the $(n-1)$-dimensional spaces on $\mathcal{P}_{2n}$; the rank $r = n$.

(3) $\mathcal{H}(2n+1, q)$: the elements of $\mathcal{P}$ are the points of a non-singular hyperbolic quadric $\mathcal{H}_{2n+1}$ of $\mathrm{PG}(2n+1, q)$, $n \geq 1$; the elements of $\mathcal{B}$ are the subspaces of the $n$-dimensional spaces on $\mathcal{H}_{2n+1}$; the rank $r = n+1$.

(4) $\mathcal{E}(2n+1, q)$: the elements of $\mathcal{P}$ are the points of a non-singular elliptic quadric $\mathcal{E}_{2n+1}$ of $\mathrm{PG}(2n+1, q)$, $n \geq 2$; the elements of $\mathcal{B}$ are the subspaces of the $(n-1)$-dimensional spaces on $\mathcal{E}_{2n+1}$; the rank $r = n$.

(5) $\mathcal{U}(n, q^2)$: the elements of $\mathcal{P}$ are the points of a non-singular Hermitian variety $\mathcal{U}_n$ of $\mathrm{PG}(n, q^2)$, $n \geq 3$; when $n$ is odd, the elements of $\mathcal{B}$ are the subspaces of the $\frac{1}{2}(n-1)$-dimensional spaces on $\mathcal{U}_n$ and the rank $r = \frac{1}{2}(n+1)$; when $n$ is even, the elements of $\mathcal{B}$ are the subspaces of the $(\frac{1}{2}n-1)$-dimensional spaces on $\mathcal{U}_n$ and the rank $r = \frac{1}{2}n$.

**Definition 7.1.** For a polar space $\mathcal{S}$ of rank $r$, the subspaces of dimension $r-1$ are the *generators* of $\mathcal{S}$.

**Definition 7.2.** Let $\mathcal{S}$ be a finite classical polar space of rank $r \geq 2$.

(1) An *ovoid* $\mathcal{O}$ of $\mathcal{S}$ is a point set that meets every generator in exactly one point.

(2) A *spread* $\mathcal{T}$ of $\mathcal{S}$ is a set of generators that partitions the point set of $\mathcal{S}$.

**Problem 7.3.** I. Establish the existence or non-existence of spreads for every polar space.
II. Establish the existence or non-existence of ovoids for every polar space.

# 8 Algebraic curves over finite fields

Let $N_1$ denote the number of points with coordinates in the ground field $\mathbf{F}_q$ of a curve $\mathcal{C}$ defined over $\mathbf{F}_q$.

**Theorem 8.1.** (i) *A non-singular plane curve $\mathcal{C}$ defined over $\mathbf{F}_q$ and of degree $d$ has genus $g = \frac{1}{2}(d-1)(d-2)$.*

(ii) *The maximum number of rational points on a curve $\mathcal{C}$ defined over $\mathbf{F}_q$ and of genus $g$ is*

$$N_q(g) \leq S_q = q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

**Problem 8.2.** I. Although the value of $N_q(3)$ is known for all $q < 100$, establish the value for every $q$.

# References

[1] J. De Beule and L. Storme (eds.), *Current Research Topics in Galois Geometries*, Nova Science Publishers, 2012.

[2] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, x + 316 pp., 1985.

[3] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Oxford University Press, 1998.

[4] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, xxii + 696 pp., 2008.

[5] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, xiii + 407 pp., 1991.

[6] J.W.P. Hirschfeld and J.A. Thas, Open problems in finite projective spaces, *Finite Fields Appl.*, submitted.

# Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$

Qing Xiang
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, USA

Joint Work with Tao Feng and Koji Momihara

Cameron-Liebler line classes are sets of lines in $\mathrm{PG}(3,q)$ having many interesting combinatorial properties. These line classes were first introduced by Cameron and Liebler [2] in their study of collineation groups of $\mathrm{PG}(3,q)$ having the same number of orbits on points and lines of $\mathrm{PG}(3,q)$. In the last few years, Cameron-Liebler line classes have received considerable attention from researchers in both finite geometry and algebraic combinatorics; see, for example, [3, 10, 11, 14, 6, 7]. In [2], the authors gave several equivalent conditions for a set of lines of $\mathrm{PG}(3,q)$ to be a Cameron-Liebler line class; Penttila [12] gave a few more of such characterizations. We will use one of these characterizations as the definition of Cameron-Liebler line class. Let $\mathcal{L}$ be a set of lines of $\mathrm{PG}(3,q)$ with $|\mathcal{L}| = x(q^2+q+1)$, $x$ a nonnegative integer. We say that $\mathcal{L}$ is a *Cameron-Liebler line class with parameter* $x$ if every spread of $\mathrm{PG}(3,q)$ contains $x$ lines of $\mathcal{L}$. Clearly the complement of a Cameron-Liebler line class with parameter $x$ in the set of all lines of $\mathrm{PG}(3,q)$ is a Cameron-Liebler line class with parameter $q^2+1-x$. So without loss of generality we may assume that $x \leq \frac{q^2+1}{2}$ when discussing Cameron-Liebler line classes of parameter $x$.

Let $(P,\pi)$ be any non-incident point-plane pair of $\mathrm{PG}(3,q)$. Following [12], we define $star(P)$ to be the set of all lines through $P$, and $line(\pi)$ to be the set of all lines contained in the plane $\pi$. We have the following trivial examples:

1. The empty set gives a Cameron-Liebler line class with parameter $x = 0$;
2. Each of $star(P)$ and $line(\pi)$ gives a Cameron-Liebler line classe with parameter $x = 1$;
3. $star(P) \cup line(\pi)$ gives a Cameron-Liebler line class with parameter $x = 2$.

It was once conjectured that the above trivial examples and their complements are all of the Cameron-Liebler line classes. The first counterexample to this conjecture was given by Drudge [5] in $\mathrm{PG}(3,3)$, and it has parameter $x = 5$. Later Bruen and Drudge [1] generalized Drudge's example into an infinite family with parameter $x = \frac{q^2+1}{2}$ for all odd $q$. This represents the only known infinite family of nontrivial Cameron-Liebler line classes before our work. Govaerts and Penttila [8] gave a sporadic example with parameter $x = 7$ in $\mathrm{PG}(3,4)$. Recent work by Rodgers suggests that there are probably more infinite families of Cameron-Liebler line classes awaiting to be discovered. In [14], Rodgers obtained new Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$ for $q \equiv 5$ or $9 \pmod{12}$ and $q < 200$. In his thesis [15], Rodgers also reported new examples with

parameters $x = \frac{(q+1)^2}{3}$ for $q \equiv 2 \pmod 3$ and $q < 150$ as joint work with his collaborators. These examples motivated us to find new general constructions of Cameron-Liebler line classes.

On the nonexistence side, Govaerts and Storme [9] first showed that there are no Cameron-Liebler line classes in $\mathrm{PG}(3, q)$ with parameter $2 < x \leq q$ when $q$ is prime. Then De Beule, Hallez and Storme [3] excluded parameters $2 < x \leq q/2$ for all values $q$. Next Metsch [10] proved the non-existence of Cameron-Liebler line classes with parameter $2 < x \leq q$, and subsequently improved this result by showing the nonexistence of Cameron-Liebler line classes with parameter $2 < x < q\sqrt[3]{\frac{q}{2}} - \frac{2}{3}q$ [11]. The latter result represents the best asymptotic nonexistence result to date. It seems reasonable to believe that for any fixed $0 < \epsilon < 1$ and constant $c > 0$ there are no Cameron-Liebler line classes with $2 < x < cq^{2-\epsilon}$ for sufficiently large $q$. We refer to [11] for a comprehensive survey of the known nonexistence results. Very recently, Gavrilyuk and Metsch [7] proved a congruence relation for Cameron-Liebler line classes in $\mathrm{PG}(3, q)$, which can be used to rule out roughly at least one half of all possible parameters $x$.

We will talk about a recent construction of a new infinite family of Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$ for $q \equiv 5$ or $9 \pmod{12}$. This family of Cameron-Liebler line classes generalizes the examples found by Rodgers in [14] through a computer search, and represents the second infinite family of Cameron-Liebler line classes. Furthermore, in the case where $q$ is an even power of 3, we construct the first infinite family of affine two-intersection sets. The first step of our construction follows the same idea as in [14]. That is, we prescribe an automorphism group for the Cameron-Liebler line classes that we intend to construct; as a consequence, the Cameron-Liebler line classes will be unions of orbits of the prescribed automorphism group on the set of lines of $\mathrm{PG}(3, q)$. The main difficulty with this approach is how to choose orbits properly so that their union forms a Cameron-Liebler line class. We overcome this difficulty by giving an explicit choice of orbits that works for our purpose. The proofs are algebraic, and involve the use of Gauss sums and the Stickelberger theorem on the prime ideal factorization of Gauss sums.

We should remark that De Beule, Demeyer, Metsch and Rodgers [4] also independently obtained the same result as ours on Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$ at almost the same time. The approaches for proving the main result are comparable but different enough to justify that we write papers separately; our approach is more algebraic while the approach taken by De Beule, Demeyer, Metsch and Rodgers is more geometric.

# References

[1] A. A. Bruen, K. Drudge, The construction of Cameron-Liebler line classes in $\mathrm{PG}(3, q)$, *Finite Fields Appl.*, **5** (1999), 35–45.

[2] P. J. Cameron, R.A. Liebler, Tactical decompositions and orbits of projective groups, *Linear Algebra Appl.*, **46** (1982), 91–102.

[3] J. De Beule, A. Hallez, and L. Storme, A non-existence result on Cameron-Liebler line classes, *J. Combin. Designs*, **16** (2008), 342–349.

[4] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $\mathcal{Q}^+(5,q)$, preprint.

[5] K. Drudge, On a conjecture of Cameron and Liebler, *Europ. J. Combin.*, **20** (1999), 263–269.

[6] A. L. Gavrilyuk, I. Y. Mogilnykh, A note on Cameron-Liebler line classes in PG$(n,4)$, `ArXiv: 1205.2351`.

[7] A. L. Gavrilyyuk, K. Metsch, A modular equality for Cameron-Liebler line classes, to appear in *J. Combin. Theory* (A).

[8] P. Govaerts, T. Penttila, Cameron-Liebler line classes in PG$(3,4)$, *Bull. Belg. Math. Soc. Simon Stevin*, **12** (2005), 793–804.

[9] P. Govaerts, L. Storme, On Cameron-Liebler line classes, *Adv. Geom.*, **4** (2004), 279–286.

[10] K. Metsch, The non-existence of Cameron-Liebler line classes with parameter $2 < x \leq q$, *Bull. Lond. Math. Soc.*, **42** (2010), 991–996.

[11] K. Metsch, An improved bound on the existence of Cameron-Liebler line classes, *J. Combin. Theory, Ser. A*, **121** (2014), 89–93.

[12] T. Penttila, Cameron-Liebler line classes in $PG(3,q)$, *Geom. Dedicata*, **37** (1991), 245–252.

[13] T. Penttila, G.F. Royle, Sets of type $(m,n)$ in the affine and projective planes of order nine, *Des. Codes Cryptogr.*, **6** (1995), 229–245.

[14] M. Rodgers, Cameron-Liebler line classes, *Des. Codes Cryptogr.*, **68** (2013), 33–37.

[15] M. Rodgers, *On some new examples of Cameron-Liebler line classes*, PhD thesis, University of Colorado, 2012.

# A modular equality for Cameron-Liebler line classes

*Alexander L. Gavrilyuk and Klaus Metsch

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai, Japan
and
N.N. Krasovsky Institute of Mathematics and Mechanics UB RAS, Ekaterinburg, Russia

Justus-Liebig-Universität, Mathematisches Institut, Gießen, Germany
and
Department of Pure Mathematics and Computer Algebra, Ghent University, Belgium

We prove that a Cameron-Liebler line class $\mathcal{L}$ in $PG(3,q)$ with parameter $x$ has the property that $\binom{x}{2}+n(n-x)\equiv 0 \pmod{q+1}$ for the number $n$ of lines of $\mathcal{L}$ in any plane of $PG(3,q)$. This property rules out roughly at least one half of all possible parameters $x$. As an application of our method, we determine the spectrum of parameters of Cameron-Liebler line classes of $PG(3,5)$. This includes the construction of a Cameron-Liebler line class with parameter 10 in $PG(3,5)$ and a proof that it is unique up to projectivities and dualities.

# Group divisible designs on the complement of a Baer subplane

Kohei Yamada
yamada.kohei@b.mbox.nagoya-u.ac.jp

Let $\mathcal{P}$ be a finite desarguesian projective plane of order $q^2$, where $q$ is a prime power. A Baer subplane of $\mathcal{P}$ is a subplane isomorphic to a projective plane of order $q$. If $\mathcal{P}'$ is a Baer subplane of $\mathcal{P}$, then the lines of $\mathcal{P}'$ give a partition of $\mathcal{P} \setminus \mathcal{P}'$ into $q^2+q+1$ subsets of $q(q-1)$ points. With this partition, many group divisible designs have been constructed on the complement of a Baer subplane. In 1968, Dembowski [1] first introduced symmetric group divisible designs (called elliptic semiplanes) on $\mathcal{P} \setminus \mathcal{P}'$ using the lines not contained in $\mathcal{P}'$, and Fuji-Hara and Kamimura [2] gave a construction of other group divisible designs (more precisely, transversal designs) on $\mathcal{P} \setminus \mathcal{P}'$ using Baer subplanes disjoint from $\mathcal{P}'$.

In this talk, we show some properties of the subgroup of $\mathrm{PGL}(3, q^2)$ fixing the set of points of $\mathcal{P}'$, we thereby provide other constructions of some group divisible designs on $\mathcal{P} \setminus \mathcal{P}'$ which include improvement of Fuji-Hara and Kamimura's designs. This talk is based on a joint work with Nobuko Miyamoto.

## References

[1] P. Dembowski, Finite Geometries. Springer, 1968.

[2] R. Fuji-Hara and S. Kamimura, Orthogonal arrays from Baer subplanes, Utilitas Math 43(1993), 65-70.

# Affine-invariant simple two-fold Steiner quadruple systems

Xiao-Nan Lu
Nagoya University, Japan

A $\lambda$-fold Steiner quadruple system (SQS) of order $v$, denoted by $S_\lambda(3,4,v)$, is a pair $(V,\mathcal{B})$, where $V$ is a finite set of $v$ points, and $\mathcal{B}$ is a collection of 4-subsets of $V$, called quadruples, such that each 3-subset (triple) of $V$ is contained in exactly $\lambda$ blocks in $\mathcal{B}$. Let $G$ be a permutation group on $V$. If $G$ leaves $\mathcal{B}$ invariant, then $G$ is called an automorphism group of $S_\lambda(3,4,v)$. In particular, $(V,\mathcal{B})$ is said to be affine-invariant if it admits the affine group of $V$. Precisely speaking, when $V$ is identified with $\mathbb{Z}_v$, the affine group is $\mathbb{Z}_v \rtimes \mathrm{Aut}(\mathbb{Z}_v) \cong \mathbb{Z}_v \rtimes \mathbb{Z}_v^\times$.

In this talk, we consider the constructions of affine-invariant $S_2(3,4,v)$, where $v$ is a prime $p$ or a prime power $p^m$, for $p \equiv 5 \pmod{12}$. We also show that the constructions guarantee that no two blocks are the same, that is, the affine-invariant $S_2(3,4,v)$ is simple.

# Optimal equi-difference conflict-avoiding codes of prime length and weight 4

Hung-Lin Fu
Department of Applied Mathematics
National Chiao Tung University
Hsin Chu, Taiwan 30010

A conflict-avoiding code (CAC) $\mathcal{C}$ of length $n$ and weight $k$ is a collection of $k$-subsets of $\mathbb{Z}_n$ such that $\Delta(x) \cap \Delta(y) = \emptyset$ for any $x, y \in \mathcal{C}$ and $x \neq y$, where $\Delta(x) = \{a - b : a, b \in x, a \neq b\}$. Let CAC$(n, k)$ denote the class of all CACs of length $n$ and weight $k$. A CAC $\mathcal{C} \in$ CAC$(n, k)$ is said to be equi-difference if any codeword $x \in \mathcal{C}$ has the form $\{0, i, 2i, \ldots, (k-1)i\}$. A CAC with maximum size is called optimal. In this paper we propose a graphical characterization of an equi-difference CAC$(p, 4)$ where $p$ is a prime, and then provide an infinite number of optimal equi-difference CACs for weight four by finding the independence number of a circulant graph.

# Day 2 (August 26, 2014)

# Tight relative $t$-designs in certain association schemes

Eiichi Bannai
Shanghai Jiao Tong University

Roughly speaking, the purpose of design theory is to find good subsets $Y$ which approximate the given space (or a set) $M$. If $M$ is the unit sphere $S^{n-1}$ in $\mathbb{R}^n$, then $Y$ are spherical designs, and if $M$ is the set $\binom{V}{k}$, i.e. the set of all $k$-element subsets of a set $V$ with $|V| = v$, then $Y$ are combinatorial $t$-designs. First we will discuss the definitions of the following $t$-designs:
(i) spherical $t$-designs (Delsarte-Goethas-Seidel [7](1977)),
(ii) combinatorial $t$-designs (Hughs (1965) or essentially far older. See also Delsarte [5] (1973). )
(iii) weighted spherical $t$-designs,
(iv) weighted combinatorial $t$-designs,
(v) Euclidean $t$-designs (on $p$ shells) (Neumaier-Seidel [9] (1988)),
(vi) relative $t$-designs (on $p$ shells) on the binary Hamming association scheme $H(n, 2)$. (The concept is defined for any Q-polynomial association scheme (Delsarte [6] (1977).)

Note that the concept in (iii) is a generalization of (i), and (v) is a generalization of (iii).
Also, the concept in (vi) is a generalization of (ii), and (vi) is a generalization of (iv).
Moreover, there is a close analogy between the two series of generalizations of the concepts:
(i) $\Rightarrow$ (iii) $\Rightarrow$ (v), and
(ii) $\Rightarrow$ (iv) $\Rightarrow$ (vi).

For each of $t$-designs $Y$ in the above definitions from (i) to (vi), we discuss Fisher type lower bound for the size $|Y|$ of $t$-design $Y$, and we call $Y$ a tight $t$-design, if $|Y|$ attains the lower bound in each of the above Fisher type lower bound.

We review the classification problems of tight $t$-designs in (i) and (ii). We remark that the case of (iii) and (iv) are reduced to (i) and (ii), respectively.
Then we review the classification problem of tight Euclidean $t$-designs in (v). Many results are obtained so far mostly only for the cases of $p = 2$. The interesting facts are that for Euclidean $t$-design $Y$, the weight function $w$ is constant for each shell, and that if $p = 2$, $Y$ has naturally the structure of a coherent configuration. Then these facts are used to study the classification problems of tight Euclidean $t$-designs on two shells.

Historically, the concept of relative $t$-designs (vi) is due to Delsarte [6] (1977), and this concept is older than the concept of Euclidean $t$-designs which was later defined by Neumaier-Seidel [9] (1988) and Delsarte-Seidel [8](1989). In a sense it seems that the concept of relative $t$-designs in association schemes predicted the concept of Euclidean $t$-designs. It seems that Euclidean $t$-designs (and in particular tight Euclidean $t$-designs)

were studied extensively in the last ten years, and the systematic study of relative $t$-designs (in particular tight relative $t$-designs) was just started very recently, in a sense modeling the study of Euclidean $t$-designs. The purpose of this talk is to explain how we can study tight relative $t$-designs in certain Q-polynomial association schemes, modeling the study of tight Euclidean $t$-designs. Our obtained results are so far very partial, compared with the study of Euclidean $t$-designs, namely we have studied so far mostly only for the case $t = 2$ and $p = 2$. We explain our main results in [3] for the binary association schemes $H(n, 2)$ and in [11] for Johnson association schemes $J(v, k)$. In the last part of the talk, I will discuss some very specific examples of such tight relative 2-designs on two shells in $J(v, k)$, and this topic has many interesting connections with other concepts.

Although our study on tight relative $t$-designs are so far very limited, I would like to emphasize that there are still rich theories in the study of tight relative 2-designs on two shells, and that these results should be interesting for the guide of future research. The purpose of this talk is to convince the audience that the time is ripe in starting the systematic study of tight relative $t$-designs in Q-polynomial association schemes.

This talk is based on the joint work with many authors, including Etsuko Bannai, Yan Zhu, Sho Suda, Hajime Tanaka and others. Details will be available in the following papers.

# References

[1] Ei. Bannai and Et. Bannai, *A survey on spherical designs and algebraic combinatorics on spheres*, European J. Combin., **30** (2009), 1392–1425.

[2] Ei. Bannai and Et. Bannai, *Remarks on the concepts of $t$-designs*, J. Appl Math Comput. 40 no. 1–2,(2012), 195–207.

[3] Ei. Bannai, Et. Bannai and H. Bannai, *On the existence of tight relative* 2*-designs on binary Hamming association schemes*. Discrete Mathematics 314 (2014) 17–37.

[4] Ei. Bannai, Et. Bannai, S. Suda and H. Tanaka, *On relative $t$-designs in polynomial association schemes*, arXiv:1303.7163

[5] P. Delsarte, *An algebraic approach to the association schemes of the coding theory*, Thesis, Universite Catholique de Louvain (1973) Philips Res. Repts Suppl. 10 (1973).

[6] P. Delsarte, Pairs of vectors in the space of an association scheme, Philips Res. Repts 32 (1977), 373–411.

[7] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Spherical codes and designs*, Geom. Dedicata 6 (1977), no. 3, 363–388.

[8] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Linear Algebra Appl. 114-115 (1989), 213–230.

[9] A. Neumaier and J. J. Seidel, *Discrete measures for spherical designs, eutactic stars and lattices*, Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988), 321-334.

[10] Z. Xiang, *A Fisher type inequality for weighted regular t-wise balanced designs*, Journal of Combinatorial Theory A, 119 (2012) 1523–1527.

[11] Y. Zhu, Ei. Bannai, and Et.Bannai, *Tight relative 2-designs on two shells in Johnson association schemes*, (in preparation).

# Families of complex Hadamard matrices in the Bose–Mesner algebra of association schemes

Ferenc Szöllősi
Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan

During a recent conference on algebraic combinatorics in Waterloo, Chris Godsil asked the existence of an infinite family of complex Hadamard matrices within the Bose–Mesner algebra of an association scheme. More precisely, he asked whether there exists some $d$-class association scheme with relation matrices $I, A_1, \ldots, A_d$ of size $n$, and continuous, non-constant scalar-vector functions $f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_d(\mathbf{x})$ mapping $\mathbf{x}$ into the complex unit circle for which the family of matrices with complex unit entries

$$H(\mathbf{x}) := I + \sum_{i=1}^{d} f_i(\mathbf{x}) A_i$$

satisfy $H(\mathbf{x})H(\mathbf{x})^* = nI$ for all $\mathbf{x}$.

By considering 3-class pseudo-cyclic association schemes we construct new, previously unknown parametric families of complex Hadamard matrices belonging to the Bose–Mesner algebra thus answering this question in the positive.

# Some remarks on operator-type cubature formulas

Masatake Hirao
e-mail: hirao@ist.aichi-pu.ac.jp
Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute, Aichi 480-1198

A *classical* cubature formula is an approximation of the definite integral of a multivariate function, expressed as a weighted average of the function values at finitely many specified points within the domain of integration. The term quadrature is often used to refer to one-dimensional cubature formulas. One of the most important problems in numerical analysis, combinatorics and related areas is to find a cubature formula with the smallest possible number of points for an rotationally symmetric integral. Many publications have been devoted to this subject. However, only a few such examples have been reported in high dimension.

Thus, in order to find smaller-points cubature formulas, we newly define a novel type of cubature formulas called *operator-type* cubature formulas. Historically, P. Turán in 1980 has initiated the question of the existence of a special class of operator-type quadrature formulas, motivated by a classical work of G.D. Birkhoff on Hermite interpolation. Moreover, e.g, Shamsiev [2] give a construction of Laplacian-type cubature formulas on the unit disk.

In this talk, we first present the concept of operator-type cubature formulas as a generalization of classical cubature formulas, and deal with the following three topics:

- A Stroud-type inequality for operator-type cubature. Especially a lower bound for Laplacian-type cubature is given.
- A series of Laplacian-type cubature attaining the bound.
- Generalizing Sobolev's Theorem on invariant polynomial-type cubature to operator-type cubature.

This is joint work with Takayuki Okuda (Hiroshima Univ., Japan) and Masanori Sawa (Kobe Univ., Japan).

# References

[1] Hirao, M., Okuda, T., Sawa, M.: Some remarks on cubature formulas with linear operators, preprint.

[2] Shamsiev, E.A.: Cubature formulas for a disk that are invariant with respect to groups of transformations of regular polyhedra into themselves. (Russian) Zh. Vychisl. Mat. Mat. Fiz. 46 (2006), 1211–1218; translation in Comput. Math. Math. Phys. 46 (2006), 1147–1154.

# Graphs with precisely three distinct eigenvalues

Ximing Cheng, *Gary Greaves, and Jack Koolen
Tohoku University, Japan

A connected regular graph with precisely three distinct eigenvalues is known as a strongly regular graph and such graphs have been the focus of much attention. In my talk I will relax the condition of regularity to consider non-regular graphs with precisely three distinct eigenvalues. I will present some new results concerning these graphs, focussing mainly on the biregular case.

# Decomposition of cubic graphs

Kenta Ozeki
National Institute of Informatics, Japan
JST, ERATO, Kawarabayashi Large Graph Project

It was conjectured by Hoffmann-Ostenhof that the edge set of every cubic graph can be decomposed into a spanning tree, a matching and a family of cycles. (Note that a matching and a set of cycles desired here are not necessarily spanning subgraphs.) We prove that the conjecture is true for 3-connected plane cubic graphs and 3-connected cubic graphs on the projective plane.

This is a joint work with Dong Ye (Middle Tennessee State University).

# Improving bounds on set-systems and codes with restricted distances

Richard M. Wilson
California Institute of Technology
Pasadena, CA 91125, USA

Some of the work I will describe is joint work with Tian Nie.

The following theorems are due to Ray-Chaudhuri and Wilson, and Ph. Delsarte, respectively. They date from circa 1970; various simple proofs are known.

**Theorem 1.** *Let $\mathcal{F}$ be a family of $k$-subsets of an $n$-set and assume for some integers $\alpha_1, \alpha_2, \ldots, \alpha_s$, between 0 and $k-1$, that*

$$|A \cap B| \in \{\alpha_1, \alpha_2, \ldots, \alpha_s\} \quad \textit{for all distinct} \quad A, B \in \mathcal{F}.$$

*Then*

$$|\mathcal{F}| \le \binom{n}{s}.$$

**Theorem 2.** *Let $\mathcal{C}$ be a $q$-ary code of length $k$ and assume for some integers $\alpha_1, \alpha_2, \ldots, \alpha_s$, between 1 and $k$, that*

$$\operatorname{dist}(\mathbf{a}, \mathbf{b}) \in \{\alpha_1, \alpha_2, \ldots, \alpha_s\} \quad \textit{for all distinct} \quad \mathbf{a}, \mathbf{b} \in \mathcal{C}.$$

(*Here* "dist" *is Hamming distance.*) *Then*

$$|\mathcal{C}| \le 1 + k(q-1) + \binom{k}{2}(q-1)^2 + \cdots + \binom{k}{s}(q-1)^s.$$

These inequalities arose because of connections to designs (tight $2s$-designs) and codes (perfect $s$-error-correcting codes). Instances of equality are extremely rare, and for most values of the $\alpha_i$'s and $k$ the inequalities are tend to be far from optimal.

Delsarte proposed a "linear programming bound" (LPB) for cliques in association schemes and showed that they imply Theorems 1 and 2. But linear programs must be run for each instance of the parameters and it is hard to extract general results. Still, the LPB can be shown to imply several inequalities, notably the Erdös-Ko-Rado Theorem.

A very different type of improvement to the upper bounds was introduced by P. Frankl and this writer in 1984.

**Theorem 3.** *Let integers $k$ and $\alpha_1, \alpha_2, \ldots, \alpha_s$, each between 1 and $k$, be given. Suppose there exists a rational polynomial $f(x)$ of degree $d$ and a prime $p$ so that*

$$f(\alpha_i) \equiv 0 \pmod{p} \quad \textit{for } i = 1, 2, \ldots, s, \quad \textit{but} \quad f(k) \not\equiv 0 \pmod{p}. \qquad (*)$$

*Then for a family $\mathcal{F}$ as in the statement of* Theorem 1,

$$|\mathcal{F}| \le \binom{n}{d}.$$

There is a similar theorem for codes, where the summation on the right need be extended only to $d+1$ terms rather than $s+1$. We focus on set-systems here, but there are analogous results for codes, and other structures.

The statement of Theorem 3 originally assumed an integer-valued polynomial $f(x)$. But the proof requires only that the values $f(\alpha_i)$ and $f(k)$ are integers (with the respective properties), and allowing $f(x)$ to be rational gives improved bounds.

As an example, when $s=2$ and $|A\cap B|\in\{\alpha,\beta\}$, Theorem 1 says $|\mathcal{F}|\le\binom{n}{2}$. But if there exists a prime divisor $p$ of $\beta-\alpha$ that does not divide $k-\alpha$, we may use the polynomial $f(x)=x-\alpha$ in Theorem 3 to deduce $|\mathcal{F}|\le n$. More generally, if the $p$-contribution to $k-\alpha$ is $p^e$ but the $p$-contribution to $\beta-\alpha$ is higher, we may consider the rational polynomial $f(x)=(x-\alpha)/p^e$. In summary,

$$|\mathcal{F}|\le n \quad \text{unless} \quad (\beta-\alpha)\mid(k-\alpha).$$

When $d$ is chosen to be the least integer for which $(*)$ holds for some rational polynomial f(x) and prime $p$, we may call the upper bound $\binom{n}{d}$ the "modular bound" (MB) for $|\mathcal{F}|$. It may be computed using algorithms for Hermite or Smith normal form to confirm the condition of Theorem 4 below, or show it does not hold.

**Theorem 4.** *Let integers $k$ and $\alpha_1,\alpha_2,\ldots,\alpha_s$ be given with $0\le\alpha_i<k$. Given a positive integer $d$, there exists a rational polynomial $f(x)$ of degree $d$ and a prime $p$ so that $(*)$ holds if and only if the vector $(1,k,k^2,\ldots,k^d)$ is NOT an integer linear combination of the rows*

$$(1,\alpha_i,\alpha_i^2,\ldots,\alpha_i^d),\quad i=1,2,\ldots,s.$$

The MB uses only the values of $k$ and the $\alpha_i$'s, and gives a bound valid for all $n$. There are numerous instances when the MB is better than the LPB, and many where the LPB is better. Examples will be given.

For large $k$, the MD is "almost always" $\le\binom{n}{s-1}$. We can make this precise in many instances. But as a small example, when $k=10$ and $s=3$, the MB for $|\mathcal{F}|$ is $\le\binom{n}{2}$ for all but eight of the 120 choices of $S=\{\alpha_1,\alpha_2,\alpha_3\}$. In those eight cases, when $\alpha_1,\alpha_2,\alpha_3$ are consecutive integers, there exist $cn^3$ 10-subsets with pairwise intersection cardinalities in $S$.

# Hankel Determinants of Sums of Consecutive Schröder Numbers

Sen-Peng Eu[1], *Tsai-Lien Wong[2], Pei-Lan Yen[2]
[1]Department of Applied Mathematics, National University of Kaohsiung, Kaohsiung 811, Taiwan
[2]Department of Applied Mathematics, National Sun Yat-sen University, Kaohsiung 804, Taiwan

For a real number $t$, let $r_\ell(t)$ be the total weight of all $t$-large Schröder paths of length $\ell$, and $s_\ell(t)$ be the total weight of all $t$-small Schröder paths of length $\ell$. For constants $\alpha, \beta$, in this talk we derive recurrence formulae for the determinants of the Hankel matrices $\det_{1\le i,j\le n}(\alpha r_{i+j-2}(t)+\beta r_{i+j-1}(t))$, $\det_{1\le i,j\le n}(\alpha r_{i+j-1}(t)+\beta r_{i+j}(t))$, $\det_{1\le i,j\le n}(\alpha s_{i+j-2}(t)+\beta s_{i+j-1}(t))$, and $\det_{1\le i,j\le n}(\alpha s_{i+j-1}(t)+\beta s_{i+j}(t))$ combinatorially via suitable lattice path models.

# Construction of new codes over the field of 9 elements

*Tsukasa Okazaki and Tatsuya Maruta
Department of Mathematics and Information Sciences,
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

An $[n, k, d]_q$ code $\mathcal{C}$ is a linear code of length $n$, dimension $k$ and minimum Hamming weight $d$ over the field of $q$ elements. A fundamental problem in coding theory is to find $n_q(k, d)$, the minimum length $n$ for which an $[n, k, d]_q$ code exists. The Griesmer bound gives a lower bound on $n_q(k, d)$ as $n_q(k, d) \geq g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$. The values of $n_q(k, d)$ are determined for all $d$ only for some small values of $q$ and $k$. For $q = 9$, $n_9(k, d)$ is known for all $d$ for $k \leq 3$. As for the case $k = 4$, the value of $n_9(4, d)$ is unknown for many integer $d$. It is already known that $n_9(4, d) = g_9(4, d)$ for $d \in \{1\text{-}7, 10\text{-}12, 19, 28\text{-}30, 64\text{-}72, 568\text{-}576, 640\text{-}801, 1054\text{-}1080\}$ and for all $d > 1215$, and that $n_9(4, d) = g_9(4, d) + 1$ for $\in \{8, 9, 17, 18, 25\text{-}27, 34, 61\text{-}63, 73\text{-}80, 141\text{-}144, 559\text{-}562, 593, 594, 602, 603, 622\text{-}639, 1194\text{-}1215\}$, see [1], [2], [5], [7]. We note that $n_9(4, d) \leq g_9(4, d) + 1$ for $577 \leq d \leq 621$ and $1135 \leq d \leq 1193$, see Lemma 3.5 in [2] and Corollary 11 in [2]. See also [3] and [3] for the nonexistence of Griesmer codes of dimension 4. We construct $[g_9(4, d), 4, d]_9$ codes for $d = 819$, 828, 837, 900, 909, 918, 981, 990, 999, and $[g_9(4, d) + 1, 4, d]_9$ codes for $d = 180$, 810, 846, 855, 864, 873, 882, 891, 927, 936, 945, 954, 963, 972, 1008, 1017, 1026, 1035, 1044, 1053, 1089, 1098, 1107, 1116, 1125, 1134. Our construction yields that $n_9(4, d) = g_9(4, d)$ for $d \in \{811\text{-}837, 892\text{-}918, 973\text{-}999\}$ and that $n_9(4, d) = g_9(4, d) + 1$ for $d \in \{964\text{-}972, 1045\text{-}1053, 1114\text{-}1116, 1122\text{-}1134\}$.

# References

[1] M. Grassl, Linear code bound, `http://www.codetables.de/`.

[2] Y. Kageyama and T. Maruta, On the construction of optimal codes over $\mathbb{F}_q$, preprint.

[3] R. Kanazawa, On the minimum length of linear codes of dimension 4, MSc Thesis, Osaka Prefecture Univ., 57pp, 2011.

[4] R. Kanazawa, T. Maruta, On optimal linear codes over $\mathbb{F}_8$, *Electron. J. Combin.*, **18**, #P34, 27pp, 2011.

[5] K. Kumegawa and T. Maruta, Nonexistence of some Griesmer codes of dimension 4 over $\mathbb{F}_q$, preprint.

[6] T. Maruta, On the minimum length of $q$-ary linear codes of dimension four, *Discrete Math.* **208/209**, 427–435, 1999.

[7] T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing*, **7**, 73–80, 2013.

# Nonexistence of some Griesmer codes of dimension 4 over finite fields

*Kazuki Kumegawa and Tatsuya Maruta
Department of Mathematics and Information Sciences,
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

An $[n,k,d]_q$ code $\mathcal{C}$ is a linear code of length $n$, dimension $k$ and minimum Hamming weight $d$ over the field of $q$ elements. A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length $n$ for which an $[n,k,d]_q$ code exists. The Griesmer bound gives a lower bound on $n_q(k,d)$ as $n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$. An $[n,k,d]_q$ code is called *Griesmer* if $n = g_q(k,d)$. The values of $n_q(k,d)$ are determined for all $d$ only for some small values of $q$ and $k$. For $k = 4$, $n_q(4,d)$ is known for all $d$ only for $q = 2,3,4$. It is known that $n_q(4,d) \geq g_q(4,d) + 1$ for $q^3/2 - q^2 - q + 1 \leq d \leq q^3/2 - q^2$ for even $q \geq 4$ [2] and for $2q^3 - rq^2 - q + 1 \leq d \leq 2q^3 - rq^2$ for $q > r, r = 3,4$ and for $q > 2(r-1), r \geq 5$ [3]. It is also known that $n_q(4,d) = g_q(4,d)+1$ for $2q^3 - 3q^2 - q + 1 \leq d \leq 2q^3 - 3q^2$ for $q \geq 4$ [3].

We prove the nonexistence of $[g_q(4,d),4,d]_q$ codes for (a) $d = q^3/2 - q^2 - 2q + 1$ for $q = 2^h$, $h \geq 3$, (b) $d = 2q^3 - 3q^2 - 2q + 1$ for $q \geq 7$, and (c) $d = 2q^3 - rq^2 - q + 1$ for $3 \leq r \leq q - q/p$, $q = p^h$ with $p$ prime.

# References

[1] R. Hill and H. Ward, A geometric approach to classifying Griesmer codes, *Des. Codes Cryptogr.*, **44**, 169–196, 2007.

[2] R. Kanazawa and T. Maruta, On optimal linear codes over $\mathbb{F}_8$, *Electron. J. Combin.*, **18**, #P34, 27pp., 2011.

[3] T. Maruta, On the minimum length of $q$-ary linear codes of dimension four, *Discrete Math.*, **208/209**, 427–435, 1999.

# New extension theorems for linear codes over finite fields

*Hitoshi Kanda and Tatsuya Maruta
Department of Mathematics and Information Sciences,
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

An $[n,k,d]_q$ code $\mathcal{C}$ is a linear code of length $n$, dimension $k$ and minimum Hamming weight $d$ over the field of $q$ elements. $\mathcal{C}$ is called *extendable* if $\mathcal{C}$ can be extended to an $[n+1,k,d+1]_q$ code. We give some new sufficient conditions for the extendability of $[n,k,d]_q$ codes. See [3] for the known extension theorems and their applications. For an $[n,k,d]_q$ code $\mathcal{C}$, the *diversity* of $\mathcal{C}$ is defined as the pair of integers $(\Phi_0,\Phi_1)$ with

$$\Phi_0=\frac{1}{q-1}\sum_{q|i,i>0}A_i,\ \ \Phi_1=\frac{1}{q-1}\sum_{i\not\equiv 0,d \pmod q}A_i,$$

where $A_i$ means the number of codewords $\boldsymbol{c}\in\mathcal{C}$ with $wt(\boldsymbol{c})=i$. It is well known that $\mathcal{C}$ is extendable if $(\Phi_0,\Phi_1)=(\theta_{k-2},0)$ and $\gcd(d,q)=1$ [1]. For ternary linear codes, it is known that an $[n,k,d]_3$ code with $\gcd(d,q)=1$ and diversity $(\Phi_0,\Phi_1)$ is extendable if $(\Phi_0,\Phi_1)\in\{(\theta_{k-2},0),(\theta_{k-3},2\cdot 3^{k-2}),(\theta_{k-2},2\cdot 3^{k-2}),(\theta_{k-1}-2\cdot 3^{k-2},3^{k-2})\}$ [2]. As a generalization of the case $(\Phi_0,\Phi_1)=(\theta_{k-1}-2\cdot 3^{k-2},3^{k-2})$ for $q=3$, we prove that an $[n,k,d]_q$ code with $\gcd(d,q)=1$ and diversity $(\Phi_0,\Phi_1)=(\theta_{k-1}-2q^{k-2},q^{k-2})$ is extendable. In [4], the extendability of $[n,k,d]_q$ codes with $\gcd(d,q)=1$ whose weights of codewords are congruent to $0,\pm 1 \pmod q$ was investigated. As a generalization of this result, we consider the extendability of $[n,k,d]_q$ codes with $\gcd(d,q)=1$ whose weights of codewords are congruent to $0,\pm d \pmod q$. We also investigate the extendability of $[n,k,d]_4$ codes with $\Phi_0=\theta_{k-3}$.

# References

[1] R. Hill and P. Lizak, Extensions of linear codes, *Proc. IEEE Int. Symposium on Inform. Theory*, pp. 345. Whistler, Canada, 1995.

[2] T. Maruta, Extendability of ternary linear codes, *Des. Codes Cryptogr.* **35** (2005) 175–190.

[3] T. Maruta, Extension theorems for linear codes over finite fields, *J. Geometry* **101** (2011) 173–183.

[4] T. Maruta and K. Okamoto, Extendability of 3-weight (mod $q$) linear codes over $\mathbb{F}_q$, *Finite Fields Appl.* **15** (2009) 134–149.

# Day 3 (August 27, 2014)

# Precoloring Extension Involving Pairs of Vertices of Small Distance

Akira Saito
Department of Information Science
Nihon University
JAPAN
E-mail : asaito@chs.nihon-u.ac.jp

This talk is based on a joint work with Chihoko Ojima and Kazuki Sano (Nihon University, Japan).

Graph coloring has many applications. One example is job scheduling. Suppose there is a concurrent computer system with multiple CPU's and a set of jobs which will be processed in this system. If the number of CPU's is not less than the number of the jobs and there are no other constraints, we can assign a CPU to each job and start processing at the same time. If we assume that each job is finished in a unit time, the whole set of jobs can also be completed in a unit time. However, there are usually other constraints. For example, two jobs may require the same resource in the system. These constraints prohibit the system from handling some jobs simultaneously and the system spends more than a unit time to complete the jobs. In such a case, we have to lay out a schedule on which the system handles them. One approach to address this problem is to represent the constraints by a graph. We represent each job by a vertex, and join a pair of vertices by an edge if the corresponding jobs cannot be processed at the same time. Then independent vertices correspond to the jobs that can be handled simultaneously. Again assuming each job is processed in a unit time, we see that the chromatic number is the optimal time to finish all the jobs.

In the real world, however, the schedule of the jobs is not always made out from scratch. Usually, a part of the schedule has been finished and fixed, and we have to lay out a schedule without tampering this partial schedule. In the context of graph coloring, it corresponds to the situation in which some vertices have already been colored. We are required to give a coloring which does not alter the colors already assigned. This problem is called precoloring.

Let $G$ be a graph and let $f\colon V(G) \to \boldsymbol{N} = \{1, 2, 3, \dots\}$. Then $f$ is a *coloring* if $f(x) \neq f(y)$ holds for every $xy \in E(G)$. If $f$ is a coloring and $|f(G)| \leq r$, $f$ is called an *$r$-coloring*, and if $G$ has an $r$-coloring, $G$ is said to be *$r$-colorable*. The *chromatic number* of $G$, denoted by $\chi(G)$, is the least number $r$ such that $G$ is $r$-colorable.

Let $P \subset V(G)$. If $c\colon P \to \boldsymbol{N}$ is a coloring of $G[P]$, where $G[P]$ is the subgraph induced by $P$, then $c$ is called a *precoloring*, or simply a coloring, of $P$. Again if $|c(P)| \leq r$, $c$ is called an $r$-coloring of $P$. A coloring of $f$ of $G$ is an *extension* of $c$ if $f|_P = c$.

For $P \subset V(G)$, even if $G$ is $r$-colorable and $\chi(P) \leq r$, an $r$-coloring of $P$ cannot always be extended to an $r$-coloring of $G$. For example, a path of even order is 2-colorable. But if we assign the same color to the endvertices, we cannot extend it to a 2-coloring of $G$. Therefore, it is natural to allow at least one extra color, and try to extend a $(\chi(G)+1)$-coloring of $P$ to a $(\chi(G)+1)$-coloring of $G$. One may expect that for a set of vertices $P$ in

an $r$-colorable graph $G$, an $(r+1)$-coloring of $P$ can be extended to an $(r+1)$-coloring of $G$ if the vertices of $P$ are sparsely distributed. For a measure of sparseness, Thomassen [3] suggested minimum distance. If $|P| \geq 2$, we define the minimum distance $d(P)$ of $P$ by $d(P) = \min\{d_G(x,y)\colon x,\ y \in P, x \neq y\}$. If $|P| = 1$, let $d(P) = +\infty$. He conjectured that if $G$ is a planar graph and $d(P) \geq 100$, then every 5-coloring of $P$ can be extended to a 5-coloring of $G$. Albertson [1] proved the conjecture in a stronger fashion.

**Theorem A** ([1])**.** *Let $G$ be an $r$-colorable graph, and let $P \subset V(G)$. If $d(P) \geq 4$, then every $(r+1)$-coloring of $P$ can be extended to an $(r+1)$-coloring of $G$.*

Note that Theorem A does not assume planarity of $G$. Moreover, the requirement of the minimum distance is much weaker than the one stated in Thomassen's conjecture.

Albertson [1] proved that the assumption on the minimum distance is best-possible. There are infinitely many triples $(G, P, f)$ such that $G$ is an $r$-colorable graph, $P \subset V(G)$ with $d(P) = 3$, $f$ is an $(r+1)$-coloring of $P$ and that $f$ cannot be extended to an $(r+1)$-coloring of $G$.

Because of the sharpness of Theorem A, if $d(P) \leq 3$, we may need additional colors to extend an $(r+1)$-coloring of $P$. However, if there are not many pairs of vertices of distance at most three, we may not need many additional colors to extend it. This was the motivation of this research.

We formalize the problem. Let $G$ be an $r$-colorable graph and let $P \subset V(G)$. For a positive integer $k$, define $\mathcal{D}_G(P,k)$ be the set of pairs of vertices of distance at most $k$:

$$\mathcal{D}_G(P,k) = \big\{\{x,y\} \subset P\colon x \neq y, d_G(x,y) \leq k\big\}.$$

We conjectured that the minimum number of additional colors required to extend a precoloring to a coloring of the whole graph is bounded by a function of $|\mathcal{D}_G(P,k)|$. We made an investigation, and found that the conjecture is true.

**Theorem 1.** *Let $k$ and $r$ be positive integers, and let $G$ be an $r$-colorable graph. Let $P \subset V(G)$. If $|\mathcal{D}_G(P,3)| \leq \frac{1}{2}k(k+1)$, then every $(r+1)$-coloring of $P$ can be extended to an $(r+k)$-coloring of $G$.*

According to this theorem, if $t = |\mathcal{D}_G(P,3)|$, then $r + O(\sqrt{t})$ colors suffice to extend an $(r+1)$-coloring of $P$.

The basic proof strategy of Theorem 1 is to partition $P$ into $k$ subsets $P_1, \ldots, P_k$ with $d(P_i) \geq 4$ $(1 \leq i \leq k)$ and apply Albertson's proof technique, using one additional color, to each $P_i$. For this purpose, we construct an auxiliary graph $H = (P, \mathcal{D}_G(P,3))$ and find a $k$-coloring of $H$. We will discuss the detail in the talk.

Next, we consider the effect of the pairs of vertices of distance at most two. As mentioned earlier, Theorem A is best-possible in terms of minimum distance. But under the assumption of $d(P) \geq 3$, Albertson and Moore [2] gave an upper bound to the number of additional colors.

**Theorem B** ([2])**.** *Let $G$ be an $r$-colorable graph and let $P \subset V(G)$. If $d(P) \geq 3$, then every $(r+1)$-coloring of $P$ can be extended to a $\left\lceil \frac{3r+1}{2} \right\rceil$-coloring of $G$.*

They also proved that the requirement of minimum distance is best-possible. They gave infinitely many triples $(G, P, f)$ such that $G$ is an $r$-colorable graph, $P \subset V(G)$ with $d(P) = 2$, $f$ is an $(r+1)$-coloring and that $f$ cannot be extended to a $\lceil \frac{3r+1}{2} \rceil$-coloring of $G$.

Starting from Theorem B, we investigated the effect of $|\mathcal{D}_G(P, 2)|$ to the number of additional colors we need to extend a coloring of $P$. Since we know that we may need more than $r+1$ colors to extend an $(r+1)$-coloring of $P$, we do not have to confine ourselves only to $(r+1)$-coloring of $P$. Therefore, we consider the situation in which $P$ is colored in $r+1$ or more colors. We obtained the following theorem.

**Theorem 2.** *Let $k$ and $r$ be positive integers with $r \geq 2$ and $k \leq r$, and let $G$ be an $r$-colorable graph. Let $P \subset V(G)$ and let $d$ be an $(r+k)$-coloring of $P$.*

1. *If $r + k \equiv 0 \pmod 2$ and $|\mathcal{D}_G(P, 2)| < 2(r + k - 1)$, then $d$ can be extended to a $\frac{3r+k}{2}$-coloring of $G$, and*
2. *if $r + k \equiv 1 \pmod 2$, $r + k \geq 13$ and $|\mathcal{D}_G(P, 2)| < 3(r + k - 1)$, then $d$ can be extended to a $\frac{3r+k+1}{2}$-coloring of $G$.*

In Theorem 2, the bound of $|\mathcal{D}_G(P, 2)|$ in the assumption is $2(r + k - 1)$ if $r + k$ is even, and $3(r + k - 1)$ if $r + k$ is odd. Though there is a large difference between these two bounds, both are actually best-possible.

**Theorem 3.** *For every pair of positive integers with $r \geq 2$, $r+k \equiv 0 \pmod 2$ and $k \leq r$, there exist infinitely many triples $(G, P, d)$ such that*

1. *$G$ is an $r$-colorable graph, $P \subset V(G)$ and $|\mathcal{D}_G(P, 2)| = 2(r + k - 1)$,*
2. *$d$ is an $(r + k)$-coloring of $P$, and*
3. *$d$ cannot be extended to a $\frac{3r+k}{2}$-coloring of $G$.*

**Theorem 4.** *For every pair of positive integer $r$ and $k$ with $r \geq 2$, $r + k \equiv 1 \pmod 2$ and $k \leq r$, there exist infinitely many triples $(G, P, d)$ such that*

1. *$G$ is an $r$-colorable graph,*
2. *$P \subset V(G)$ and $|\mathcal{D}_G(P, 2)| = 3(r + k - 1)$,*
3. *$d$ is an $(r + k)$-coloring of $P$, and*
4. *$d$ cannot be extended to a $\frac{3r+k+1}{2}$-coloring of $G$.*

In Theorem 2, there is an assumption $r + k \geq 13$ when $r + k$ is odd. It is a technical condition coming from the current proof. We believe that this assumption is not necessary.

Also in Theorem 2, we assume $k \leq r$. For $k > r$, the bound of $|\mathcal{D}_G(P, 2)|$ is no longer best-possible.

**Theorem 5.** *Let $r$ and $k$ be a pair of integers with $k > r \geq 2$, and let $G$ be an $r$-colorable graph. Let $P \subset V(G)$ and let $d$ be an $(r+k)$-coloring of $P$.*

1. *If $r < k < \frac{3r-7}{2}$ and $|\mathcal{D}_G(P,2)| < \left\{\frac{1}{2}(k+3r-4)(k-r+3), (k-r+2)(k+r-1)\right\}$, then $d$ can be extended to an $(r+k)$-coloring of $G$, and*

2. *if $k > \frac{3r-7}{2}$ and $|\mathcal{D}_G(P,2)| < \min\left\{\frac{1}{2}(k+1)(k+2), (k-r+2)(k+r-1)\right\}$, then $d$ can be extended to an $(r+k)$-coloring of $G$.*

Note that while the bounds of $|\mathcal{D}_G(P,2)|$ in (1) and (2) of Theorem 2 are linear functions and sharp, the bounds in Theorem 5 are quadratic functions of $k$. Moreover, we no longer need an additional color to extend a precoloring of $P$. We do not know whether the bounds in Theorem 5 are sharp.

In order to prove Theorems 2 and 5, we first give an $r$-coloring $f$ of $G$, ignoring the precolor of $P$. Then we re-color $P$ according to the given precoloring. Finally, we adjust the color of vertices which have a neighbor in $P$. For this purpose, we prepare a pair of colors for each color class of $f$ and try to use either of them for adjustment. If neither color works at some vertex $v$, then $v$ is adjacent with two vertices $x$, $y$ in $P$ having the two colors we have prepared. But this means $d_G(x,y) \leq 2$ and $\{x,y\}$ contributes to $|\mathcal{D}_G(P,2)|$. In order for this counting to lead us to the required bounds, we have to find an optimal assignment of two colors prepared for each color class. This corresponds to find an appropriate matching of an auxiliary graph on colors, and an element from matching theory comes in. We will see the detail of this proof strategy in the talk.

# References

[1] M.O. Albertson, You can't paint yourself into a corner, J. Combin. Theory Ser. B **73** (1998), 189 – 194.

[2] M.O. Albertson and E.M. Moore, Extending graph colorings, J. Combin. Theory Ser. B **77** (1999), 83 – 95.

[3] C. Thomassen, Color-critical graphs on a fixed surface, J. Combin. Theory Ser. B **70** (1997), 67 – 100.

# Day 4 (August 28, 2014)

# Integer 4-flows and Short Cycle Covers

Genghua Fan
Center for Discrete Mathematics, Fuzhou University
Fuzhou, Fujian 350108, China
E-mail: fan@fzu.edu.cn

**Extended Abstract.** Graphs may have loops and parallel edges. The sets of vertices and edges of a graph $G$ are denoted by $V(G)$ and $E(G)$, respectively. A *cycle* is a graph in which each vertex has even degree, while a *circuit* is a minimal nonempty cycle. The *length* of a cycle is the number of edges it contains. A collection of cycles of a graph $G$ *covers* $G$ if each edge of $G$ is in at least one of the cycles; such a collection is called a *cycle cover* of $G$. The length of a cycle cover is the sum of lengths of the cycles in the cover. The *Shortest Cycle Cover Problem* is to find a cycle cover of shortest length. So far, most of the known short cycle covers consist of at most three cycles. For a bridgeless graph $G$, we denote by $cc(G)$ the minimum length of a cycle cover of $G$, consisting of at most three cycles.

The best known upper bound for $cc(G)$ is $\frac{5}{3}|E(G)|$, established 40 years ago by Alon and Tarsi [1] and Bermond, Jackson, and Jaeger [2]. It is still the best known bound. For some classes of graphs, improved bounds have been obtained. Jamshy, Raspaud, and Tarsi [6] proved that if $G$ has a nowhere-zero 5-flow, then $cc(G) \leq \frac{8}{5}|E(G)|$. Jackson [5] proved that if $G$ is cubic, then $cc(G) \leq \frac{64}{39}|E(G)|$, which was improved [4] to $cc(G) \leq \frac{44}{27}|E(G)|$, and then to $cc(G) \leq \frac{34}{21}|E(G)|$ by Kaiser et al. [7]. In the same paper, Kaiser et al. [7] also proved that $cc(G) \leq \frac{44}{27}|E(G)|$ if $G$ has minimum degree 3. However, the proofs in [7] did not work if $G$ has loops. Thus the bound $\frac{44}{27}|E(G)|$ obtained in [7] is for loopless graphs. (Note that we may obtain a bridgeless graph with minimum degree 3 from any bridgeless graph by adding loops to vertices of degree 2.) We have the following improvements.

**Theorem 1.** *If $G$ is a bridgeless cubic graph, then $cc(G) < \frac{29}{18}|E(G)|$.*

**Theorem 2.** *Let $G$ be a bridgeless graph in which each vertex has degree at least 3. Then $cc(G) < \frac{278}{171}|E(G)|$, and if $G$ is loopless, then $cc(G) < \frac{218}{135}|E(G)|$.*

**Remark.** In the theorem above, if $G$ has a loop at a vertex of degree more than 4, then we may remove the loop and the resulting graph still has minimum degree 3. Thus the loopless condition may be relaxed to "no loop at vertices of degree 4".

Let $G$ be a graph with an orientation. For each vertex $v \in V(G)$, $E^+(v)$ denotes the set of non-loop edges with tail $v$, and $E^-(v)$ the set of non-loop edges with head $v$. Let $\mathbf{Z}_k$ denote the additive group of integers modulo $k$. Let $f$ be a function from $E(G)$ to $\mathbf{Z}_k$. If for each vertex $v \in V(G)$,

$$\sum_{e \in E^+(v)} f(e) \; = \; \sum_{e \in E^-(v)} f(e),$$

then $f$ is called a $k$-flow in $G$, and $f(e)$ is the *flow-value* of $e$. (It was called a $\mathbf{Z}_k$-flow in the literatures.) For a $k$-flow $f$ in a graph $G$, let $E_0(f) = \{e : \ e \in E(G),\ f(e) = 0\}$. $f$ is *nowhere-zero* if $E_0(f) = \emptyset$.

An edge is said to be *contracted* if it is deleted and its ends are identified. For a subgraph $H$ in a graph $G$, the *contraction* of $H$, denoted by $G/H$, is the graph obtained by contracting all the edges of $H$.

The proofs of the theorems above rely on the following result on integer 4-flows.

**Theorem 3.** *Let $G$ be a bridgeless graph with a circuit $C$ of length $\ell$. Suppose that $G/C$ has a nowhere-zero 4-flow. If $\ell \leq 19$ or if each vertex of $C$ has degree 3 in $G$, then $G$ has a 4-flow $\phi$ such that $E_0(\phi) \subseteq E(C)$ and $|E_0(\phi)| \leq \lceil \frac{\ell}{4} \rceil - 1$.*

An immediate consequence of Theorem 3 is the following result of Catlin [3], whose original proof is quite involved.

**Corollary** ([3]). *Let $C$ be a circuit in a graph $G$ and $|E(C)| \leq 4$. If $G/C$ has a nowhere-zero 4-flow, then so does $G$.*

We believe that some conditions in Theorem 3 are not necessary, and conjecture:

**Conjecture.** *Let $C$ be a circuit in a bridgeless graph $G$. If $G/C$ has a nowhere-zero 4-flow, then $G$ has a 4-flow $\phi$ such that $E_0(\phi) \subseteq C$ and $|E_0(\phi)| \leq \lceil \frac{|C|}{4} \rceil - 1$.*

# References


[1] N. Alon and M. Tarsi, Covering multigraphs by simple circuits, *SIAM J. Algebraic Discrete Methods* 6 (1985) 345–350.

[2] J.C. Bermond, B. Jackson, and F. Jaeger, Shortest coverings of graphs with cycles, *J. Combin. Theory Ser. B* 35 (1983) 297–308.

[3] P. A. Catlin, Double cycle covers and the Petersen graph, *J. Graph Theory* 13 (1989) 465–483.

[4] G. Fan, Short cycle covers of cubic graphs, *J. Graph Theory* 18 (1994) 131–141.

[5] B.Jackson, Shortest circuit covers of cubic graphs, *J. Combin. Theory Ser. B* 60 (1994) 299–307.

[6] U. Jamshy, A. Raspaud, and M. Tarsi, Short circuit covers for regular matroids with a nowhere zero 5-flow, *J. Combin. Theory Ser. B* 42 (1987) 354–357.

[7] T. Kaiser, D. Kral, B. Lidicky, P. Nejedly, AND R. Samal, Short cycle covers of graphs with minimum degree three, *SIAM J. Discrete Math.* 24 (2010) 330–355.

# Latin Squares Become Graph Endomorphisms

Artur Schaefer
School of Mathematics and Statistics
University of St. Andrews

Synchronization theory forms a link between finite group theory, semigroup theory and graph theory. In particular, a permutation group $G$ on $n$ points is synchronizing, if the semigroup $\langle G, t\rangle$ contains a constant function, for all non-bijective maps $t$ on $n$ points. Synchronizing groups are primitive and the famous 2-transitive groups are synchronizing. In fact, the synchronizing property lies properly between 2-transitivity and primitivity.

In 2009, Neumann established a connection between synchronizing groups and so called 'section-regular' partitions [3]. Using these partitions one is able to apply combinatorial methods to determine maps $t$ not synchronized by a group $G$ ($\langle G, t\rangle$ has no constant function). Another link was made between synchronization and graphs by Cameron and Kazanidis in 2008 [1]. They proved that a group $G$ is synchronizing if and only if there is no non-trivial graph $X$ with clique number equal to the chromatic number, such that $G \leq Aut(X)$. However, if $G$ does not synchronize a map $t$, then $t$ forms a proper endomorphism of a graph $X$. By searching for these proper endomorphisms and section-regular partitions, it was easy to find many non-synchronizing primitive groups and maps.

Therefore, by trying to classify the maps which are synchronized by primitive groups, Araujo recently conjectured that primitive groups synchronize all non-uniform maps (maps whose kernel classes do not have the same size) [2]. In 1995, Rystsov proved a particular case of this conjecture, namely: A transitive permutation group is primitive if and only if it synchronizes every map of rank $n-1$ (=size of its image).

In this talk, we are going to prove Araujo's conjecture in another case. Due to the famous theorem of O'Nan-Scott on the classification of primitive groups, it is known that the group $Sym(n) \wr Sym(m)$ forms one of the five classes of primitive groups. In particulary, this family of groups induces the graphs given by the Hamming association scheme. The points of the graphs given by this scheme are the $m$-tuples in $\mathbb{Z}/n\mathbb{Z}$; the $i$th-association class is the graph where two points are adjacent if the Hamming distance of these tuples is equal to $i$.

In the case of $Sym(n) \wr Sym(2)$, for any $n$, the scheme consists of two graphs, only; the square lattice graph and its complement. Starting with these two graphs, we are not only able to show that Araujo's conjecture holds, but also, we are able to determine combinatorially the number and the structure of their proper endomorphisms. It turns out that the proper endomorphisms of the square lattice graph are Latin squares of order $n$.

Afterwards, we will increase the dimension and consider the equivalent of the square lattice graph and its complement in dimension $m$, which, in fact, belong to the 1st-association class. Here, it becomes necessary to generalize Latin squares to Latin hypercubes to describe the proper endomorphisms of these new graphs. Finally, we will take a look at graphs given by the $(m-1)$st-association class.

# References

[1] P.J. Cameron, P.A. Kazanidis, Cores of symmetric graphs. J. Aust. Math. Soc. 85(2), 145–154 (2008).

[2] P.M. Neumann, Primitive Permutation Groups and their Section-Regular Partitions, Michigan Math. J.58, (2009).

[3] J. Araujo, P.J. Cameron, Primitive Groups Synchronize Non-uniform Maps of Extreme Ranks, (2013).

# The weighted complexity of the line digraph of a digraph

Iwao Sato
Oyama National College of Technology, Oyama
Tochigi 323-0806, JAPAN

Let $D$ be a connected digraph (oriented graph). A *(directed) spanning tree* of $D$ is a subdigraph containing all vertices of $D$, having no cycles, in which one vertex (the *root*) has outdegree 0, and every other vertex has outdegree 1. The *complexity* $\kappa(D)$ of $D$ is the number of directed spanning trees of $D$.

Now we consider a weight function $x : V(D) \cup A(D) \longrightarrow \mathbf{C}$, where $x(v_i)$ and $x(v_i, v_j)$ are a nonzero complex number for $v_i \in v(D)$ and $(v_i, v_j) \in A(D)$, respectively. Set $x_v = x(v)$ for $v \in V(D)$ and set $x_e = x(e)$ for $e \in A(D)$. Furthermore, let $x(v_i, v_j) = 0$ for $(v_i, v_j) \notin A(D)$. We define two polynomials as follows: $\kappa^{edge}(D, x) = \sum_T \prod_{e \in A(T)} x_e$ and $\kappa^{vertex}(D, x) = \sum_T \prod_{e \in A(T)} x_{t(e)}$, where $T$ runs over all spanning trees of $D$. Then $\kappa^{edge}(D, x)$ and $\kappa^{vertex}(D, x)$ are called the *edge weighted complexity* and the *vertex weighted complexity* of $D$, respectively. For a fixed vertex $v \in V(D)$, we define two polynomials as follows: $\kappa^{edge}(D, v, x) = \sum_{\mathrm{root}(T)=v} \prod_{e \in A(T)} x_e$ and $\kappa^{vertex}(D, v, x) = \sum_{\mathrm{root}(T)=v} \prod_{e \in A(T)} x_{t(e)}$, where $T$ runs over all spanning trees of $D$ with a root $v$.

Let $D$ be a digraph. Then the *directed line graph* $\mathcal{L}D = (A(D), F)$ is the digraph which has as vertices the arcs of $D$, and has as arcs the set $F = \{(e, f) \in A(D) \times A(D) \mid t(e) = o(f)\}$.

Levine [10] presented expressed the vertex weighted complexity on spanning trees (with a fixed root) of the directed line graph of a digraph $D$ in terms of the edge weighted complexity on spanning trees (with a fixed root) of $D$. A vertex $v$ of a digraph is called a *source* if $\mathrm{indeg}(v) = 0$.

**Theorem 1**[Levine] Let $D$ be a finite digraph without sources. Then $\kappa^{vertex}(\mathcal{L}D, x) = \kappa^{edge}(D, x) \prod_{i=1}^{n} d_i^{r_i - 1}$, where $n = \mid V(D) \mid$, $m = \mid A(D) \mid$ and $r_i = r_{v_i} = \mathrm{indeg}(v_i)$, $d_i = d_{v_i} = \sum_{o(e)=v_i} x_e$ $(1 \leq i \leq n)$ .

**Theorem 2**[Levine] Let $D$ be a finite digraph, and let $e_* = (w_*, v_*)$ be an arc of $D$. Suppose that $\mathrm{indeg}(v) \geq 1$ for all vertices $v \in V(D)$, and $\mathrm{indeg}(v_*) \geq 2$. Then $\kappa^{vertex}(\mathcal{L}D, e_*, x) = x_{e_*} \kappa^{edge}(D, w_*, x) d_{v_*}^{r_{v_*} - 2} \prod_{v \neq v_*} d_v^{r_v - 1}$.

For a connected digraph $D$ with vertices $v_1, \cdots, v_n$, let $x : V(D) \cup A(D) \longrightarrow \mathbf{C}$ be a weight function of $D$. Set $x(v_i, v_j) = x_{ij}$ for $i, j = 1, \ldots, n$. Then the *formal Laplacian matrix(edge-weighted Laplacian)* $\Delta^{edge} = \Delta^{edge}(D) = (g_{ij})$ of $D$ is defined as follows(see [3]): $g_{ii} = \sum_{j \neq 1} x_{1j}$; $g_{ij} = -x_{ij} (i \neq j)$. Furthermore, the *vertex-weighted Laplacian* $\Delta^{vertex} = \Delta^{vertex}(D) = (d_{uv})_{u,v \in V(D)}$ of $D$ is defined as follows(see [5]): $d_{uu} = \sum_{o(e)=u} x(t(e))$; $d_{uv} = -x(v)$ $(u \neq v)$.

We express the characteristic polynomial of the vetex-weighted Laplacian of the directed line graph of a digraph $D$ in terms of the edge-weighted Laplacian of $D$. As a corollary, we obtain Theorem 1. Furthermore, we present another formula for the vertex-weighted complexity of the directed line graph with a fixed root.

# Cyclic constructions for cluttered orderings of the complete bipartite graph

Tomoko Adachi
Department of Information Sciences, Toho University, 274-8510, Japan
adachi@is.sci.toho-u.ac.jp

The desire to speed up secondary storage systems has lead to the development of *disk arrays* which achieve performance through disk parallelism. While performance improves with increasing numbers of disks the chance of data loss coming from *catastrophic failures*, such as head crashes and failures of the disk controller electronics, also increases. To avoid high rates of data loss in large disk arrays one includes redundant information stored on additional disks — also called *check disks* — which allows the reconstruction of the original data — stored on the so-called *information disks* — even in the presence of disk failures. These disk array architectures are known as *redundant arrays of independent disks* (RAID).

Minimizing the number of disk operations when writing to consecutive disks leads to the concept of 'cluttered orderings' which were introduced for the complete graph by Cohen et al (2001).

Furthermore, in the case of a complete bipartite graph, Mueller et al. (2005) gave a cyclic construction for a cluttered ordering of the complete bipartite graph by utilizing the notion of a wrapped $\Delta$-labelling.

Let $h$ and $t$ be two positive integers. For each parameter $h$ and $t$, we define a bipartite graph denoted by $H(h;t) = (U, E)$. Its vertex set $U$ is partitioned into $U = V \cup W$ and consists of the following $2h(t+1)$ vertices:

$$\begin{aligned} V &:= \{v_i | 0 \le i < h(t+1)\}, \\ W &:= \{w_i | 0 \le i < h(t+1)\}. \end{aligned}$$

The edge set $E$ is partitioned into subsets $E_s$, $0 \le s < t$, defined by

$$\begin{aligned} E'_s &:= \{\{v_i, w_j\} | s \cdot h \le i, j < s \cdot h + h\}, \\ E''_s &:= \{\{v_i, w_{h+j}\} | s \cdot h \le j \le i < s \cdot h + h\}, \\ E'''_s &:= \{\{v_{h+i}, w_j\} | s \cdot h \le i \le j < s \cdot h + h\}, \\ E_s &:= E'_s \cup E''_s \cup E'''_s, \quad \text{for } 0 \le s < t, \\ E &:= \bigcup_{s=0}^{t-1} E_s. \end{aligned}$$

For the number of edges holds $|E| = t \cdot (h^2 + \frac{h(h+1)}{2} + \frac{h(h+1)}{2}) = th(2h+1)$.

Mueller et al. (2005) gave three cyclic constructions in the case of $H(h;1)$, $H(h;2)$ and $H(1;t)$. Adachi and Kikuchi (2014) give a cyclic construction in the case of $H(h;3)$. In this talk, we show these cyclic constructions.

Tariq Rahim
FAST-NU, Peshawar, KPK, Pakistan
tariq.rahim@nu.edu.pk

Global parameters of a graph such as its edge density, chromatic number, can influence the local substructure of a graph. How many edges, for instance, do we have to give a graph on $n$ vertices to be sure that, no matter how these edges are arranged, the graph will contain a $K^r$ subgraph for some given $r$. Will some sufficiently high average degree or chromatic number ensure that such a substructure occur. Questions of this type are among the most natural ones in graph theory, and there is a host of deep and interesting results. Collectively these are known as extremal graph theory. In this talk, one such global parameter known as the degree distance of a graph $G$ is discussed. We would discuss extremal properties of graphs with respect to this parameter.

# Towards the graph minor theorem for directed graphs

Ken-ichi Kawarabayashi
National Institute of Informatics

The seminal graph minor theory is one of the deepest results in all of mathematics, but it only works for undirected graphs. What about directed graphs?

Researchers come to know that there is a big difference. So the first step would be to show "the excluded grid theorem" for digraphs. For undirected graphs, this was originally proved by Robertson and Seymour in Graph Minors V, and is one of the most central results in the study of graph minors. It has found numerous applications in algorithmic graph structure theory.

Reed, and Johnson, Robertson, Seymour and Thomas (in 1997) conjectured an analogous theorem for directed graphs, i.e. the existence of a function $f(k)$ such that every digraph of directed tree-width at least $f(k)$ contains a directed grid of order $k$. In an unpublished manuscript from 2001, Johnson, Robertson, Seymour and Thomas give a proof of this conjecture for planar digraphs.

In this talk, we shall report recent progress (joint work with Stephan Kreutzer). We shall discuss the following:

1. The excluded grid theorem for directed graphs with no $H$-minor;
2. The half-integral grid theorem;
3. Some applications to the disjoint paths problem.

# The List Coloring Conjecture for Complete Graphs

Uwe Schauz
Department of Mathematical Science
Xian Jiaotong-Liverpool University
Suzhou 215123, China
uwe.schauz@xjtlu.edu.cn

The list-chromatic index of a graph $G$ is the smallest number $k$, such that any assignment of $k$ allowed colors to the edges of $G$ permits a correct edge coloring, i.e., a correct coloring $e \mapsto c_e$ with colors $c_e$ chosen from the $k$-lists $L_e$ of allowed colors. The List Coloring Conjecture says that, for every graph $G$, the list-chromatic index of $G$ is equal to the chromatic index of $G$, which refers to the more special case of equal $k$-lists for all edges. We prove that the list-chromatic index of $K_{p+1}$ is $p$, for all odd primes $p$. This implies that the List Coloring Conjecture holds for complete graphs with less than 10 vertices. It also shows that there exist arbitrarily big complete graphs for which the conjecture holds, even among the complete graphs of class 1. Our proof combines the Quantitative Combinatorial Nullstellensatz with a group action on symmetric Latin squares. It displays various ways of using this strengthened Combinatorial Nullstellensatz.

# On Constraints in Networks with Fixed Degrees of Nodes

*P. Selin and H. Obara
Graduate School of Electrical and Electronics Engineering, Akita University,
1-1 Tegata Gakuen, Akita, 010-8502 Japan, selin@wm.akita-u.ac.jp

## 1. Introduction

Classes of networks (weighted graphs) with fixed degrees of nodes, the arc weights (capacities) of which do not exceed a given parameter, are investigated. The characteristic functions depending on the coordinates of vector and the parameter are given, the non-negativity of these functions is the criterion of the existence of a network the degrees of nodes of which are equal to the coordinates of the vector, and the arc weights do not exceed the given parameter. A sets of nodes of the networks from the specified classes are partitioned into two subsets. The variable quantities are the sums of arc weights on each subset and the sum of the weights of the arcs which are incident to the two subsets. The formulas specifying the upper and lower bounds for these variables are obtained.

## 2. General definitions

All $n$-vertex networks will be considered with the fixed set of nodes $U(n) = \{u_1, \dots, u_n\}$ and identified with the arc (and loop) capacities function $C = (c_{ij})$, $c_{ij} = c_{ji} \geq 0$, $1 \leq i, j \leq n$. Degree of the node is the sum of the weights of arcs (and loop) which are incident to the node: $\deg u_i = \sum_{j=1}^{n} c_{ij}$, $1 \leq i \leq n$. Denote $\mathbb{R}_+^n = \{\mathbf{A} = (a_1, \dots, a_n) : a_i \geq 0, \quad 1 \leq i \leq n\}$. Let $c \geq 0$ is the constraint to the arc (loop) weights. We say that vector $\mathbf{A} \in \mathbb{R}_+^n$ is *c-realizable* (into the network) if there exists a network $C = C(\mathbf{A})$ such that $\deg u_i = a_i$, $1 \leq i \leq n$ and $c_{ij} \leq c \ \forall i, j$. Network $C(\mathbf{A})$ is called a *c-realization* of the vector $\mathbf{A}$. We assume that the vector $\mathbf{A} \in \mathbb{R}_+^n$ generates a set of networks with loops $\Gamma_L(\mathbf{A}; c) = \{C(\mathbf{A}) = (c_{ij}) : c_{ij} \leq c \ \forall i, j\}$. A set of networks without loops — $c$-realizations of the vector $\mathbf{A}$ we denote $\Gamma(\mathbf{A}; c) = \{C(\mathbf{A}) \in \Gamma_L(\mathbf{A}; c) : c_{ii} = 0 \quad \forall i\}$. To investigate the bipartite networks, introduce the notation: $\mathbb{R}_{+,=}^{n,m} = \{(\mathbf{A}, \mathbf{B}) : \mathbf{A} \in \mathbb{R}_+^n, \mathbf{B} \in \mathbb{R}_+^m, \sum_{i=1}^{n} a_i = \sum_{j=1}^{m} b_j\}$. All $n, m$-vertex bipartite networks will be considered with the fixed parts $U(n) = \{u_1, \dots, u_n\}$, $V(m) = \{v_1, \dots, v_m\}$ and identified with the arc capacities function $C = (c_{ij})$, $c_{ij} \geq 0$, $1 \leq i \leq n$, $1 \leq j \leq m$. For a pair of vectors $(\mathbf{A}, \mathbf{B}) \in \mathbb{R}_{+,=}^{n,m}$ through the $\Gamma(\mathbf{A}, \mathbf{B}; c)$ we denote the set of bipartite networks-$c$-realizations of pair $(\mathbf{A}, \mathbf{B})$, for which $\deg u_i = a_i$, $1 \leq i \leq n$, $\deg v_j = b_j$, $1 \leq j \leq m$: $\Gamma(\mathbf{A}, \mathbf{B}; c) = \{C(\mathbf{A}, \mathbf{B}) = (c_{ij}) : c_{ij} \leq c \ \forall i, j, \ a_i = \sum_{j=1}^{m} c_{ij}, \ 1 \leq i \leq n, \quad b_j = \sum_{i=1}^{n} c_{ij}, \ 1 \leq j \leq m\}$. Without loss of generality we assume that the coordinates of vector $\mathbf{A}$ and the individual vectors of pair $(\mathbf{A}, \mathbf{B})$ are arranged in nonincreasing order ($\mathbf{A} \in \overline{\mathbb{R}}_+^n$, $(\mathbf{A}, \mathbf{B}) \in \overline{\mathbb{R}}_{+,=}^{n,m}$). *Let $c \geq 0$ and $k \in \mathbb{Z}$, $k \geq 1$. For $\mathbf{A} \in \overline{\mathbb{R}}_+^n$ the values* $\delta_k(\mathbf{A}; c) = ck(k-1) - \sum_{\substack{i \geq k+1 \\ a_i \geq ck}} (a_i - ck) - \sum_{i \leq k} a_i + \sum_{i \geq k+1} a_i, ck \leq a_k + c$, $\Delta_k(\mathbf{A}; c) = ck + \delta_k(\mathbf{A}; c), ck \leq a_k$, *are called the characteristic functions (CF) [1]. For $(\mathbf{A}, \mathbf{B}) \in \overline{\mathbb{R}}_{+,=}^{n,m}$ the CF [2] is defined as* $\delta_k(\mathbf{A}, \mathbf{B}; c) = \sum_{j=1}^{m} b_j - \sum_{b_j \geq ck} (b_j - ck) - \sum_{i=1}^{k} a_i$, $1 \leq k \leq n$. Non-negativity of CF are the criteria of $c$-realizability of a vector [1] and a pair of vectors [2].

`Proposition.` *1) Let* $\mathbf{A} \in \overline{\mathbb{R}}_+^n$ *and* $c \geq 0$. *a)* $\Gamma(\mathbf{A};c) \neq \varnothing \iff \delta_k(\mathbf{A};c) \geq 0$, $\forall k \in \{k : k \geq 1, ck \leq a_k + c\}$; *b)* $\Gamma_L(\mathbf{A};c) \neq \varnothing \iff \Delta_k(\mathbf{A};c) \geq 0$, $\forall k \in \{k : k \geq 1, ck \leq a_k\}$. *2) Let* $(\mathbf{A},\mathbf{B}) \in \overline{\mathbb{R}}_{+,=}^{n,m}$ *and* $c \geq 0$. $\Gamma(\mathbf{A},\mathbf{B};c) \neq \varnothing \iff \delta_k(\mathbf{A},\mathbf{B};c) \geq 0$, $\forall k\ 1 \leq k \leq n$. Denote $\delta(\mathbf{A};c) = \begin{cases} |\min_k \delta_k(\mathbf{A};c)|, & \Gamma(\mathbf{A};c) = \varnothing, \\ 0, & \Gamma(\mathbf{A};c) \neq \varnothing; \end{cases}$ $\Delta(\mathbf{A};c) = \begin{cases} |\min_k \Delta_k(\mathbf{A};c)|, & \Gamma_L(\mathbf{A};c) = \varnothing, \\ 0, & \Gamma_L(\mathbf{A};c) \neq \varnothing; \end{cases}$ $\delta(\mathbf{A},\mathbf{B};c) = \begin{cases} |\min_k \delta_k(\mathbf{A},\mathbf{B};c)|, & \Gamma(\mathbf{A},\mathbf{B};c) = \varnothing, \\ 0, & \Gamma(\mathbf{A},\mathbf{B};c) \neq \varnothing. \end{cases}$

## 3. Main result

Let $\mathbf{A} \in \mathbb{R}_+^n$, $\mathbf{B} \in \mathbb{R}_+^m$ and $\sum_{j=1}^m b_j - \sum_{i=1}^n a_i = \gamma(\mathbf{A},\mathbf{B})$. If $\gamma(\mathbf{A},\mathbf{B}) \geq 0$ then there exists such number $\alpha_{\mathbf{A},\mathbf{B}}$ for which $\sum_{i=1}^n a_i = \sum_{j=1}^m b_j - \gamma(\mathbf{A},\mathbf{B}) = \sum_{j=1}^m \min(\alpha_{\mathbf{A},\mathbf{B}}, b_j)$. Define the vector $\mathbf{B}^{\alpha_{\mathbf{A},\mathbf{B}}} = \left( b_j^{(\alpha_{\mathbf{A},\mathbf{B}})} : b_j^{(\alpha_{\mathbf{A},\mathbf{B}})} = \begin{cases} \alpha_{\mathbf{A},\mathbf{B}}, & b_j \geq \alpha_{\mathbf{A},\mathbf{B}}, \\ b_j, & b_j < \alpha_{\mathbf{A},\mathbf{B}} \end{cases}, 1 \leq j \leq m \right)$.

Let $\mathbf{A} \in \overline{\mathbb{R}}_+^n$ and $U(n) = U_1 \cup U_2$, $U_1 \cap U_2 = \varnothing$. Let us introduce two vectors $\mathbf{A}_1 = (a_i : u_i \in U_1)$, $\mathbf{A}_2 = (a_i : u_i \in U_2)$. We assume $\gamma(\mathbf{A}_1,\mathbf{A}_2) \geq 0$ and put $\gamma_1 = 0$, $\gamma_2 = \gamma(\mathbf{A}_1,\mathbf{A}_2)$.

`Theorem.` *For* $\mathbf{A} \in \overline{\mathbb{R}}_+^n$ *and* $r \in \mathbb{Z}$, $1 \leq r \leq 2$ *holds [1]: a) If* $\Gamma(\mathbf{A};c) \neq \varnothing$ *then* $\delta(\mathbf{A}_1, \mathbf{A}_2^{\alpha_{\mathbf{A}_1,\mathbf{A}_2}};c) + \gamma_r \leq 2\delta(U_r) \leq \sum_{u_i \in U_r} a_i - \max(\delta(\mathbf{A}_1;c), \delta(\mathbf{A}_2;c)), \max(\delta(\mathbf{A}_1;c), \delta(\mathbf{A}_2;c)) \leq \delta(U_1,U_2) \leq \sum_{u_i \in U_1} a_i - \delta(\mathbf{A}_1, \mathbf{A}_2^{\alpha_{\mathbf{A}_1,\mathbf{A}_2}};c)$; *b) If* $\Gamma_L(\mathbf{A};c) \neq \varnothing$ *then* $\delta(\mathbf{A}_1, \mathbf{A}_2^{\alpha_{\mathbf{A}_1,\mathbf{A}_2}};c) + \gamma_r \leq 2\delta(U_r) + \delta_L(U_r) \leq \sum_{u_i \in U_r} a_i - \max(\Delta(\mathbf{A}_1;c), \Delta(\mathbf{A}_2;c)), \max(\Delta(\mathbf{A}_1;c), \Delta(\mathbf{A}_2;c)) \leq \delta(U_1,U_2) \leq \sum_{u_i \in U_1} a_i - \delta(\mathbf{A}_1, \mathbf{A}_2^{\alpha_{\mathbf{A}_1,\mathbf{A}_2}};c)$, *where* $\delta(U_r) = \sum_{\substack{u_i,u_j \in U_r \\ i<j}} c_{ij}$, $\delta_L(U_r) = \sum_{u_i \in U_r} c_{ii}$, $\delta(U_1,U_2) = \sum_{\substack{u_i \in U_1 \\ u_j \in U_2}} c_{ij}$. The result has applications in the theory "Flows in networks", since the partition of nodes defines the network cut.

## 4. References

[1] P. S. Selin and V. I. Tsurkov (forthcoming 2014), "Method of Characteristic Functions for the Classes of Networks with Fixed Degrees of Nodes" J. of Comp. Syst. Sci. Intl., Vol. 53.

[2] V. Tsurkov and A. Mironov, Minimax under Transportation Constraints, Kluwer Acad. Publishers, Dordrecht, 1999.

# Hereditary-shellable simplicial complexes and extendability of shellings

Masahiro Hachimori[1] and Kenji Kashiwabara[2]
[1] Facalty of Engineering, Information and Systems, University of Tsukuba
Tsukuba, Ibaraki 305-8573, Japan; E-mail: hachi@sk.tsukuba.ac.jp
[2] Dept. of General Systems Studies, University of Tokyo
Komaba, Meguro, Tokyo 153-8902, Japan; E-mail: kashiwa@idea.c.u-tokyo.ac.jp

Shellability of simplicial complexes is a property that enables us to treat topological properties of the complexes in a combinatorial way. The definition is as follows: a simplicial complex $\Gamma$ is *shellable* if there is an ordering $F_1, F_2, \ldots, F_t$ of facets (= maximal faces) of $\Gamma$ satisfying that $(\overline{F}_1 \cup \cdots \cup \overline{F}_{j-1}) \cap \overline{F}_j$ is a $(\dim F_j - 1)$-dimensional pure complex for all $2 \leq j \leq t$, where $\overline{F}$ means the simplicial complex formed by $F$ and its subfaces, and a simplicial complex is *pure* if all its facets are of the same dimension. The ordering of the facets satisfying this condition is called a *shelling*. (Note that our definition is the modern one that can be applied for nonpure complexes ([2]).)

For a subset $W \subseteq V$ of the vertex set $V$ of $\Gamma$, the restriction $\Gamma[W]$ is the subcomplex consisting of the faces of $\Gamma$ whose vertices are within $W$. We say $\Gamma$ is *hereditary-shellable* if any restriction (including $\Gamma$ itself) is shellable. Interesting fact is that a simplicial complex is a matroid if and only if any restriction of the complex is "pure and shellable" (= shellable in the classical definition) (e.g., [1, Sec. 7.3]). Herediaty-shellable simplicial complexes, which we discuss in this talk, is a generalization of matroids by replacing "pure and shellable" by "shellable". This generalization opens a variety of new concepts and many problems, as is discussed in [5, Sec. 3].

A simplicial complex $\Gamma$ is *extendably shellable* if any partial shelling can be extended to a complete shelling ([4]). Björner and Eriksson [3] showed that every 2-dimensional matroid complex (= matroid of rank 3) is extendably shellalble. In this talk, we show that if a 2-dimensional simplicial complex $\Gamma$ is hereditary-shellable, then its pure 2-skeleton $\mathrm{pure}_2(\Gamma)$ is extendably shellable. Here, $\mathrm{pure}_2(\Gamma)$ is the subcomplex of $\Gamma$ that has all 2-faces of $\Gamma$ as its facets. This theorem is a strengthening of the result of Björner and Eriksson.

# Recerences

[1] A. Björner, The homology and shellability of matroids and geometric lattices, in "Matroid Applications", (N. White ed.), Cambridge Univ. Press (1992), 226-283.

[2] A. Björner and M. Wachs, Shellable nonpure complexes and posets. I & II, *Trans. Amer. Math. Soc.* **348** (1996), 1299-1327 & **349** (1997), 3945-3975.

[3] A. Björner and K. Eriksson, Extendable shellability for rank 3 matroid complexes, Discrete Math. **132** (1994), 373-376.

[4] G. Danaraj and V. Klee, Which spheres are shellable?, Annals of Discrete Mathematics **2** (1978), 33-52.

[5] M. Hachimori and K. Kashiwabara, Obstructions to shellability, partitionability, and sequential Cohen-Macaulayness , J. Combin. Theory, Ser. A **108** (2011), 1608-1623.

# DERD-Domination in Graphs

Sunilkumar M. Hosamani[1] and Marcin Krzywkowski[2]

[1] Department of Mathematics, Rani Channamma University, Belagavi, Karnataka State, India

[2] Department of Mathematics, Instytut Matematyczny Polskiej Akademii Nauk

A set $D \subseteq V(G)$ is called an equitable dominating set if every vertex $v \in V - D$ there exists a vertex $u \in D$ such that $uv \in E(G)$ and $|deg(u) - deg(v)| \leq 1$. An equitable dominating set $D$ is said to be DERD-dominating set for $G$ if every vertex in $V(G)$ is dominated by at least two vertices in $D$ and $\langle V - D \rangle$ has no isolated vertices. The minimum cardinality of such a dominating set is called DERD-domination number of a graph and it is denoted by $\gamma_{cl}^{e}(G)$. In this paper we initiate a study of this new domination parameter and obtained some sharp upper bounds as well as lower bounds and obtained Nordhaus-Gaddum type results. Finally, we show that the decision problem for finding $\gamma_{cl}^{e}(G)$-sets is NP-complete.

# Day 5 (August 29, 2014)

# Group factorization and cryptography

Tran van Trung
Institut für Experimentelle Mathematik,
Universität Duisburg-Essen, Essen, Germany

Extended Abstract

Group factorization is a topic in finite groups which finds significant applications in cryptography. We begin with a description of the concept of covers and logarithmic signatures for finite groups. Let $\mathcal{S}$ be a subset of a finite group $\mathcal{G}$. Let $\alpha = [A_1, \ldots, A_s]$ with $s \geq 2$ be an ordered collection of ordered subsets $A_i = \{a_{i,1}, \ldots, a_{i,r_i}\}$ of $\mathcal{G}$ such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in $\log |\mathcal{G}|$. We say that $\alpha$ is a *cover* for $\mathcal{S}$, if every product $a_{1,j_1} \cdots a_{s,j_s}$ lies in $\mathcal{S}$ and every $g \in \mathcal{S}$ can be written as

$$g = a_{1,j_1} \cdots a_{s,j_s} \tag{1}$$

with $a_{i,j_i} \in A_i$. If the expression in (1) is unique for every $g \in \mathcal{S}$, then $\alpha$ is called a *logarithmic signature* (LS) for $\mathcal{S}$. The subsets $A_i$ are called the *blocks* and the vector $(r_1, \ldots, r_s) = (|A_1|, \ldots, |A_s|)$ the *type* of $\alpha$. If $\mathcal{S} = \mathcal{G}$, then $\alpha$ is a cover (resp. logarithmic signature) for $\mathcal{G}$. The $s$-tuple $(a_{1,j_1}, \cdots, a_{s,j_s})$ in (1) is called a *factorization* of $g$ with respect to $\alpha$. Let $\Gamma = \{(\mathcal{G}_\ell, \alpha_\ell)\}_{\ell \in \mathbb{N}}$ be a family of pairs, where the $\mathcal{G}_\ell$ are groups and $\alpha_\ell$ covers for $\mathcal{G}_\ell$. We say that $\Gamma$ is *tame* if there exists a probabilistic polynomial time algorithm $\mathcal{A}$ for factorizing all $g \in \mathcal{G}_\ell$ with respect to $\alpha_\ell$ as given in Equation (1). $\Gamma$ is called *wild* otherwise. In general, the problem of finding a factorization in Equation (1) with respect to a given cover is presumedly intractable. There is strong evidence in support of the hardness of the problem. For example, let $\mathcal{G}$ be a cyclic group and let $g$ be a generator for $\mathcal{G}$. Let $\alpha = [A_1, A_2, \ldots, A_s]$ be any cover for $\mathcal{G}$, where the elements of $A_i$ are written as powers of $g$. Then a factorization in Equation (1) with respect to $\alpha$ amounts to solving the Discrete Logarithm Problem in $\mathcal{G}$. Let $\gamma : \mathcal{G} = \mathcal{G}_0 > \mathcal{G}_1 > \cdots > \mathcal{G}_s = 1$ be a chain of subgroups of $\mathcal{G}$, and let $A_i$ be an ordered, complete set of right (or left) coset representatives of $\mathcal{G}_{i-1}$ in $\mathcal{G}_i$. Then $[A_1, \ldots, A_s]$ forms a logarithmic signature for $\mathcal{G}$, called a *transversal logarithmic signature* (TLS). TLSs belong to the class of *periodic* logarithmic signatures and are examples of tame LS. The class of *aperiodic* and *strongly aperiodic* logarithmic signatures are relevant for constructing cryptographic primitives [1], [12]. The problem of generating covers for a group $\mathcal{G}$ is treated in [14]. It is worth mentioning that the concept of logarithmic signatures for finite groups, also known as group factorizations, has a rather long history, whereas covers were introduced for cryptographic applications in the 1990s [7].

The crucial point making covers and LS interesting for use in cryptography is the fact that if the factorization problem is intractable, they essentially induce one-way functions. This can be seen as follows. Let $\alpha = [A_1, A_2, \ldots, A_s]$ be a cover of type $(r_1, r_2, \ldots, r_s)$ for

$\mathcal{G}$ with $A_i = [a_{i,1}, a_{i,2}, \ldots, a_{i,r_i}]$ and let $m = \prod_{i=1}^{s} r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_j$ for $i = 2, \ldots, s$. Let $\tau$

$$\tau : \quad \mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s} \to \mathbb{Z}_m$$

$$\tau(j_1, j_2, \ldots, j_s) := \sum_{i=1}^{s} j_i m_i$$

denote the canonical bijection from $\mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s}$ on $\mathbb{Z}_m$.

Define the surjective mapping $\breve{\alpha}$ induced by $\alpha$ as follows.

$$\begin{aligned} \breve{\alpha} &: \mathbb{Z}_m \to \mathcal{G} \\ \breve{\alpha}(x) &:= a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}, \end{aligned}$$

where $(j_1, j_2, \ldots, j_s) = \tau^{-1}(x)$.

Since $\tau$ and $\tau^{-1}$ are efficiently computable, the mapping $\breve{\alpha}(x)$ is efficiently computable. Conversely, given a cover $\alpha$ and an element $g \in \mathcal{G}$, to determine any element $x \in \breve{\alpha}^{-1}(g)$ it is necessary to obtain any one of the possible factorizations of type (1) for $y$ and determine indices $j_1, j_2, \ldots, j_s$ such that $g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$. This is possible if and only if $\alpha$ is tame. Once a vector $(j_1, j_2, \ldots, j_s)$ has been determined, $\breve{\alpha}^{-1}(g) = \tau(j_1, j_2, \ldots, j_s)$ can be computed efficiently. Thus the problem of finding a factorization of an element $g \in \mathcal{G}$ with respect to cover $\alpha$ is equivalent to the problem of finding a preimage for $g$ in $\mathbb{Z}_m$ of the induced mapping $\breve{\alpha}$.

The very first application of logarithmic signatures in cryptography dates back to the 1980s [5], where the symmetric key cryptosystem called Permutation Group Mappings (PGM) is proposed on the basis of tame logarithmic signatures for permutation groups. It was not until the middle of the 1990s when the concept of covers was introduced, group factorizations have found their increasing usefulness in public key cryptography [7], [4], [9], [2], [15], [8]. In [7] the public key cryptosystems $MST_1$ and $MST_2$ have been presented. Essentially $MST_1$ is built on the following theoretical results stating that a logarithmic signature for a group $\mathcal{G}$ induces a permutation in the symmetric group $\mathcal{S}_{|\mathcal{G}|}$ and that $\mathcal{S}_{|\mathcal{G}|}$ is generated by permutations induced from transversal logarithmic signatures for $\mathcal{G}$ [3], [6], [7]. The cryptosystem $MST_2$ may be viewed as a generalization of the ElGamal cryptosystem on the basis of covers for abelian or non-abelian groups. The public key cryptosystem $MST_3$ [4] has been proposed in the 2000s. The basic idea for constructing $MST_3$ can be briefly described as follows. Starting with a random cover $\alpha$ for a subset of a non-abelian group $\mathcal{G}$ one forms a random cover $\tilde{\alpha}$ by using a so-called two-sided transform. Then, using $\tilde{\alpha}$ and a tame logarithmic signature $\beta$ for the center of $\mathcal{G}$ one then constructs a random cover $\gamma$ for a second subset of $\mathcal{G}$. Make $\alpha$ and $\gamma$ public and keep $\beta$ and the information used in transforming $\alpha$ to $\tilde{\alpha}$ secret. The secret constitutes the trapdoor for the cryptosystem. It has been suggested that the Suzuki 2-groups could be used for an instantiation of $MST_3$ [4]. A further improved version of the $MST_3$ published in 2010 [15] by incorporating group homomorphisms into the design approach has substantially strengthened the security of the scheme. That paper also includes an extensive study of the security of the scheme by heuristic and algebraic methods.

The paper [10] introduces a new approach to designing cryptographic pseudorandom number generator (PRNG) based on random covers for abelian groups. It turns out that this type of PRNG is very efficient and produces strongly pseudorandom bit sequences as they have been thoroughly tested by using the NIST Statistical Test Suite and the Diehard battery of statistical tests, see also [11].

Currently [8] we discover a method of using structures called *group factorization lattices* combined with random covers for abelian groups to build a new type of digital signature schemes. It has been found that the algebraic cryptanalysis for symmetric key cryptosystems that involves solving *Multiple Right Hand Sides* equations (MRHS) over finite fields may be used in investigating security of the new schemes.

In this talk we will elaborate the approaches towards using group factorization for designing cryptographic primitives as outlined above and discuss some recent progress.

# Recerences

[1] B. Baumeister and J.-H. de Wiljes, Aperiodic logarithmic signatures, *J. Math. Cryptol.* **6** (2012), 21–37.

[2] S. R. Blackburn, C. Cid and C. Mullan, Cryptanalysis of the $MST_3$ Public Key Cryptosystem, *J. Math. Cryptol.* **3** (2009), 321–338.

[3] A. Caranti, and F. Dalla Volta, The round functions of cryptosystem PGM generate the symmetric group, *Des. Codes Cryptogr.* **38** (2006), 147–155.

[4] W. Lempken, S. S. Magliveras, TvT and W. Wei, A public key cryptosystem based on non-abelian finite groups, *J. Cryptol.* **22** (2009), 62–74.

[5] S. S. Magliveras, A cryptosystem from logarithmic signatures of finite groups, In *Proceedings of the 29'th Midwest Symposium on Circuits and Systems*, Elsevier Publishing Company, (1986), 972–975.

[6] S. S. Magliveras and N. D. Memon, The Algebraic Properties of Cryptosystem PGM, *J. Cryptol.* **5** (1992), pp. 167-183.

[7] S. S. Magliveras, D. R. Stinson and TvT, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups, *J. Cryptol.* **15** (2002), 285–297.

[8] S. S. Magliveras, P. Svaba and TvT, $\mathsf{MST}_{\mathsf{Sig}}$ : a signature scheme based on covers for finite groups, *2014 (in preparation).*

[9] S. S. Magliveras, P. Svaba, TvT and P. Zajac, On the security of a realization of cryptosystem $MST_3$, *Tatra Mt. Math. Publ.* **41** (2008), 1-13.

[10] P. Marquardt, P. Svaba and TvT, Pseudorandom number generators based on random covers for finite groups, *Des. Codes Cryptogr.* **64** (2012), 209–220.

[11] P. Marquardt, P. Svaba and TvT, $\mathsf{MST_g}$ : Cryptographically strong pseudorandom number generator and its realization, *Preprint*.

[12] R. Staszewski and TvT, Strongly aperiodic logarithmic signatures, *J. Math. Cryptol.* **7** (2013), 147–179.

[13] P. Svaba, TvT and P. Wolf, Logarithmic signatures for abelian groups and their factorization, *Tatra Mt. Math. Publ.* **57** (2013), 1–13.

[14] P. Svaba and TvT, On generation of random covers for finite groups, *Tatra Mt. Math. Publ.* **37** (2007), 105–112.

[15] P. Svaba and TvT, Public key cryptosystem $MST_3$: cryptanalysis and realization, *J. Math. Cryptol.* **4** (2010), 271–315.

[16] M. I. G. Vasco, A. I. P. del Pozo, P. T. Duarte, A note on the security of $MST_3$, *Des. Codes Cryptogr.* **55** (2010), 189–200.

# Defect property of $\mathbb{Z}^2$ figure codes

Włodzimierz Moczurad
Faculty of Mathematics and Computer Science, Jagiellonian University,
Łojasiewicza 6, 30-348 Kraków, Poland
wkm@ii.uj.edu.pl

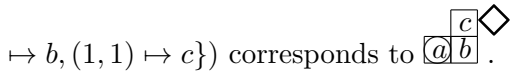
*We survey the defect property for several kinds of two-dimensional words, i.e., $\mathbb{Z}^2$ "pictures" or "figures" that can be defined as labelled polyominoes with various operations of catenation. The well-known defect theorem states that if a finite set of words is not a code, then the words can be expressed as a product of words from a smaller set. This property does not carry over to the $\mathbb{Z}^2$ settings, except for few special cases. We show a sufficient condition for this to happen.* *This work has been supported by a National Science Centre (NCN) grant no. 2011/03/B/ST6/00418.*

Extensions of classical words and codes are widely studied. Examples include Aigrain and Beauquier's polyomino codes; two-dimensional rectangular pictures of Giammarresi and Restivo; Karhumäki, Mantaci and Restivo's tree codes; and symbolic picture languages of Costagliola et al. Unfortunately, properties related to decipherability rarely carry over to $\mathbb{Z}^2$; this is also true of the defect theorem. In its classical version, the defect theorem states that if $X$ is a finite non-code (there exists a word in $X^*$ with two different $X$-factorizations), then there exists a code $Y$ such that $X \subseteq Y^*$ and $|Y| < |X|$. Whilst it has been shown that the defect property can be extended e.g. to trees, the property fails in many simple cases of $\mathbb{Z}^2$ figures.

In this paper we survey three possible settings of $\mathbb{Z}^2$ figures, based on definitions formulated in our previous work: undirected figures and directed figures with a merging and non-merging catenation. First, we recall the results for undirected figures. Then we show that no defect property can be obtained for directed figures, both merging and non-merging, unless strong uniformity restrictions are imposed. To this end we prove a sufficient condition for a set of directed figures to exhibit the defect property.

To illustrate the idea, an informal definition and an example of a non-code that fails the defect property are given below.

**Definition.** Let $\Sigma$ be a finite, non-empty alphabet. Let $D \subseteq \mathbb{Z}^2$ be finite and non-empty, $b, e \in \mathbb{Z}^2$ and $\ell : D \to \Sigma$. A quadruple $(D, b, e, \ell)$ is a *directed figure* (over $\Sigma$) with domain $D$, start point $b$, end point $e$, and labelling function $\ell$. In a graphical representation of a figure, each point $p \in D$ is represented by a unit square in $\mathbb{R}^2$ with bottom left corner in $p$. The label is shown inside the square unless $|\Sigma| = 1$. A circle marks the start point and a diamond marks the end point of the figure. Figures are considered up to translation, hence we do not mark the coordinates; for instance

$(\{(0,0),(1,0),(1,1)\},(0,0),(2,1),\{(0,0)\mapsto a,(1,0)\mapsto b,(1,1)\mapsto c\})$ corresponds to 

.

Non-merging catenation of figures $x$ and $y$ is obtained by translating $y$ so that its start point is aligned with the end point of $x$ and taking a union of domains and labelling

functions, provided the figures do not overlap. A merging catenation uses an additional merging function to resolve possible overlap collisions.

**Example.** Let $|\Sigma| = 1$ and

$$X = \{w = \text{  },\ x = \text{  },\ y = \text{  },\ z = \text{}\}.$$

Clearly $wx = yz$, implying that $X$ is not a code. However, no $Y$ exists such that $|Y| < 4$ and $X \subseteq Y^*$.

# Numbers of lines on surfaces in the projective 3-space over finite fields

*Masaaki Homma and Seon Jeong Kim
Department of Mathematics and Physics, Kanagawa University
Hiratsuka 259-1293, Japan
Department of Mathematics and RINS, Gyeongsang National University
Jinju 660-701, Korea

Let $S$ be a nonsingular surface in $\mathbb{P}^3$ of degree $d \geq 2$ over $\mathbb{F}_q$. The number of $\mathbb{F}_q$-lines on $S$ will be denoted by $\nu_q(S)$. As a corollary of our previous works on numbers of points on surfaces [1, 2], we have the following statement.

**Theorem .** $\nu_q(S) \leq ((d-1)q+1)d$. *Furthermore if equality holds, then* $d$ *is either* 2 *or* $\sqrt{q}+1$ (*when* $q$ *is a square*) *or* $q+1$, *and the surface* $S$ *is projectively equivalent to one of the following surfaces over* $\mathbb{F}_q$:

(i) $X_0X_1 - X_2X_3 = 0$ *if* $d = 2$;

(ii) $X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} + X_3^{\sqrt{q}+1} = 0$ *if* $d = \sqrt{q}+1$;

(iii) $X_0X_1^q - X_0^qX_1 + X_2X_3^q - X_2^qX_3 = 0$ *if* $d = q+1$.

# Recerences

[1] M. Homma and S. J. Kim, *An elementary bound for the number of points of a hypersurface over a finite field*, Finite Fields Appl. 20 (2013) 76–83.

[2] M. Homma and S. J. Kim, Numbers of points of surfaces in the projective 3-space over finite fields, preprint, Oct. 2013.

# The existence of perfect $(p, 3, f, \rho)$-difference systems of sets with $p = 3f + 1, 4f + 1$

Shoko Chisaki
(Joint work with Nobuko Miyamoto)
Tokyo University of Science, Japan

**Keywords:** Difference systems of sets, Cyclotomic coset, Cyclotomic numbers

A *Difference Systems of Sets (DSS)* with parameters $(n, \tau_0, \ldots, \tau_{t-1}, \rho)$ is a collection $\mathcal{F}$ of $t$ disjoint subsets (called blocks) $Q_i \subseteq \{0, 1, \ldots, n-1\},\ |Q_i| = \tau_i,\ 0 \le i \le t-1$, such that the multiset

$$\triangle\mathcal{F} = \{a - b \pmod n | a \in Q_i,\ b \in Q_j,\ 0 \le i, j \le t-1,\ i \ne j\} \tag{2}$$

contains every number $i,\ 1 \le i \le n-1$, at least $\rho$ times. A DSS is *perfect* if every number $i$ is contained exactly $\rho$ times in the multiset (2). A DSS is *regular* if all blocks $Q_i$ are of the same size ($\tau_0 = \tau_1 = \cdots = \tau_{t-1} = m$). We use the notation $(n, m, t, \rho)$ for a regular DSS on $n$ points with $t$ blocks of size $m$.

Let $p = ef + 1$ be an odd prime and $\alpha$ be a primitive element in $\mathbb{F}_p$. Put $\epsilon = \alpha^e$. We consider a collection $\mathcal{F}$ of $f$ subsets $Q_0, \ldots, Q_{f-1}$ of $\mathbb{F}_p$ defined by

$$Q_0 = \{0, 1, s\},\ s \in \mathbb{F}_p,\ s \ne 0, 1$$

and

$$Q_i = \epsilon^i Q_0 + \sum_{j=0}^{i-1} \epsilon^j u = \{\sum_{j=0}^{i-1} \epsilon^j u,\ \epsilon^i + \sum_{j=0}^{i-1} \epsilon^j u,\ \epsilon^i s + \sum_{j=0}^{i-1} \epsilon^j u\},\ 0 \le i \le f-1,$$

where $u$ is an element of $\mathbb{F}_p \setminus \{0\}$. We can rewrite the $Q_i$ using the following variables:

$$u' = u(\epsilon - 1)^{-1},\ v = u'(u' + 1)^{-1},\ \text{and } w = u'(u' + s)^{-1}.$$

Obviously, we can assume that $u' \ne -1$ and $u' \ne -s$, since $Q_0$ and $Q_1$ have element in common if $u' = -1$ or $u' = -s$. Hence we have $Q_i = \{u'(\epsilon^i - 1), u'(\epsilon^i v^{-1} - 1), u'(\epsilon^i w^{-1} - 1)\}$, $0 \le i \le f-1$.

**Theorem 1.** There exists a regular DSS with parameters $(p, 3, f, \rho)$, where

$$\rho = \min_{0 \le l \le e-1} \{ \sum_{(h,k) \in \{0,b,c\}^2} (l - a + h, h - k)_e - |\{\pm 1, \pm s, \pm(s-1)\} \cap C_l^e| \ \}.$$

Now, we remark that the set $\{\pm 1, \pm s, \pm(s-1)\}$ is a multiset.

In this talk, we will give the lower bound of the parameter $\rho$ of regular DSS. In addition, we show the condition of $s$ and $u$ such that a collection $\mathcal{F}$ forms a perfect DSS for $e = 3$ and 4.

# Generalized VC dimension and Sauer lemma for classes of subsets of product sets

Artem Chernikov, Daniel Palacin and *Kota Takeuchi
*University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8571 Japan
e-mail: kota@math.tsukuba.ac.jp

VC-dimension (Vapnik-Chervonenkis dimension) was introduced by Vapnik and Chervonenkis in VC theory related to statistical learning theory which was developed in 1960-1990. Formally, for a given set $X$ and a class $\mathcal{C} \subset X$, VC-dimension $V(\mathcal{C})$ is the minimum natural number $n$ or $\infty$ such that there is no subset $A \subset X$ of cardinality $n$ with $2^A = \{A \cap C : C \in \mathcal{C}\}$. (Sometimes VC-dimension is defined as $V(\mathcal{C}) - 1$.) So we can say that VC-dimension expresses a complexity of $\mathcal{C}$. One of the most fundamental facts of VC-dimension is the following lemma, called Sauer-Shelah lemma, obtained in the study of finite combinatorics, model theory, and statistical learning theory:

**Fact 1** (Sauer, Shelah, Vapnik and Chervonenkis)**.** *The inequation* $\pi_{\mathcal{C}}(k) \leq \sum_{i<d} \binom{k}{i}$ *holds where* $d = V(\mathcal{C}) \leq k < \infty$*. Especially,* $\log \pi_{\mathcal{C}}(k) = O(\log k)$*.*

Here, the shutter function $\pi_{\mathcal{C}}$ is defined as $\pi_{\mathcal{C}}(k) = \max\{|A \cap C| : |A| = k, A \subset X\}$.

It is known by model theorists that the class of the definable sets in a mathematical structure $M$ has finite VC-dimension if and only if $M$ has no independent property called NIP. (Model theory is a branch of mathematical logic.) In 2005, Shelah introduced $n$-dependent property and started the model theory of $n$-dependent structures. Recently the authors noticed a correspondence of a generalization of VC-dimension and $n$-dependent property in a joint work on $n$-dependent property.

In this talk, we introduce $\mathrm{VC}_n$-dimension $V_n(\mathcal{C})$ and shutter function $\pi_{\mathcal{C},n}$ for a given class $\mathcal{C} \subset X^n$, and prove the following theorem, a generalization of Sauer-Shelah lemma:

**Theorem 2.** *The inequation* $\pi_{\mathcal{C},n}(k) \leq \sum_{i<z} \binom{k^n}{i}$ *holds where* $d = V_n(\mathcal{C}) << k < \infty$ *and* $z = z_n(k, d)$ *is the Zarankiewicz number for hypergraph. Especially,* $\log \pi_{\mathcal{C}}(k) = O(k^{n-\epsilon} \log k)$ *with* $\epsilon = \dfrac{1}{d^{n-1}}$*.*

Zarankiewicz number $z_n(k, d)$ is from extremal graph theory, defined by the minimum natural number $z$ such that for every $n$-partite $n$-uniform hypergraph $(G, E)$, if each part of $G$ is size $k$ and $E$ has size $\geq z$, then there is a complete $n$-partite $n$-uniform hypersubgraph $(G', E') \subset (G, E)$ such that each part of $G'$ is size $d$. The first statement of the theorem is proved by a method called shifting technique, with considering a subset of the product as a hypergraph. The exact value of $z_n(k, d)$ is still unknown except $n = 1$ (trivially $z_1(d, k) = d$), but some upper bounds are known. The last claim in the theorem is proven by using a bound given by Erdös.

(The authors are not specialists of extremal graph theory, so any advice is welcome!)

# Recerences

[1] Erdös, P. “On extremal problems of graphs and generalized graphs.” Israel Journal of Mathematics 2.3 (1964): 183-190.

[2] Shelah, Saharon. ”Strongly dependent theories.” arXiv preprint math/0504197 (2005).