Combinatorial Design Theory

Peter Dukes (University of Victoria),
Esther Lamken (University of California),
Richard Wilson (California Institute of Technology)

November 9 – November 14, 2008

1 Overview

Combinatorial design theory is the study of arranging elements of a finite set into patterns (subsets, words, arrays) according to specified rules. Probably the main object under consideration is a balanced incomplete block design, or BIBD. Specifically, a (v, k, λ)-BIBD is a pair $(V, \mathcal{B})$, where V is a set of v elements and $\mathcal{B}$ is a collection of subsets, or blocks, of V such that

- every block contains exactly k points; and
- every pair of distinct elements is contained in exactly λ blocks.

Variations on this definition are commonly considered, and the term 'design' includes these similar contexts.

Design theory is a field of combinatorics with close ties to several other areas of mathematics including group theory, the theory of finite fields, the theory of finite geometries, number theory, combinatorial matrix theory, and graph theory, and with a wide range of applications in areas such as information theory, statistics, computer science, biology, and engineering. Like most areas of combinatorics, design theory has grown up with computer science and it has experienced a tremendous amount of growth in the last 30 years. The field has developed subfields and groups depending on the main techniques used: combinatorial, algebraic, and algorithmic/computational. There are also groups primarily involved with applications such as in coding theory, cryptography, and computer science. As design theory has grown, researchers have become increasingly specialized and focussed in subfields. In recent years, design theory has also become quite interdisciplinary with researchers found in both mathematics and computer science departments as well as occasionally in engineering or applied mathematics groups and in industrial groups. The primary objective of this workshop was to gather together researchers of all levels from different groups and from several different areas of design theory in one place with the goal of exchanging ideas and techniques from different areas.

In a time when the internet and electronic mail dominate our research communication, people forget how much the casual conversations and comments at workshops and conferences add to our research. The excitement generated at our BIRS workshop in November reminded us all how much we have to gain from spending time together and far away from our usual distractions and responsibilities. We were successful at gathering a diverse group of researchers from all levels and from several different areas of design theory. The talks spanned the field of design theory and included applications in computer science and information theory. One of the younger participants, a post-doctoral fellow, commented at the start of his talk that he'd never before had the opportunity to hear talks in so many different areas of design theory and he was really enjoying it. Each participant was given the opportunity to speak and present new research. For the new researchers and some of our foreign visitors, the talks served as an introduction to their research and interests. Many of the senior researchers used this opportunity to present the state of the art on a problem followed by a number of open problems. There were also two focused discussion sessions on open problems and conjectures - one on decompositions of graphs and the other on one-factorizations. The heart of this workshop was very much the open problems from the talks and the two discussion sessions. It was these problems that sparked the continued discussions into the evenings, on the hikes, and occasionally late into the night. Most people left for home excited about new work and projects.

2 Presentation Highlights and Open Problems

2.1 Graph decompositions

Decompositions of graphs were the focus of one of our discussion sessions as well as some of the talks. A large number of combinatorial design problems can be described in terms of decompositions of graphs (sometimes endowed with an edge-coloring) into prespecified subgraphs. In [18] in 1975, Rick Wilson proved necessary and sufficient conditions on n for the existence of a G-decomposition of K_n where G is a simple digraph on k vertices and K_n denotes the complete directed graph on n vertices. He also described applications and connections in design theory. It soon became clear that there were nice applications of a more colorful version of his theorem.

Consider finite edge-r-colored directed graphs where edge-r-colored means that each edge has a color chosen from a set of r colors. Let $K_n^{(r)}$ be the complete directed graph on n vertices with exactly r directed edges, one of each color, between any ordered pair of vertices. A family $\mathcal{F}$ of subgraphs of a graph K will be called a decomposition of K if every edge $e \in E(K)$ belongs to exactly one member of

$\mathcal{F}$. Given a family $\mathcal{G}$ of edge-r-colored digraphs, a $\mathcal{G}$-decomposition of K is a decomposition $\mathcal{F}$ such that every graph $F \in \mathcal{F}$ is isomorphic to some graph $G \in \mathcal{G}$. In 2000, Esther Lamken and Rick Wilson established a very general result for the more colorful case, [12]. They proved necessary and sufficient conditions on n for $\mathcal{G}$-decompositions of $K_n^{(r)}$ where $\mathcal{G}$ is a family of simple edge-r-colored digraphs. They provided new proofs for the asymptotic existence of resolvable designs, near resolvable designs, group divisible designs, and grid designs and proved the asymptotic existence of skew Room-d-cubes and the asymptotic existence of $(v, k, 1)$-BIBDs with any group of order $k-1$ as an automorphism group. More recently, edge-r-colored decompositions and the main result from [12] have been used to establish existence results for Steiner systems that admit automorphisms with large cycles [19], designs with mutually orthogonal resolutions [10], resolvable graph designs [5], group divisible designs with block sizes in any given set K [16], and $\{k\}$-frames of type g^u [16].

The first talk in this area was by Amanda Malloch on joint work with Peter Dukes on the asymptotic existence of equireplicate G-decompositions. These are graph decompositions in which every point appears as a vertex of exactly the same number of G-blocks. Although BIBDs trivially enjoy this property, where G is regarded as the complete graph K_k, graphs G which are not regular require additional necessary conditions to admit equireplicate G-decompositions. Extending this work to a family of graphs, or to edge-colored graphs, remain interesting open problems. Several of Wilson's techniques were revisited in this talk, providing a good introduction to the first discussion session.

To start off that discussion session, Rick Wilson recalled a problem of interest to many of us: finding a proof of 'Gustavsson's Theorem'. Gustavsson's result, [9], says the following: Let H be a graph with h edges. There exists $N = N(H)$ and $\epsilon = \epsilon(H)$ such that for all $n > N$ if G is a graph on n vertices and m edges with $\delta(G) \geq n(1-\epsilon)$, $gcd(H)|gcd(G)$, and $h|m$, then G has an H-decomposition. This result appeared in a 1991 thesis from Stockholm University; it has not been published in a refereed journal and the author has long since left the academic world. Thus far, no one who has looked at the thesis has been convinced that it contains a detailed proof of this main result. Unfortunately, the result, which has nice applications, has made its way into the literature. It is important that either a detailed and complete proof be found or a flaw exposed in the thesis. As a result of our discussions, several of us discussed perhaps organizing a focused small research group to try and settle the problem. In the meantime, Peter Dukes has volunteered to put the thesis in .pdf form so that it is available to everyone. All of us hope that this added attention will lead to a solution to the problem of 'Gustavsson's Theorem'.

The talk by Rick Wilson was motivated by applications of edge-r-colored graphs where the graphs in $\mathcal{G}$ are no longer simple; one came from a problem on perfect cycle systems [15] and the second from nested balanced designs [17]. Rick Wilson described joint work with Anna Draganova and Yukiyasu Mutoh on the most general result for decompositions. They prove necessary and sufficient conditions for n for $\mathcal{G}$-decompositions of $K_n^{(r)}$ where $\mathcal{G}$ is a family of edge-r-colored digraphs. As of the end of the workshop, there were no examples of applications which required this full generality. One of the open questions was to find such applications. At the end of Rick's talk on the last day, Charlie Colbourn asked him if it was possible to determine necessary and sufficient conditions for the existence of a PBD with block sizes in a finite set K where the proportion of blocks of given sizes is specified. Rick has now been able to settle this problem by using a special case of the work in [12]. Perhaps generalizing this work will give us an application that requires the full generality of the new work by Draganova, Mutoh, and Wilson.

The above topics consider general graphs G and therefore results are limited to asymptotic existence. Some of the other talks dealt with concrete graph decompositions and their connections to design theory. Alex Rosa described the state of the art for decompositions of the complete 3-uniform hypergraph into Hamiltonian cycles. The problem of decomposing the complete k-uniform hypergraph into Hamiltonian cycles remains open. Curt Lindner discussed his favorite open problem on embedding partial odd cycle systems. Recently, Darryn Bryant and Daniel Horsley were able to settle Curt's conjecture on the best possible embedding for partial Steiner triple systems, [1]. The problem of finding the best possible embedding for partial odd cycle systems for cycle length greater than or equal to 5 is completely open. Curt discussed his work on the case for 5-cycles and pointed out it was unlikely to be close to the density bound.

2.2 Applications

There are numerous applications of combinatorial design theory. At the workshop, new applications were discussed in computer science, codes, networks, and information theory.

A (k, v)-hash function is a function from a domain of size k to a range of size v. An $(N; k, v)$-hash family is a set of N (k, v)-hash functions. A perfect hash family PHF$(N; k, v, t)$ (of strength t) is an $(N; k, v)$-hash family with the property that for every t-subset of the domain, at least one of the N functions maps the subset onto t distinct elements of the range. Hash functions have long been of interest in computer science and cryptography. In a recent development, Charlie Colbourn and Alan Ling have discovered that perfect hash families provide one of the best explicit constructions for covering arrays. Covering arrays are of interest in the design of experiments and in areas such as software/hardware testing and circuit testing. Charlie Colbourn described their work showing that forbidding certain sets of configurations in classical constructions for orthogonal arrays produces new perfect, separating, and distributing hash families. For fixed parameters, each forbidden configuration leads to solving a set of linear equations, and therefore, computational techniques can be used. Charlie listed several new results for the existence of covering arrays. A great deal of work remains to be done in this area to find good covering arrays. As we left BIRS, Charlie and Alan were discussing joint work with Aiden Bruen using some of his techniques from finite geometry and coding theory for constructing covering arrays and hash families. Aiden's talk was on connections between designs and codes and he described some new geometric ways of looking at the generator matrices of codes.

There are close connections between design theory and coding theory. For example, techniques from design theory are useful in constructing families of codes. Two of the talks mentioned connections between designs and optimal codes. Alan Ling described new work on constructing perfect-deletion-correcting codes that are optimal. He discussed constructions for q-ary 2-deletion- correcting codes of length 4 and q-ary 3-deletion-correcting codes of length 5 that are both perfect and optimal. As Alan noted, there are a number of open questions in this area for finding optimal codes.

Esther Lamken also mentioned that one of the motivations for constructing designs with orthogonal resolutions is some very new connections, due to Etzion [7], between these designs and optimal doubly constant weight codes.

Quantum information theory is presently making use of mutually unbiased bases, an application discussed in Hadi Kharaghani's presentation. A Hadamard matrix H is a matrix with entries in $\{\pm 1\}$ such that distinct rows are orthogonal. For $m \times m$ Hadamard matrices, one has $HH^\top = mI$. Two Hadamard matrices H, K of order $m = n^2$ are called unbiased if $HK^t = nL$, where L is another Hadamard matrix of order m. From a set of mutually unbiased Hadamard matrices, one can deduce the existence of mutually unbiased bases in $\mathbb{R}^m$. This application of design theory was very nicely received, with several interesting questions and discussions following the talk.

2.3 Existence of designs with various conditions

The central problem in design theory is determining the existence of designs. Determining the full spectrum for a class of designs usually requires a combination of techniques, combinatorial, algebraic/geometric, and computational. Existence problems and questions were described in several of the talks.

One of the most powerful techniques for determining the existence of combinatorial designs is the idea of PBD-closure, introduced by Rick Wilson in the early 1970's, [20]. The main idea is to break up blocks of a pairwise balanced design, using small examples of designs to create larger ones. Often, properties are inherited in the resultant design from the ingredients. PBD-closure underlies many existence results including the asymptotic results mentioned above on edge-colored graph decompositions. One of the highlights for constructions at the workshop was a novel – though possibly bizarre – application of PBD-closure by Peter Dukes [4] to the existence of adesigns. An adesign is a set system $(V, \mathcal{A})$, where V is a set of v points and $\mathcal{A}$ is a collection of blocks of size k, having the condition that all unordered pairs of points have a different frequency. Peter showed that by making use of 'padding by BIBDs' he can use PBD-closure to construct adesigns.

Difference sets afford another pervasive method for construction of combinatorial designs. In his talk, Qing Xiang included an update on some conjectures on difference sets. Let G be an additively written group of order v. A k-subset D of G is a (v, k, λ)-difference set of order $n = k - \lambda$ if every nonzero element of G has exactly λ representations as a difference $d - d'$ of distinct elements from D. In the early 1980s, Lander conjectured the following, [13]. Let G be an abelian group of order v and D a (v, k, λ)-difference set in G. If p is a prime dividing both v and $k - \lambda$, then the Sylow p-subgroup of G is not cyclic. This conjecture implies another well known conjecture due to Ryser that a cyclic (v, k, λ)-difference set can only exist if v and $k - \lambda$ are co-prime. Qing noted that Lander's conjecture is now known to be true when $k - \lambda = p^\ell$ where $p > 3$; this is due to work by Leung, Ma, and Schmidt [14]. Qing also described new work on the existence of skew Hadamard difference sets. Due to the speaker's unique expertise in this area, the talk was a very helpful survey for participants at the workshop. Much discussion was generated following the talk.

Broadly, several of the other talks fall into the category of constructive design theory.

Jeff Dinitz described joint work with Alan Ling and Adam Wolfe on N_2 resovable latin squares where they completely settled the existence of these designs. An N_2 resolvable latin square is a latin square with no 2×2 subsquares that also has an orthogonal mate. They used several different types of techniques to show that they could establish the existence of N_2 resolvable latin squares for all orders n with $n \neq 2, 4, 6, 8$.

Don Kreher also described joint work with Melissa Keranen, William Kocay, and Ben Li on problems for the existence of partial Steiner triple systems; they investigated resolvable, cyclic, and arbitrary regular Steiner triple systems. Don also relayed an interesting problem for triple systems. He asked whether it is possible to decompose the triples on 13 points not covered by a projective plane into nine Steiner triple systems. Alex Rosa extended the question to i projective planes and $11 - 2i$ Steiner triple systems, while Peter Dukes and Charlie Colbourn discussed preliminary approaches to the computation.

In 1989, Ron Graham asked if the 1-block intersection graphs of Steiner triple systems are Hamiltonian. This question has led to an investigation of the more general problem of ordering the blocks of designs to meet specified properties. Other ways of ordering the blocks of designs include Gray codes and universal cycles. Megan Dewar described her thesis work investigating the existence of Gray codes and universal cycles for twofold triple systems and cyclic BIBDs. She presented several new results and noted a number of open problems in this area. Her thesis has been submitted to the Canadian Mathematics Society for publication as a monograph. It represents the definitive survey on these problems.

Esther Lamken gave a survey on the state of the art for designs with sets of d mutually orthogonal resolutions. Techniques in this area include combinatorial recursions combined with direct constructions as well as using edge-r-colored decompositions of graphs. The majority of the known existence results are for balanced incomplete block designs. There are a large number of open questions in this area particularly for t-designs ($t \geq 3$) and for all designs with d mutually orthogonal designs and $d \geq 3$. Her survey will include a list of open problems in this area, [11]. At the end of her talk and during the discussion sessions, Alex Rosa added several nice open problems in this area such as the generalized Room square problem. Many of these problems were investigated over 30 years ago without success. Jeff Dinitz and Esther Lamken have already started to investigate one of the problems Alex mentioned: finding a doubly resolvable analogue to Baranyai's theorem or a generalized Room square. One of the most intriguing open questions in this area came up again in the discussion session on 1-factorizations.

What is the upper bound for the size d of a largest set of mutually orthogonal resolutions? The current known upper bounds all come from very straightforward counting arguments. In many cases, there are constructions to show that these upper bounds can be met. However, in the case of 1-factorizations or orthogonal resolutions for $(v, 2, 1)$-BIBDs (also known as Room d-cubes), the simple counting upper bound gives us $d \leq v - 3$. Despite a great deal of work, no one has ever succeeded in constructing more than $\frac{v-2}{2}$ mutually orthogonal resolutions for a $(v, 2, 1)$-BIBD. The best construction in this area is due to Dinitz from 1980, [2]. In the early 1970's, Gross, Mullin, and Wallis conjectured that the bound for d for Room d-cubes of order $v - 1$ was $\frac{v-2}{2}$, [8]. However, in the 1980's Luc Teirlinck pointed out a connection between these designs and some nice structures in finite geometry. His work led him to believe that the bound should really be the counting bound of $v - 3$ for v sufficiently large. Settling these conjectures is one of the most interesting problems in this area.

The discussion session on 1-factorizations was started by Jeff Dinitz. He described new work on perfect 1-factorizations and in particular on perfect Room squares. A perfect Room square is one where both the row and column 1-factorizations are perfect; so it contains a pair of orthogonal perfect 1-factorizations. Jeff showed us the first new perfect Room square constructed in the last 20 years - a perfect Room square on 52 elements. This design was constructed by Adam Wolfe and was done with a considerable amount of computational work, [21]. He gave us a list of the known perfect Room squares and noted that the full existence problem remains open.

2.4 Existence and structural results for t-designs

Whereas classical design theory is generally concerned with arrangements of objects subject to pairwise constraints, t-designs extend this notion to t-wise constraints. A t-(v, k, λ) design is a pair $(V, \mathcal{B})$ where V is a set of v points and $\mathcal{B}$ is a family of k-subsets, called blocks, of V such that each distinct t-subset of V occurs in precisely λ blocks.

Masa Jimbo described new work on constructing cyclic Steiner quadruple systems. A Steiner quadruple system SQS(v) is a 3-$(v, 4, 1)$ design. If an SQS(v) admits a cycle of length v as an automorphism, it is said to be cyclic. He presented new recursive constructions and produced a number of new designs using computational techniques. In fact, the constructed designs enjoy the property that all units in the ring $\mathbb{Z}_v^\times$ act by multiplication as automorphisms. Along with the cyclic structure, these SQS have a very rich automorphism group.

Another existence result for t-designs was presented by Niranjan Balachandran. In his talk, and in informal discussions following, Niranjan discussed a large λ theorem for candelabra systems. These are especially useful in recursive constructions, where various holes can be filled with known small designs.

To complement the above existence results, there was also discussion of structure in t-designs. Two talks stand out along these lines.

Şule Yazıcı discussed defining sets in her talk. A set of blocks that is a subset of a unique t-(v, k, λ) design $D = (V, \mathcal{B})$ is a defining set of that designs. A defining set is minimal if it does not properly contain a defining set of D. Şule described several new algorithms and computational work on finding defining sets for t-designs.

Peter Dukes spoke on extensions of his doctoral thesis [3], where convexity is used to obtain additional structure on t-designs. Specifically, the approach considers the $\binom{v}{t} \times \binom{v}{k}$ zero-one inclusion matrix W_t of t-subsets versus k-subsets of a v-set V. The convex cone generated by columns of W_t is shown to be useful in ruling out various configurations in t-designs. Roughly speaking, this illustrates structure which does not even depend on using 'integral' weights for blocks. This is one nice example where our workshop touched upon techniques from pure mathematics.

3 Outcome

The workshop was very successful for a number of reasons. It goes without saying that each attendee benefited from the presence of others, perhaps working in important related areas but with limited opportunity for collaboration. Indeed, design theory is spread quite thinly across the world. It is also a fairly specialized field of research. Consequently, the workshop offered us a rare opportunity for detailed in-person collaboration.

Despite having limited numbers, the consensus from our participants is that we struck a good balance bringing together a variety of researchers from a variety of locations. Although pairs of researchers occasionally meet, a workshop of this kind is especially helpful for larger collaborations. For example, Peter Dukes, Esther Lamken and Alan Ling discussed possible approaches to the construction of resolvable group divisible designs. As indicated previously, several participants expressed interest in investigating 'Gustavsson's Theorem'. Whether motivated by applications or theory, we left the workshop feeling that this problem of decomposing of 'almost complete' graphs is one of the next major directions in design theory. We are hopeful that the workshop's varied slate of topics, methods and applications can help initiate research on this (and the other open problems we identified).

Another benefit was the inclusion of a few young researchers, including Niranjan Balachandran, Megan Dewar and Amanda Malloch. They were given a chance to present in an informal atmosphere, yet at the same time in a focused setting populated by area experts. Obviously, this rare combination can serve as an important boost in one's career development. For instance, Amanda Malloch received positive and helpful feedback on her Master's thesis work from Rick Wilson, on whose articles the thesis is based. Charlie Colbourn pointed out potential applications of the work.

A nice additional surprise was the mention of work of various other young researchers not in attendance. This included reference to the research of Robert Bailey, Mariusz Meska, and Adam Wolfe, among others. More generally, the workshop indirectly affected (or felt the effects of) the research of many who were not present.

Perhaps most importantly, we are confident that in time this workshop will continue to have important reverberations in design theory, as new collaborations are fostered and new ideas mature.

References

[1] D. Bryant and D. Horsley, A proof of Lindner's conjecture on embeddings of partial Steiner triple systems, *J. Combin. Designs* **17** (2009) 63–89.

[2] J.H. Dinitz, New lower bounds for the number of pairwise orthogonal symmetric latin squares, *Congr. Numer.* **23** (1979), 393–398.

[3] P. Dukes, Convexity and the structure of designs, in press.

[4] P. Dukes, PBD-Closure for Adesigns and Asymptotic Existence of Sarvate-Beam triple systems, *Bull. Inst. of Combin. and its Applications* **54** (2008), 5–10.

[5] P. Dukes and A.C.H. Ling, Asymptotic existence of resolvable graph designs, *Canad. Math. Bull.* **50** (2007), 504–518.

[6] A. Draganova, Y. Mutoh, and R.M. Wilson, More on decompositions of edge-colored complete graphs, in special issue of *Discrete Math.* for the proc. of Com@MaC Conference on Association Schemes, Codes and Designs, Pusan National University, Busan, Korea, 2004.

[7] T. Etzion, Optimal doubly constant weight codes, *J. Combin. Designs* **16** (2008), 137–151.

[8] K.B. Gross, R.C. Mullin, and W.D. Wallis, The number of pairwise orthogonal symmetric Latin squares, *Utilitas Math.* **4** (1973), 239–251.

[9] T. Gustavsson, *Decompositions of large graphs and digraphs with high minimum degree*, Ph.D. Thesis, Mathematics, Stockholm University, 1991.

[10] E.R. Lamken, Designs with mutually orthogonal resolutions and edge-colored decompositions of graphs, submitted.

[11] E.R. Lamken, Survey of designs with orthogonal resolutions, in preparation.

[12] E.R. Lamken and R.M. Wilson, Decompositions of edge-colored complete graphs, *J. Combin. Theory, Series A* **89** (2000), 149–200.

[13] E.S. Lander, *Topics in algebraic coding theory*, Cambridge University Press, Cambridge, 1983.

[14] K.H. Leung, S.L. Ma, and B. Schmidt, Nonexistence of abelian difference sets: Lander's conjecture for prime power orders. *Trans. Amer. Math. Soc.* **356** (2004), 4343–4358.

[15] E.M. Li Marzi, C.C. Lindner, R. Rania, and R.M. Wilson, $\{2, 3\}$-perfect m-cycle systems are equationally defined for $m = 5, 7, 8, 9$, and 11 only, *J. Combin. Designs* **12** (2004), 449–458.

[16] J. Liu, Asymptotic existence theorems for frames and group divisible designs, *J. Combin. Theory, Series A* **114** (2007), 410–420.

[17] Y. Mutoh, *Decompositions of a complete graph into colorwise simple graphs*, Ph.D. Thesis, Keio University, Japan, 2003.

[18] R.M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph. In *Proc. Fifth British Combinatorial Conference, (C. St. J.A. Nash-Williams and J. Sheehan, eds.)*, Congressus Numerantium XV, 647–659, 1975.

[19] R.M. Wilson, Existence of Steiner systems that admit automorphisms with large cycles, Codes and designs (Columbus, OH, 2000), 305–312, *Ohio State Univ. Math. Res. Inst. Publ.*, **10**, de Gruyter, Berlin, 2002.

[20] R.M. Wilson, An existence theory for pairwise balanced designs: II, The structure of PBD-closed sets and the existence conjectures, *J. Combin. Theory, Series A* **13** (1972), 246–273.

[21] A. Wolfe, A perfect one-factorization of K_{52}, *J.Combin. Designs*, DOI 10.1002/jcd.20194.