Séminaire BOURBAKI juin 2015
67ème année, 2014-2015, n$^{\text{o}}$ 1100

DESIGNS EXIST!
[after Peter Keevash]

by **Gil KALAI**

INTRODUCTION

A set S of q-subsets of an n-set X is a *design* with parameters (n, q, r, λ) if every r-subset of X belongs to exactly λ elements of S. There are some necessary *divisibility conditions* for the existence of such a design, namely that

$$\binom{q-i}{r-i} \text{ divides } \lambda\binom{n-i}{r-i}, \quad 0 \le i \le r-1. \tag{1}$$

To see that the divisibility conditions are necessary, fix any i-subset I of X and consider the sets in S that contain I.

The following result was conjectured in the 19th century and was recently proved by Peter Keevash.

THEOREM 0.1 ([Kee14]). — *For fixed q, r, and λ, there exist $n_0(q, r, \lambda)$ such that if $n > n_0(q, r, \lambda)$ satisfies the divisibility conditions (1) then a design with parameters (n, q, r, λ) exists.*

In other words, for fixed q, r, and λ, the divisibility conditions are sufficient apart from a finite number of exceptional values of n.

A case of special interest is when $\lambda = 1$. A design of parameters $(n, q, r, 1)$ is called a *Steiner system* of parameters (n, q, r). The question if Steiner systems of given parameters exist goes back to works of Plücker, Kirkman, and Steiner. Until Keevash's result not a single Steiner system for $r > 5$ was known to exist.

The presentation of Keevash's work in this paper is based on Keevash's original paper [Kee14], his Jerusalem videotaped lectures [KeeV], and his subsequent paper [Kee15]. It is also based on lecture notes and personal explanations by Jeff Kahn. (This version is still a draft.)

1. REGULARITY, SYMMETRY AND RANDOMNESS

1.1. Between regularity and symmetry

An object is "regular" if it looks locally the same (for a certain notion of "locality"), and it is "symmetric" if it admits a transitive group action (on its "local" pieces). The interplay between regularity and symmetry is of interest in several parts of mathematics. For example, a regular graph is a graph where every vertex is adjacent to the same number of neighbors, and every graph whose group of automorphisms act transitively on its vertices is regular. Regular graphs need not be symmetric (most of them have no non-trivial automorphisms), but there are still various connections between general regular graphs and symmetry.

Designs are regular objects. (The local pieces can be regarded as the r-subsets of the ground set.) You can get them from groups acting transitively on r-sets.

PROPOSITION 1.1. — *Let Γ be a t-transitive permutation group. Then the orbit of a set of size k is a block design so that every set of size r belongs to the same number of blocks.*

However, it follows from the classification of finite simple groups that

THEOREM 1.2. — *Let Γ be a t-transitive permutation group, $t > 5$, then G is A_n or S_n.*

1.2. The probabilistic method and quasi-randomness

The proof of the existence of designs is probabilistic. In order to prove the existence of objects of some kind satisfying a property **P**, one proves that for a suitable probability distribution on all objects of this kind there is a positive probability for property **P** to hold. The probabilistic method is of central importance in combinatorics (and other areas) [AS00]. Keevash defines a complicated combinatorial process with random ingredients for building a design, and shows that with positive probability it leads to the desired construction.

Quasi-randomness refers to deterministic properties of mathematical structures which allows them to behave (for certain restricted purposes) "as if they were random." [(1)] Quasi random properties of primes are, of course, of much importance. In graph theory, a sequence of graphs G_n (where G_n has n vertices) is quasi-random if the number of induced 4-cycles C_4 is $\frac{1}{64}\binom{n}{4}(1 + o(1))$. This important notion was introduced independently by Thomasson [Tho85] and by Chung, Graham, and Wilson [CGW89] (with extensions to hypergraphs by Chung and Graham [CG89]). A sequence of subsets $A_n \subset \{1, 2, \ldots, n\}$ can be called quasi-random (for certain purposes), if the maximum Fourier coefficients of 1_{A_n} tends to zero with n.

1. There are even cases that quasi-randomness of some kind can be attributed to arbitrary structures as is the case in Szemerédi regularity lemma which describes quasi-random structure on arbitrary graphs.

Quasi randomness is a central concept in modern combinatorics and two examples are its usage in Szemerédi's theorem and many of its extensions, and in the study of expanders and Ramanujan graphs. The first move made by Keevash is to vastly extend the situation in discussing very general decomposition of quasirandom hypergraphs.

2. KEEVASH'S RESULTS: EDGE-DECOMPOSITION OF QUASI-RANDOM HYPERGRAPHS AND THE NUMBER OF DESIGNS

Keevash vastly extended theorem 0.1 to describe sufficient conditions for general H-decompositions of quasirandom hypergraphs. We will describe in this section the general results closely following [Kee14] Section 1.1.

A hypergraph G consists of a vertex set $V(G)$ and an edge set $E(G)$, of subsets of $V(G)$. If every edge has size r we say that G is an r-uniform hypergraph. For $I \subset V(G)$, the *link* $G(I)$ of R is the $(r|I|)$-uniform hypergraph

$$G(I) = \{S \subset V(G) \backslash I : I \cup S \in E(G)\}.$$

For an r-uniform hypergraph H, an H-decomposition of G is a partition of $E(G)$ into sub-hypergraphs isomorphic to H. Let K_r^q be the complete r-uniform hypergraph on q vertices, namely, an r-uniform hypergraph whose edges are all r-subsets of a set of size q. A Steiner system with parameters (n, q, r) is equivalent to a K_r^q-decomposition of K_r^n

The next definition generalizes the necessary divisibility conditions described above. Suppose G is an r-uniform hypergraph. We say that G is K_q^r-divisible if $\binom{q-i}{r-i}$ divides $|G(I)|$ for any i-set $I \subset V(G)$, for all $1 \leq i \leq r$.

We come now to a crucial notion of quasirandomness. Suppose G is an r-uniform hypergraph on n vertices. We say that G is (c, h)-*typical* if there is some $p > 0$ such that for any set A of $(r1)$-subsets of $V(G)$ with $|A| \leq h$ we have

$$(1 - c)p^{|A|}n \leq |\cap_{S \in A} G(S)| \leq (1 + c)p^{|A|}n. \tag{2}$$

Keevash's main theorem (still in a somewhat simplified form) is

THEOREM 2.1. — *Let $1/n \ll c \ll d, 1/h \ll 1/q \leq 1/r$. Suppose that G is a K_q^r divisible (c, h)-typical r-uniform hypergraph on n vertices with $|G| > dn^r$. Then G has a K_q^r-decomposition.*

Theorem 0.1 follows by applying Theorem 2.1 with $G = K_n^r$. Thus for fixed values of q and r and large values of n, the divisibility conditions are sufficient for the existence of Steiner systems. The next theorem gives a good asymptotic estimate for the number of Steiner systems. (It also follows from a more general result for counting decomposition of (c, h)-typical hypergraphs.) For Steiner triple systems tighter asymptotic estimates are known [Wil74]. For related results and conjectures see also [LL15+].

FIGURE 1. Kirkman's problem

THEOREM 2.2. — *The number $S(n,q,r)$ of Steiner systems with parameters (n,q,r) (where n satisfies the divisibility conditions) satisfies*

$$\log S(n,q,r) = (1+o(1))\binom{q}{r}^{-1}\binom{n}{r}(q-r)\log n. \tag{3}$$

3. SOME HISTORY, TWO LANDMARKS, AND A RELAXATION

We will give now a brief description of the history of designs based on [Wil03]. Our discussion is centered around (and hence biased toward) general existence theorems. It is perhaps right to start the history with Kirkman. The earliest general existence result is given in Kirkman's 1847 paper where he constructed a Steiner triple system (as called today) for every n which is 1 or 3 modulo 6. The prehistory is even earlier. Plücker encountered Steiner triple systems in 1830 while working on plane cubic curves. Woolhouse asked about the number of Steiner triple systems in the "Lady's and Gentleman's Diary" edited by him in 1844 (and again in 1846). Combinatorial designs are closely related to mathematical constructions that were studied since ancient times like Latin squares and Greco-Latin squares. Steiner, unaware of Kirkman's work, posed the question on the existence of Steiner triple systems in 1853 (leading to a solution by Reiss published in 1859.)

It is common to start the story of designs with Kirkman's schoolgirl problem. Kirkman proposed in 1850, again in the "Lady's and Gentleman's Diary," his famous problem on "fifteen young ladies," with solutions by himself, Cayley, Anstice, Pierce, and others. There are fifteen schoolgirls who take their daily walks in rows of threes.

It is required to arrange them daily for a week so that no two schoolgirls will walk in the same row more than once.

Kirkman's question can be asked in greater generality for every $n = 3 (\mathrm{mod}\, 6)$ and a partial solution was offered in 1852 by Spottiswoode. The general question was settled independently by Xi (a schoolteacher from Mongolia) in the mid '60s and by Ray-Chaudhuri and Wilson in 1972. Sylvester asked (as reported by a 1850 paper by Cayley) if we can divide all $\binom{15}{3}$ triples into 13 different solutions of Kirkman's problem and this was settled by Denniston in 1974. Sylvester's question for general n is still open.

In the first half of the 20th century combinatorial designs played an important role in experimental designs in statistics, in group theory, and were closely related to error-correcting codes which are among the most important real-life applications of mathematics. Many interesting examples of designs were discovered. We already mentioned that there are no t-transitive groups for $t > 5$ other than S_n and A_n. The only 4-transitive groups other than A_n and S_n are the Mathieu groups, M_{24} (5-transitive), M_{23}, M_{12} (5-transitive), and M_{11}. The Mathieu groups were introduced in 1861 and 1873, and they are closely related to designs. Indeed M_{24} and M_{12} can be described as the automorphism groups of Steiner systems. In 1938 Witt described the group M_{24} as the automorphism group of the *Witt design*, which is a Steiner system of parameters $(24, 8, 5)$, thus giving a definite existence proof. Mathieu groups and Witt designs are closely related to the Golay error-correcting codes, discovered in 1949, which have much practical use. In the early 1960s Hanani solved the question on the existence of designs for $(q, r) = (4, 2), (4, 3)$ and $(5, 3)$.

3.1. Wilson's and Teirlink's constructions

The existence conjecture for the case $r = 2$, namely when every pair of elements belong to λ blocks, was solved by Wilson in 1972.

THEOREM 3.1 (Wilson [Wil72a, Wil72b, Wil75]). — *If n satisfies the divisibility conditions and is large enough then designs of parameters $(n, q, 2, \lambda)$ exist.*

In 1987 Teirling showed that for a large λ depending on q and r (but not on n) designs exist!

THEOREM 3.2 (Teirlink [Tei87]). — *For every q and r there is $\lambda = \lambda(k, r)$ such that designs of parameters (n, q, r, λ) exist.*

3.2. The necessary conditions for designs are sufficient for something

We can regard the question of finding a design as an integer programming question. We need to find 0-1 solutions to a system of equations: The variables α_S are associated to q-subsets S of $[n]$ and for every r-set we have an equation $\sum_{R \subset S} \alpha_S = 1$. It is a

common practice to look at a generalized notion of solution and Wilson [Wil74] and Graver and Jurkat [GJ73] asked for integral solutions [2]. They proved:

THEOREM 3.3 (Wilson [Wil73]; Graver and Jurkat [GJ73])
For every n, q, r, λ, if n satisfies the divisibility conditions then integral designs exists.

The proof of this result is not difficult and the existence of integral designs plays an important role in Keevash's work.

4. THE GREEDY RANDOM METHOD

4.1. A probabilistic heuristic and a simple application of the probabilistic method

Consider a q-hypergraph with n vertices and $b = \binom{n}{r}/\binom{q}{r}$ edges. Write $a = \binom{n}{q}$. There are altogether $\binom{a}{b}$ such hypergraphs. Given a set R of r vertices what is the distribution of the number of edges containing R? This is a Poisson distribution of parameter 1. The probability that R is contained in a unique edge is $1/e$. If these probabilities were statistically independent we could conclude that Steiner triple systems of parameters n, q, r exist and that their number is $\binom{a}{b}e^{-b}$. We will refer to this argument and estimates it gives as the *probabilistic heuristic*.

Of course, there is neither statistical independence nor good reasons to think that lack of independence is not devastating. [3] Indeed the probabilistic heuristic is completely blind to the divisibility conditions.

What we can do is to choose c edges at random for some $c < b$ so that every r-set is included in *at most* one of them. Doing so shows that we can find $b/(1 + log\binom{k}{r})$ edges so that every set of size r is included in at most one edge. Here we do not need randomness and we can just add edges in a greedy way. Erdős and Hanani conjectured in 1963 that there are $b(1 - o(1))$ edges so that every r-set is covered at most once, or, equivalently, there are $b(1 + o(1))$ edges so that every r-set is covered at least once.

4.2. Rödl nibble and approximate designs

The greedy-random method (it is also called in the literature "incremental-random method" and "semi-random method") is based on the idea of adding to our desired objects elements in small chunks (or even one at a time). The general idea can be traced to works of Ajtai-Komlos-Szemerédi on Ramsey numbers. In [Rod85] Rödl used

2. Another generalized notion of solution, the linear programming relaxation, replaces the 0-1 variables by real numbers in the interval [0,1]. This is useful to several related combinatorial packing and covering problems. I am not aware of it being used for our problem.

3. We note that an important theme in the "probabilistic method" is to prove (when statistical independence does not apply) that certain rare events still have positive probability. There are various methods that were developed for this purpose [AS00].

a certain greedy-random process known as the Rödl nibble to prove the Erdős -Hanani conjecture.

THEOREM 4.1 (Rödl [Rod85]). — *For every fixed q and r there exist a nearly Steiner system of parameters (n, q, r), namely a system of $(1 + o(1))\binom{n}{r}\binom{q}{r}^{-1}$ q-subsets of $[n]$ such that every r set is included in at least one block in the system.*

The idea is this. You choose at random ϵb blocks and show that (with high probability) they form a very efficient covering of the r-sets they cover. Then you show that (again, with high probability) both the hypergraph of unused q-blocks and the the hypergraph of uncovered r-sets are quasirandom. This allows you to proceed until reaching $(1 - o(1))\binom{n}{r}\binom{q}{r}^{-1}$ q-subsets of $[n]$ such that every r set is included in at most one block in the system. (At this point you can add arbitrary blocks to cover the remaining r-sets.) It was later discovered that a variant of this process where you add one block at a time also works.

4.3. Pippinger-Spencer and beyond

The greedy random method and, in particular, variants of the Rödl nibble had important applications in combinatorics over the years. A general framework for the Rödl nibble was laid by Frankl and Rodl [FR85] with the definite result given by Pippinger and Spencer [PS89].

We consider an auxiliary hypergraph: the vertices correspond to r-sets and the edges correspond to q-sets. For this hypergraph the task is to find a large matching – a collection of pairwise disjoint edges, or a small covering a collection of edges covering all vertices.

The result of Pippinger and Spencer asserts that it is enough that

(i) all vertices have the same degree d (or roughly the same degree) and

(ii) every pair of vertices are included in at most $o(d)$ edges.

This level of abstraction is crucial for some further important applications of Rödl's method [Kah96, Spe95, KR97, Kah00, Vu00] and form a crucial ingredients of Keevash's proof.

5. KEEVASH'S PROOF: THE TEMPLATE, THE NIBBLE, THE OCTAHEDRON, AND THE SHUFFLE

In this section we will present a very rough outline of Keevash proof for a very special (but important) case. We will deal only with decompositions of graphs into edge-disjoint triangles. Part of the proof consists of repeated reference (with complicated and subtle details) to the greedy-random method. These parts are quite difficult and long, however we will largely take them for granted.

The difficulty in applications of the greedy-random methods (and other probabilistic arguments) for packing problems is in the last stages. Once we packed a large number of

objects the probabilistic arguments do not apply and some backtracking is needed. In some cases, a careful preprocessing of our combinatorial object can assist the required backtracking. In our case, we need an auxiliary collection of triangles called the *template* defined via a combination of algebra and probability. Both for the applications of the greedy random method and for and the appellate and algebraic parts, the general case is more difficult than the special case of triangles.

5.1. Edge-decomposition into triangles

When is it possible to decompose the edges of a graph G into edge-disjoint triangles? We say that G is *trivisible* if (i). The number of edges in G is divisible by 3, and every vertex has an even degree. Next we define the *density* $d(G)$ of a graph as the number of edges divided by $\binom{n}{2}$ where n is the number of vertices. G is (c,t)-*typical* if for every set X of at most k vertices

$$(1+c)d(G)^{|X|} \leq |\cap_{x\in X} N_x| \leq (1+c)d(G)^{|X|}.$$

Here, N_x is the set of neighbors of a vertex v. We denote by V the set of vertices of G.

THEOREM 5.1. — *For every $d > 0$ there is $c > 0$ such that if G is trivisible, $(c,16)$-typical, and $d(G) > d$ then G admits a triangle-decomposition.*

Remark 5.2. — Bootstrapping this result Keevash proves that $(c,2)$-typicality suffices. (Our level of description is not detailed enough to show how typicality is actually used.)

5.2. The template

We choose a so that $2^{a-2} < n \leq 2^{a-1}$. We consider a random map from V into $F^*_{2^a}$ (the non-zero elements of a field with 2^a element). We let T to be those triangles $\{x,y,z\}$ in G such that $x+y+z=0$. We let $G^* = \cup T$, namely the union of all edges in triangles in T.

Note that the number of triangles in the template is roughly $K^3 d(G)^3 \binom{n}{3}$ where K is some constant between $1/2$ and $1/4$.

5.3. The plan

Plan: Start with an approximate triangle decomposition and apply a sequence of repairs.

5.4. Steps 1: nibble

We want to use the nibble (greedy random) method to find a collection N of edge-disjoint triangles whose union is most of $G\backslash G^*$. We will not modify N any further. In order for the method to work we need to assume that G^* and $G\backslash G^*$ and (G, G^*) are "nice" (namely, quasi-random in various ways), as well as various other conditions that allow to implement the initial nibble and to allow the entire argument to go through. All these conditions hold with high probability. We need also that $G\backslash G^*\backslash(\cup N)$ is sparse (having only small degrees), this also holds with high probability.

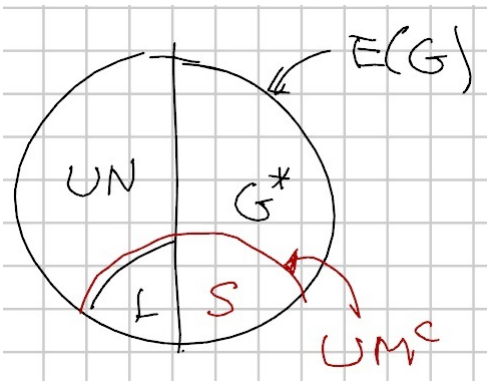

FIGURE 2. Step 2 (picture out of scale; the size of the right side is a small fraction of the whole)

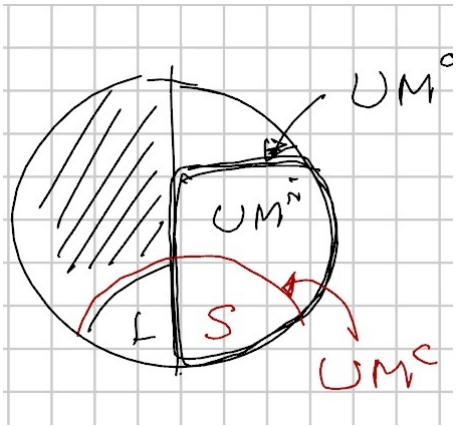

FIGURE 3. Step 3 (picture out of scale)

5.5. Step 2: cover

After packing most of $G \backslash G^*$ with triangles of N, we cover the left over part L of $G \backslash G^*$ by a collection M^c of edge-disjoint triangles each having two edges from G^*. This defines a set S of edges from G^*. See Figure 2.

5.6. Step 3: hole

Now we create two sets M^{out} and M^{in} of edge disjoint triangles in G^*, having the property that $\cup M^{\text{out}} = S \uplus M^{\text{in}}$ ($\uplus$ denotes disjoint union). (When I say "we create" this accounts for using the nibble method and at times further massaging our initial steps.)

5.7. The octahedron

Here is a detail of the argument taken in separation which we will use in Step 4. Suppose we start with the complete graph K_n (or with a smaller quasi random graph containing G^*), with an edge disjoint collection of triangles, and we want to eliminate an edge $e = \{v, w\}$ not in G^* which is contained in one triangle. We look at two

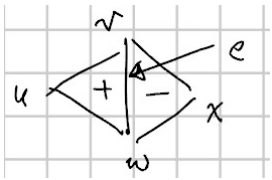

FIGURE 4. The rombus

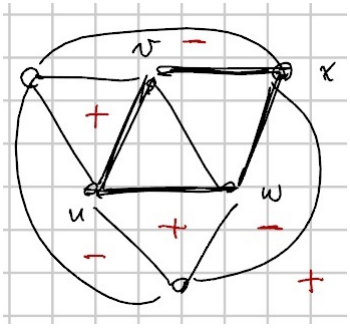

FIGURE 5. The octahedron

triangles containing e (Fig. 4) and embed them into an octahedron (Fig 5). We can now use other triangles in the octahedron to move to a new set of edge-disjoint triangles, covering all the edges except e.

5.8. How to proceed: dream and reality

Consider $M_1 = M^c \cup M^{\text{in}}$, $M_2 = M^{\text{out}}$ and then $\cup M_1 = L \uplus \cup M^{\text{out}}$.

Dream plan: suppose that $M^{\text{out}} \subset T$ (in words, all triangles in M^{out} are in the template). Then we are in good shape: We consider the decomposition $N \cup (T \backslash M^{\text{out}}) \cup M_1$!

However, there is no reason to think that this can be achieved.

Reality plan: what eventually works is to find two sets of edge-disjoint triangles M_3 and M_4 with edges in G^* with the following properties:

- $\cup M_3 = \cup M_4$,
- $M_3 \subset T$
- $M_2 \subset M_4$,

and use the decomposition

$$N \cup (T \backslash M_3) \cup (M_4 \backslash M_2) \cup M_1. \tag{4}$$

5.9. Two remarks

Remark 5.3. — A reason for having an elbow room to use the nibble probabilistic method to get a perfect design is that our nibbling is taking place in a large hypergraph and we need to have the required effect on a smaller hypergraph representing a tiny (but bounded below with n) fraction of the vertices.

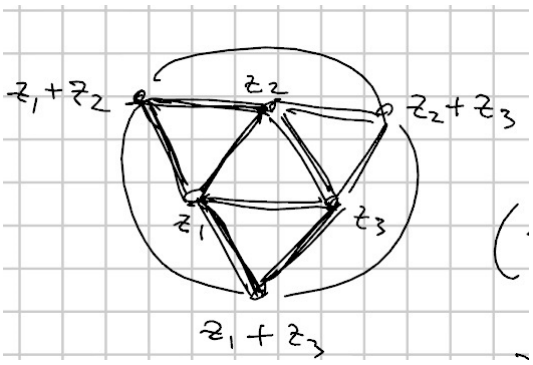

FIGURE 6. The shuffle

Remark 5.4. — Some arguments about "canceling boundaries" are of importance in the proof. Unlike with usual homology here the boundaries are not signed and the octahedron is a "cycle" w.r.t. such an unsigned "boundary" operator. We note that these type of boundaries and the important role of octahedra can be seen also in the hypergraph regularity theorems [RS04, Gow07], and in the early work [CG89] on quasirandom hypergraphs.

5.10. Step 4: The shuffle

It is "left" to find M_3 and M_4. Here, we need to explain how to implement our plan, and to indicate how the precise definition of the template triangles enters the picture.

Consider five elements $x_1, x_2, x_3, t_1, t_2 \in F^*$ with x_1, x_2, x_3 linearly independent over $Z/2Z$, $t_1 \neq t_2$. Write $t_3 = t_1 + t_2$, and $X = \text{span} < x_1, x_2, x_3 >$ (over $Z/2Z$). (Reminder: F was a field with 2^a elements and F^* are its non-zero elements.)

The *shuffle* $S_{x,t}$ is a complete tripartite 3-uniform hypergraph with 24 vertices. We have three sets $X + t_1$, $X + t_2$, and $X + t_3$ of eight vertices each, and consider all 8^3 triangles with one vertex taken from each set. (There is a positive probability that all triangles of the shuffle are supported by our graph.)

We will consider two decompositions of the shuffle into edge-disjoint triangles.

Decomposition I: All triangles of the form $x + t_1, y + t_2, x + y + t_3$.

Decomposition II: Translate of decomposition I by (x_1, x_2, x_3).

Note that all triangles in decomposition I are in the template. But since $x_3 \neq x_1 + x_2$ no triangle in decomposition II is in the template.

Now we can describe the random greedy construction of M_3, M_4. We consider a random available shuffle and add decomposition II to M_4 and decomposition I to M_3. Using the nice quasirandom properties we are careful to maintain throughout our construction (this requires also "massaging" M_1 and M_2 in the process), there are many available choices for the shuffle, and repeated use of it allows to achieve the desired M_3 and M_4. "□"

5.11. Quoting Calegary's reflection on Keevash's proof

"Random construction which 'nearly' solves the combinatorial problem, and then adjusting the result around the margins by formally expressing the error as a linear combination of formal 'differences' of designs of uniformly bounded size, and then treating 'negative' quantities of these small designs as 'holes' in the big uniform quantity.

Exactly the same idea (at this abstract level) is the key to the recent Kahn-Markovic proof of the Ehrenpreis conjecture [KM11], where one first uses a probabilistic (i.e. ergodic theoretic) argument to cover a hyperbolic surface with an almost equidistributed collection of pairs of pants with an almost prescribed geometry, almost all of which can be glued up, and then shows that the error can be formally glued up if one uses 'negative' pieces, which one then interprets as holes in big uniform collection (I like to think of these 'negative' pants as 'holes in the Dirac pants sea'...)

Exactly the same idea again was used by Alden Walker and I recently to show that random groups contain fundamental groups of closed surfaces [CW13] ; we first build 'most' of the surface by a random matching argument, then glue up the error formally using 'negative' pieces (of bounded size), which can then be pulled out of the collection that was already matched.

No doubt the details of the constructions diverge considerably beyond this 'family resemblance' (this is already true in the latter two examples, where I understand the details of what is going on), but this resemblance at the abstract level seems to me to be much more than a triviality."

6. PACKING, COVERING, AND DESIGNS - A FEW OTHER ADVANCES AND OPEN PROBLEMS

Keevash's achievement is extraordinary in solving a major open problem in combinatorics, and in developing and implementing with great difficulty and ingenuity a completely unexpected machinery. I will mention in this section other important advances regarding packing, covering, designs, and highly regular combinatorial objects, and mention a few open problems.

Finite projective planes. — We mainly discussed the situation when q and r are fixed and n goes to infinity. Understanding other regimes of parameters is also of great interest. The famous problem on the existence of projective planes of non-prime power order can be formulated as:

(1) Are there any designs of parameters $(q+1, 2, q^2+q+1, 1)$ when q is not a prime-power?

The central question regarding uniqueness of projective planes of prime order can be formulated as:

(2) Are there any designs of parameters $(q+1, 2, q^2+q+1, 1)$ when q is a prime, except those coming from a finite field?

There is an important result by Fischer and Erdős-deBruijn which asserts that the number b of blocks in a design is at least n. A beautiful argument due to Ryser is that if you consider the $n \times b$ incidence matrix of a design the rows $v_1, v_2, \ldots, v_b$ are always linearly independent. Indeed for some $x > y$,

$$\begin{aligned}\Big\langle \sum \alpha_i v_i, \sum \alpha_i v_i \Big\rangle &= x \sum_i \alpha_i^2 + y \sum_{i \neq j} \alpha_i \alpha_j \\ &= x \sum_i \alpha_i^2 + y \sum_{i \neq j} \alpha_i \alpha_j \\ &= (x-y) \sum_i \alpha_i^2 + y \Big(\sum_i \alpha_i \Big)^2,\end{aligned}$$

which can vanish only when all α_is vanish. This implies that a $(q+1, 2, n, 1)$ designs do not exist if $n < q^2 + q + 1$.

It is hard to point the finger on where and why the "probabilistic heuristic" will fail for $(q, 2, n)$ designs when both q and n tend to infinity. It will certainly be interesting to understand this matter. It is also hard but of much interest to understand when regularity implies symmetry.

Further decompositions and stronger regularity. — Can we find a design admitting a decomposition into disjoint perfect matching and, more generally, into disjoint designs with other parameters? We can seek structures with various recursive decompositions, and, ask also if we can decompose the complete hypergraph into such designs? In particular we can ask if "Kirkman systems" and "Sylvester systems" exist for constant q and r and large n when the corresponding divisibility conditions hold?

This is a good time to mention the classical result by Baranyai [BAR75] asserting that K_r^n can be decomposed into perfect matchings whenever r divides n. Baranyai's proof used ideas from linear programming.

We can also ask about stronger regularity conditions: Given a design S of parameters (n, q, r, λ) when is there a design of parameters $(n+1, q+1, r+1, \lambda)$ all whose links are isomorphic to S?

Pseudomanifolds, manifolds, and buildings. — Block designs with parameters $(n, q, q-1, 2)$ are *pseudomanifolds*. Considered as topological spaces they represent spaces with singularities of codimension at least two. The Heawood Conjecture proved by Ringel and Young asserts that for $q = 3$ such objects exist even if you require them to represent a prescribed triangulated surface. In higher dimensions you can impose various regularity conditions related to the conditions for block designs. For example, Altshuler [Alt78] constructed pseudomanifolds with a common prescribed vertex-link. Triangulations of $2d$-dimensional manifolds can have the property that every set of d vertices belongs to some face of dimension $2d$. When $d > 1$ there are only a handful of such triangulations known. A remarkable example is the 9-vertex triangulation of CP^2 by Kuhnel and Lassman [KL81]. Like for designs we can expect that infinite families for every d exist. Tits' Buildings are, of course, very regular

combinatorial structures. Buildings, like projective geometries of dimension greater than two, represent a regime where regularity has strong algebraic consequences.

Designs, t-wise independent permutations, conjugacy tables, and local central limit theorems. — Kuperberg, Lovett, and Peled [KLP12] used a novel probabilistic technique to show the existence of regular combinatorial objects and to approximately count them. They constructed and estimated the number of block designs of parameter (n, q, r, λ), e.g., in a regime where the number of blocks and the values of q, r, and λ are $n^{O(r)}$. In fact, the precise condition they need is that $\lambda = (n/r)^{\Omega(r)}$.

They developed local central limit theorems which enabled them to analyze the problem reformulated via a random walk on a lattice with a prescribed set of allowed steps.

A family of permutations on n elements is t-wise uniform if it acts uniformly on tuples of t elements. In another application of the method, Kuperberg, Lovett and Peled showed that there exist families of t-wise independent permutations for all t, whose size is $n^{O(t)}$. (Before their work constructions of small families of t-wise independent permutations were known only for $t = 1, 2, 3$.)

An independent body of works with a related method of developing and using local central limit theorems is by Barvinok and Hartigan [BH12] for approximately counting matrices with prescribed rows and column sums (contingency tables), graphs with prescribed degree sequences, and for approximately computing volumes of certain polytopes.

For related techniques for enumerating regular structures, see also [CM05, CGG+10]. When it comes to counting designs and regular structures, a good place to begin is in counting regular graphs. This is a fascinating problem on which a lot is known [MW90] and more is left to be explored.

Vertex-packing of small graphs in large random graphs. — An important problem in probabilistic combinatorics is the problem of vertex packing small graphs H into large random graphs G. The situation for perfect matching (when H is a single edge) is classic but even when H is a triangle this posed a difficult challenge for some decades until resolved by Johansson, Kahn and Vu [JKV08] again using a novel probabilistic technique. The surprising idea is to start with a much larger random graph and incrementally *remove* edges. I don't know to what extent randomness can be replaced by quasirandomness (of some kind) for packing problems of this kind.

Packing trees. — Consider $n-1$ trees T_1,$T_2 \ldots, T_n$ where T_i has i vertices.

Conjecture (Gyárfás, 1963): There exists an edge-disjoint decomposition of K_n into $n-1$ parts so that the ith part is isomorphic to T_i.

REFERENCES

[AS00] N. Alon & J. Spencer, *The Probabilistic Method*, Wiley, New York, 2000.

[Alt78] A. Altshuler, 3-pseudomanifolds with preassigned links, *Trans. Amer. Math. Soc.* 241 (1978), 213–237.

[BAR75] Zs. Baranyai, On the factorization of the complete uniform hypergraph, in A. Hajnal, R. Rado, and V. T. Sós, *Infinite and Finite Sets,* Proc. Coll. Keszthely, 1973, Colloquia Math. Soc. János Bolyai 10, North-Holland,1975, pp. 91–107.

[BH12] A. Barvinok & J. A. Hartigan, An asymptotic formula for the number of non-negative integer matrices with prescribed row and column sums, *Trans. Amer. Math. Soc.* 364 (2012), 4323–4368.

[CW13] D. Calegari & A. Walker Random groups contain surface subgroups, to appear in *Jour. Amer. Math. Soc.*, arXiv:1304.2188.

[CM05] E. R. Canfield & B. D. McKay, Asymptotic enumeration of dense 0-1 matrices with equal row sums and equal column sums, *Electron. J. Combin.* 12 (2005), Research Paper 29, 31 pp. (electronic).

[CGG+10] E. R. Canfield, Z. Gao, C. Greenhill, B. D. McKay & R. W. Robinson, Asymptotic enumeration of correlation-immune Boolean functions, *Cryptogr. Commun.* 2 (2010), 111–126.

[CGW89] F. Chung, R. L. Graham & R. M. Wilson, Quasi-random graphs, *Combinatorica* 9 (1989), 345–362.

[CG89] F. Chung & R. L. Graham, Quasi-random hypergraphs, *Random Structures and Algorithms* 1 (1990), 105–124.

[CD06] C. J. Colbourn & J. H. Dinitz, *Handbook of Combinatorial Designs,* 2nd ed. Chapman & Hall / CRC, Boca Raton, 2006.

[EH63] P. Erdős & H. Hanani, On a limit theorem in combinatorial analysis, *Publicationes Mathematicae Debrecen* 10(1963), 10–13.

[FR85] P. Frankl & V. Rödl, Near perfect coverings in graphs and hypergraphs, *European J. Combinatorics* 6 (1985), 317–326.

[Gow07] W. T. Gowers, Hypergraph Regularity and the multidimensional Szemerédi Theorem, *Annals of Math.* 166(2007), 897–946.

[GJ73] J. E. Graver & W. B. Jurkat, The module structure of integral designs, *J. Combinatorial Theory Ser. A* 15(1973), 75–90.

[Han61] H. Hanani, The existence and construction of balanced incomplete block designs, *Annals Mathematical Statistics* 32 (1961), 361–386.

[Han65] H. Hanani, A balanced incomplete block design, *Annals Mathematical Statistics* 36(1965), 7–11.

[JKV08] A. Johansson, J. Kahn & V. Vu, Factors in Random Graphs, *Random Structures and Algorithms* 33 (2008), 1-28.

[Kah96] J. Kahn, Asymptotically good list-colorings, *J. Combinatorial Theory Ser. A* 73 (1996) 1–59.

[Kah00] J. Kahn, Asymptotics of the list chromatic index for multigraphs, *Random Structures and Algorithms* 17 (2000), 117–156.

[KM11] J. Kahn & V. Markovic, The good pants homology and the Ehrenpreis conjecture, *Ann. of Math.* 182 (2015)1–72, arXiv:1101.1330

[Kee14] P. Keevash, The existence of designs, arXiv:1401.3665.

[KeeV] P. Keevash, Videotaped lectures, Jerusalem 2015. https://youtube/tN6oGXqS2Bs?list=PLTn74Qx5mPsSU6ysUXk-ssF6sZtvh-a-o

[Kee15] P. Keevash, Counting designs, arXiv:1504.02909.

[KR97] A. Kostochka & V. Rödl, Partial Steiner systems and matchings in hypergraphs, *Random Structures and Algorithms* 13 (1997), 335–347.

[KL81] W. Kühnel & G. Lassman, the unique 3-neighborly 4 manifold with 9 vertices, *J. Combin. Th. Ser. A* 35 (1983), 173–184.

[KLP12] G. Kuperberg, S. Lovett & R. Peled, Probabilistic existence of regular combinatorial objects, Proc. 44th ACM STOC, 2012.

[LL15+] N. Linial & Z. Luria, An upper bound on the number of high-dimensional permutations, *Combinatorica,* to appear.

[MW90] B. D. McKay & N. C. Wormald, Asymptotic enumeration by degree sequence of graphs of high degree, *European J. Combin.* 11 (1990), 565–580.

[N-W70] C. St. J. A. Nash-Williams, An unsolved problem concerning decomposition of graphs into triangles, *Combinatorial Theory and its Applications III,* North Holland (1970), 1179–1183.

[PS89] N. Pippinger & J. H. Spencer, Asymptotic behaviour of the chromatic index for hypergraphs, *J. Combinatorial Theory Ser. A* 51 (1989), 24–42.

[Rod85] V. Rödl, On a packing and covering problem, *European J. Combinatorics* 6 (1985), 69–78.

[RS04] V. Rödl & J. Skokan, Regularity lemma for uniform hypergraphs, *Random Structures and Algorithms* 25 (2004), 1–42.

[Spe95] J. Spencer, Asymptotic packing via a branching process, *Random Structures and Algorithms* 7 (1995), 167–172.

[Tei87] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, *Discrete Math.* 65 (1987), 301–311.

[Tho85] A. Thomason, Pseudo-random graphs, in: *Proceedings of Random Graphs,* Poznań 1985, M. Karoński, ed., *Annals of Discrete Math.* 33 (North Holland 1987), 307–331.

[Vu00] V. Vu, New bounds on nearly perfect matchings in hypergraphs: higher codegrees do help, *Random Structures and Algorithms* 17 (2000), 29–63 (2000).

[Wil72a] R. M. Wilson, An existence theory for pairwise balanced designs I. Composition theorems and morphisms, *J. Combinatorial Theory Ser. A* 13 (1972), 220–245.

[Wil72b] R. M. Wilson, An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures, *J. Combinatorial Theory Ser.* A 13 (1972), 246–273.

[Wil75] R. M. Wilson, An existence theory for pairwise balanced designs III. Proof of the existence conjectures, *J. Combinatorial Theory Ser. A* 18 (1975), 71–79.

[Wil73] R. M. Wilson, The necessary conditions for t-designs are sufficient for something, *Utilitas Math.* 4(1973), 207–215.

[Wil74] R. M. Wilson, Nonisomorphic Steiner Triple Systems, *Math. Zeit.* 135 (1974), 303–313.

[Wil03] R. Wilson, The early history of block designs, *Rend. del Sem. Mat. di Messina* 9 (2003), 267–276.

Gil KALAI

Hebrew University of Jerusalem
Institute of Mathematics
Givat-Ram
Jerusalem 91904, Israel
and
Department of Mathematics and Computer Science
Yale University
New Haven CT, USA
E-mail : kalai@math.huji.ac.il