Workshop on Statistical Designs and Related Combinatorics 2014

Dates: December 13 to 15, 2014
Venue: Kinosaki International Arts Center

Program
December 13

１３：３０～１３：５０　Tetsuji Taniguchi（Hiroshima Inst. Tech.）
Hoffman graphs with the smallest eigenvalue at least -3

１３：５０～１４：０５　Kazutaka Isaka（Nagoya Univ.）
Optimal combinatorial structure in group testing with erasures

１４：０５～１４：２５　Kumi Kobata（Kinki Univ.）
Enumeration of 2-connected graphs whose complement is also 2-connected

１４：３５～１４：５０　Lingfeng Chen（Nagoya Univ.）
Low conflict codes with weight 4 and conflict 2

１４：５０～１５：１０　Mieko Yamada（Tokyo Woman's Christian Univ.）
Menon-Hadamard difference sets obtained from a local field by natural projections

１５：１５～１５：３０　Jun Asahina（Gifu Univ.）
A new series of optimal tight conflict-avoiding codes of odd length and weight 3

１５：３０～１５：５０　Yuichiro Fujiwara（Caltech）
TBA

１６：００～１６：５０　Ryoh Fuji-Hara（Univ. Tsukuba）
Classification of Authentication codes and a new model

December 14

９：１５～９：３０　Kohei Yamada（Nagoya Univ.）
A Graham-Lovász's problem on distance matrices of graphs and affine resolvable designs

９：３０～９：５０　Chin-Mei Fu (Tamkang Univ.)
Four-cycle systems with four-regular leaves

９：５０～１０：０５　Yuuki Kageyama（Osaka Prefecture Univ.）
Geometric construction of optimal linear codes

１０：１５～１０：３５　Shinya Fujita（Yokohama City Univ.）
Covering problem on edge-colored hypergraphs

１０：３５～１０：５０　Hitoshi Kanda（Osaka Prefecture Univ.）
On the 3-extendability of quaternary linear codes

１０：５０～１１：１０　Hung-Lin Fu (National Chiao Tung Univ.)
Learning a hidden hypergraph

１１：２０～１２：００　Naoyuki Tamura（Kobe Univ.）
SAT solver and its application to combinatorial problems

１３：３０～１３：４５　Shohei Satake（Nagoya Univ.）
Asymmetry of digraphs – A digraph analogue of a theorem of Erdős-Rényi

１３：４５～１４：０５　Kazuki Matsubara（Matsunaga High School）
Some existence of pairwise additive cyclic BIB designs with block size 2 and 3

１４：１０～１４：２５　Syunpei Ishi （Kumamoto Univ.）
Codes from complete bipartite graphs

１４：２５～１４：４５　Ying Miao（Univ. Tsukuba）
On an extension of collaboration distance

１４：５５～１５：４５　Sanpei Kageyama（Hiroshima Inst. Tech.）
On the Kageyama number in forty-four years

１５：５５～１８：２０　Free discussion

１８：３０～　**Banquet**　（KKR Kinosaki Gembu）

December 15

９：３０～９：４５　Xiao-Nan Lu（Nagoya Univ.）
Affine-invariant quadruple systems and related number theoretical conjecture

９：４５～１０：０５　Koji Momihara（Kumamoto Univ.）
New projective two-intersection sets and related Hadamard difference sets

１０：０５～１０：２０ Satoshi Noguchi（Nagoya Univ.）
q-ary cyclic codes with large minimum distance and their relation to combinatorial designs

１０：３０～１０：５０　Hiroshi Yumiba（Inter. Inst. Nat. Sci.）
Existence conditions for balanced fractional 2^m factorial designs of resolution $\mathrm{R}^*(\{1\}|\Omega_\ell)$ with $N < \nu_\ell(m)$

１０：５０～１１：０５　Yoshitaka Koga（Kumamoto Univ.）
A MacWillams equivalent theorem for higher weights

１１：１０～１１：２５　Shoko Chisaki（Tokyo Univ. Science）
Some existence of perfect difference systems of sets

１１：２５～１１：４５　Akihiro Munemasa（Tohoku Univ.）
A parametric family of complex Hadamard matrices

１１：４５～１１：５０　Closing

Organizers:
Ying Miao (Univ. Tsukuba)
Masanori Sawa (Kobe Univ.)
Masatake Hirao (Aichi Prefectural Univ.)
Kohei Yamada (Nagoya Univ.)
Xiao-Nan Lu (Nagoya Univ.)

Hoffman graphs with the smallest eigenvalue at least -3

Tetsuji Taniguchi

Hiroshima Institute of Technology, Japan

t.taniguchi.t3@cc.it-hiroshima.ac.jp

Hoffman graphs were introduced by Woo and Neumaier [3] to extend the results of Hoffman [1]. Hoffman proved what we would call Hoffman's limit theorem which asserts that, in the language of Hoffman graphs, the smallest eigenvalue of a fat Hoffman graph is a limit of the smallest eigenvalues of a sequence of ordinary graphs with increasing minimum degree.

Woo and Neumaier [3] gave a complete list of fat indecomposable Hoffman graphs with smallest eigenvalue at least $-1-\sqrt{2}$. Moreover they [3, Open Problem 4] raised the problem of classifying fat Hoffman graphs with smallest eigenvalue at least -3.

In [2], we showed that the special graph $\mathcal{S}^{-}(\mathfrak{H})$ of a such a Hoffman graph $\mathfrak{H}$ is isomorphic to one of the Dynkin graphs A_n, D_n, or extended Dynkin graphs $\tilde{\mathsf{A}}_n$ or $\tilde{\mathsf{D}}_n$. Also we showed that, even when the Hoffman graph $\mathfrak{H}$ does not admit an integral representation, its special graph $\mathcal{S}(\mathfrak{H})$ can be represented by one of the exceptional root lattices E_n $(n = 6, 7, 8)$.

In this talk, we introduce Hoffman graph and its representation. Moreover we talk about some results and problems.

References

[1] A. J. Hoffman, On graphs whose least eigenvalue exceeds $-1-\sqrt{2}$, Linear Algebra Appl. 16 (1977), 153–165.

[2] H. J. Jang, J. Koolen, A. Munemasa, and T. Taniguchi, On fat Hoffman graphs with smallest eigenvalue at least -3, Ars Math. Contemp., 7 (2014), 105–121.

[3] R. Woo and A. Neumaier, On graphs whose smallest eigenvalue is at least $-1-\sqrt{2}$, Linear Algebra Appl. 226-228 (1995), 577–591 .

Optimal combinatorial structure in group testing with erasures

Kazutaka Isaka

Nagoya University, Japan

Group testing is an experimental technique that was used to test the infections of disease by R. Dorfman in 1943. The testing method has been studied for the purpose of reducing the number of tests.

In a group testing, there are many items to be tested. By making a number of groups consisting of items and by testing those groups, we obtain testing results of groups. From such results we may find positive items efficiently. Thus, group testing is a method to reduce the number of tests rather than inspecting the items individually for the purpose of identifying positive items among a large number of items.

There are similarities between group testing and the LDPC code which is one of the error correcting codes. Nakano (2013) focused his attention on the optimal structure of group testing and LDPC codes. He characterized the optimal structure of pooling designs of group testing under the condition of no errors among the results of group test. And he compared the difference between group testing and LDPC codes.

In this talk, an optimal combinatorial structure related to pooling matrix for group testing is discussed when errors occur in the results.

Enumeration of 2-connected graphs whose complement is also 2-connected

Kumi Kobata*[1], Shinsei Tazawa and Tomoki Yamashita[1]

[1] *Kinki University, Japan*

It is well known that the complement of a disconnected graph is connected. By this fact, it is easy to count connected graphs whose complement is also connected.

In this talk, we will show a result concerning the enumeration of graphs such that both itself and its complement are also 2-connected. In order to get the enumeration, we characterized the following two families of graphs:
(i) the graphs such that it has connectivity one and its complement is disconnected,
(ii) the graphs such that both itself and its complement have connectivity one

The characterization is a generalization of a result due to Akiyama and Harary in 1979. Moreover, it gives a result on counting the number of 2-connected self-complementary graphs as a corollary, which was obtained by Akiyama and Harary in 1981.

Low conflict codes with weight 4 and conflict 2

Lingfeng Chen

Nagoya University, Japan

The problem of communication for multiple users on a collision channel has been considered as the protocol sequences theory. In general, we assign a $\{0, 1\}$ sequence of length n as a codeword to each user. The time axis is divided into slots. Each user can send copies of an information packet in the position 1's of his/her codeword among a consequent time slots of length n. When M users send information packet at the same time, a user send his information packet successfully, if and only if it exists a slot which is 1 in his codeword and 0 in the other users' codewords. Conflict-avoiding codes (CAC) is a kind of efficient codes used in the technology of communication on a collision channel. However, in a CAC, only a few users can be allowed to send their information on a same channel at the same time. In my research, a new codes related to CAC is proposed, called a low conflict codes, which increases the number of users remarkably than CAC with a relatively high efficiency. In my research, low conflict codes with weight 4 and maximum conflict 2 is investigated. In this talk, an upper bound of users $M_2[n, 4]$ of the number of $n = 2^a 3^b$ is given and optimal codes achieving the bound are given.

Menon-Hadamard difference sets obtained from a local field by natural projections

Mieko Yamada

Tokyo Woman's Christian University, Japan

We know there exists a family of Menon-Hadamard difference sets over Galois rings of characteristic of an ever power of 2 and of an odd extension degree, which has an embedded structure. As the projective limit of Galois rings is a valuation ring of a local field, the projective limit of these Menon-Hadamard difference sets is a non-empty subset of a valuation ring of a local field.
Conversely, does there exist a subset of a local field whose image by the natural projection always gives a difference set over a Galois ring? We will show an example answer to this problem in this talk. A family of Menon-Hadamard difference sets is obtained from a subgroup of a valuation ring of a local field by natural projections. Furthermore this family also has an embedded structure. The formal group and the p-adic logarithm function serve an important role.

A new series of optimal tight conflict-avoiding codes of odd length and weight 3

Jun Asahina*[1], Tokuji Yoshino[2], Koji Momihara[2] and Miwako Mishima[1]

[1] *Gifu University, Japan*
[2] *Kumamoto University, Japan*

A *conflict-avoiding code* (CAC) of length n and weight k is a collection $\mathcal{C}$ of k-subsets, called *codewords*, of $\mathbb{Z}_n(=\mathbb{Z}/n\mathbb{Z})$ such that $\Delta(C)\cap\Delta(C')=\emptyset$ for any distinct codewords $C,C'\in\mathcal{C}$, where $\Delta(C)$ is the set of symmetric differences arising from C. Let $\Delta(\mathcal{C})=\bigcup_{C\in\mathcal{C}}\Delta(C)$. Obviously, $\Delta(\mathcal{C})\subseteq\mathbb{Z}_n\setminus\{0\}$. Especially when $\Delta(\mathcal{C})=\mathbb{Z}_n\setminus\{0\}$, $\mathcal{C}$ is said to be *tight*. The class of all the CACs of length n and weight k is denoted by $\mathrm{CAC}(n,k)$, and the maximum size of codes in $\mathrm{CAC}(n,k)$ by $M(n,k)$, i.e., $M(n,k)=\max\{|\mathcal{C}|:\mathcal{C}\in\mathrm{CAC}(n,k)\}$. A code $\mathcal{C}\in\mathrm{CAC}(n,k)$ is said to be *optimal* if $|\mathcal{C}|=M(n,k)$.

The main objective of the study of CACs has been to determine $M(n,k)$. The spectrum of $M(n,3)$ has been settled for even n by Levenshtein and Tonchev (2005), Jimbo et al. (2007), Mishima et al. (2009) and Fu et al. (2010). As for odd n, the problem of determining $M(n,3)$ is far from the full settlement even if certain properties are imposed on a code. Actually, a necessary and sufficient condition for the existence of a 'tight equidifference' (thus optimal) code in $\mathcal{C}\in\mathrm{CAC}(n,3)$ has been known due to Momihara (2007) and Fu et al. (2013), though their conditions are fairly complex and need to be examined every prime factor of n.

In this talk, we will show that there exists an optimal tight code in $\mathrm{CAC}(n=3^{3u+1}p^e,3)$ for any $u\geq 0, e\geq 1$ and non-Wieferich prime p such that $p\equiv 3 \pmod 8$ and $p\neq 3$, which is in fact a new series of odd length n for which $M(n,3)$ can be determined exactly.

TBA

Yuichiro Fujiwara

California Institute of Technology, USA

TBA

Classification of Authentication codes and a new model

Ryoh Fuji-Hara

University of Tsukuba, Japan

Gus Simmons first introduced the concept of authentication scheme in 1982. Participants in his model consist of three members, sender, receiver and opponent. Let S be the set of source states which are information with meaning, M be the set of messages encrypted from source states, and E be the the set of encryption rules (functions from S to M). The model of G. Simmons assumed that the opponent have two kind of attacks, impersonation and substitution. G. Simmons also suggested that an encryption rule is not necessary to be a function, which means, for each s of S and each e of E , $e(s)$ is not necessary to be one message, i.e. it can be a set of messages. In the system, the sender chooses one from the set randomly and sends it to the receiver. The system is called splitting authentication system. There is a model that the sender or receiver may deceive the other. In the system, we need one more participant called an arbiter. A code for the such model is called A^2-code. There are two types of models with respect to information to send, one is that the sender sends only a message to the receiver, the other one is a model to send an encrypted message with its source to the receiver. We show a classification of authentication codes and the conditions of perfect codes. We would like to introduce a new model and the conditions of a perfect code of the model including an idea to construct the code.

A Graham-Lovász's problem on distance matrices of graphs and affine resolvable designs

Kohei Yamada

Nagoya University, Japan

Let $n_+(G)$ and $n_-(G)$ be the number of positive and negative eigenvalues of a distance matrix of a graph G, respectively. The values $n_+(G)$ and $n_-(G)$ of certain graph are studied Graham and Lovász (Adv. in Math. 29, 60–88 (1978)) asked whether there exists an undirected and connected graph G with $n_+(G) > n_-(G)$. Azarija (Discrete Math., 315/16, 65–68 (2014)) proved that every conference graph of order $v > 9$ satisfies $n_+(G) = n_-(G) + 1$.

We showed that, if there exists a symmetric 2-(v, k, λ)-design with $k - \lambda > 1$, then there exists a graph with $n_+(G) = n_-(G)(= v)$. Furthermore, if the symmetric design satisfies $v - 4k + 5 < 0$ in addition, then there is a graph with $n_+(G) = n_-(G) + 1$.

In this talk, we mainly present another class of graphs with $n_+(G) > n_-(G)$ which is not (strongly) regular in connection with affine resolvable 2-designs.

Four-cycle systems with four-regular leaves

Chin-Mei Fu* and Yu-Fong Hsu

Tamkang University, Taiwan

A decomposition of a graph G is a collection $\mathcal{H} = \{H_1, H_2, \ldots, H_s\}$ of subgraphs of G such that $E(H_1) \cup E(H_2) \cup \cdots \cup E(H_s) = E(G)$ and $E(H_i) \cap E(H_j) = \emptyset$ for $i \neq j$. If H_i is isomorphic to a graph H for each $i = 1, 2, \ldots, s$, then we say that G has an *H-decomposition* or G can be decomposed into H. If H is isomorphic to a copy of k-cycle, then we say G has a k-cycle decomposition or G can be decomposed into k-cycles and $\mathcal{H}$ is a *k-cycle system* of G.

A quartic graph is a graph which is 4-regular. Let K_n be a complete graph with n vertices and Q_t be a quartic graph with t vertices. In this talk, we solve the existence problem of 4-cycle systems of $K_n - Q_t$, except $t \leq n < (4t-5)/3$ and $t \geq 13$.

Geometric construction of optimal linear codes

Yuuki Kageyama*[1] and Tatsuya Maruta[2]

[1,2] *Osaka Prefecture University, Japan*

[1] y.kageyama1x@gmail.com

[2] maruta@mi.s.osakafu-u.ac.jp

A linear code of length n, dimension k and minimum Hamming weight d over $\mathbb{F}_q$, the field of q elements, is called an $[n, k, d]_q$ code. 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. In this talk, we construct a q-divisible $[q^2 + q, 5, q^2 - q]_q$ code through projective geometry. Using the geometric methods such as projective dual and geometric puncturing, we construct optimal codes, giving $n_q(5, d) = g_q(5, d)+1$ for $q^4-q^3-q^2+1 \leq d \leq q^4-q^3-2q$, $q \geq 3$, where $g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$.

Covering problem on edge-colored hypergraphs

Shinya Fujita

Yokohama City University, Japan

For $r \geq 2$, $\alpha \geq r - 1$ and $k \geq 1$, let $c(r, \alpha, k)$ be the smallest integer c such that the vertex set of any non-trivial r-uniform k-edge-colored hypergraph $\mathcal{H}$ with $\alpha(\mathcal{H}) = \alpha$ can be covered by c monochromatic connected components. Here $\alpha(\mathcal{H})$ is the maximum cardinality of a subset A of vertices in $\mathcal{H}$ such that A does not contain any edges. An old conjecture of Ryser is equivalent to $c(2, \alpha, k) = \alpha(r - 1)$ and a recent result of Z. Király states that $c(r, r - 1, k) = \lceil \frac{k}{r} \rceil$ for any $r \geq 3$. In this work, we make the first step to treat non-complete hypergraphs, showing that $c(r, r, r) = 2$ for $r \geq 2$ and $c(r, r, r + 1) = 3$ for $r \geq 3$. This talk is based on the following paper:

S. Fujita, M. Furuya, A. Gyárfás and Á. Tóth, *A note on covering edge colored hypergraphs by monochromatic components*, Electronic J. Combin. Vol. 21(2) (2014).

On the 3-extendability of quaternary linear codes

Hitoshi Kanda*[1], Tatsuya Maruta[2]

[1,2] *Osaka Prefecture University, Japan*

[1] jinza80kirisame@gmail.com

[2] maruta@mi.s.osakafu-u.ac.jp

Let $\mathbb{F}_q$ denote the field of q elements. An $[n,k,d]_q$ *code* is a linear code over $\mathbb{F}_q$ of length n with dimension k and minimum Hamming weight d. The *diversity* of $\mathcal{C}$ is defined from the weight distribution as the pair (Φ_0, Φ_1) with

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

where A_i denotes the number of codewords of $\mathcal{C}$ with weight i. For an $[n,k,d]_q$ code $\mathcal{C}$ with generator matrix G, $\mathcal{C}$ is l-*extendable* if there exist l vectors $h_1, \cdots, h_l \in \mathbb{F}_q^k$ such that the extended matrix $[G, h_1^{\mathrm{T}}, \cdots, h_l^{\mathrm{T}}]$ generates an $[n+l, k, d+l]_q$ code $\mathcal{C}'$. Especially when $l = 1$, $\mathcal{C}$ is called *extendable*. It is known that an $[n,k,d]_4$ code with diversity (Φ_0, Φ_1), $k \geq 3$, d odd, is extendable if one of the following conditions holds: (a) $\Phi_0 = \theta_{k-4}$, (b) $\Phi_1 = \Phi_{1,2}$, (c) $\Phi_{1,2} = 0$, (d) $\Phi_0 + \Phi_{1,2} < \theta_{k-2} + 4^{k-2}$, (e) $\Phi_0 + \Phi_{1,2} = \theta_{k-2} + 2 \cdot 4^{k-2}$, where $\Phi_{1,2} = (\sum_{i \equiv 2 \pmod 4} A_i)/3$ and $\theta_j = (4^{j+1}-1)/3$. We consider the 3-extendability of $[n,k,d]_4$ codes with $d \equiv 1 \pmod 4$.

Learning a hidden hypergraph

Hung-Lin Fu

National Chiao Tung University, Taiwan

Motivated by the study of complex group testing problems we derive the equivalent formulation in graph theory: Given a hypergraph $G = (V, E)$ where the vertices would represent the items and edges would represent the complexes, the main task is to identify all edges by edge detecting queries of the form "$Q(S)$: does S induce at least one edge of G?" Here S is a subset of V. For convenience, we let $V = [n] = \{1, 2, 3, \ldots, n\}$. A query on a subset S of $[n]$ can be represented by $Q(S)$, and $Q(S) = 1$ means the outcome is yes and $Q(S) = 0$ otherwise. It has been studied by several authors where the size of each complex is restricted to be 2. In the talk, we shall report some progress on the case where the complexes are larger than 2. Mainly, adaptive algorithms are obtained in learning a hidden r-uniform hypergraph where $r \geq 3$.

SAT solver and its application to combinatorial problems

Naoyuki Tamura

Kobe University, Japan

A propositional satisfiability testing problem (SAT) is a problem to find an assignment which satisfies the given propositional formula. Recent performance improvement of SAT solvers makes SAT-based approaches applicable for solving hard and practical combinatorial problems. In this talk, we provide an introduction to SAT, SAT solvers, and SAT-based approaches.

Asymmetry of digraphs –A digraph analogue of a theorem of Erdős-Rényi

Shohei Satake

Nagoya University, Japan

A graph G is *asymmetric* if it does not admit any nontrivial automorphism. In the paper "Asymmetric Graphs" (Acta Mathematica Hungarica 14 (3): 295-315, 1963), Erdős and Rényi defined the *asymmetry* of a given graph G to be the number $A(G)$ of deleted/added edges such that the resulting graph is no longer asymmetric. They showed that

$$A(G) \leq [\frac{n-1}{2}] \quad (\forall G \in \mathcal{G}_n)$$

where $\mathcal{G}_n$ denotes the set of all simple graphs with n vertices, and the bound is asymptotically best by using probabilistic methods. In this talk, we propose a measure of asymmetry of directed graphs, and discuss what an Erdős-Rényi type bound should be and whether our bound could be best asymptotically. This is joint work with Masanori Sawa (Kobe University) and Masakazu Jimbo (Nagoya University).

Some existence of pairwise additive cyclic BIB designs with block size 2 and 3

Kazuki Matsubara*[1] and Sanpei Kageyama[2]

[1] *Matsunaga High School, Japan*
[2] *Hiroshima Institute of Technology, Japan*

Let $\boldsymbol{N} = (n_{ij})$ be the usual $v \times b$ incidence matrix of a BIBD(v, b, r, k, λ). For a BIB design $(V, \mathcal{B})$, let σ be a permutation on V. For a block $B = \{v_1, \ldots, v_k\} \in \mathcal{B}$ and a permutation σ on V, let $B^\sigma = \{v_1^\sigma, \ldots, v_k^\sigma\}$. When $\mathcal{B} = \{B^\sigma | B \in \mathcal{B}\}$, σ is called an *automorphism* of $(V, \mathcal{B})$. If there exists an automorphism σ of order $v = |V|$, then the BIB design is said to be *cyclic*.

Let $s = v/k$, where s need not be an integer unlike other parameters. A set of ℓ BIBD(v, b, r, k, λ) is called ℓ *pairwise additive BIB designs*, denoted by ℓ PAB(v, k, λ), if ℓ corresponding incidence matrices $\boldsymbol{N}_1, \ldots, \boldsymbol{N}_\ell$ $(2 \leq \ell \leq s)$ of the BIB design satisfy that $\boldsymbol{N}_{i_1} + \boldsymbol{N}_{i_2}$ is the incidence matrix of a BIBD$(v^* = v = sk,\ b^* = b,\ r^* = 2r,\ k^* = 2k,\ \lambda^* = 2r(2k-1)/(sk-1))$ for any distinct $i_1, i_2 \in \{1, 2, ..., \ell\}$. Furthermore, in ℓ PAB(v, k, λ), if $\boldsymbol{N}_1, \ldots, \boldsymbol{N}_\ell$ are cyclic and the jth initial block of $\boldsymbol{N}_{i_1} + \boldsymbol{N}_{i_2}$ is a set-union of the jth initial blocks of $\boldsymbol{N}_{i_1}$ and $\boldsymbol{N}_{i_2}$ for any distinct $i_1, i_2 \in \{1, 2, ..., \ell\}$ and $1 \leq j \leq b/v$, then the ℓ PAB(v, k, λ) is said to be *cyclic*, denoted by ℓ PACB(v, k, λ).

The purpose of this talk is devoted to show the existence and non-existence of ℓ PACB$(v, k, 1)$ with $k = 2, 3$.

Codes from complete bipartite graphs

Syunpei Ishi

Kumamoto University, Japan

Jungnickel and Vanstone (1997) prove that the binary code generated by complete graph K_n is contained in the Hamming code of length $2^m - 1$ if and only if n is one of the number 2, 3 and 6. So it is natural to study the problem when the binary code generated by the complete bipartite graph is contained in some binary Hamming code. In this talk, we explain some basic results on graphic codes and give an answer of the problem.

On an extension of collaboration distance

Ying Miao

University of Tsukuba, Japan

Collaboration distance measures the co-authorship of scientific papers between two researchers, with range consisted of non-negative integers and infinity. VIP number is the collaboration distance between a person and a VIP, who has collaborated with a large and broad number of peers. Martin Tompa (1989; 1990) proposed a directed graph version of the VIP number problem, and Michael Barr (2001) suggested rational VIP numbers, generalizing the idea that a person who has written p joint paper with VIP should be assigned VIP number $1/p$. In this talk, we extend the definition of collaboration distance in the range of 0 and 1 to the rational number field, and propose a weighted directed graph version of the VIP number problem. Detailed descriptions will be given in computing Kageyama number and Fuji-Hara number.

On the Kageyama number in forty-four years

Sanpei Kageyama

Hiroshima Institute of Technology, Japan

I began to interest myself in combinatorics by attending Professor R. C. Boses lecture on the falsity of Eulers conjecture about the non-existence of two orthogonal Latin squares of order 2 (mod 4) at Hiroshima university on 24 Oct. 1968. This was originally announced on 25 April 1959 at 557th Meeting of American Mathematical Society in New Yorker Hotel, USA. Since 1970 I have served forty-four years in six faculties of three universities in Japan, and an Indian statistical institute, ISEC, Kolkata, in India under UNESCO, a university of Illinois, Chicago, in USA under AFOSR, and an agricultural university of Pozna in Poland under PAN as joint appointments. Also I have visited many academic places abroad to do some joint works on design of experiments and others. I am so happy to have many close friends in the world, especially in India, Poland, USA, Greece and Japan. Much time has been spent also for smooth development of several international journals as editors. In the period a large number of papers (it may be 337 in number as of Oct. 2014) and some books are published also from Springer, and several special issues in international journals are edited as a guest. In such my literature there are single papers (called Kageyama number 0) and joint papers with friends (having Kageyama number 1). I do not know how many people have Kageyama numbers more than one. Personal history under such status will be revisited along with a current problem for the classification on existence of affine alpha-resolvable 2-assoicate partially balanced incomplete block designs that I am very keen to solve.

Affine-invariant quadruple systems and related number theoretical conjecture

Xiao-Nan Lu

Nagoya University, Japan

Let $(V, \mathcal{B})$ be a t-(v, k, λ) design. $(V, \mathcal{B})$ is said to be cyclic if it admits an automorphism consisting of a cycle of length v. Without loss of generality, V can be identified with $\mathbb{Z}_v$, the additive group of integers mod v. Furthermore, if every unit of $\mathbb{Z}_v$ is a multiplier of $(V, \mathcal{B})$, i.e., $\alpha B \in \mathcal{B}$ holds for all $B \in \mathcal{B}$ and $\alpha \in \mathbb{Z}_v^\times$, then $(V, \mathcal{B})$ is said to be affine-invariant, where $\mathbb{Z}_v^\times$ is the multiplicative group of $\mathbb{Z}_v$. In particular, an affine-invariant 3-$(v, 4, \lambda)$ design is also called an affine-invariant Steiner quadruple system if $\lambda = 1$, an affine-invariant λ-fold quadruple system otherwise. The problem of determining the existence of affine-invariant quadruple systems of order v was proved to be equivalent to the existence of 1-factors of some graphs for specified families of parameters v (Lu and Jimbo, 2015+). On the other hand, let us recall the journey of proving the existence of cyclic Steiner quadruple systems. Köhler first proposed a family of graphs for this problem in 1979. Along this direction, Siemon published a series of research papers from 1987 on Köhler's graphs. Eventually, he reduced the essential problem of finding 1-factors to a number theoretical conjecture until 1998, which is said to be the complete interval problem.

In this talk, we will present an analogue of Siemon's complete interval problem and will show how the connection between graphs and "complete intervals" is established. We will lastly discuss evaluation of asymptotic behaviors of some functions related to "complete intervals".

New projective two-intersection sets and related Hadamard difference sets

Koji Momihara*[1] and Qing Xiang[2]

[1] *Kumamoto University, Japan*
[2] *Delaware University, USA*

A Hadamard difference set is a difference set with parameters $(4m^2, 2m^2 - m, m^2 - m)$. The main problem in the study of Hadamard difference sets is for each integer m, which groups of order $4m^2$ contain a Hadamard difference set.

In 1992, Xia found a construction of Hadamard difference sets in the group $H \times \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_t}^4$, where H is either group of order 4, and each p_i is a prime congruent to 3 modulo 4. In 1997, Wilson and Xiang obtained a general method for constructing Hadamard difference sets in the groups $H \times \mathbb{Z}_p^4$, where H is either group of order 4 and p is an odd prime, assuming the existence of certain projective two-intersection sets in $PG(3, p)$. They found examples of projective two-intersection sets satisfying the condition of their construction only for $p = 5, 13, 17$. More precisely, they regarded the four-dimensional vector space over $\mathbb{F}_p$ associated with $PG(3, p)$ as $\mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$, and considered projective two-intersection sets with the prescribed automorphism

$$T := \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix},$$

where ω is a primitive element of $\mathbb{F}_{p^2}$. However, they could not show the existence of such projective two-intersection sets in $PG(3, p)$ for primes $p > 17$ with $p \equiv 1 \pmod 4$. Immediately after their paper, Chen finally succeeded to prove the existence of projective two-intersection sets in $PG(3, p)$ satisfying the condition of Wilson-Xiang's construction of Hadamard difference sets for any prime $p \equiv 1 \pmod 4$. Here, Chen's projective two-intersection sets in $PG(3,p)$ have the prescribed automorphism

$$T' := \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^2 \end{pmatrix},$$

and therefore the original existence problem of projective two-intersection sets with the prescribed automorphism T has been remained unsolved.

The objective of this talk is to give a solution for the original problem on the existence of projective two-intersection sets with the prescribed automorphism T.

q-ary cyclic codes with large minimum distance and their relation to combinatorial designs

Satoshi Noguchi

Nagoya University, Japan

Let q be a power of a prime and m be an integer. In this talk, we show a construction of $[q^m - 1, (q-s)^m, d]$ cyclic code C over $GF(q)$, where $d \geq s\frac{q^m-1}{q-1}$ and $1 \leq \forall s \leq q-1$. Also, we show the relation between extended codes $\bar{C}$ of C and combinatorial designs.

Existence conditions for balanced fractional 2^m factorial designs of resolution $\mathrm{R}^*(\{1\}|\Omega_\ell)$ with $N < \nu_\ell(m)$

Yoshifumi Hyodo[1,2], Masahide Kuwada[2] and Hiromu Yumiba[*2]

[1] *Okayama University of Science, Japan*
[2] *International Institute for Natural Sciences, Japan*

We consider a fractional 2^m factorial design derived from a simple array (SA) such that the $(\ell+1)$-factor and higher-order interactions are assumed to be negligible, where $\ell = 2, 3$. Under these situations, if the main effect is estimable, and furthermore some of the remaining non-negligible factorial effects may or may not be estimable, then a design is said to be of resolution $\mathrm{R}^*(\{1\} \,|\, \Omega_\ell)$. Using the algebraic structure of the TMDPB association scheme, we give a necessary and sufficient condition for an SA to be a balanced fractional 2^m factorial design of resolution $\mathrm{R}^*(\{1\} \,|\, \Omega_\ell)$, where the number of assemblies is less than the number of non-negligible factorial effects.

A MacWillams equivalent theorem for higher weights

Yoshitaka Koga

Kumamoto University, Japan

The MacWilliams equivalent theorem states that there is a weight preserving linear transformation between $[n, k]$ codes C and C' over a finite field $GF(q)$ if and only if C and $C'$are monomially equivalent, and furthermore the linear transformation agrees with the associated monomial transformation on every codeword in C.

In this talk, we mention a generalization of this result for a higher weight preserving transformation between linear code over a finite field.

Some existence of perfect difference systems of sets

Shoko Chisaki* and Nobuko Miyamoto

Tokyo University of Science, Japan

A difference systems of sets (DSS) with parameters $(n, \{\tau_i : 0 \leq i \leq t-1\}, \rho)$ is a collection of t disjoint τ_i-subsets (called blocks) Q_i, $0 \leq i \leq t-1$, of any finite abelian group G of order n such that every non-identity element of G appears at least ρ times in the multiset

$$\{a - b \ (\mathrm{mod}\ n) | a \in Q_i,\ b \in Q_j,\ 0 \leq i, j \leq t-1,\ i \neq j\}. \tag{1}$$

If all blocks Q_i are of the same size, a DSS is regular. If every element i, $1 \leq i \leq n-1$, is contained in exactly ρ times in the multiset (1), a DSS is perfect. A regular DSS on n points with t blocks of size m is denoted by (n, m, t, ρ)-DSS.

Let $p = ef + 1$ be an odd prime. Suppose that $\mathbb{F}_p$ is a finite field of order p and α is a primitive element in $\mathbb{F}_p$. Put $\epsilon = \alpha^e$. We consider a collection $\mathcal{F}$ of f subsets $Q_0, Q_1, \ldots, Q_{f-1}$ of $\mathbb{F}_p$, for $f \geq 2$, defined as

$$Q_0 = \{a_1, a_2, \ldots, a_m\},\ a_k \in \mathbb{F}_p,\ a_k \neq a_l,\ 1 \leq k, l \leq m,$$

and

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

where u is an element of $\mathbb{F}_p \backslash \{0\}$.

In this talk, we will show some existence of $(p, e, f, e(f-1))$-DSS using a collection $\mathcal{F}$, and give some numerical results.

A parametric family of complex Hadamard matrices

Akihiro Munemasa

Tohoku University, Japan

If q is a prime power with $q \equiv 2 \pmod 3$, then the cyclotomic association scheme of class 3 on the finite field with q^2 elements is amorphic. This is because each of the three nontrivial relations defines a strongly regular graph of Latin square parameters. We show that taking appropriate linear combinations of the adjacency matrices yields a continuous family of complex Hadamard matrices. Our computer experiments show that, for the smallest case where $q = 5$, none of the member of this family is decomposable into generalized tensor product.

This is based on joint work with Takuya Ikuta and Ferenc Szöllősi.