Combinatorics of block designs and finite geometries

Sharad S. Sane

Department of Mathematics,
Indian Institute of Technology Bombay,
Powai, Mumbai 76
sane@math.iitb.ac.in

November 10, 2013

A quote from Gian Carlo Rota

In the words of Gian Carlo Rota (Preface: Studies in Combinatorics published by the MAA):

Block Designs are generally acknowledged to be the most complex structures that can be defined from scratch in a few lines. Progress in understanding and classification has been slow and has proceeded by leaps and bounds, one ray of sunlight being followed by years of darkness. ⋯ the subject has been made even more mysterious, a battleground of number theory, projective geometry and plain cleverness. This is probably the most difficult combinatorics going on today ...

A quote from Gian Carlo Rota

In the words of Gian Carlo Rota (Preface: Studies in Combinatorics published by the MAA):

Block Designs are generally acknowledged to be the most complex structures that can be defined from scratch in a few lines. Progress in understanding and classification has been slow and has proceeded by leaps and bounds, one ray of sunlight being followed by years of darkness. $\cdots$ the subject has been made even more mysterious, a battleground of number theory, projective geometry and plain cleverness. This is probably the most difficult combinatorics going on today ...

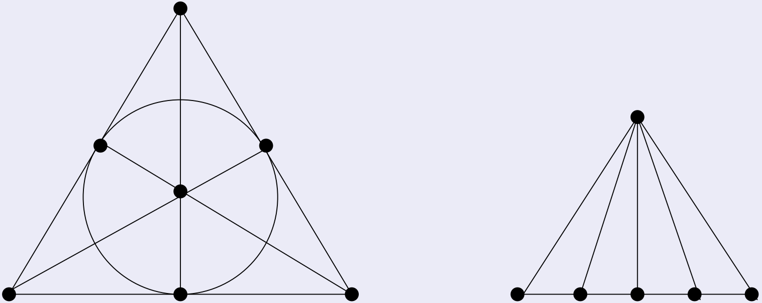
What to expect in this talk?

Block designs are (finite) configurations of points and blocks (lines) that satisfy certain additional requirements. Study of block designs initially began due to their importance in the statistical theory of design of experiments. These configurations were later found to be extremely useful in many other mathematical branches such as coding theory and finite group theory. Finite geometries, which are geometries over finite fields and similar finite algebraic structures provide examples of good block designs that also satisfy additional regularity conditions. The talk will mainly focus on author's work on symmetric designs (which are designs with equally many points and blocks), quasi-symmetric designs (which have two block intersection numbers) and related strongly regular graphs and some classification theorems related to these objects.

Block Design or Just a Design

By an incidence structure, we mean a triple, consisting of the set of points, the set of blocks (a block is nothing but a distinguished subset of the point-set) and the incidence (a point belongs or does not belong to a block). An incidence structure is called a design (balanced incomplete block design or a 2-design) if every block has a constant size k, which is strictly less than v, the number of points and any two points occur together (are commonly contained in) the same number λ of blocks. If v is the number of points, b the number of blocks and r the number of blocks containing a given point, then such a configuration is called a (v, b, r, k, λ)-design or sometimes also called a (v, k, λ)- design.

Fano Plane



Fisher Inequality

A non-trivial (one in which the block size is less than the number of points) satisfies the following basic inequality:

Fisher inequality We always have $v \leq b$, i.e., the number of points is less than or equal to the number of blocks. Further if D is a design with $v = b$, the incidence structure in which blocks are points and points are blocks is also a design with the same parameter set (v, k, λ).

Fisher Inequality

A non-trivial (one in which the block size is less than the number of points) satisfies the following basic inequality:

Fisher inequality We always have $v \leq b$, i.e., the number of points is less than or equal to the number of blocks. Further if D is a design with $v = b$, the incidence structure in which blocks are points and points are blocks is also a design with the same parameter set (v, k, λ).

Symmetric Design

A design with $v = b$ is called a symmetric design

Fisher inequality asserts that the dual of a symmetric design is also a symmetric design. In fact, we have:

Symmetric Design

A design with $v = b$ is called a symmetric design

Fisher inequality asserts that the dual of a symmetric design is also a symmetric design. In fact, we have:

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Theorem The following are equivalent for any design D.

1. D is a symmetric design.
2. $r = k$.
3. Any two blocks of D intersect in λ points.
4. The dual of D is also symmetric design.

For the reasons of structural symmetry and better connections with group theory, symmetric designs are objects of considerable interest.

Hadamard Symmetric Designs

Let H denote a Hadamard matrix of order $4t$. This is a matrix of order $4t$ with entries ± 1 such that any two rows of H are orthogonal. Multiplying rows/columns by -1 does not change the Hadamard property and hence we can assume w.l.o.g. that H is in a standard form. That is the first row and the first column of H consist only of $+1$'s. Then deleting the first row and the first column of H and changing -1's to zeros, we get an incidence matrix of a $(v, k, \lambda) = (4t-1, 2t-1, t-1)$ symmetric design which is called a Hadamard symmetric design. This procedure is reversible and hence the existence of a Hadamard matrix and a Hadamard symmetric design go hand in hand.

Projective Designs

We have already seen the special example of Fano plane. In general, we can look at a projective space of dimension 2 over $GF(q)$ and declare its points as points and its lines as blocks of a symmetric design. This is called a projective plane and has parameters $(q^2 + q + 1, q + 1, 1)$. This construction works for every prime power q. More generally, we may take an n-dimensional projective space over $GF(q)$ and declare its points as points and its hyperplanes as blocks of a symmetric design. This is called a projective design and has parameters

$$v = \frac{q^{n+1} - 1}{q - 1}, \; k = \frac{q^n - 1}{q - 1}, \; \lambda = \frac{q^{n-1} - 1}{q - 1}$$

Projective Designs

We have already seen the special example of Fano plane. In general, we can look at a projective space of dimension 2 over $GF(q)$ and declare its points as points and its lines as blocks of a symmetric design. This is called a projective plane and has parameters $(q^2 + q + 1, q + 1, 1)$. This construction works for every prime power q. More generally, we may take an n-dimensional projective space over $GF(q)$ and declare its points as points and its hyperplanes as blocks of a symmetric design. This is called a projective design and has parameters

$$v = \frac{q^{n+1} - 1}{q - 1}, \; k = \frac{q^n - 1}{q - 1}, \; \lambda = \frac{q^{n-1} - 1}{q - 1}$$

Existence Question of Symmetric De sings

Many constructions of symmetric designs are known. The existence question for Symmetric designs is the question of constructing a $(0, 1)$-matrix satisfying the matrix equations given above. Algebraic number theory has been employed in order to answer this existence question and the relevant seminal result is called the Bruck-Ryser-Chowla theorem . Unfortunately, it works only in one direction. That is, it provides us with only a necessary condition which, may not be sufficient. For example, it is not known whether there is a projective plane of order twelve but it is known, thanks to the Bruck-Ryser-Chowla theorem that

If q is the order of a projective plane such that $q \equiv 1, 2 \ (mod\ 4)$ then q is a sum of two integer squares. In particular, there are no projective planes of orders q such that $q \equiv 6 \ (mod\ 8)$.

The non-existent plane of order ten

An extensive search for almost 200 hours on the fastest CRAY computer available then proved in the late 1980s that there is no projective plane of order ten.

Constructions

There have also been a large number of new constructions of new symmetric designs in recent times. Based, in terms of ideas, on an earlier work of an Africa settled Indian named Dinesh Rajkundlia, Ionin in the last decade constructed new families of symmetric designs many of which were open questions for a long time. About 23 infinite families of symmetric designs are known.

On all the Known Constructions

- When $\lambda = 1$, we have a projective plane of order q with parameters $(q^2+q+1, q+1, 1)$. These exist for every prime power q. No other examples are known.
- When $\lambda = 2$, we have a biplane with parameters $(\binom{k}{2}+1, k, 2)$. These are known to exist for the following values of k: $3, 4, 5, 6, 9, 11, 13$. No other examples are known.
- When $\lambda = 3$, all the known examples have k bounded by 15.
- When $\lambda \geq 4$, all the known examples have k bounded by $\lambda^2 + \lambda$.

On all the Known Constructions

- When $\lambda = 1$, we have a projective plane of order q with parameters $(q^2 + q + 1, q + 1, 1)$. These exist for every prime power q. No other examples are known.
- When $\lambda = 2$, we have a biplane with parameters $(\binom{k}{2} + 1, k, 2)$. These are known to exist for the following values of k: $3, 4, 5, 6, 9, 11, 13$. No other examples are known.
- When $\lambda = 3$, all the known examples have k bounded by 15.
- When $\lambda \geq 4$, all the known examples have k bounded by $\lambda^2 + \lambda$.

On all the Known Constructions

- When $\lambda = 1$, we have a projective plane of order q with parameters $(q^2+q+1, q+1, 1)$. These exist for every prime power q. No other examples are known.
- When $\lambda = 2$, we have a biplane with parameters $(\binom{k}{2}+1, k, 2)$. These are known to exist for the following values of k: $3, 4, 5, 6, 9, 11, 13$. No other examples are known.
- When $\lambda = 3$, all the known examples have k bounded by 15.
- When $\lambda \geq 4$, all the known examples have k bounded by $\lambda^2 + \lambda$.

On all the Known Constructions

- When $\lambda = 1$, we have a projective plane of order q with parameters $(q^2 + q + 1, q + 1, 1)$. These exist for every prime power q. No other examples are known.
- When $\lambda = 2$, we have a biplane with parameters $(\binom{k}{2} + 1, k, 2)$. These are known to exist for the following values of k: $3, 4, 5, 6, 9, 11, 13$. No other examples are known.
- When $\lambda = 3$, all the known examples have k bounded by 15.
- When $\lambda \geq 4$, all the known examples have k bounded by $\lambda^2 + \lambda$.

Conjectures

M.Hall's conjecture: $\forall\lambda \geq 2$, there exist only finitely many symmetric (v, k, λ).
Stronger:$\forall\lambda \geq 4$, k satisfies $k \leq \lambda^2 + \lambda$.

The Design Extension Problem

Symmetric designs with parameters (v, k, λ) where k equals $q^2 + q$ and λ equals q are also related to the famous design extension theorem of Cameron. We will refrain from discussing the actual statement of Cameron extension theorem since it is connected with the original problem of permutation group extensions.

Non-isomorphism questions

An isomorphism ϕ between two symmetric designs D_1 and D_2 is a pair (ϕ', ϕ'') of two permutations, the first from the point-set of D_1 to the point-set of D_2 and the second from the block-set of D_1 to the block-set of D_2 such that the incidence is preserved. When D_1 equals D_2 this is called an automorphism and it is easily seen that the set of automorphisms of a symmetric design form a group. This is one way in which we can actually construct a symmetric design from a group. This is called the method of difference set. For example developing the initial block $(0, 1, 3)$ modulo 7 gives us all the 7 blocks of the Fano plane.

Numbers of non-isomorphic Symmetric Designs

Producing a large number of non-isomorphic symmetric designs (with the same parameters) is a pertinent question. This question was first handled in the case of Hadamard symmetric designs by Bhat-Nayak , Shrikhande and Singhi. For the case of projective designs (the point-hyperplane incidence structure), this was done first by Kantor and later by Jungnickel. In both the cases, the lower bounds are asymptotically exponential.

Designs of Ahrens Szekeres Type

Designs of Ahrens-Szekeres type, are those designs with $k = \lambda^2 + \lambda$. Among various lower bounds proved in a paper by Gharge and S, one is in terms of Catalan numbers and one is in terms of special partitions of integers. Since both these numbers are exponential, the established lower bound is also exponential. We conclude by pointing that there is a marked difference between techniques employed by the earlier authors (Shrikhande, Singhi, Jungnickel) and those in the recent paper. In the former situation, techniques are recursive while in the latter situation they are direct and depend on graph isomorphisms as well as partition functions in number theory.

Take a design D, not necessarily symmetric. An integer x is called a block intersection number of D if we have two blocks X and Y the cardinality of whose intersection is x. Which numbers occur as block intersection numbers of a design? Thanks to the proof of Fisher's inequality, we see that D has exactly one block intersection number iff it is a symmetric design.

A design with two block intersection numbers x and y (with $x < y$ by convention) is called a Quasi-symmetric design.

Reasons for studying quasi-symmetric designs are many. A mundane and practical reason is that symmetric designs are more difficult to study (this is not completely true but sometimes believed to be so). On a more serious level quasi-symmetric design allows one to construct its block graph which in most cases of interest can be shown to be strongly regular. Finally quasi-symmetric designs are connected with combinatorial configurations arising out of finite simple groups.

A design with two block intersection numbers x and y (with $x < y$ by convention) is called a Quasi-symmetric design.

Reasons for studying quasi-symmetric designs are many. A mundane and practical reason is that symmetric designs are more difficult to study (this is not completely true but sometimes believed to be so). On a more serious level quasi-symmetric design allows one to construct its block graph which in most cases of interest can be shown to be strongly regular. Finally quasi-symmetric designs are connected with combinatorial configurations arising out of finite simple groups.

An Example

Let D be a point-block incidence structure constructed from $AG(n, q)$ an affine geometry of dimension n over a field with q elements by taking as points the points of the geometry and as blocks all the affine hyperplanes (where $n \geq 2$). Parameters of D as a quasi-symmetric design are:

$$v = q^n, \quad k = q^{n-1}$$

$$\lambda = q^{n-2}, \quad x = 0, \quad y = q^{n-2}$$

One More Example

Let D be a point-block incidence structure constructed from $PG(n,q)$ a projective geometry of dimension n over a field with q elements by taking as points the points of the geometry and as blocks the subspaces of codimension two (where $n \geq 3$). Parameters of D as a quasi-symmetric design are:

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{n-1}-1}{q-1}$$

$$\lambda = \frac{q^{n-1}-1}{q-1}, \quad x = \frac{q^{n-3}-1}{q-1}, \quad y = \frac{q^{n-2}-1}{q-1}$$

One More Example

Let D be a point-block incidence structure constructed from $PG(n, q)$ a projective geometry of dimension n over a field with q elements by taking as points the points of the geometry and as blocks the subspaces of codimension two (where $n \geq 3$). Parameters of D as a quasi-symmetric design are:

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{n-1}-1}{q-1}$$

$$\lambda = \frac{q^{n-1}-1}{q-1}, \quad x = \frac{q^{n-3}-1}{q-1}, \quad y = \frac{q^{n-2}-1}{q-1}$$

Witt Design

There are other classes of examples particularly the affine geometries (where $x = 0$) There is also a classical object called the Witt design on 23 points which is associated with the Mathieu group M_{23} on 23 letters.

Block Graph

Define the block graph Γ of a quasi-symmetric design D by taking as vertices of Γ the blocks of D. Make two vertices adjacent iff the corresponding blocks intersect in x points. Let N denote the incidence matrix of D and A, the adjacency matrix of Γ. Recall that we have already established the following matrix equations:

$$NN^t = (r-\lambda)I\ \lambda J, \quad N^tJ = kJ, \quad NJ = rJ$$

Block Graph

Define the block graph Γ of a quasi-symmetric design D by taking as vertices of Γ the blocks of D. Make two vertices adjacent iff the corresponding blocks intersect in x points. Let N denote the incidence matrix of D and A, the adjacency matrix of Γ. Recall that we have already established the following matrix equations:

$$NN^t = (r-\lambda)I \ \lambda J, \quad N^tJ = kJ, \quad NJ = rJ$$

Here, D is quasi-symmetric and hence the following matrix equation connects N^tN and A:

$$\begin{aligned} N^tN &= kI + xA + y(J - I - A) \\ &= (k-y)I + (x-y)A + yJ \end{aligned}$$

Here, D is quasi-symmetric and hence the following matrix equation connects N^tN and A:

$$\begin{aligned} N^tN &= kI + xA + y(J - I - A) \\ &= (k-y)I + (x-y)A + yJ \end{aligned}$$

Since N^tN commutes with J it follows that A also commutes with J which is just the same thing as saying that Γ is a regular graph. If we can now show that besides the degree of regularity, A has exactly two other eigenvalues, then Γ must be a strongly regular graph. But NN^t and N^tN have the set of non-zero eigenvalues. So, N^tN has eigenvalues $rk, r-\lambda$ and 0. The eigenvalue rk is a simple eigenvalue of N^tN that corresponds to the largest simple eigenvalue of A which is also the degree of regularity of Γ. Hence A has exactly two other eigenvalues proving that the block graph is strongly regular.

The fact that under the mild condition that the block graph and its complement be connected is sufficient to frame the study of quasi symmetric designs in terms of strongly regular graphs has some nice consequences. If one treats a symmetric design as a degenerate (or limiting) case of a quasi symmetric design, then a coauthored result of mine shows that for a fixed pair $(x, y) = (0, y)$ of block intersection numbers, if we let $k \to \infty$, then the resulting structure has to turn out to be a symmetric design showing in some sense that:

A formulation of M. Hall conjecture for the general class of quasi symmetric designs with $x = 0$ is not considerably harder than Hall conjecture for symmetric designs and thus the real difficulty lies in the symmetric case.

A large number of results proved in the last thirty years are around the theme outlines on the previous slides, Among these is the classification result for quasi-symmetric 3-designs in terms of a certain Diophantine equation and its use in studying the 4-design problem that was solved by Ray-Chaudhuri and Wilson. Some of these are listed on the next slide.

1. Quasi-symmetric 2,3,4-designs. Combinatorica 7 (1987), no. 3, 291-301
2. Finiteness questions in quasi-symmetric designs. J. Combin. Theory Ser. A 42 (1986), no. 2, 252-258
3. Quasi-symmetric designs and biplanes of characteristic three. J. Combin. Theory Ser. A 60 (1992), no. 1, 104-116
4. A short proof of a conjecture on quasi-symmetric 3-designs. Discrete Math. 96 (1991), no. 1, 71-74

1. Quasi-symmetric 2,3,4-designs. Combinatorica 7 (1987), no. 3, 291-301
2. Finiteness questions in quasi-symmetric designs. J. Combin. Theory Ser. A 42 (1986), no. 2, 252-258
3. Quasi-symmetric designs and biplanes of characteristic three. J. Combin. Theory Ser. A 60 (1992), no. 1, 104-116
4. A short proof of a conjecture on quasi-symmetric 3-designs. Discrete Math. 96 (1991), no. 1, 71-74

1. Quasi-symmetric 2,3,4-designs. Combinatorica 7 (1987), no. 3, 291-301
2. Finiteness questions in quasi-symmetric designs. J. Combin. Theory Ser. A 42 (1986), no. 2, 252-258
3. Quasi-symmetric designs and biplanes of characteristic three. J. Combin. Theory Ser. A 60 (1992), no. 1, 104-116
4. A short proof of a conjecture on quasi-symmetric 3-designs. Discrete Math. 96 (1991), no. 1, 71-74

1. Quasi-symmetric 2,3,4-designs. Combinatorica 7 (1987), no. 3, 291-301
2. Finiteness questions in quasi-symmetric designs. J. Combin. Theory Ser. A 42 (1986), no. 2, 252-258
3. Quasi-symmetric designs and biplanes of characteristic three. J. Combin. Theory Ser. A 60 (1992), no. 1, 104-116
4. A short proof of a conjecture on quasi-symmetric 3-designs. Discrete Math. 96 (1991), no. 1, 71-74

1. Some characterizations of quasi-symmetric designs with a spread. Des. Codes Cryptogr. 3 (1993), no. 2, 155-166
2. The structure of triangle-free quasisymmetric designs. Discrete Math. 64 (1987) no. 2-3, 199-207
3. A characterization of projective subspaces of codimension two as quasi-symmetric designs with good blocks. Discrete Math. 306 (2006), no. 14, 1493-1501
4. On a class of quasi-symmetric designs. J. Combin. Math. Combin. Comput. 57 (2006), 103-106

1. Some characterizations of quasi-symmetric designs with a spread. Des. Codes Cryptogr. 3 (1993), no. 2, 155-166
2. The structure of triangle-free quasisymmetric designs. Discrete Math. 64 (1987) no. 2-3, 199-207
3. A characterization of projective subspaces of codimension two as quasi-symmetric designs with good blocks. Discrete Math. 306 (2006), no. 14, 1493-1501
4. On a class of quasi-symmetric designs. J. Combin. Math. Combin. Comput. 57 (2006), 103-106

1. Some characterizations of quasi-symmetric designs with a spread. Des. Codes Cryptogr. 3 (1993), no. 2, 155-166
2. The structure of triangle-free quasisymmetric designs. Discrete Math. 64 (1987) no. 2-3, 199-207
3. A characterization of projective subspaces of codimension two as quasi-symmetric designs with good blocks. Discrete Math. 306 (2006), no. 14, 1493-1501
4. On a class of quasi-symmetric designs. J. Combin. Math. Combin. Comput. 57 (2006), 103-106

1. Some characterizations of quasi-symmetric designs with a spread. Des. Codes Cryptogr. 3 (1993), no. 2, 155-166
2. The structure of triangle-free quasisymmetric designs. Discrete Math. 64 (1987) no. 2-3, 199-207
3. A characterization of projective subspaces of codimension two as quasi-symmetric designs with good blocks. Discrete Math. 306 (2006), no. 14, 1493-1501
4. On a class of quasi-symmetric designs. J. Combin. Math. Combin. Comput. 57 (2006), 103-106

It is strange and pathetic that not too many tools are available for the studying quasi-symmetric designs. Among the most powerful tool that gives a necessary condition for the existence of a strongly regular graph are the Krein conditions. These have been applied to the study of quasi-symmetric designs with some success. Besides graph theory, another important tool is coding theory. It is perhaps true that the subject, despite several constructions, is still at its beginning stage and more tools for constructions may evolve in time to come.

THANK YOU VERY MUCH