Asymptotic Existence of Combinatorial Designs

Alan C.H. Ling, Department of Computer Science

University of Vermont

Overview of the research

- Combinatorial design theory including pairwise balanced designs, group divisible designs, triple systems.
- Coding theory, sequence designs and connection to design theory.
- Applications of design theory to computer science, engineering and computational biology.

Graph Designs

- G be a finite undirected simple graph.
- A G-*block* (or simply *block*) on a set X is an embedding $G \hookrightarrow X$.
- A G-*decomposition* of a multigraph H is a collection of G-blocks on $X = V(H)$ whose edge sets partition $E(H)$.
- A G-decomposition of λK_v (the multigraph with v vertices and λ edges between every pair of vertices) is also known as a G-*design* of *order* v and *index* λ, or GD(v, G, λ).
- When G is the complete graph K_k, this is denoted a BIBD(v, k, λ).

Resolvable G-designs

- A set of G-blocks on X whose vertex sets partition X is called a *resolution class*.
- A G-decomposition is said to be *resolvable* if its collection of blocks can be partitioned into resolution classes.
- A resolvable G-decomposition of λK_v is called a resolvable G-design, or RGD(v, G, λ). When G is the complete graph K_k, this is denoted RBD(v, k, λ).

A specific example

- G is a graph on 3 vertices $\{a, b, c\}$ with edges $\{\{a, b\}, \{a, c\}, \{b, c\}\}$.
- $X = \{0, 1, 2, \ldots, 8\}$, and the decomposition is
- $\{0, 1, 2\}, \{3, 4, 5\}, \{6, 7, 8\}$,
- $\{0, 3, 6\}, \{1, 4, 7\}, \{2, 5, 8\}$,
- $\{0, 4, 8\}, \{1, 5, 6\}, \{2, 3, 7\}$, and
- $\{0, 5, 7\}, \{1, 3, 8\}, \{2, 4, 6\}$.

Examples

- RBD$(v, 2, 1)$ are *one-factorizations* of the complete graph K_v.
- BIBD$(v, 3, 1)$ are known as *Steiner triple systems*.
- RBD$(v, 3, 1)$ are better known as *Kirkman triple systems*.
- these objects exists “whenever possible”.
- the set of integers v for which there exists a RGD(v, G, λ) is presently unknown for virtually all other graphs G and $\lambda \in \mathbb{Z}^+$.

Asymptotic Existence Results

- (Wilson) Given fixed integers $k \geq 2$ and $\lambda \geq 1$, there exists v_0 such that BIBD(v, k, λ) exist for all $v \geq v_0$ that satisfy the necessary conditons $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.
- (Ray-Chaudhuri and Wilson) Given a fixed integer $k \geq 2$, there exists v_0 such that RD$(v, k, 1)$-designs exist for all integers $v \geq v_0$ that satisfy the necessary conditions $v-1 \equiv 0 \pmod{k-1}$ and $v \equiv 0 \pmod{k}$.

Asymptotic Existence Results

- (Lu) Given fixed integers $k \geq 2$ and $\lambda \geq 1$, there exists v_0 such that RD(v, k, λ) exist for all integers $v \geq v_0$ that satisfy the necessary conditions $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $v \equiv 0 \pmod{k}$.

Necessary Conditions for Graph designs

- G has n vertices, e edges, and degree sequence $d_1, d_2, \ldots, d_n$, so that $\sum_i d_i = 2e$.
- $D = \gcd\{d_1, \ldots, d_n\}$. By counting in two ways the number of edges of λK_v, and the degree of each vertex in λK_v

$$\lambda v(v-1) \equiv 0 \pmod{2e} \quad (1)$$

$$\text{and } \lambda(v-1) \equiv 0 \pmod{D} \quad (2)$$

Asymptotic Existence

- Wilson proved that the necessary condition is asymptoticly sufficient.
- Lamken and Wilson extended this further into “edge-colored” block designs.

More Necessary Conditions for RGD

- For a GD(v, G, λ) to have a resolution class
- $v \equiv 0 \pmod{n}$.
- every point of X appears in the same number $r = \lambda n(v-1)/2e$ of blocks of the design.
- there is a (nonnegative) integer combination of degrees, say $\sum t_i d_i = \lambda(v-1)$ such that $\sum t_i = r$, the common number of blocks through any point.

Result for asymptotic RGDs.

Theorem 1 *(Dukes and Ling) Let $\lambda \in \mathbb{Z}$, $\lambda \geq 0$. Suppose G is a simple graph with n vertices, e edges, and degrees d_i. Then there exists v_0 such that RGD(v, G, λ) exist for all $v \geq v_0$ satisfying the necessary condition.*

Group Divisible Designs

- Let v, k, λ be positive integers. A group divisible design (GDD) of order v is a triple $(X, \mathcal{G}, \mathcal{B})$, where
- X is a set of v elements,
- $\mathcal{G}$=$\{G_1, G_2, \ldots, G_n\}$ is a set of subsets of X which partition X (called groups),
- $\mathcal{B}$ is a family of subsets of X of size k,
- every pair of elements from X is in exactly λ blocks if they are form different groups, and zero blocks if they are in the same group.
- if all groups are of the same size m, such GDD is said to be of type m^n, and is denoted by (k, λ)-GDD of type m^n.

Asymptotic Results

- (Chang) Given fixed $k \geq 2, \lambda \geq 1$, and $m \geq 1$, there exists n_0 such that a (k, λ)-GDD of type m^n exists whenever $n \geq n_0$ and $\lambda m(n-1) \equiv 0 \pmod{k-1}$ and $\lambda m^2 n(n-1) \equiv 0 \pmod{k(k-1)}$.
- (Mohacsy) Let k and n be fixed integers satisfying $2 \leq k \leq n$. Then there exists m_0 such that $(k, 1)$-GDD of type m^n exists for all integers $m \geq m_0$ if the conditions $m(n-1) \equiv 0 \pmod{k-1}$ and $m^2 n(n-1) \equiv 0 \pmod{k(k-1)}$ are satisfied.

A consequence

- Give fixed $2 \leq k \leq n$ and $m \geq 1$, there exists a $(k, 1)$-GDD of type m^n whenever $m(n-1) \equiv \pmod{k-1}$ and $m^2 n(n-1) \equiv 0 \pmod{k(k-1)}$ except possibly for a finite number of pairs (m, n).
- Proof is by PBD closure of the set $\{n|$ there exists a $(k, 1)$-GDD of type $m^n\}$.

Liu's result on frames

- Liu proved an asymptotic result on k-frames (a special type of k-GDD of type m^n with an additional property.)
- (Conjecture) Given integers $k \geq 2$ and $m \geq 1$, there exists n_0 such that a $(k, 1)$-RGDD of type m^n exists for all integers $n \geq n_0$ that satisfy the necessary conditions $m(n-1) \equiv 0 \pmod{k-1}$ and $mn \equiv 0 \pmod{k}$.

Asymptotic result for RGDDs

- (Chan, Dukes, Lamken and Ling) Given fixed integers $m, \lambda \geq 1$ and $k \geq 2$, there exists an integer n_0 such that for $n \geq n_0$, there exists a resolvable (k, λ)-RGDD of type m^n if and only if $\lambda m(n-1) \equiv 0 \pmod{k-1}$ and $mn \equiv 0 \pmod{k}$.

Ideas

- Main challenge is that for many m, there is no known example of k-RGDD of type m^n for any n (Example, $m = 2$.)
- Our idea was to construct some examples, and then apply recursion.

Examples

- if there exists a RBD$(v,k,1)$,k-RGDD of type $(mn)^k$, k-GDD of type m^n with less than $\frac{v-1}{k-1}$ color classes, then there exists a k-RGDD of type m^{vn}.
- Inflate the RBD$(v,k,1)$ by the RTD(k,mn), leaving mn copies of the RBD$(v,k,1)$ unfilled. Fill in the groups by k-GDD of type m^n and combine the color classes on the rows, with the resolution classes on the RBDs.
- Use frames to get examples for many congruence classes, and then apply recursive constructions for the asymptotic results.

Extention to G-RGDD

- Two different ways to obtain examples for G-RGDD;
- Modify the above construction to use RGDs, and G-GDDs as input instead of RBDs and k-GDDs.
- An alternative way is to start with a RGD(v, G) design and a v-RGDD of type m^n. Fill in each block of size v with a RGD(v, G), one can obtain a G-RGDD of type m^n.
- Then some recursive constructions and tedious computation can be used to prove the final result.

Open Problems

- Is there a RGDD version of the result on the asymptotic existence of k-RGDD of type m^n for large n?
- Existence of k-RGDD of type m^n with finite number of possible exceptions?
- Existence of k-GDD of type $m^n u^1$ with finite number of possible exceptions? (The problem is still open even when $k = 4$!).

Jamison's Problem

- Suppose G is a path of length n.
- The existence problem for decomposing K_n into G is solved.
- Is there a decomposition in which no two copies of G has more than two vertices in common?

Super Simple Designs

- a BIBD(v, k, λ) is super-simple if any two blocks has at most two points in common.
- It has been used to construct specific small perfect hash families and related objects.
- It is not known if the existence of super-simple BIBD(v, k, λ) is asymptoticly sufficient.
- The set is PBD-closed.

Construct Examples

- Wilson's Theory on the choice function over finite field to construct block/graph designs.
- It does not guarantee that any two blocks intersect in at most two points.
- Need to distribute the cosets to each block in such a way that any two blocks share at most one coset.
- Apply recursive constructions to get to other congurence classes.

q-qary Constant-Weight Codes

- X and R are sets, X finite R^X denotes the set of vectors of length $|X|$, where each component of a vector $u \in R^X$ has value in R and is indexed by an element of X, that is, $\mathbf{u} = (\mathbf{u_x})_{\mathbf{x} \in \mathbf{X}}$.
- A q-ary code of length n is a set $\mathcal{C} \subset Z_q^X$, for some X of size n. The elements of $\mathcal{C}$ are called codewords.
- The support of a vector $u \in Z_q^X$ is the set $\{x \in X : u_x \neq 0\}$.
- The weight of $u \in Z_q^X$ is defined as $||u|| = |\text{supp(u)}|$.
- The distance induced by this norm is called the Hamming distance so that $d_H(u, v) = ||u - v||$, for $u, v \in Z_q^X$.
- A code C is said to have distance d if the distance of any distinct two codes is at least d.

- A code is said to be have constant weight w if every codeword in C has weight w.
- Given q and $|X|$, what is the largest size of C?

$A_q(n, 2w-3, w)$

- Johnson Bound and an earlier result by (Chee et. al.) implies any upper bound of the order of n^2q^2.
- If the support of the codes is super-simple, then it implies that the distance between any two codewords is at least $2w-3$.
- In particular, if we can construct w-GDD of type $(q-1)^n$ in which the “support” of the GDD is super simple, the codewords derived from the GDD would construct an optimal code.
- this can be done via a generalization of the super-simple property of the edge-colored block designs.

Balanced sampling designs avoding contiguous units

- Consider a finite ordered population of v identifiable units, labeled as $0, 1, 2, \ldots, v-1$.
- Let A_i denote a quantitative characteristic A for unit i.
- A_i are unknown, but they can observed for any unit.
- Observation of a sample of k units at a time can be used to obtain an estimate the popular total.
- In some applications, contiguous units of the v units are less likely to appear together than units that are further apart.
- Hedayat, Rao and Stufken justify this idea in terms of the variance of the Horvitz-Thompson estimator.

Balanced sample designs avoiding contiguous units

- A BSEC(v, k, λ), is a block design with the properties that
- each block is a set of k different units,
- any two contiguous units do not appear simultaneously in any of the blocks,
- any two noncontiguous units appear simultaneously in the same number of λ blocks.

Result on BSECs

- (Hedayat, Rao and Stufken) For $k \geq 3$, if a BSEC(v, k, λ) exists, then $v \geq 3k$; for $k = 3, 4$ a BSEC(v, k, λ) exists for some λ if $v \geq 3k$.
- (Colbourn et. al.) provided a solution for $k = 3, 4$.
- (Dukes et. al). provided a solution for all k and for some λ.
- Fixing k and λ, is it true that such designs exist for large enough v?

Idea

- This problem is equivalent to decomposing a complete graph, K_v minus a Hamiltonian cycle into K_k.
- Examples are possible to obtain by recursive construction due to the existence of k-GDD of type 3^n as the leave is a 2-regular graph.
- Using product constructions to make the 3-cycles to “stitch” together to become a Hamiltonian cycle.
- It involves an extension of a type of design called Holey GDDs.

Hamilton-Waterloo problem: the case of Hamiltonian cycle and 3

- Decompose K_v into r Hamiltonian cycle and resolvable classes of K_3.
- The hardest case turns out be be 1 Hamiltonian cycle!
- Dinitz et. al. solves this for all but a few possible exceptions.
- Is it possible to otain such a decomposition for large v for a fix k?

Polygon designs

- In BSEC, we cover λ copies of all pairs of K_v except when they are adjacent.
- What if we only cover pairs that are at least distance d apart?
- It becomes polygon designs!
- The problem is open even for $k = 3$!
- Dukes et. al. provides a solution for large λ.
- Can an asymptotic existence result be established?
- This is not equivalent to Hamilton-Waterloo problem!