THESIS

IMPRIMITIVELY GENERATED DESIGNS

Submitted by

Aaron Lear

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Summer 2022

Master's Committee:

Advisor: Anton Betten

Henry Adams
Aaron Nielsen

ABSTRACT

IMPRIMITIVELY GENERATED DESIGNS

Designs are a type of combinatorial object which uniformly cover all pairs in a base set V with subsets of V known as blocks. One important class of designs are those generated by a permutation group G acting on V and single initial block $b \subset V$. The most atomic examples of these designs would be generated by a primitive G. This thesis focuses on the less atomic case where G is imprimitive.

Imprimitive permutation groups can be rearranged into a subset of easily understood groups which are derived from G and generate very symmetrical designs. This creates combinatorial restrictions on which group and block combinations can generate a design, turning a question about the existence of combinatorial objects into one more directly involving group theory. Specifically, the existence of imprimitively generated designs turns into a question about the existence of pair orbits of an appropriate size, for smaller permutation groups.

This thesis introduces two restrictions on combinations of G and b which can generate designs, and discusses how they could be used to more efficiently enumerate imprimitively generated designs.

TABLE OF CONTENTS

Chapter 1

The title

Notation note

Function application is on the right. The set X's powerset is denoted $X\mathcal{P}$. The size k subsets of X are denoted $\binom{X}{k} \subset X\mathcal{P}$.

1.1 What are designs?

A $2-(v,k,\lambda)$ design D (which "design" will refer to in this paper) is a combinatorial structure consisting of a base set V with v elements and a set of subsets $B \subset \binom{V}{k} \subset V\mathcal{P}$ (called blocks) each of size $2 \leq k < v$, such that $\forall x \neq y \in V$ there exist exactly λ many $b \in B$ such that $x, y \in b$.

A design encapsulates the concept of taking subsets from a set of objects while making sure every pair of objects is "connected equally" by those subsets. Specifically when the subsets must have uniform size. This concept has some direct connections to real situations which will be discussed later.

1.2 What is imprimitive?

Note that all groups G in this paper are assumed to be permutation groups with underlying set Ω_G.

A transitive permutation group G is imprimitive when there is a nontrivial partition of Ω_G which is preserved by all $g \in G$. Another way of saying this is that the underlying set can be divided into disjoint subsets (called imprimitivity classes) and if two points are together in one of those classes then all $g \in G$ must map them together inside a class.

An imprimitive G must permute all the partition classes transitively because G is transitive on points inside those classes. Meaning in particular that the classes must be the same size. So

imprimitive groups can be thought of as partitioning Ω_G into classes $c_i \in C$. All elements of G permute each c_i in some way, and then permute the c_i.

1.3 What is "ly generated"?

A permutation group G on the base set V and a subset $b \subset V$ generate the block set $bG = \{bg : g \in G\}$. Since the base set is implied every design can be treated as equivalent to a block set. And every block set corresponds to a design if and only if every pair of points in V is contained by the same number of blocks $b' \in bG$. Designs which can be generated in this way are called imprimitive designs.

So the paper is about finding initial V, $b \subset V$, and imprimitive $G \leq Sym_V$ for which bG uniformly contains $\binom{V}{2}$. This is not the same as finding all designs, or even all designs generated from one block, but that would be hard so we'll go with this.

Chapter 2

Wreath products

A wreath product $G \wr H$ is a group on the base set $\Omega_G \times \Omega_H$. It consists of all ways to first permute each copy of Ω_G by (possibly different) $g \in G$ and then permute the copies by $h \in H$.

Noteably, for a set $V = X \times Y$, the wreath product $Sym_X \wr Sym_Y$ is the maximum subgroup of Sym_V defining $X \times Y$ as an imprimitivity partition. Every imprimitive group is a subgroup of some $Sym_X \wr Sym_Y$.

Formally, group elements $w \in G \wr H$ can be identified with one $h \in H$ in addition to a choice function $f : \Omega_H \to G$ where $jf = g_j \in G$. Then w is defined as the permutation associated with (f, h) whose action on $(i, j) \in \Omega_G \times \Omega_H$ is $(i, j)w = (i(jf), jh) = (ig_j, jh)$.

This means that given two group elements $w_1, w_2 \in G \wr H$ corresponding respectively to $(f_1, h_1), (f_2, h_2)$, the composition $w_1 w_2$ is the permutation taking (i, j) to $(i(jf_1)((jh_1)f_2), jh_1h_2)$. This permutation corresponds to (f, h_1h_2) where f is defined by $(j)f = (jf_1)((jh_1)f_2)$.

2.1 Explicit design construction

Knowing that all imprimitive designs are generated by a subgroup of some wreath product ensures that all imprimitive designs can be generated in the following way. The notation will be used throughout the paper.

Choose a set c and and index set $C = \{1, 2, ..., n\}$. The underlying set is defined as the set product $V = c \times C$. Since C represents a partition of V into imprimitivity classes, $c_i \subset V$ will denote the subset $(c \times \{i\}) \subset (c \times C)$.

Choose a point transitive permutation group $G \leq Sym_c \wr Sym_C$. Choose a subset $b \subset V$. Then the block set is defined as $bG = \{b \cdot g : g \in G\}$.

Chapter 3

Powersets and graphs

When discussing combinatorial objects powersets are inevitably important. Relating them to specific graphs can be convenient.

$X\mathcal{P}$ can be viewed as a hypercube with vertex set $X\mathcal{P} \cong {\mathbb{F}_2}^X$ and an edge between two vertices iff the corresponding sets differ by one element. Ie one set is the other union a singleton. This is known as the Hamming space of dimension $|X|$. (Unfortunately the Hamming graph is something else.) The Hamming distance between sets $x, y \in X\mathcal{P}$ is the length of a shortest path between x and y in the Hamming space. Since each such path consists of removing all elements of $x - y$ and adding all elements $y - x$, one element per edge, the Hamming distance is equal to $|x| + |y| - 2|x \cap y|$.

A similar family of graphs, known as Johnson graphs, have their vertex set restricted to $\binom{X}{n}$ for some n with an edge between sets x and y iff their intersection is size $n - 1$. Ie their Hamming distance is 2. More generally the distance in a Johnson graph is the Hamming distance divided by 2.

Chapter 4

General facts about designs

Some basic facts about designs won't be used in this paper but may be helpful for more general understanding of designs:

Given a point $x \in V$ there are $v-1$ pairs $\{x,y\} \in \binom{V}{2}$ containing x. Each of these are contained in λ blocks. Blocks will be repeated $k-1$ times in the multiset of blocks containing a pair containing x. So the axioms and parameters of a design already determine $r = \frac{\lambda(v-1)}{k-1}$, an additional parameter describing how many blocks any point is contained in.

Going further, there are vr combinations of a $b \in B$ and a $v \in b$ (these are known as "flags"). Dividing out redundancy again $|B| = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)}$. The equation can alternatively be seen by thinking of a design as a bipartite graph with vertex sets V and B, and with an edge between $x \in V$ and $b \in B$ iff $x \in b$. The number of edges can then either be counted as vr or $|B|k$.

Fisher's Inequality states that for any design, $|B| \geq |V|$. Or equivalently that $r \geq k$. The truth of the inequality is equivalent to the claim that every subset $B \subset \binom{V}{k}$ of size $|B| < v$ covers $\binom{V}{2}$ unevenly (for $2 \leq k < v$). The following proof also provides an alternate characterization of designs relevant to applications.

Theorem 1 (Fisher's Inequality [1])**.** *A design has* $|V| \leq |B|$.

Proof. One equivalent way to define a block set is letting B be an abstract set and choosing points from $B\mathcal{P}$. An injective function $f : V \to B\mathcal{P}$ can be viewed as choosing which blocks contain a particular point.

The set of blocks which contains any pair $\{x,y\} \in \binom{V}{2}$ is exactly the intersection of xf and yf in $B\mathcal{P}$. Uniform coverage is equivalent to there being some λ such that every intersection of two points in Vf is in $\binom{B}{\lambda}$.

It was previously seen that any design must have some constant r such that any $Vf \subset \binom{B}{r}$. If there are two points in $\binom{B}{r}$ and the intersection of two points is in $\binom{B}{\lambda}$, then the distance between the two points is the constant $2(r - \lambda)$.

In summary any block set which can be a design corresponds to some equidistant subset of a Johnson graph on $\binom{B}{r}$. A design must fulfill the additional requirement that every $b \in B$ has the same number of points in it so this isn't an exact equivalence. But additional requirements are not necessary for the proof because it's already true that there is no equidistant subset $X \subset \binom{B}{r}$ such that $|X| > |B|$.

Each element x of a uniformly d Hamming distance set $X \subset {\mathbb{F}_2}^B \cong B\mathcal{P}$ serves as a constraint on any other point $w \in {\mathbb{F}_2}^B$ being d Hamming distance from every element of X. For a given $x \in X$ this constraint on a variable $w \in {\mathbb{F}_2}^B$ is expressible as $|\{b \in B : bx \neq bw\}| = |\{b \in B : bx + bw = 1\}| = d$. These constraints can be viewed similarly to linear equations where the values of all but one of the outputs in $\{b \in B : bx \neq 1\}w$ determine the last value. The expansion of the constraints to linear equations allows an analogy to dimension.

Embedding $\mathbb{F}_2$ into $\mathbb{Z}$ (ie sending 0 and 1 in $\mathbb{F}_2$ to 0 and 1 in $\mathbb{Z}$) allows an equivalent formulation of the constraints. Namely, given $x, w \in {\mathbb{F}_2}^B \subset \mathbb{Z}^B$, w is d Hamming distance from x iff it satisfies the equation $\sum_{b \in B} bx + bw - 2(bx) \cdot (bw) = d$, where bw are variables describing w's coordinates in $\mathbb{Z}^B$ and bx are constants 0 or 1 determined by x's coordinates.

Given the assumption that x and w both have r many 1 coordinates (meaning they are both in the embedded $\binom{B}{r}$) the equation simplifies to $r - d/2 = \sum_{b \in B}(bx) \cdot (bw) = \sum_{b:bx=1} bw$. So the constraint on vertices of a Johnson graph of being d Hamming distance from x when embedded in the $|B|$-dimension module $\mathbb{Z}^B$ is equivalent to a linear function defining a $|B| - 1$ dimension hyperplane in the module. The set of points which are d Hamming distance from all of X is the intersection of these hyperplanes and the embedded ${\mathbb{F}_2}^B$.

When considering an equidistant set X with distance d, the distance constraint of any $x \in X$ is not implied by the constraints for $X - \{x\}$. In particular x is not d distance from itself. So each hyperplane does reduce the dimension of the intersection by at least 1. The restriction to the

embedding of ${\mathbb{F}_2}^B$ also suggests another restriction given by the equation $\sum_{b \in B} bw = r$, which must be independent if there is a solution to the system of the other equations inside of ${\mathbb{F}_2}^B$.

If $w \notin X$ but is d distance from it then there must be $|B| + 1$ independent linear equations on the $|B|$ many variables bw, a contradiction.

□

The interesting point is that there is an analogue of "dimension" of $\binom{B}{r}$ scaling with the size of the base set $|B|$ and not affected by r, for $0 < r < |B|$.

Chapter 5

History and connections

5.1 Finite geometry

The Greeks reasoned by starting from a list of assumed axioms and manipulating them to ensure their further statements were correct. Euclid produced a list of axioms for standard Euclidean geometry in what might now be seen as $\mathbb{R}^2$, such as one could draw on a sheet of papyrus.

From a modern perspective Euclid's original axioms might be found wanting. He defined a point as "that which has no part" and a line as "breadthless length". Slightly more usefully he related points and lines by saying

- The ends of a line are points.
- A straight line is a line which lies evenly with the points on itself.
- Parallel straight lines are straight lines which, being in the same plane and being produced indefinitely in both directions, do not meet one another in either direction.

So lines contain points and a pair of points defines a straight line. Also, parallel lines exist and all other lines intersect. These two ideas would become the foundation of modern geometry.

After Georg Cantor invented set theory in the 1870s it became a popular topic to more rigorously state mathematical problems in terms of axioms about symbols representing sets. Moritz Pasch gave the first modern axiomatization of Euclidean geometry in *Vorlesungen über neuere Geometrie*, declining to define points except as elements of a set, of which lines are subsets. In particular straight lines of Euclidean geometry are defined as sets which intersect in at most one point. Furthermore parallel pairs of lines which intersect at no point exist and satisfy further axioms.

Standard projective geometry is a modification of Euclidean geometry in which all lines meet at some point. This topic was invented by Pappus of Alexandria and became widely studied by

Renaissance artists who wanted to understand perspective as the projection of a 3d world onto 2d human vision caused parallel lines to come together in the distance. Projective geometry was also given modern axiomatizations, replacing the axioms about parallel lines in standard geometry with the requirement that all lines intersect in exactly one point.

Later on Gino Fano began applying modern geometrical axiomatization of projective planes to finite base sets. Along with some non-triviality assumptions and his assumption that all lines have the same size k, a finite projective plane is a finite set V and a set of subsets $B \subset \binom{V}{k}$ (called lines) which satisfy the following axioms:

- Any two distinct points are contained together in exactly one line.
- Any two distinct lines have exactly one point in their intersection.

The study of finite projective planes superseded affine ones presumably because the projective plane axioms are more symmetrical and were considered prettier. However finite affine planes are closely related to finite projective planes, with it being possible to convert between an instance of either type of object and an instance of the other. So in some sense it doesn't really matter.

Eventually, finite geometry grew into a more general combinatorial subfield: the study of finite axiomatic structures often defined using some variant of "points" and "lines" but with axioms differing from those for traditional geometry. The axioms were often informed by specific problems so that the set of resultant mathematical objects were the possible solutions to the problem

One problem stated previously to the 1870s paradigm shift towards formal logic was Kirkman's schoolgirl problem, which was given in 1850. It stated "Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast." The solution to this problem and most generalizations became known as Steiner systems, which are designs with $\lambda = 1$. (If you want your young ladies to walk such that any size t subset is only allowed λ many times as opposed to any pair of them you actually want a t-design.) Eventually, problems more practical than micromanaging the social lives of schoolgirls were found to be related to designs, leading to them being a major topic in combinatorics.

This paper specifically discusses block transitive, point imprimitive designs (ie designs generated by an imprimitive G). Most (but not all) known examples of this type of finite projective plane are isomorphic to the Desarguesian finite projective planes (finite projective planes obtained by modifying a vector space). Verifying this is nontrivial even for planes with bounded parameters, and won't be discussed in detail.[2] However it is notable that despite other techniques being used to classify "small" transitive, imprimitive finite projective planes, the same concept of "inner and outer pairs" introduced by Delandtsheer and Doyen to study block transitive, point imprimitive designs[3] is still foundational to the proof. So the invention of combinatorial designs has contributed back to the study of classical finite geometry.

5.2 Experiment design

Widespread study of 2-designs originated from Ronald Fisher's investigation into formally optimizing scientific experiments.[4]

Ideally, a scientific experiment will isolate every independent variable possibly influencing the outcome and vary it while keeping every other variable fixed. However, in reality limitations on resources and experiment specific restrictions will often make such an experiment impossible to carry out. For instance when doing medical testing it can be difficult to find a large enough set of monozygotic siblings or human clones to provide identical test conditions. This is exacerbated when attempting to study the interaction between multiple variables. To get complete information on how n variables interact it would be necessary to run a number of tests scaling exponentially with n.

Fisher's idea was that in cases where complete uniformity or symmetry is not possible it is still desirable to distribute the inconsistencies in a regular manner so that their effect might be mitigated or gauged. He discovered that a variety of combinatorial structures, including designs, could be used to mathematically optimize this "regularity" depending on assumptions about the specific experiment.

For a specific example of an experiment which 2-designs are relevant to: When testing combinations of fertilizer composition and plant variety for crop yields it is important to test all combinations simultaneously to control for weather, and to have sufficiently large plots for a decent sample size. However it is simultaneously desirable to limit the area used in the experiment to minimize the variance of geography and soil composition.

To account for geography and soil an experimenter might decide not to organize their crops in the most obvious manner (ie contiguous plots containing each fertilizer and plant combination). Instead they could decide their primary concern is to compare the yields of different fertilizer/plant combinations and make the assumption that simultaneous changes to the geography or soil inside their experiment won't reverse the comparative inequality between yields of pairs of fertilizer/plant combinations. Then one way to improve their experiment would be dividing plots into k subsections and planting a different combination in each. The goal would be to make sure every pair of distinct combinations is together in some plot so that they can be compared while accounting for geography. To help mitigate their assumption they could even organize the experiment such that any two combinations are present in $\lambda > 1$ plots together so that they could analyze trends in comparative yield changing with geography. Furthermore in order to maximize the minimum amount of data on any pair it might be desirable to make λ a constant and have all pairs present in exactly λ plots.

More abstractly the set of plant/fertilizer combinations V and the set of plots B can be viewed as vertices of a bipartite graph. Determining the specifics of the experiment is equivalent to choosing edges between those sets indicating that a combination is going to be planted in a given plot. The axioms defining a design correspond to desired properties of the experiment. The requirement than any pair from V be adjacent to a $b \in B$ means they would be planted in the same plot and could be compared while accounting for geography. The requirement that all pairs are adjacent to exactly λ many b means all pairs can be compared in λ many different plots.

This means that using a graph corresponding to a combinatorial design will achieve the experimenter's goals. Conversely, having goals equivalent to all the axioms of a combinatorial structure

will mandate finding an instance of that structure in order to meet those goals. (Technically a further assumption has to be made to force a satisfactory experiment to be a design. Different plots could have the same fertilizer/plant combinations planted and would still be distinct. But two sets containing the same elements are axiomatically the same set.)

The experiment's compartmentalization can be taken further. Instead of testing all combinations of fertilizer and plant it might be necessary to only take a sampling of combinations. But a design can define a relation between the set of plant types and the set of fertilizers such that any two fertilizers are simultaneously applied to λ many types of plant and can be compared that way. It may be impossible to grow all necessary pairs simultaneously but arranging the growing periods with a design can ensure that pairwise comparisons still exist. Etc.

Of course this is not perfect. Testing a function on only a subset of its inputs does not provide all information about the function. Experiments can only be simplified if the outcome function has some kind of property which allows untested outcomes to be inferred from the set of tested outcomes, or if only some information about the outcome function is required. But conversely if such properties or limitations are present then brute force testing each input might be redundant and testing a subset of inputs could provide the same information more efficiently.

5.3 Error correcting codes

Discussion of lost and redundant information may be reminiscent of information theory and error correcting codes. Discussion of equidistant subsets of Hamming spaces may have been more so. In fact designs are relevant here too.

When electronically transmitting data as a sequence of ones and zeros (ie an element of $\{0,1\}^n$) bits will occasionally get flipped. To deal with this when trying to communicate a particular sequence $s \in \{0,1\}^n$ the sender will convert it into a longer sequence $s* \in \{0,1\}^m$ where the extra bits contain redundant information. This way if a bit gets flipped the inconsistency with redundant information will alert the receiver. With enough redundant information the receiver will even be able to figure out which bit was flipped and the original $s*$ which was sent. And reversing the

conversion from $s*$ to s they will know the intended message. Conversions of sequences s to $s*$ with properties that allow retrieval of the original s even when $s*$ has bits flipped are known as error correcting codes.

When considering binary sequences of length m it is common to view them as graph with vertex set $\{0,1\}^m$ (the vertices being referred to as 'words' or 'strings') and an edge between two vertices when they differ in exactly one coordinate, known as the Hamming space of dimension m. This is the same Hamming space discussed relating to powersets, since $\{0,1\}^m$ is isomorphic to the powerset of an m element set. The Hamming distance between any two words in the graph is equivalent to the minimum number of bits that must be flipped to convert one sequence to the other. An error correcting code can be viewed as a selection of vertices or "code words" in a Hamming space chosen by a function $* : \{0,1\}^n \to \{0,1\}^m$.

The method of finding a valid code word $s*$ from an arbitrary sequence $w \in \{0,1\}^m$ is to find the code word with minimum Hamming distance from w. Since it is assumed that bits are flipped with low probability the closest code word is the most likely sequence to have been sent given what was received. Ideally every point in the m-dimensional Hamming space will be within some constant c edges of exactly one code word. Such a code is called "perfect" and is desirable because it allows every possible received word to be converted to a unique $s \in \{0,1\}^n$ which was the most probable original message. The set of words within c edges of $s*$ are also known as the c-radius ball around $s*$.

As was previously seen designs correspond to equidistant (specifically distance $2(r-\lambda)$) subsets of a Hamming space $X \subset B\mathcal{P}$. (Again note that additional conditions are required, meaning the converse is not necessarily true.) Which makes them not only error correcting codes, but good ones (assuming X is large and most received strings are covered in some ball) that "spread out" their error correction as much as possible. The fact that $X \subset \binom{B}{r}$ gives them the additional property that they have the same Hamming distance from the word of all 0's (known as Hamming weight). Such codes are called constant weight codes.

Note that having some bias in sent encoded messages can change the expected effectiveness of error correction. If all messages sent are constant weight then it doesn't matter if a code is bad at correcting a sufficiently asymmetric received string. Such a code will have less error correcting ability when transmitting the same amount of original information with the same number of message bits, compared to a perfect code. However other benefits may outweigh this consideration.

Having constant weight can be desirable in applications where transitions between states are used to convey information in a continuous medium as opposed to easily parsable discrete strings. For instance when the sender and receiver of a signal don't share a reliable clock a larger number of transitions can help the receiver judge the intended time interval between different bits of information. There can also be other medium specific advantages. For instance when communicating with radio signals people will sometimes alter their frequencies in a predetermined way over the course of a message, to prevent eavesdropping. If there is a known average of expected wavelengths it can help the receiver calibrate and better match the sender's frequencies.

5.4 Explicit examples

Example 1. *Fix any vertex set V and a natural number k such that $2 \leq k \leq |V|$. Let $B = \binom{V}{k}$. Then the design D defined by V and B is the complete hypergraph with edges of size k. By symmetry all pairs of vertices are contained in the same number of edges so it is a design. This is also known as a trivial design.*

Example 2. *Let the vertex set V be divided into two equal sized subsets $V_1 \cup V_2 = V$, $|V_1| = |V_2| = |V|/2 = n$. Let $k = 3$ and $B = \{X \cup Y | X \in \binom{V_1}{2}, Y \in \binom{V_2}{1}\} \cup \{X \cup Y | X \in \binom{V_1}{1}, Y \in \binom{V_2}{2}\}$. That is, B consists of all pairs from V_1 and one element from V_2, and vice versa. The pairs of elements both in one of V_1, V_2 are contained in exactly n blocks. The pairs of elements one each from V_1, V_2 are contained in $2(n-1)$ blocks. So V and B form a design iff $n = 2(n-1)$, meaning $n = |V_1| = |V_2| = 2$.*

Example 3. *Let the vertex set V be divided into two equal sized subsets $V_1 \cup V_2 = V$, $|V_1| = |V_2| = |V|/2 = n$. Let $5 \leq k \leq |V|$ and $B = \{X \cup Y | X \in \binom{V_1}{2}, Y \in \binom{V_2}{k-2}\} \cup \{X \cup Y | X \in$*

$\binom{V_1}{k-2}, Y \in \binom{V_2}{2}\}$. *That is,* B *consists of all pairs from* V_1 *together with all order* $k-2$ *subsets of* V_2*, and vice versa. The pairs of elements both from* V_1 *or* V_2 *are contained in the same number of blocks. (Specifically in* $\binom{n}{k-2} + \binom{n-2}{k-4}\binom{n}{2}$ *blocks.) The pairs of points with one each from* V_1 *and* V_2 *are contained in the same number of blocks. (Specifically in* $2\binom{n-1}{1}\binom{n-1}{k-3}$ *blocks.) So* V, B *form a design iff* $\binom{n}{k-2} + \binom{n-2}{k-4}\binom{n}{2} = 2\binom{n-1}{1}\binom{n-1}{k-3}$. *It turns out one solution to this equation is* $n = 8$*,* $k = 6$.

The automorphism groups of the last two designs are $Sym_n \wr Sym_2$ because they are the freest possible designs which preserve a given partition of an initial block.

Chapter 6

Proving things about designs

Since the defining characteristic of designs is uniform covering of $\binom{V}{2}$, a natural approach to proving something about a design is to partition $\binom{V}{2}$ and then prove things about the partition. Specifically, if X and Y partition $\binom{V}{2}$, then any design satisfies three properties.

- X must be covered uniformly.
- Y must be covered uniformly.
- X and Y must be covered the same amount, on average.

If a condition contradicts any of these properties for any partition of $\binom{V}{2}$ then it must not be present in a design.

6.1 G is point transitive

For an example of this, consider a corollary of Block's Lemma[1] (name unrelated). Block proved a more general fact about linear algebra but this paper presents a proof which is more thematically consistent with future proofs.

Theorem 2. *If bG is a design then G must be transitive.*

Proof. If G is not transitive then it respects a partition $X \sqcup Y = V$. This naturally extends to a partition of $\binom{V}{2}$ with three sets. $\binom{X}{2}$, $\binom{Y}{2}$, and $\binom{V}{2} - \binom{X}{2} - \binom{Y}{2}$. The last set being all pairs with one element from X and the other from Y. G must also respect this partition, since it fixes X and Y setwise.

Similarly $b \subset V$ is partitioned into $b \cap X$ and $b \cap Y$; which extends to a partition of $\binom{b}{2}$ into $\binom{b\cap X}{2}$, $\binom{b\cap Y}{2}$, and $\binom{b}{2} - \binom{b\cap X}{2} - \binom{b\cap Y}{2}$.

For every $g \in G$, bg covers the partition of $\binom{V}{2}$ in the same ratio as b, since bg has the same number of points in X and Y. This means bG cumulatively covers the partition in the same ratio as b does.

A necessary requirement for $\binom{V}{2}$ to be covered uniformly by bG is that its partition subsets are covered proportionally to the number of elements in each subset. This is equivalent to the requirement that $\binom{|X|}{2} : \binom{|Y|}{2} : |X||Y|$ is the same triple ratio as $\binom{|b\cap X|}{2} : \binom{|b\cap Y|}{2} : |b \cap X||b \cap Y|$.

This can't be true. There are no numbers $m' > m$ and $n' > n$ such that $\binom{m}{2} : \binom{n}{2} : mn$ is equal to $\binom{m'}{2} : \binom{n'}{2} : m'n'$. To see this note that $\binom{n}{2}$ scales sub-quadratically while mn scales quadratically. If $\binom{n'}{2} = k^2\binom{n}{2}$ then $\frac{n'}{n} > k$. Meaning that if $\binom{m'}{2}$ and $\binom{n'}{2}$ both increase by a factor of k^2 then $\frac{m'n'}{mn} > k^2$.

□

An intuitive interpretation of this result is that, even up to scaling, the distribution of pairs in a partitioned set is uniquely determined by the set and partition sizes. Thus a block distribution respecting asymmetry in the underlying set (in the sense of the intersection size of blocks with a partition being invariant) can not be uniform when covering pairs from the underlying set. Since designs are defined in terms of uniformly covering pairs from the underlying set this means no such block distribution can be a design.

Chapter 7

Combinatorial restrictions on designs

7.1 Existence

The values $|c|$, $|C|$, and the numerical distribution of b's k points as subsets of c_i already determine whether an imprimitive, block transitive design with those parameters exists, even without considering any group theory. This is because those values determine whether b covers pairs inside of and between different c_i in the same ratio as those types of pairs exist in all of V.

Delandtsheer and Doyen introduced the idea of using "inner pairs" and "outer pairs" as a partition of $\binom{V}{2}$ to study imprimitive designs.[3] Given $V = c \times C$, the inner pairs $pair_{in}$ are all pairs $\{x, y\} \in \binom{V}{2}$ such that $x, y \in c_i$ for some i. All remaining pairs are the outer pairs $pair_{out}$; $\{x, y\} \in \binom{V}{2}$ s.t. $\exists c_i \neq c_j$ with $x \in c_i$ and $y \in c_j$.

Any block b contains some number of inner and outer pairs denoted $b_{in} = |\binom{b}{2} \cap pair_{in}|$ and $b_{out} = |\binom{b}{2} \cap pair_{out}|$. Any group G preserving C as a partition also preserves the sets $pair_{in}$ and $pair_{out}$ in $\binom{V}{2}$. Therefore all blocks $b' \in bG$ in the orbit of b under G have $b'_{in} = b_{in}$ and $b'_{out} = b_{out}$. This implies that any set of blocks which are generated by G must cover inner and outer pairs of C in the same ratio as any one of the blocks. Ie any pair in $pair_{in}$ will be covered b_{in} times by bG for every b_{out} times bG covers a pair in $pair_{out}$.

Note that $|pair_{in}| = |C||\binom{c}{2}|$ and $|pair_{out}| = |\binom{C}{2}||c|^2$. So a necessary condition for bG to evenly cover all pairs of elements in V is that $b_{in} : b_{out} = |C||\binom{c}{2}| : |\binom{C}{2}||c|^2$. In reduced form $b_{in} : b_{out} = |c| - 1 : (|C| - 1)|c|$.

Lemma 1. *An imprimitively generated block set bG covering the inner and outer pairs proportionally to the size of those sets is equivalent to the truth of $\frac{b_{out}}{b_{in}} = \frac{(|C|-1)|c|}{|c|-1}$.*

The same condition is also sufficient for the existence of an imprimitive design. Specifically, $B = b(Sym_c \wr Sym_C)$ is completely symmetrical relative to C. Any block in B corresponds to another block in B given any permutations of C and the c_i. This implies B covers all of $pair_{in}$ the

same number of times and all of $pair_{out}$ the same number of times. So B defines a design if and only if both sets of pairs are covered proportionally to their size.

7.2 Bounds on design parameters

Recall that for a $2-(v,k,\lambda)$ design λ refers to the number of times any pair in $\binom{V}{2}$ is covered, $v = |V|$, and $k = |b|$ (any block).

Theorem 3 (Delandtsheer, Doyen [3])**.** *Let bG be a design, with imprimitive G. Let $c \times C \cong V$ define imprimitivity classes of G with $|c| \geq 2$ and $|C| \geq 2$.*

Then there exist positive integers m and n such that $|c| = \frac{\binom{k}{2}-n}{m}$ and $|C| = \frac{\binom{k}{2}-m}{n}$. Furthermore, n is the number of inner pairs contained in b and $m|c|$ is the number of outer pairs contained in b.

The parameters m and n are called Delandtsheer-Doyen parameters and the range of their possible values over designs is sometimes studied. Rearranging the Delandtsheer-Doyen parameter formulas implies that if $|c| \cdot |C| = |V| > (\binom{k}{2} - 1)^2$, no m and n satisfying the formula exist. This is therefore an upper bound on the possible size of block transitive, imprimitive designs with a given block size.

The theorem's initial implications about the Delandtsheer-Doyen parameters were already effectively covered during the discussion of inner and outer pairs:

Any pair of the triple values $|c|$, $|C|$, and $|V|$ fixes a ratio $|pair_{in}| : |pair_{out}|$. Similarly any pair of $n = b_{in}$, $m|c| = b_{out}$, and $k = |b|$ fixes $b_{in} : b_{out}$. So any pair of parameters from one triple and a single parameter from the other triple determines necessary values of all parameters, in order for those parameters to describe a valid design. The statement is specifically providing the determined n and $m|c|$, given the triple of values $|c|$, $|C|$, and k. And of course both n and $m|c|$ must be integers.

The remaining implication of the theorem is that m must be an integer. Ie b_{out} must be a multiple of $|c|$. This follows from the fact that $b_{in} : b_{out} = (|c|-1) : (|C|-1)|c| = \frac{|c|-1}{|C|-1} : |c|$, since $|c|$ and $|c|-1$ don't share factors.

The specific bound Delandtsheer and Doyen produced isn't immediately intuitive. However, recall the proof of Theorem 2 demonstrated that the possible ratios of partition sets are uniquely determine by $|V|$. Something similar is true here, except that instead of a ratio only being possible once it is only possible finitely many times.

The inner:outer pair ratio $\frac{|pair_{out}|}{|pair_{in}|} = \frac{(|C|-1)|c|}{|c|-1}$ is mostly determined by $|C|-1$, and adjusted slightly with multiplication by $\frac{|c|}{|c|-1}$. The possible contributions of different $|c|$ are $\frac{x+1}{x}$ for natural numbers $x \geq 1$ and so in particular are always within a factor of 2. This means that there is no choice of different $|c|$ such that partitions with $|C| = x$ and $|C| > 2x$ will have the same inner:outer ratio.

There are only finitely many ways to partition k points, with each choice producing an inner:outer pair ratio. This determines the possible values of $|c|$ and $|C|$ which also produce that ratio, and there are basic bounds like the one above showing that values for $|c|$ and $|C|$ which are too far apart can not produce the same ratio. So the specific bounds aside, it's not surprising that a bound exists and there are only finitely many block transitive, point imprimitive designs for a given k.

Often, people are interested in finding designs with a specific parameters instead of the existence of more general designs discussed in this paper. In particular finite projective planes are designs with $\lambda = 1$. Better bounds may exist when restricting the particular v, k, and λ values considered.

Chapter 8

The Universal Embedding Theorem

Recall $c_i \subset V = (c \times C)$ denotes the subset $(c \times \{i\}) \subset (c \times C)$.

Consider an arbitrary transitive, imprimitive permutation group $G \leq Sym_c \wr Sym_C$. Let H be the permutation group defined by G's induced action on C. Let G_X denote the subgroup of G which fixes $X \subset V$ setwise. Then for any $c_i \subset c \times C$ let $N_i \leq Sym_c$ be the permutation group defined by G_{c_i}'s action on c_i. (Technically G_{c_i} is acting on c_i and N_i is defined under the bijection $c \cong c_i$.)

Up to isomorphism N_i is actually independent of i. Ie the action of G_{c_i} on c_i is isomorphic to the action of G_{c_j} on c_j. This is because G is transitive and preserves the partition $\{c_1, ..., c_i, ..., c_j, ..., c_{|C|}\}$, so there is an element $g \in G$ mapping the c_i elements to the c_j elements, meaning $G_{c_i} = gG_{c_j}g^{-1}$ and G_{c_j} are conjugates.

The Universal Embedding Theorem relates G with the N_i and H defined from G.

Theorem 4 (Universal Embedding Theorem; Krasner, Kaloujnine [5][6])**.** *Given a point transitive* $G \leq Sym_c \wr Sym_C$ *and* $i \in C$*:*

$G \cong G' \leq N_i \wr H \leq Sym_c \wr Sym_C$.

Proof. Recall all $g \in Sym_c \wr Sym_C$ can be associated with a pair $g \sim (f, h) \in {Sym_c}^C \times Sym_C$. Each pair consists of a choice function $f : C \to Sym_c$ choosing one permutation $jf \in Sym_c$ per $j \in C$ and also a single permutation $h \in Sym_C$. Conversely every distinct (f, h) permutes $c \times C$ in a distinct way. Intuitively the pairs correspond to internally permuting each of the $|C|$ copies of c and then permuting the copies. That is, the action of g on $c \times C$ can be viewed as independently acting on each $c_i \cong c$ with the permutation $if \in Sym_c$, and then permuting the indices by h.

The main idea of this proof is to permute the c_j such that they "line up" the isomorphic $N_j \cong N_i$ with each other. Meaning for any $c_j \neq c_i \subset V$ there exists a $(f, h) \sim g' \in G'$ st $jh = i$ and $jf = id_{Sym_c}$. Which would then imply easy conjugation of multiplication by the permuted N_j.

This will be accomplished by choosing a group element for each $j \neq i$ which defines an "identity mapping" from c_i to c_j.

Explicitly, for each $j \neq i$ there is some group element $g_j \in G$ with a corresponding $h_j \in H$ such that $jh_j = i$. Fix one such g_j for all $j \neq i$ and let g_i be id_G. Denote the pair associated with g_j as $g_j \sim (f_j, h_j)$.

Then define a permutation $\phi : V \to V$ which permutes each c_j by sending all $(x, j) \in (c \times \{j\})$ to $(x(jf_j), j)$. ϕ induces an automorphism of $Sym_c \wr Sym_C$ by permuting the underlying set.

One convenient way to represent this is to view ϕ as an element of $Sym_c \wr Sym_C$. Specifically, the $(f, h) \sim \phi$ has $h = id_H$ and for all j, $jf = jf_j$. Then ϕ defines a map $\Phi : Sym_c \wr Sym_C \to Sym_c \wr Sym_C$ by $g\Phi = \phi^{-1} g \phi$, a conjugation of $Sym_c \wr Sym_C$. As a conjugation Φ maps $G \leq Sym_c \wr Sym_C$ to an isomorphic subgroup $G' = G\Phi$ and all that is necessary for the theorem to be true is that $G' \leq N_i \wr H$.

The set of (f, h) which are associated with a $g \in N_i \wr H$ is easily defined. They are exactly the pairs such that $h \in H$ and $\forall j \in C$, $jf \in N_i$. Now consider arbitrary $(f, h) \sim g \in G$. To see that $(f', h) \sim \phi^{-1} g \phi \in G'$ does have all $jf' \in N_i$, consider any arbitrary j and let $jh = k$. So $jf' = (jf_j)^{-1}(jf)(kf_k)$.

But this is also how $g_j^{-1} g g_k$ permutes c_i. Broken apart, g_j^{-1} maps the i coordinate to j while permuting c_i by the inverse of the way g_j permutes c_j as it is sent to c_i. Then g permutes by jf while sending j to k, and g_k permutes by kf_k when sending k back to i. All of g_j, g, and g_k are elements of G so $g_j^{-1} g g_k$ is also an element of G. And the composition fixes i, so $g_j^{-1} g g_k \in G_{c_i}$, meaning $(jf_j)^{-1}(jf)(kf_k) \in N_i$.

□

In fact something stronger is true. Φ was not only an isomorphism but a "permutational isomorphism". That is an isomorphism induced by a bijection between the underlying sets of G and G' as permutation groups.

8.1 Why were we talking about this?

Permutationally isomorphic groups will generate isomorphic block sets (when the initial block is also moved by the permutation). In this case the Universal Embedding Theorem shows that any point transitive $G \leq Sym_c \wr Sym_C$ is effectively contained in the wreath product $N_i \wr H$. And only groups with this property must be considered to generate all imprimitive designs, up to isomorphism. For notational convenience, from now on let all $G \leq N \wr H \cong N_i \wr H$ (since the distinction between N_i doesn't matter to designs, up to isomorphism).

The structure of bG closely echoes that of G. The simplification of G's structure to something resembling $N \wr H$ is therefore helpful when describing its action on an initial block and allows a description of bG analogous to $N \wr H$.

Chapter 9

Group actions on blocks

9.1 Describing arbitrary imprimitive permutation groups

Consider the structure of $G \leq N \wr H$ from the perspective of $(f, h) \sim g \in G$. Since $G \leq N \wr H$, f is a choice of one $p \in N$ per $i \in C$. Since G is transitive, for every $i, j \in C$ there is a guaranteed $(f, h) \sim g \in G$ such that $ih = j$. Because N is the action of G on any fixed c_j, for each $p \in N$ and $j \in C$ there exists $(f', h') \sim g' \in G$ such that $jh' = j$ and $jf' = p$. Composing these produces a group element gg' which takes an arbitrary c_i to arbitrary c_j while permuting by any arbitrary $p \in N$.

In some sense this means G acts on V similarly to $N \wr H$. G can map every c_i just as freely as $N \wr H$ does. And because of this it also maps each c_i in some way that no $K \wr H$ can for $K \lneq N$. The only difference between G and $N \wr H$ is that while $N \wr H$ can permute each c_i in an arbitrary way simultaneously (it is completely free given the constraints of permuting each c_i by a $p \in N$ and C by $h \in H$), G potentially has further restrictions on how it maps multiple $c_i \neq c_j \in C$ at the same time.

One way of describing this is that the set of $(f, h) \sim g \in N \wr H$ is all of $N^C \times H$. Ie the set of all pairs with any $f \in N^C$ and $h \in H$. By contrast $(f, h) \sim g \in G$ might be restricted to f in some subset $F \subset N^C$. In fact there is further possible complexity.

Example 4. *For this example let C_n be the permutation group which acts as a cycle on $n \geq 3$ elements. Let the dihedral group D_n be the permutation group which is generated by that cyclic permutation group and an additional element which "flips" the cycle in the usual way.*

Consider the group $D_n \wr D_3$. The set of $(f, h) \sim g \in D_n \wr D_3$ is the complete set of pairs with a function from $\{1, 2, 3\}$ to D_n and $h \in D_3$. Now consider the subset of pairs $(f, h) \in S \subset D_n \wr D_3$ where for all $i \in \{1, 2, 3\}$, $if \in C_n$ if and only if $h \in C_3$. So conversely $if \in D_n - C_n$ iff

$h \in D_3 - C_3$. The set S does not contain all $f \in {D_n}^{\{1,2,3\}}$ since there exists f with $1f \in C_n$ and $2f \notin C_n$.

It can be verified that S corresponds to a transitive strict subgroup $G < D_n \wr D_3$ and that the $N \wr H$ defined from G is $D_n \wr D_3$.

The example shows that not only could the set of functions f which are part of a pair $(f, h) \sim g \in G$ be restricted, the restriction might not be uniform and could vary further with h.

Inspired by this, for a given $G \leq N \wr H$ and any set $X \subset H$ let F_X denote the set of f such that there exists $h \in X$ with $(f, h) \sim g \in G$. Also let $F = F_H$.

Then some previously discussed facts can be expressed as follows. (Recall $H_{\{i\}}$ is the subgroup of H stabilizing i.)

- $\bigcup_{h \in H} F_{\{h\}} = F \subset N^C$.
- For all $i \in C$, $\{if : f \in F_{(H_{\{i\}})}\} = \{if : f \in F\} = N$.
- $G \cong \bigcup_{h \in H}(F_{\{h\}} \times \{h\}) \subset N^C \times H \cong N \wr H$.
- $G = N \wr H$ iff $\forall h \in H$, $F_{\{h\}} = N^C$.

The natural action of G on $\bigcup_{h \in H}(F_{\{h\}} \times \{h\})$ (ie itself) has any $(f, h) \sim g \in G$ map the set $F_{\{h'\}} \times \{h'\}$ injectively into the set $F_{\{h'h\}} \times \{h'h\}$. Since inverses exist this creates a bijection between $F_{\{h'\}}$ and $F_{\{h'h\}}$. More generally any $F_{\{h\}}$ and $F_{\{h'\}}$ have equal size.

Then a corollary of the above facts gives an easy description of the difference between any G and the corresponding $N \wr H$.

- For all $h \in H$, $|F_{\{h\}}| = |F_{\{id_H\}}|$.
- $G = N \wr H$ iff $F_{\{id_H\}} = N^C$.

9.2 A limitation of this description

However, the set $F_{\{id_H\}}$ does not determine $G < N \wr H$.

Example 5. *Let $N = D_n$ with $n \geq 3$. Let H be any permutation group with a subgroup $H' < H$ of order $|H'| = \frac{|H|}{2}$. Let $F_{\{id_H\}}$ be the set of $f \in {D_n}^C$ such that $if \notin C_n$ for an even number of $i \in C$. Now consider the set of pairs $S = \{(f, h) \in N^C \times H : f \in F_{\{id_H\}} \iff h \in H'\}$. That is, all permutations in $D_n \wr H$ where an even number of cycles were reversed and the set of cycles was permuted by $h \in H'$, as well as all permutations where an odd number of cycles were reversed and the set of cycles was permuted by $h \in H - H'$.*

It can be verified that S corresponds to a transitive strict subgroup $G < D_n \wr H$ and that the $N \wr H$ defined from G is $D_n \wr H$.

In particular, S is exactly the set of (f, h) where f and h have the same parity (in the respective senses of reversing an even number of cycles / being contained in H'). Given an initial permutation (f_1, h_1), further permuting by any $(f_2, h_2) \in S$ will change the parity of the number of reversed cycles exactly when $f_2 \notin F_{\{id_H\}}$ and multiplication by h_2 swaps h_1 between the two cosets of H' in H exactly when $h_2 \notin H'$. So permutations $g \in G \cong S$ maintain the relationship between these two types of parity and G is closed under multiplication.

The example shows that for fixed $N = D_n$ and base set C, groups G with the same $F_{\{id_H\}}$ can be defined using an arbitrary H and subgroup of size $|H'| = \frac{|H|}{2}$. In particular, some H have multiple, non-isomorphic subgroups of that size. Using these for the example construction creates non-permutationally isomorphic G defining the same N, H, and $F_{\{id_H\}}$.

9.3 Representing blocks

Initial blocks b can be defined by a choice of some subset of c, for each i. Denote the elements of b in the i coordinate as $b_i = \{x \in c : (x, i) \in b\}$. The possible images of b_i under the action of N are b_iN, the setwise orbit of b_i. This could also be viewed as N acting on $b_i \in c\mathcal{P}$.

Similarly to how group elements $g \in G$ correspond to (f, h) with $f : C \to N$, the blocks $b \subset V$ correspond to $w : C \to c\mathcal{P}$, which maps coordinates i to sets $b_i = iw$. Alternatively, w can be augmented by $h \in H$ to more easily keep track of the image bG of an initial b. This notation simply uses h to keep track of permutations of coordinates instead of permuting the outputs of w.

Explicitly, $(w, h) \in (c\mathcal{P})^C \times H$ is the block b such that $b_i = (ih^{-1})w$. Ie the block b defined by taking the b' with $b'_i = iw$ and permuting the coordinates of b' by h. This augmented definition is how blocks will be described in this paper.

Note that, unlike the correspondence between (f, h) and g, the correspondence between (w, h) and b is not a bijection. Different (w, h) could still correspond to the same block since a particular permutation need not change a given set.

9.4 Acting on blocks

The augmented definition allows for an easier description of the block set generated by $(w, h_1) \sim b$ when acted on by a group of $(f, h_2) \sim g \in G$. For any $(w, h_1) \sim b$ and $(f, h_2) \sim g$, the image $bg \sim (w, h_1) \cdot (f, h_2)$ is a new block (w', h_1h_2) where $iw' = (iw)((ih_1)f) = b_{ih_1}((ih_1)f)$.

Starting from an initial $b \sim (\{i \to b_i\}, id_H)$ and given any $g \sim (f, h)$, this means that $bg \sim (\{i \to b_i(if)\}, h)$. Using the previous section's description of G, $bG \cong (\{i \to b_i\}, id_H)(\bigcup_{h \in H}(F_{\{h\}} \times \{h\})) = \{(\{i \to b_i(if)\}, h) : h \in H, f \in F_{\{h\}}\}$.

(With the caveat that elements of bG might be represented redundantly over all combinations of h and f.)

9.5 Redundancy

Something to note about the caveat is that the redundancy is the result of elements of G fixing b setwise. Ie $G_{\{b\}}$ could be a nontrivial subgroup. In this case, the fact that G transitively generates bG means that every other block in bG is fixed by a conjugate subgroup of $G_{\{b\}}$.

One implication of this uniform redundancy is that it has no effect on uniform pair coverage. The pairs in $\binom{V}{2}$ are covered uniformly by the multiset $[(\{i \to b_i(if)\}, h) : h \in H, f \in F_{\{h\}}]$ iff they are covered uniformly by bG. Each pair is just covered $|G_{\{b\}}|$ as many times. So one possible strategy to find designs is to first find multisets generated by b and $\bigcup_{h \in H}(F_{\{h\}} \times \{h\})$ which uniformly cover pairs, and then later eliminate duplicates.

9.6 Converting block sets to pair orbits

The block multisets can be viewed as G acting on b to generate the orbit bG while distinguishing resulting blocks which were generated by different $g \in G$. (In the future this paper will refer to these as "multi-orbits" and denote them $[bG]$.) Doing this results in a block multiset satisfying the coverage axioms iff the corresponding block set does. This means that uniform coverage can actually be determined by the size of the subset of G which takes an initial b to cover a given pair in $\binom{V}{2}$ (or the reverse).

The size of the subset of $\bigcup_{h \in H} W_{\{h\}} \times \{h\}$ which covers an arbitrary pair $r \in \binom{V}{2}$ is equal to the number of group elements $(f, h) \sim g \in G$ which takes an initial $b \in \bigcup_{h \in H} W_{\{h\}} \times \{h\}$ to an image $bg \supset r$. Each of these g corresponds to a $g^{-1} \in G$ which takes r to an image $rg^{-1} \subset b$. So all pairs $\binom{V}{2}$ are covered a uniform number of times by the block set bG iff all pair multi-orbits of G's action on $\binom{V}{2}$ contain the same number of subsets of b. And this happens iff the number of $g \in G$ such that $rg \subset b$ is the same for all $r \in \binom{V}{2}$.

Lemma 2. *Given $b \sim (\{i \to b_i\}, id_H)$ and $G \cong \bigcup_{h \in H} F_h \times \{h\}$:*

The block set bG defines a design iff the multiset $[(\{i \to b_i(if)\}, h) : h \in H, f \in F_{\{h\}}]$ covers all pairs in $\binom{V}{2}$ the same number of times. That multiset covers a given $r \in \binom{V}{2}$ once for each $g \in G$ such that $r \subset bg$.

The observation that uniform pair coverage can be equated to proportional inclusion of pair orbits into b immediately has a nice corollary.[7] If bG is a design then G generates pair orbits which are contained in the same ratio by b. Adding additional permutations $g \in Sym_V$ to G can never break apart these orbits, only combine them. So any $G' > G$ also generates pair orbits that are covered in the same ratio by b, and all such bG' are also designs.

9.7 Describing arbitrary imprimitive block sets

It would be convenient to more succinctly list which functions $w = \{i \to b_i(if)\}$ create a valid block $(w, h) \sim b' \in bG$, for a given h. When the block set is generated by permutations $G \cong \bigcup_{h \in H}(F_{\{h\}} \times \{h\})$, the answer is the set $\{w = \{i \to b_i(if)\} : f \in F_{\{h\}}\}$. So for the

convenient list, define W_X to be $\{w = \{i \to b_i(if)\} : f \in F_X\}$. As before W will denote W_H. This definition relates each $f \in F_{\{h\}}$ with the $w \in W_{\{h\}}$ generated by f. Ie (w, h) is the image of b under the permutation (f, h). So $bG \cong \bigcup_{h \in H}(W_{\{h\}} \times \{h\})$ (up to redundancy).

The orbits $b_iN \subset \binom{c}{|b_i|}$ of each b_i over all blocks in bG have analogous restrictions to the permutations $N \leq Sym_c$ on c_i over all $g \in G$.

Under the action of both G and $N \wr H$, an arbitrary permutation in N can be applied to any $(b_i \times \{i\}) \subset c_i$, while moving c_i from the i to an arbitrary j coordinate. Since each coordinate can be permuted independently, $b(N \wr H)$ is the set of all possible pairs $(w, h) \in (c\mathcal{P})^C \times H$ such that w has only outputs $iw \in b_iN$. In other words, w is a choice of one element from b_i's orbit under N, for each i.

Denote this set of functions as $U = \{w = \{i \to b_i(if)\} : f \in N^C\}$. Note that this is a superset of $W = \{w = \{i \to b_i(if)\} : f \in F\}$ which is in turn a superset of all $W_{\{h\}} = \{w = \{i \to b_i(if)\} : f \in F_{\{h\}}\}$.

Echoing the relationship between G and $N \wr H$, bG is a subset of $b(N \wr H) \cong U \times H$. $W_{\{h\}}$ is the set of combinations of orbit elements that could actually have been arrived at given the action of $F_{\{h\}}$ on the chosen b_i, so it is a subset of U, which is all possible choices of an element from each orbit.

9.8 U as a choice of orbits

Note that U only actually depends on N and a choice of its induced set orbits in c (or equivalently induced orbits on $c\mathcal{P}$) to be defined. And conversely any $w \in U$ determines the same choice function of set orbits $\{i \to (iw)N\}$. Meaning U does not actually require specific b_i to be defined. So U is an implicit choice of orbits in $c\mathcal{P}$ without any relation to a specific original block b or group $G \leq N \wr H$.

To make this choice explicit, let U_i denote the orbit $(iw)N \subset c\mathcal{P}$ where w is an arbitrary element of U. Furthermore, let U be definable directly as a choice of orbits. Ie, given orbits $U_i \subset c\mathcal{P}$ of N's induced action on $c\mathcal{P}$, let $U = \{w \in (c\mathcal{P})^C : \forall i \in C(iw \in U_i)\}$.

This perspective is useful when attempting to find designs because it delays the more complicated choices of a $G \leq N \wr H$ and specific b until after the simpler ones of a $N \wr H$ and one of the many equivalent blocks under that very uniform group's action. Furthermore, recalling the section on redundancy, describing coverage in terms of orbits allows coverage to be measured with the size of subsets of G, rather than blocks.

Chapter 10

Converting to group theory

10.1 Recapping the problem so far

The goal is to find block transitive, point imprimitive designs. Ie designs generated from one initial block b and permutation group G, such that G acts imprimitively on the base set V, partitioning it into $c \times C$ (with the copies of c denoted c_i). It happens that groups which can generate such designs must be point transitive.

The existence of a design generated by b and the freest imprimitive group partitioning V into $c \times C$ (ie $Sym_c \wr Sym_C$) is purely combinatorial. It is completely determined by the ratio of "inner and outer pairs" when b is partitioned, compared to the ratio of inner and outer pairs in $c \times C$. The remaining question is which subgroups of $Sym_c \wr Sym_C$ produce distinct designs.

Any point transitive subgroup $G \leq Sym_c \wr Sym_C$ can be permuted into a subgroup of the closely related group $N \wr H \leq Sym_c \wr Sym_C$, where H is G's projection onto C and N is how G permutes any copy of c when it is not being exchanged with other copies. A notable implication is that for both G and $N \wr H$, any c_i can by permuted by any element of N while being sent to any c_j.

To consider all transitive, imprimitive permutation groups it is enough to consider all $N \wr H$ and let G be any transitive subgroup that satisfies the conditions:

- Its projection onto C is H.
- Any c_i can by permuted by any element of N while being sent to any c_j.

These are necessary and sufficient conditions for G to correspond to $N \wr H$ in the way defined by the Universal Embedding Theorem.

$N \wr H$ is the freest group with these properties and can be expressed as the set of all pairs $(f, h) \in N^C \times H$ where $h \in H$ determines how C is permuted and f is an independent choice of any $p \in N$ to permute each c_i by. Any other G considered is a subset.

For a given G, the f paired with a given $h \in H$ such that $(f, h) \sim g \in G$ are sets $F_{\{h\}} \subset N^C$. So $G \cong \bigcup_{h \in H} F_{\{h\}} \times \{h\}$. These $F_{\{h\}} \times \{h\}$ correspond to conjugates of the subgroup $F_{\{id_H\}} \times \{id_H\}$ and are the same permutations up to conjugation by an element of G. Given an initial block b, the set of blocks generated by $F_{\{h\}} \times \{h\}$ are $W_{\{h\}} \times \{h\}$ and any block set generated by G is $bG \cong \bigcup_{h \in H} W_{\{h\}} \times \{h\}$.

This representation may redundantly refer to blocks, but it will do so uniformly so that any uniform covering of $\binom{V}{2}$ by a transitively generated bG corresponds to a valid design.

A block can be viewed as a choice of a subset $b_i \subset c_i$ from each c_i. This can also be seen as a choice of orbits $U_i \subset c\mathcal{P}$, followed by a choice of element $b_i \in U_i$. The set of all choice functions from C into a determined set of orbits U_i is denoted U, and can be viewed as all possible choices of orbit elements after the orbits have been determined. $U \times H \cong b(N \wr H)$ for any block b defined by $b_i \in U_i$, and $U \times H$ contains all other block sets generated by b and $G \leq N \wr H$. (Since $U \times H = \bigcup_{h \in H} U \times \{h\} \supset \bigcup_{h \in H} W_{\{h\}} \times \{h\}$.)

So the initial goal is equivalent to looking for $G \leq N \wr H$ (satisfying the universal embedding conditions), a choice of $|C|$ many orbits U_i from N's induced action on $c\mathcal{P}$, and a block $b \sim (w, id_H) \in U \times H$, such that the pair orbits generated by G are contained in b the same proportion of times.

10.2 What was the point of that?

The point was that the property of all pair orbits being covered an equal proportion of times by b can be simplified using group theory. Specifically, the set of inner pairs and outer pairs can be considered separately. The resemblance of G to the very symmetrical $N \wr H$ allows pair orbits on the larger group G to be looked at as pair orbits in the smaller groups N and H.

Note that a choice of orbits $\{i \to U_i\}$ already determines the ratio of inner and outer pairs covered by blocks b with components $b_i \in U_i$. So choosing N and a choice of its set orbits U already determines the total inner-outer ratio.

This means that, given a choice of orbits U with an inner : outer ratio equal to that of $c \times C$, a block set generated by $b \sim (w, id_H) \in U \times H$ and $G \leq N \wr H$ is a design iff the set of inner pair multi-orbits all contain the same number of subsets of b and the same is separately true for outer pair multi-orbits.

10.3 Uniform covering of inner pairs

Inner pairs being covered uniformly can immediately be simplified.

The subsets of G taking c_i to various c_j are conjugate cosets. In particular, G can exchange the c_i without permutation, so the multi-orbit of $s \times \{i\} \subset c_i$ can be viewed as the same multi-subset of $c\mathcal{P}$, repeated in each coordinate. Specifically, the coset of G leaving c_i at c_i is a subgroup $G' \leq G$ and $[s(if) : (f, h) \sim g \in G'] \subset c\mathcal{P}$ exactly corresponds to the subset of $[s'g : g \in G]$ with elements in any fixed c_j (for nonempty s).

Furthermore, $[s(if) : (f, h) \sim g \in G'] \subset [c\mathcal{P}]$ is actually a multiple of the multiset $[sN] = [sp : p \in N]$. This follows from the fact that $\phi : G' \to N$ defined by $(f, h)\phi = if$ is a group homomorphism. $|G'|/|N|$ is a constant independent of the original s being considered so for the sake of verifying uniform inner pair coverage the multi-orbits $[s(if) : (f, h) \sim g \in G'] \subset [c\mathcal{P}]$ can be simplified and replaced by $[sp : p \in N]$.

The net result of these observations is that the multi-orbit of any inner pair $r \in \binom{c}{2}$ can be counted as $[rN] \times C$. The number of times this multi-orbit is contained by b will be the sum over all $i \in C$ of the number of times $[rN]$ is contained by b_i.

Lemma 3. *All inner pairs of $c \times C$ are evenly covered by bG (with $G \leq N \wr H$) if and only if*

$$\sum_{i \in C} |\{p \in N : rp \subset b_i\}|$$

is constant over all $r \in \binom{c}{2}$.

Note that this equivalence has nothing to do with a choice of specific $b \in U$. The multi-orbit $[rN]$ will intersect $u \subset c$ the same number of times for every $u \in U_i$ because N also transitively

generates U_i. The equivalence also has no connection to H. So doing all this has shown that only choices of $c \times C$, N, and U are relevant to uniform coverage of inner pairs. And recall, only $c \times C$ and the $|b_i|$ are relevant to the ratio of inner and outer pair coverage.

The benefit is that when searching for designs, restrictions on $c \times C$, N, and U can be considered first while verifying uniform inner pair coverage and inner/outer coverage ratio satisfy the requirements of a design. It is only necessary to check various $G \leq N \wr H$ and specific choices of b to determine whether a block set with uniform outer pair coverage exists, and this can occur after already eliminating any possibilities that violate any other restriction.

10.4 Uniform covering of outer pairs

It is still true that pair coverage can be expressed as the number of sets in a multi-orbit which are contained by b. So the immediate equivalent to outer pairs being uniformly covered is every outer pair multi-orbit $[\{v, v'\}G]$ containing the same number of subsets of $b \in U$.

10.4.1 Understanding outer pair orbits

Consider the outer pair multi-orbits generated by $N \wr H$. Without loss of generality each outer pair contains elements $(x_i, i), (x_j, j) \in c \times C$ with coordinates $i \neq j \in C$. The choice of i and j completely determine an orbit since each copy of c can be permuted independently by $N \wr H$. The outer pair orbits of $c \times C$ directly correspond to the pair orbits of H on its base set C.

Now consider the outer pair multi-orbits generated by an arbitrary $G \leq N \wr H$. These orbits are a partition of the orbits generated by $N \wr H$. Furthermore, the partition is uniform in a useful way.

Recall that G can equivalently be expressed as $\bigcup_{h \in H} F_{\{h\}} \times \{h\}$. So the multi-orbit generated by the pair $\{(x_i, i), (x_j, j)\}$ is:

$$[\{(x_i(if), ih), (x_j(jf), jh)\} : (f, h) \in \bigcup_{h \in H} F_{\{h\}} \times \{h\}]$$

An important observation is that because $|F_{\{h\}}|$ is independent of h, these pairs are evenly distributed between h. So any multi-orbit of outer pairs can be evenly projected onto the multi-orbit of the corresponding $\{i, j\}$ under the action of H.

10.4.2 Projecting onto C

Let any multi-subset $S \subset [\mathcal{P}(c \times C)]$ be "C-equivalent" to $S' \subset [\mathcal{P}(c \times C)]$ exactly when the multiset of their C coordinates is the same. (This will be referred to as "projecting onto C".) Similarly let $S \subset [\mathcal{P}(c \times C)]$ be "C-equivalent" to $S' \subset [\mathcal{P}C]$ when S' is exactly the projection of S onto C.

In particular two pair multi-orbits generated by G on V which project onto the same pair multi-orbit generated by H on C are "C-equivalent pair multi-orbits". $rG, r'G \in \binom{V}{2}$ are C-equivalent pair multi-orbits iff there are $i \neq j \in C$ such that both rG and $r'G$ contain a pair with one element in c_i and one element in c_j.

Specifically, C-equivalent pair multi-orbits will always project onto the same pair multi-orbit generated by H, with further multiplicity $|F_{\{h\}}|$.

Let $T \subset \binom{C}{2}$ be a pair orbit generated by H. Let R be the set of all pairs $r \in \binom{V}{2}$ which are C-equivalent to a pair $t \in T$. Ie R is the set of all outer pairs with C coordinates in the same H orbit. Another way of viewing R is as a pair orbit generated by $N \wr H$. Technically R is not C-equivalent to T, but T is a constant multiple away from being C-equivalent.

10.4.3 Restricting possible H

In order for each multi-orbit generated by G to be contained in a b the same number of times, the corresponding orbits must be contained in the same ratio. Because R is partitioned by these orbits, it is also necessary for all of R to be contained in that ratio. Since R is completely symmetrical given any specific choice of subsets $\{b_1, b_2, ...\}$, this condition is only dependent on the choice of values $\{|b_1|, |b_2|, ...\}$. This provides an intermediary restriction when determining which H can possibly be the projection of a G which generates a design.

The number of pairs in R contained by any b is $\sum_{\{i,j\}\in T} |b_i||b_j|$, and the total number of pair is $|c|^2|T|$. So the only possible H has all pair orbits T maintain that ratio. Also, $|c|^2$ is a constant and can be canceled when comparing ratios.

Lemma 4. *A necessary condition for bG (with $G \leq N \wr H$) evenly covering all outer pairs of $c \times C$ is that*

$$\frac{\sum_{\{i,j\}\in T} |b_i||b_j|}{|T|}$$

is constant over all pair orbits T defined by H's action on C.

Similarly to the previous requirement for inner pairs, this requirement has nothing to do with a specific choice of b or any other group. It can actually be decided prior to the condition on inner pairs because that depends on choosing orbits which b_i are in, while this condition only depends on $|b_i|$.

The main difference is that condition being an "if and only if" while this condition is a one directional "only if". To actually enumerate designs it will be necessary to find a better restriction on G and b. (Or just start checking the remaining options with brute force).

10.4.4 What is left to do?

The previous lemma corresponds to whether the "average" of all C-equivalent multi-orbit equivalence classes are covered uniformly by b. It would still be possible to satisfy the condition with a C-equivalent set of multi-orbits such that two members have a different number of elements contained in b, as long as the number of elements in b averages out over all orbits in the class. If the equation is satisfied then every C-equivalent set of orbits is in some sense covered uniformly compared to the others. The only remaining condition is that each set of orbits must internally be uniformly covered.

Lemma 5. *bG uniformly covers outer pairs if and only if the condition from the previous lemma is satisfied and every two C-equivalent outer pair orbits are contained the same proportion of times by b.*

$$\frac{|\{r \in O : r \subset b\}|}{|O|} = \frac{\sum_{\{i,j\} \in T} |b_i||b_j|}{|c|^2|T|}$$

This is not a very useful condition. Testing it directly would require determining every individual outer pair orbit's ratio of containment in b. That is the same brute force check that could have been done 10 pages ago immediately after realizing uniform pair coverage is equivalent to proportional containment of pair orbits. If that must be found anyway then the information gained from Lemma 4 is completely pointless.

So why did I waste so much of your time? One answer is that while the seperation of outer pair testing into Lemmas 4 and 5 is pointless from a purely mathematical standpoint there is a reason to do so from the perspective of computation.

10.5 An open ended question

It was probably always inevitable that outer pair coverage could not be simplified to the same extent as inner pair coverage. After all, specific choices of G and b presumably start to matter somewhere.

Because simplification is difficult, at this point design search becomes more open ended. Searching will improve alongside ability to select b and $G \leq N \wr H$ satisfying uniform outer pair coverage from other other choices that have not yet been eliminated, as well as ability to identify when b and G will create an already generated block set and avoid redundant computation.

Chapter 11

Result

11.1 Theorem

Combining previous lemmas produces the following theorem.

Theorem 5. *Let $G \leq Sym_c \wr Sym_C$ be a transitive permutation group acting imprimitively on the base set $V = c \times C$. Let $b \subset V$ be a block and bG the block set generated by G's action on b. Then:*

By the Universal Embedding theorem it may be assumed that $G \leq N \wr H$ where the projection of G satisfies the two conditions:

- *The projection of G onto C is H.*
- *G can permute any $c_i = c \times \{i\} \subset c \times C$ by any $p \in N$ while sending it to any c_j.*

The block set bG defines a design if and only if all the following are true:

1. *The ratio of outer and inner pairs is the same for $c \times C$ and b.*

   That is, let $out_V \subset \binom{V}{2}$ be the set of pairs with different C coordinates and in_V be the pairs with the same C coordinate. Let $out_b = out_V \cap \binom{b}{2}$ and $out_b = out_V \cap \binom{b}{2}$. Let $b_i \subset c$ be the c coordinates of elements of b which have coordinate i in the C coordinate. So $b_i \times \{i\} = b \cap c_i$. Then:

$$\frac{(|C|-1)|c|}{|c|-1} = \frac{|out_V|}{|in_V|} = \frac{|out_b|}{|in_b|} = \frac{\sum_{i<j \in C} |b_i||b_j|}{\sum_{i \in C} |\binom{|b_i|}{2}|}$$

2. *All outer pair orbits defined by $Sym_c \wr H$ acting on V are contained the same proportion of times by b.*

   Equivalently, the following expression is constant over pair orbits O of H's action on C.

$$\frac{\sum_{\{i,j\}\in O} |b_i||b_j|}{|O|}$$

3. *All inner pairs are contained the same number of times by bG.*

   Equivalently, the following expression is constant over a representative $r \in O$ of every pair orbit O generated by N's action on c.

$$\sum_{i\in C} |\{p \in N : rp \subset b_i\}|$$

4. *All outer pairs r contained in the same orbit $r(Sym_c \wr H)$ are covered an equal number of times by bG. In combination with requirement 2, this implies all outer pairs are covered the same number of times.*

   Equivalently, every outer pair orbit O generated by $G \leq N \wr H$ acting on V is contained by b the same proportion of times as the pair orbit T, generated by $Sym_c \wr H$, which contains O.

$$\frac{|\{r \in O : r \subset b\}|}{|O|} = \frac{\sum_{\{i,j\}\in T} |b_i||b_j|}{|c|^2|T|}$$

Proof. bG is a design if and only if all pairs $\binom{V}{2}$ are covered by the same number of blocks. Condition 1 is equivalent to inner and outer pairs being contained the same number of times "on average". Which is a necessary condition for uniform coverage overall. The equivalence with the given condition was seen for Lemma 1.

It is necessary for all inner pairs to be covered uniformly. The equivalence in Condition 3 was seen for Lemma 3.

It is necessary for all outer pairs to be covered uniformly. This was seen to be equivalent to the necessary and sufficient combination of Conditions 2 and 4, for Lemmas 4 and 5.

These three guarantees of uniform coverage combine to guarantee total uniform coverage, implying bG is a design if they are all true.

□

What was the point of breaking the outer pair conditions apart, when in conjunction they're equivalent to the immediate condition that all outer pair orbits are contained by b uniformly?

Only the last condition is "global" in the sense that it needs to check the majority of orbits defined by one of the largest objects which is relevant to the problem (G) and requires a specific choice of b. (Recall that for condition 3, b_i can equivalently be any other element in the same orbit $b_i N$, though the theorem does not explicitly state this.) Prior conditions are more local, only using N and H instead of G and only requiring more specific detail on b over time.

This matters to the enumeration of designs because the search tree of all possibilities can be pruned earlier. Put another way, the theorem can almost directly be converted into nested for-loops that progressively reduce the set of pairs $\{b, G\}$ which can potentially generate a design.

11.2 Basic Algorithm

Each of the tests 1 through 4 in the preceding theorem do not depend on any structure which is yet to be defined and not necessary to the test itself. This makes for an easy conversion from the theorem to a corresponding algorithm which enumerates all designs. Each condition corresponds to a for-loop.

Notation

"Next case" means to run the next case of the current for-loop. After a for-loop is finished the algorithm returns to the next case of the previous for-loop. It was written like this to avoid too much embedding. It can also be viewed as natural for the algorithm to be written like this, since each condition in the theorem is progressively narrowing down the set of all possibilities.

"$|b_i|$" is being treated as a single variable name. It just coincidentally happens to look like a later variable name when you delete part of it. So the fact that "$|b_i|$" appears earlier does not actually mean that the variable "b_i" has been decided.

Pseudocode

For (integers c, C):

For ($|C|$-tuples of integers $0 \leq |b_i| \leq |c|$):

If not {

$$\frac{(|C|-1)|c|}{|c|-1} = \frac{\sum_{i<j \in C} |b_i||b_j|}{\sum_{i \in C} |\binom{|b_i|}{2}|}$$

} then next case

For (transitive $H \leq Sym_C$):

Define $PairOrbits_H$

If not constant for all ($O \in PairOrbits_H$) {

$$\frac{\sum_{\{i,j\} \in O} |b_i||b_j|}{|O|}$$

} then next case, else set k to that constant

For (transitive, imprimitive $N \leq Sym_C$):

Define $PairOrbits_N$, $|b_i|Orbits_N$

Choose $Rep_O \in O$ for every $O \in PairOrbits_N$

For ($|C|$-tuples of orbits $N\_Orbit_i \in |b_i|Orbits_N$):

Choose $Rep_i \in N\_Orbit_i$ for every N_Orbit_i

If not constant for all ($O \in PairOrbits_N$) {

$$\sum_{i \in C} |\{p \in N : (Rep_O)p \subset Rep_i\}|$$

} then next case

For ($G \leq N \wr H$):

Define $OuterPairOrbits_G$

For ($b \cong |C|$-tuples of $b_i \in N\_Orbit_i$):

If for all ($O \in OuterPairOrbits_G$) {

$$\frac{|\{r \in O : r \subset b\}|}{|O|} = \frac{k}{|c|^2}$$

} then print G, b

11.3 Improving the algorithm

The given algorithm won't be winning any prizes for coding. It's seven nested for-loops. A progressive restriction of which G and b must be considered until the algorithm eventually gives up and says "just brute force the rest". So there is room for improvement.

The most obvious starting point is eliminating redundant computation. For instance, putting an ordering on $|C|$-tuples of integers and only testing one representative case will eliminate many permutationally isomorphic block sets. Similar reductions in redundant calculation can be achieved in other places, but involve more detailed coding and memory usage.

From a mathematical standpoint, there are many short, closed form conditions on combinations of parameters which this paper completely ignores. It could be a good idea to run parameters by those conditions before churning out generated orbits, and this becomes increasingly true as the sizes of the groups grow.

It's also very plausible additional conditions exist which are similar to the two that were introduced, in that they eliminate cases with less computation than later tests would have required. Such tests could also be turned into for-loops and nested with the conditions in the theorem. Or combined and rearranged in other ways by someone who knows more programming than nesting for-loops.

Finally, even perfect theoretical optimization of the computational complexity of an algorithm does not guarantee it is the best one. Sometimes an algorithm with a worse theoretical bound on runtime is used instead of a more mathematically impressive counterpart because back in reality it runs faster, and that's what people care about. It is even possible that running the suggested tests in a different order could provide an immediate improvement to runtime. Taking advantage of b's decreasing generality could matter less than some unforseen interaction between a test and

the distribution of all solutions. Different arrangements of tests would have to be tried to actually know what works the best.

11.4 Math and computation

Presumably what came before this section was math. There were a lot of pages of set and group notation for that to not be true. But there's a significant difference between the resulting theorem and most published theorems. Every condition here contained a summation. No easily expressible set of parameters were eliminated. In short, there was no new closed form expression.

Instead, the possible solutions to an infinitely large problem were restricted by the solutions to two other infinitely large problems. It was not even a reduction. If you want to know about bG, even if Pythia shows up and tells you that $b(N \wr H)$ is a design you still have more computing to do.

That's not ideal but it is life. As far as humanity can tell, hard computational tasks exist. We suspect that there will never be nice, closed form expressions telling us about every instance of every combinatorial object. While that is true there will always be some point where actually computing every instance of a structure comes down to "just brute force it". The best you can do is convert that brute force problem into more tractable ones.

Sometimes those imperfect tests can even come in handy back in the world of pure math. Throughout the paper I've talked about Delandtsheer and Doyen's invention of inner and outer pairs, and how it has become a significant idea in finite geometry and design theory. That concept wasn't even mentioned in their abstract or introduction. It was just a tool they used to obtain some closed form bounds. Despite this, the tool is arguably more significant than what the bounds actually are.

Bibliography

[1] Peter Dembowski. *Finite geometries*. Classics in Mathematics. Reprint of the 1968 original. Berlin: Springer-Verlag, 1997, pp. xii+375. ISBN: 3-540-61786-8.

[2] Anton Betten, Gregory Cresp, and Cheryl Praeger. "Line-transitive, point-imprimitive linear spaces: the grid case". In: *Innovations in Incidence Geometry [electronic only]* 8 (Jan. 2008). DOI: 10.2140/iig.2008.8.117.

[3] Anne Delandtsheer and Jean Doyen. "Most block-transitive t-designs are point-primitive". In: *Geom. Dedicata* 29.3 (1989), pp. 307–310. ISSN: 0046-5755. DOI: 10.1007/BF00572446. URL: https://doi.org/10.1007/BF00572446.

[4] R.A. Fisher. *The Design of Experiments*. The Design of Experiments. Oliver and Boyd, 1935. URL: https://books.google.com/books?id=-EsNAQAAIAAJ.

[5] Marc Krasner and Lev Kaluznin. "Produit complet des groupes de permutations et problème d'extension de groupes III". In: *Acta scientiarum mathematicarum.* 14 (1951), pp. 69–82. ISSN: 0001-6969.

[6] Cheryl E. Praeger and Csaba Schneider. *Permutation groups and Cartesian decompositions*. Vol. 449. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2018, pp. xiii+323. ISBN: 978-0-521-67506-2. DOI: 10.1017/9781139194006. URL: https://doi.org/10.1017/9781139194006.

[7] Peter J. Cameron and Cheryl E. Praeger. "Block-transitive t-designs I: point-imprimitive designs". In: *Discrete Mathematics* 118.1 (1993), pp. 33–43. ISSN: 0012-365X. DOI: https://doi.org/10.1016/0012-365X(93)90051-T. URL: https://www.sciencedirect.com/science/article/pii/0012365X9390051T.

[8] Carmen Amarra, Alice Devillers, and Cheryl E. Praeger. *Delandtsheer–Doyen parameters for block-transitive point-imprimitive 2-designs*. 2020. DOI: 10.48550/ARXIV.2009.00282. URL: https://arxiv.org/abs/2009.00282.