POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

CCCLXVII

WOJCIECH KORDECKI

Random matroids

WARSZAWA 1997

Wojciech Kordecki
Institute of Mathematics
Technical University of Wrocław
Wybrzeże Wyspiańskiego 27
50-370 Wrocław, Poland
E-mail: kordecki@im.pwr.wroc.pl

Published by the Institute of Mathematics, Polish Academy of Sciences
Typeset in TEX at the Institute
Printed and bound by
Publishing House of the Warsaw University of Technology
ul. Polna 50, 00-644 Warszawa

P R I N T E D I N P O L A N D

ISSN 0012-3862

CONTENTS

1991 *Mathematics Subject Classification*: Primary 05B35; Secondary 60C05.
Received 27.3.1995; revised version 10.2.1997.

Introduction

Systematic studies of random graphs were initiated by Erdős and Rényi [10] in 1960. Their fundamental paper provided inspiration for many investigations in the field of discrete random structures. Since that year a huge number of papers have been written on random graphs and their generalizations.

The book by Bollobás [7] offers a systematic study of the theory of random graphs. The chapter "Random Graphs" [22] in [13] written by Karoński gives a brief review of typical problems.

Because matroids are natural generalizations of graphs, the theory of random graphs is naturally applicable to the theory of random matroids. It seems that particular problems from reliability theory and percolation theory should lead to random matroids in cases where discrete structures in such problems cannot be described by graphs, but can be described by more general structures such as matroids.

However, the first papers on random matroids were written as late as fifteen years after the first paper of Erdős and Rényi. Lomonosov [35] proved theorems about the rank of random matroids in 1974. His definition of random matroids was based on the traditional definition of random graphs. One year later, Knuth [27] presented another algorithmic approach to the definition of random matroids.

After 1980, several papers were published by Kelly, Oxley and Welsh, devoted to problems of the distribution of the rank of random matroids representable on finite fields. Also, the problem of the number of small matroids (e.g. cycles, independent sets, subspaces of small rank) in random matroids was considered. Note that analogous problems within the theory of random graphs were investigated extensively at that time.

The theory of random matroids is mainly devoted to matroids being random subsets of finite geometries, as in the case of random graphs, subgraphs of such regular structures as complete graphs K_n and complete bipartite graphs $K_{m,n}$. General cases are seldom considered. Similarly in this monograph, most results and problems are related to matroids representable on finite fields. The majority of results presented below concern limit problems, such as Poisson and normal convergence, and existence problems in large structures.

The aim of this work is to present a unified treatment of random matroids and recent developments in this area. In Section 2, we introduce basic ideas of matroid theory, including finite geometries, and give examples of such structures. In Section 3, we present some probabilistic tools that are required later. In particular, this section includes basic facts about Poisson convergence and normal convergence and Markov processes on finite lattices.

Section 4 gives definitions of random matroids and considers random matroids which are random submatroids of a fixed matroid. Additionally, this section provides a brief sketch of the algorithmic definition of random matroids.

In Section 5 and Section 6 a particular case where random matroids are submatroids of finite projective geometries is presented. Such random matroids were introduced by Kelly and Oxley [23] in 1982. In Section 6, slightly more general matroids than projective geometries will be investigated. In Section 7, we present some open problems.

A significant part of this monograph was done during my stay at the Department of Discrete Mathematics at the Adam Mickiewicz University in Poznań. I would like to thank Michał Karoński, Tomasz Łuczak and Andrzej Ruciński for friendly cooperation, discussions and many helpful comments.

2. Matroids

2.1. Notations and basic properties. We refer the reader to [46] and [49] as the fundamental monographs on matroid theory. The recent monograph [39] by Oxley (published in 1992) emphasizes the geometrical nature of matroids rather than their graph-theoretical character.

Let E be a finite nonempty set and $\mathcal{P}$ a family of its nonempty subsets such that

$$(C1) \qquad C_1 \in \mathcal{P},\ C_2 \in \mathcal{P},\ C_1 \subseteq C_2 \Rightarrow C_1 = C_2.$$

The pair $S = (E, \mathcal{P})$ is called a *clutter*. The family of all minimal sets $D \subseteq E$ such that for every $C \in \mathcal{P}$, $C \cap D \neq \emptyset$, is denoted by $\overline{\mathcal{P}}$. The pair $\overline{S} = (E, \overline{\mathcal{P}})$ is called a *blocker* of S. It is clear that $\overline{S}$ is a clutter and $\overline{\overline{S}} = S$.

Example 2.1.1 (Two-terminal graph). Let G be a connected nonoriented graph with two distinguished vertices x_{In}, x_{Out} and a set E of edges. Define $P \in \mathcal{P}$ if and only if P is the set of edges of some minimal path joining x_{In} and x_{Out}.

Example 2.1.2 (All-terminal graph). Let G be a connected nonoriented graph. Define $P \in \mathcal{P}$ if and only if P is the set of edges of some spanning tree in G.

Example 2.1.3 (Cycle graph). Let G be a connected nonoriented graph. Define $P \in \mathcal{P}$ if and only if P is the set of edges of some cycle of G.

The family $\mathcal{C}$ is called a family of *circuits* if $(E, \mathcal{C})$ is a clutter and moreover

$$(C2) \qquad C', C'' \in \mathcal{C}, C' \neq C'', x \in C' \cap C'' \Rightarrow \exists C \in \mathcal{C} : C \subseteq C' \cup C'' \setminus \{x\}.$$

The pair $M = (E, \mathcal{C})$ is called a *matroid* on the ground set E, and every $C \in \mathcal{C}$ is called a *circuit*. A one-element circuit is called a *loop*.

Example 2.1.4. It is easy to see that the clutter from Example 2.1.3 satisfies formula (2.1.1) below (thus it is a matroid), but the clutters from Examples 2.1.1 and 2.1.2 do not satisfy (2.1.1).

A set I is called an *independent* set if I has no circuit. The family of all such I is denoted by $\mathcal{I}(M)$. Every maximal independent set is a *basis*. It is well-known that every

basis has the same number of elements. The family of all bases is denoted by $\mathcal{B}(M)$. The number of elements of a maximal independent set in a set A is called the *rank* of A and it is denoted by $\varrho(A)$. Every maximal set of a given rank is called a *flat*. The family of all flats is denoted by $\mathcal{J}(M)$. A flat of rank $\varrho(E)-1$ is called a *hyperplane*. Let us define the *span* $\sigma(A)$ of $A \subseteq E$ as

$$\sigma(A) = \bigcap_{A \subseteq B \in \mathcal{J}} A. \tag{2.1.1}$$

Any one of the families $\mathcal{C}$, $\mathcal{I}$, $\mathcal{B}$, $\mathcal{J}$ or functions ϱ and σ, defined above, determines the matroid M uniquely. Thus, one can define the matroid M as a pair $(E,\mathcal{I})$, $(E,\mathcal{B})$, $(E,\mathcal{J})$, (E,ϱ) or (E,σ). A matroid is *free* if all subsets of E are independent.

Example 2.1.5. Let E be the set of columns of an $m \times n$ matrix A over the field F, and let $\mathcal{I}$ be the set of linearly independent subsets of E. Then $M[A] = (E,\mathcal{I})$ is a matroid.

By definition, a matroid M is *representable* over the field F if and only if it is isomorphic to $M[A]$ for some matrix A over F.

Lemma 2.1.1. *If $A \subset B'$, $A \subset B''$, $B' \neq B''$ and $\varrho(B') = \varrho(B'') = \varrho(A)+1$ then $(B'\backslash A) \cap (B''\backslash A) = \emptyset$.* ∎

The matroid $M^* = (E,\varrho^*)$ *dual* to a given matroid $M = (E,\varrho)$ may be defined as a matroid with the rank function

$$\varrho^*(A) = |A| + \varrho(E \setminus A) - \varrho(E) \tag{2.1.2}$$

(called the *corank* function) or equivalently,

$$\mathcal{B}^* = \{E\backslash B : B \in \mathcal{B}\}$$

defines $M^* = (E,\mathcal{B}^*)$.

The formula (2.1.2) determines the families $\mathcal{I}^*$, $\mathcal{B}^*$, $\mathcal{C}^*$ and $\mathcal{J}^*$. Then we can denote the duals of $(E,\mathcal{I})$, $(E,\mathcal{B})$ and $(E,\mathcal{J})$ by $(E,\mathcal{I}^*)$ etc. Elements of $\mathcal{B}^*$ are *cobases*, elements of $\mathcal{C}^*$ are *cocircuits*.

If $M = (E,\mathcal{C})$, then the duals are denoted by $M^* = (E,\mathcal{C}^*)$ ($M^* = (E,\varrho^*)$ etc.). It is well known that $M^{**} = M$. If $L = \{e\}$ is a loop in M^* then by L^* we denote a *coloop* in M.

Let $T \subset E$. The *restriction* $M|T$ of a matroid M to T is defined as the matroid on T such that

$$\mathcal{I}(M|T) = \{I : I \subset T,\ I \in \mathcal{I}(M)\}.$$

The *contraction* $M.T$ of a matroid M to T is defined as the matroid $M = (E,\varrho^T)$ such that

$$\varrho^T(A) = \varrho(A \cup (E \setminus T)) - \varrho(E \setminus T)$$

for any $A \subseteq T$. For $T = E \setminus \{e\}$, we use the abbreviations $M^{-e} = M|(E \setminus \{e\})$ and $M^{\times e} = M.(E \setminus \{e\})$. It is well known that $(M|T)^* = M^*.T$ and $(M.T)^* = M^*|T$.

If for some $T \subseteq E$, $M' = M|T$, then M' is called a *submatroid* of M. The notation $T \subset M$ means that T is a proper submatroid of the matroid M. If M' is a submatroid of M, isomorphic to a given matroid M_0, then M' will be called a *copy* of M_0.

If $M_i = (E_i, \mathcal{C}_i)$, $i = 1, \ldots, n$, then by $M_1 \cup \ldots \cup M_n$ we mean the matroid $M = (E, \mathcal{C})$ such that $E = E_1 \cup \ldots \cup E_n$ and $\mathcal{C}$ is the minimal family of circuits such that $\mathcal{C}_i \subseteq \mathcal{C}$.

A matroid is called *graphic* if there exists a graph such that $E(G)$ is the set of its edges and $\mathcal{C}(G)$ is a set of its cycles and M is isomorphic to $(E(G), \mathcal{C}(G))$. Such a matroid is denoted by $M(G)$. It is known that not every matroid is graphic.

EXAMPLE 2.1.6. Let $E = \{1, 2, \ldots, 7\}$. Define $\mathcal{X}_3$ as the following family of subsets of E:

$$\mathcal{X}_3 = \{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,7\}, \{2,5,6\}, \{3,4,6\}, \{3,5,7\}\}.$$

Let $\mathcal{X}_4 = \{A : A = E \setminus B,\ B \in \mathcal{X}_3\}$. The basis $\mathcal{B}$ of the matroid F_3 (the Fano matroid of rank 3, i.e. the Fano plane) is formed by all the three-element sets not contained in $\mathcal{X}_3$. The family of circuits $\mathcal{C}$ consists of all sets from $\mathcal{X}_3$ and $\mathcal{X}_4$. The dual matroid $F_3^* = F_4$ (the Fano matroid of rank 4) is the family of circuits $\mathcal{C}^* = \mathcal{X}_4$. The matroids F_3 and F_4 are not graphic.

Example 2.1.6 will be considered in geometric terms in Section 2.3.

If M is a matroid on E with rank function ϱ, its *rank generating function* $R(M; x, y)$ is defined by

$$R(M; x, y) = \sum_{A \subseteq E} x^{\varrho(E) - \varrho(A)} y^{|A| - \varrho(A)}. \tag{2.1.3}$$

The *Tutte polynomial* $T(M; x, y)$ is defined by

$$T(M; x, y) = R(M; x - 1, y - 1). \tag{2.1.4}$$

From (2.1.2)–(2.1.4) one can obtain the following obvious result.

LEMMA 2.1.2. *For an arbitrary matroid M and its dual M^*,*

$$R(M; x, y) = R(M^*; y, x), \quad T(M; x, y) = T(M^*; y, x). \ \blacksquare$$

EXAMPLE 2.1.7. Consider the Fano matroid $F_3 = (E, \varrho)$ and $A \subset E$. If $|A| \leq 2$, then $\varrho(A) = |A|$. If $|A| \geq 4$ then $\varrho(A) = 3$. If $|A| = 3$ then we have seven sets A such that $\varrho(A) = 2$ and 28 sets A such that $\varrho(A) = 3$. Hence from (2.1.3) and (2.1.4) we obtain

$$\begin{aligned} T(F_3; x, y) = {} & 28 + 21(x-1) + 7(x-1)^2 + (x-1)^3 + 35(y-1) + 7(x-1)(y-1) \\ & + 21(y-1)^2 + 7(y-1)^3 + (y-1)^4. \end{aligned}$$

Therefore we get

$$T(F_3; x, y) = -28 + 3x + 4x^2 + x^3 + 3y + 7xy + 6y^2 + 3y^3 + y^4$$

and from Lemma 2.1.2

$$T(F_4; x, y) = -28 + 3x + 7xy + 6x^2 + 3x^3 + x^4 + 3y + 4y^2 + y^3.$$

Oxley and Welsh [40] proved the following result.

THEOREM 2.1.3. *There is a unique real-valued function satisfying these relationships*:

$$f(M) = f(N) \tag{2.1.5}$$

for isomorphic M and N;

$$f(M) = af(M^{-e}) + bf(M^{\times e}) \tag{2.1.6}$$

for fixed nonzero real numbers a and b, provided $\{e\}$ is not a separator of M;

$$f(M_1 \cup M_2) = f(M_1)f(M_2) \tag{2.1.7}$$

for any pair of disjoint matroids M_1, M_2;

$$f(L) = y \tag{2.1.8}$$

where L is a loop and

$$f(L^*) = x \tag{2.1.9}$$

where L^* is a coloop. Moreover, this function is given by

$$f(M) = a^{\varrho^*(E)} b^{\varrho(E)} T(M; x, y). \ \blacksquare \tag{2.1.10}$$

The chapter "The Tutte Polynomial and Its Applications" in [50] written by Brylawski and Oxley gives an extensive review of that area (see also the chapter "The Möbius Functions and the Characteristic Polynomial" by Zaslawsky in [51]).

Let E be a finite set and suppose the operator $c : 2^E \to 2^E$ satisfies the following conditions:

(i) $c(\emptyset) = \emptyset$,

(ii) $A \subseteq c(A)$,

(iii) $A \subseteq B \Rightarrow c(A) \subseteq c(B)$,

(iv) $c(c(A)) = c(A)$.

Then the operator c is called a *closure* operator. The set A is *convex* if $A = c(A)$. Let $\mathcal{B} = \{A : A = c(A)\}$. The family $\mathcal{B}$ is a family of convex sets if

(a) $\emptyset \in \mathcal{B}, \quad E \in \mathcal{B}$,

(b) $A, B \in \mathcal{B} \Rightarrow A \cap B \in \mathcal{B}$.

The operator c is determined by $c(A) = \bigcap_{A \subseteq B \in \mathcal{B}} B$.

Let $\mathcal{P}$ be a clutter. Then it is easy to obtain the following result.

PROPOSITION 2.1.4. *The operator c defined as follows:*

$$c(A) = \{s \in E : \forall_{B \in \mathcal{P}} \ s \in B \Rightarrow A \cap B \neq \emptyset\} \tag{2.1.11}$$

is a closure operator. ∎

If a closure operator c has the *exchange property*

(E) $$x, y \notin c(A), x \in c(A \cup y) \Rightarrow y \in c(A \cup x)$$

then c is a span and (E, c) is a matroid of flats.

The chapter "Introduction to Greedoids" in [50] written by Björner and Ziegler gives some additional material related to the above facts (closure operator, matroids and antimatroids, etc.).

Suppose a family of convex sets forms a lattice with $\mathbf{0} = \emptyset$ and $\mathbf{1} = E$. Let $x \lessdot y$ mean that $x \leq y$ and if $x \leq z$ and $z \leq y$, then either $x = z$ or $z = y$. Recall that the *Jordan–Dedekind property* means that every chain $(s_0 \lessdot \ldots \lessdot s_k)$ has the same length k. The rank $\varrho(s)$ is the length of the chain $(\mathbf{0} \lessdot \ldots \lessdot s)$. The lattice of flats of any matroid has the Jordan–Dedekind property.

2.2. Gaussian coefficients. Let $q \neq 1$ and k be natural numbers and $x \geq 0$ a real. In this paper, q is assumed to be fixed and the following notation will be used.

Let

$$[x] = \frac{q^x - 1}{q - 1},$$

$$[x]_k = [x][x-1]\dots[x-k+1] = \prod_{j=1}^{k} \frac{q^{x-j+1} - 1}{q - 1}, \quad [x]_0 = 1,$$

$$[k]! = [k]_k, \quad [0]! = 1.$$

The *Gaussian coefficients* are defined as follows:

$$\begin{bmatrix} x \\ k \end{bmatrix} = \frac{[x]_k}{[k]!} = \prod_{j=1}^{k} \frac{q^{x-j+1} - 1}{q^j - 1} \quad \text{for} \quad 0 \leq k \leq x,$$

$$\begin{bmatrix} x \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} x \\ k \end{bmatrix} = 0 \quad \text{for } k < 0 \text{ or } k > x.$$

Thus

$$\begin{bmatrix} x \\ 1 \end{bmatrix} = [x], \quad \begin{bmatrix} x \\ 2 \end{bmatrix} = \frac{[x][x-1]}{q+1}.$$

For a positive integer k,

$$[k] = \sum_{j=0}^{k-1} q^j = 1 + q + \ldots + q^{k-1}.$$

Note that

$$\lim_{q \to 1} [x]_k = (x)_k \quad \text{and} \quad \lim_{q \to 1} \begin{bmatrix} x \\ k \end{bmatrix} = \binom{x}{k}$$

where $(x)_k = x(x-1)\dots(x-k-1)$.

Numerical values of $\begin{bmatrix} x \\ k \end{bmatrix}$ for some q, k and integers x are tabulated in the Appendix (Table 1).

In the next sections, we shall need some simple equalities, bounds and approximations.

$$[x] - [y] = q^y [x - y] \quad \text{for } x \geq y,$$

$$[x] - [x-1] = q^{x-1},$$

$$[x]_n = [x]_k [x-k]_{n-k},$$

$$[x]_k = (-1)^k q^{kx - \binom{k}{2}} [-x+k+1]_k,$$

$$\begin{bmatrix} x+1 \\ k+1 \end{bmatrix} = \begin{bmatrix} x \\ k \end{bmatrix} + q^{k+1} \begin{bmatrix} x \\ k+1 \end{bmatrix} = q^{x-k} \begin{bmatrix} x \\ k \end{bmatrix} + \begin{bmatrix} x \\ k+1 \end{bmatrix},$$

$$\begin{bmatrix} x \\ k \end{bmatrix} = (-1)^k q^{kx - \binom{k}{2}} \begin{bmatrix} -x+k-1 \\ k \end{bmatrix}.$$

For nonnegative integers n:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix},$$

$$\begin{bmatrix} n \\ 0 \end{bmatrix} < \begin{bmatrix} n \\ 1 \end{bmatrix} < \ldots < \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix} = \begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix} > \ldots > \begin{bmatrix} n \\ k \end{bmatrix},$$

and (see [23])

$$q^{k(n-k)} \leq \begin{bmatrix} n \\ k \end{bmatrix} \leq q^{k(n-k-1)} < q^{kn}, \tag{2.2.1}$$

$$q^{kn-\binom{k}{2}} \geq (q-1)^k [n]_k \geq \beta q^{kn-\binom{k}{2}}, \tag{2.2.2}$$

where

$$\beta = \prod_{i=1}^{\infty} (1 - q^{-i}), \tag{2.2.3}$$

$$(q-1)^k [n]_k \sim q^{kn-\binom{k}{2}} \quad \text{if } kq^{-n+k} = o(n). \tag{2.2.4}$$

The following Euler identity (see, for example [34], p. 87) may be useful for computing the value of β:

$$\prod_{i=1}^{\infty} (1 - x^i) = 1 + \sum_{k=1}^{\infty} (-1)^k (x^{(3k^2-k)/2} + x^{(3k^2+k)/2}).$$

The following formula is well-known (see for example [34], p. 109):

$$b_r = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} a_k \Leftrightarrow a_r = \sum_{k=0}^{r} (-1)^{r-k} q^{\binom{r-k}{2}} \begin{bmatrix} r \\ k \end{bmatrix} b_k, \tag{2.2.5}$$

for $r = 0, 1, \ldots$, where $\{a_r\}$ and $\{b_r\}$ are real sequences. Formula (2.2.5) is a particular case of a general property known as the Möbius Inversion (see [51], p. 116).

More information about Gaussian coefficients may be found in Goulden and Jackson [12]. However, let us point out that if $q \geq 1$ and $x \to \infty$, some formulae are not valid.

2.3. Projective geometries. Finite projective geometries have a position among representable matroids analogous to that of complete graphs in graph theory. Only a brief sketch of the theory of projective geometries is presented below. The monograph by Hirschfeld [15] gives a detailed and self-contained exposition of this area. Oxley in [39] gives a brief but comprehensive exposition in terms of matroid theory.

Let $GF(q)$ be a Galois field, where q is a prime power and let $V(r, q)$ be an r-dimensional vector space on $GF(q)$. Let $\mathcal{L}$ be the lattice of subspaces of V. Atoms of $\mathcal{L}$ constitute the *points* of a *projective geometry* $PG(r-1, q)$ of dimension $r-1$. Assume that the empty set has dimension -1. Let $e \in \mathcal{L}$. If e is a subspace of dimension $k-1$ and $k > 2$, then let the rank of e, $\varrho(e)$, be k. Define the subspace A of rank k of $PG(r-1, q)$ as the set of all points $p < e$. Then $\varrho(A) = k$. Note, however, that we have to distinguish between a subspace of rank k of $PG(r-1, q)$, a subspace of dimension $k-1$ of the vector space V and an element of the lattice $\mathcal{L}$ of rank k. If x is a point and l is a line and $x \in l$, then we say that the point x *is on* the line l, or that the line l *passes through* or *contains* x. If the line l contains two distinct points x, y we call it the line xy. If distinct points x, y, z are on a common line l, we say that they are *collinear*.

Projective geometries can be defined in an axiomatic way (see [46], p. 193). A projective geometry satisfies the following axioms:

1. Any two distinct points are on exactly one line.

2. Let x, y, w, z be four distinct points such that no three points are collinear. If xy intersects zw, then xz intersects yw.

3. Each line contains at least three points.

Every geometry of dimension $n > 2$ is isomorphic to $PG(n, q)$ defined above.

It is well known that $PG(r-1, q)$ is a matroid $(E, \mathcal{J})$, where E is the set of points and $\mathcal{J}$ is the family of all subspaces of the geometry. A matroid M is *representable* if there exists $PG(r-1, q)$ such that M is isomorphic to some submatroid of $PG(r-1, q)$. It is well known that the ground set E of $PG(r-1, q)$ has $[r]$ elements and $\begin{bmatrix} r \\ k \end{bmatrix}$ rank-k subspaces. Subspaces of rank 2 (2-flats) are called *lines* and subspaces of rank $r-1$ are called *hyperplanes*.

EXAMPLE 2.3.1. The Fano matroid of rank 3, defined in Example 2.1.6, is the simplest case of a projective geometry: $F_3 = PG(r-1, q)$, $r = 3$ and $q = 2$. Let $V = \{0, 1\}^3$. One-dimensional (and one-element) subspaces of V are points of $PG(2, 2)$. Every line has three points, as in Figure 2.3.1.

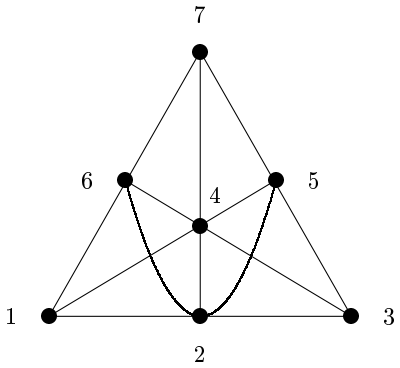

Fig. 2.3.1. Fano plane of rank 3, $PG(2, 2)$

Recall that the subspaces of $PG(r-1, q)$ form a modular geometric lattice. Hence if $A, B \in \mathcal{J}$, then $\varrho(A \cup B) = \varrho(A) + \varrho(B) - \varrho(A \cap B)$ (see Welsh [46], p. 195). The following lemma (cf. Oxley [38]) is frequently used.

LEMMA 2.3.1. *The number of rank-s subspaces of $PG(r-1, q)$ which meet a fixed rank-t subspace in a subspace of rank u is*

$$\begin{bmatrix} r-t \\ s-u \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} q^{(s-u)(t-u)}$$

and, in particular, the number of rank-s subspaces containing a fixed subspace of rank u is

$$\begin{bmatrix} r-u \\ s-u \end{bmatrix}. \quad (2.3.1)$$

■

From Lemma 2.3.1 we immediately obtain the following results:

LEMMA 2.3.2. *The number of pairs of rank-s subspaces of $PG(r-1,q)$ which meet in a subspace of rank u is*

$$\begin{bmatrix} r \\ s \end{bmatrix} \begin{bmatrix} r-s \\ s-u \end{bmatrix} \begin{bmatrix} s \\ u \end{bmatrix} q^{(s-u)^2}. \ \blacksquare$$

Also

$$\sum_{s=0}^{d} \begin{bmatrix} r-d \\ d-s \end{bmatrix} \begin{bmatrix} d \\ s \end{bmatrix} q^{(d-s)^2} = \begin{bmatrix} r \\ d \end{bmatrix}. \tag{2.3.2}$$

Voigt [45] proved the following result.

LEMMA 2.3.3. *The number of k-tuples of mutually disjoint rank-s subspaces of $PG(r-1,q)$ is*

$$\prod_{j=0}^{k-1} \begin{bmatrix} r-js \\ s \end{bmatrix} q^{s^2\binom{k}{2}}. \ \blacksquare$$

Note that from any of the above two lemmas, we deduce that the number of disjoint pairs of rank-s subspaces of $PG(r-1,q)$ is $\begin{bmatrix} r \\ s \end{bmatrix} \begin{bmatrix} r-s \\ s \end{bmatrix} q^{s^2}$.

LEMMA 2.3.4. *There are $[r-u]$ rank-$(u+1)$ subspaces α_i containing a fixed rank-u subspace V. For every pair i,j such that $i \neq j$, we have $\alpha_i \cap \alpha_j = V$. Moreover,*

$$\bigcup_{i=1}^{[r-u]} \alpha_i = PG(r-1,q). \tag{2.3.3}$$

P r o o f. From Lemma 2.3.1, by substituting $s = u+1$ and $t-u$ in (2.3.1) we obtain the first assertion. Because $\varrho(\alpha_i \cap \alpha_j) < \varrho(\alpha_i)$ and $V \subset \alpha_i$, we obtain the second one. Then (2.3.3) follows from the equality

$$[r-u]([u+1]-[u]) + [u] = [r-u]q^u + [u] = [r]. \ \blacksquare$$

Denoting by Γ the set of all rank-d subspaces in $PG(r-1,q)$ and

$$\Gamma(\alpha) = \{\beta \in \Gamma : \alpha \cap \beta \neq \emptyset\}$$

we have from (2.3.2),

$$|\Gamma(\alpha)| = \sum_{k=1}^{d} \begin{bmatrix} r-d \\ d-u \end{bmatrix} \begin{bmatrix} d \\ u \end{bmatrix} q^{(d-u)^2} = \begin{bmatrix} r \\ d \end{bmatrix} - \begin{bmatrix} r-d \\ d \end{bmatrix} q^{d^2}. \tag{2.3.4}$$

Kelly and Oxley in [23] proved the following results.

LEMMA 2.3.5. *If B is a basis of $PG(r-1,q)$, there are precisely $(q-1)^{r-1}$ elements e of $PG(r-1,q)$ such that $B \cup \{e\}$ is a circuit.* $\blacksquare$

Let $\mathcal{I}_{r,k}$ and $\mathcal{C}_{r,k}$ be the collections of k-element independent sets and k-element circuits of $PG(r-1,q)$, respectively. Hence, by simple computation we have

$$|\mathcal{I}_{r,k}| = \frac{q^{\binom{k}{2}}}{k!}[r]_k \tag{2.3.5}$$

and additionally, using Lemma 2.3.5, we obtain

$$|\mathcal{C}_{r,k}| = \frac{q^{\binom{k-1}{2}}}{k!}(q-1)^{k-2}[r]_{k-1} \quad \text{for } k \geq 3. \tag{2.3.6}$$

Let m_i denote the number of members of $\mathcal{C}_{r,k}$ which meet $C \in \mathcal{C}_{r,k}$ in exactly i elements. Let n_i denote the number of members of $\mathcal{I}_{r,k}$ which meet $I \in \mathcal{I}_{r,k}$ in exactly i elements. This number does not depend on the choice of C or I.

LEMMA 2.3.6.

$$m_i \le \begin{cases} \dfrac{1}{(k-i)!}\binom{k}{i} q^{\binom{k-1}{2}-\binom{i}{2}} (q-1)^{k-2} [r-i]_{k-i-1} & \text{if } \ 0 \le i \le k-1, \\ 1 & \text{if } \ i = k. \end{cases}$$

and

$$n_i \le \frac{1}{(k-1)!}\binom{k}{i} q^{\binom{k}{2}-\binom{i}{2}} [r-i]_{k-i} \quad \text{for } \ 0 \le i \le k. \ \blacksquare$$

2.4. Special classes. Let $T \subset M$ and

$$d(T) = \frac{|T|}{\varrho(T)}$$

denote the *density* of T (see e.g. [37]), and

$$\gamma(M) = \max\{d(T) : T \subseteq M\}.$$

Let

$$\eta(M) = \min\left\{ \frac{|M| - |T|}{\varrho(M) - \varrho(T)} : T \subset M, \ \varrho(T) < \varrho(M) \right\}.$$

After Cunningham [9], we refer to $\eta(M)$ as the *strength* of the matroid M. The two functions γ and η are closely related. One can prove (see [8]) that for any loopless matroid M having a loopless dual M^*,

$$\eta(M^*) = \frac{\gamma(M)}{\gamma(M)-1}, \qquad \gamma(M^*) = \frac{\eta(M)}{\eta(M)-1}.$$

The definitions of $\gamma(M)$ and $\eta(M)$ give

$$\eta(M) \le d(M) \le \gamma(M). \tag{2.4.1}$$

Let

$$\varepsilon = \min\{\varrho(T)(d(M) - \gamma(T)) : T \subset M\}$$

denote the *balance index* (see [18], for graphs).

Let $e(G)$ denote the number of edges and $v(G)$ denote the number of vertices of the graph G. Let

$$\overline{d}(G) = \frac{e(G)}{v(G)}$$

denote the density of the graph G for nonempty G (i.e. $e(G) > 0$) and

$$d^*(G) = \frac{e(G)}{v(G)-1}.$$

If G is connected, then $d(M(G)) = d^*(G) > \overline{d}(G)$. A matroid M is *balanced* if $\gamma(M) = d(M)$ and is *strictly balanced* if $\gamma(T) < d(M)$ for all $T \subset M$. The graph G is *balanced* if $\overline{d}(G) = \max_{H \subseteq G} \overline{d}(H)$, strongly balanced if $d^*(G) = \max_{H \subseteq G} d^*(H)$ and strictly balanced if $\overline{d}(G) > \max_{H \subset G} \overline{d}(H)$. It is easy to see that $\eta(M) = d(M)$ iff M is balanced and $\eta(M) < d(M)$ iff M is strictly balanced.

Moreover, M is balanced iff $\varepsilon(M) \geq 0$ and M is strictly balanced iff $\varepsilon(M) > 0$.

Let $\mathcal{M}$ be a family of matroids. Let

$$\varepsilon(\mathcal{M}) = \min_{M \in \mathcal{M}} \varepsilon(M). \tag{2.4.2}$$

We have the following result (see [28]), which is a counterpart to the lemma of Karoński [18] for matroids.

LEMMA 2.4.1. *Let $\mathcal{B}$ be a family of balanced matroids, each of which has m elements and rank k. Suppose that each matroid M_i, $i = 1, \ldots, n$, is isomorphic to some matroid from $\mathcal{B}$, and for at least one pair M_i, M_j, $i \neq j$, we have*

$$\sigma(M_i) \cap \sigma(M_j) \neq \emptyset \quad \textit{and} \quad F_n = M_1 \cup \ldots \cup M_n.$$

Then

$$|F_n| \geq \frac{m}{k} \varrho(F_n) + \varepsilon(\mathcal{B}). \ \blacksquare$$

Let $f_r^{(k)}$ denote the number of flats of rank k in $M(r)$. Clearly $|M(r)| = f_r^{(1)}$. We call the family $\{M(r)\}_{r=1}^{\infty}$ *exponentially growing* if there exists a function g_r such that

$$f_r^{(k)} \asymp g_r^k,$$

for any fixed k. Let K_n be a complete graph on n vertices. It is obvious that $M(K_n)$ and $PG(r-1, q)$ are exponentially growing with $g_r = r$ if $M(r) = M(K_n)$ and $g_r = q^r$ if $M(r) = PG(r-1, q)$.

3. Probabilistic tools

Throughout this monograph, we will use the following notation: $g(n) = o(f(n))$ for $\lim_{n\to\infty} g(n)/f(n) = 0$, $g(n) = O(f(n))$ for $|g(n)/f(n)| < C = \text{const}$, $f(n) \sim g(n)$ for $\lim_{n\to\infty} g(n)/f(n) = 1$ and $f(n) \asymp g(n)$ for $g(n) = O(f(n))$ and $f(n) = O(g(n))$. We write $\{A_n\}$ a.s. for $\lim_{n\to\infty} \operatorname{Prob}(A_n) = 1$ or simply a.s. A when $A = A_n$.

3.1. Poisson convergence. Let $(\Omega, \mathcal{S}, \operatorname{Prob})$ be a probability space. Consider a sequence of random variables X_n, $n = 1, 2, \ldots$, defined on $(\Omega, \mathcal{S}, \operatorname{Prob})$. The distribution of the random variables $\{X_n\}$ converges to a Poisson distribution with mean λ if for each $j = 0, 1, 2, \ldots$,

$$\lim_{n\to\infty} \operatorname{Prob}(X_n = j) = \frac{\lambda^j e^{\lambda}}{j!}.$$

If $\operatorname{E} X_n^k \to \operatorname{E} X^k$ as $n \to \infty$, $k = 1, 2, \ldots$, then $X_n \to X$ in distribution, provided that X is uniquely determined by its moments. The method of moments plays a crucial role in proving convergence to a Poisson distribution, but does not give the rate of such convergence. Moreover, this method leads to very complicated calculations. Therefore, we try to use more recent methods such as exponential bounds and the Stein–Chen method for Poisson approximation.

Let I_α be an indicator 0-1 random variable, $\alpha \in \Gamma$ (a set of indices) with $\pi_\alpha = \operatorname{Prob}(I_\alpha = 1)$. Let $X = \sum_{\alpha\in\Gamma} I_\alpha$, $\lambda = \operatorname{E} X$, $\sigma^2 = \operatorname{Var} X$.

Janson, L uczak and Ruciński [18] proved (see also [17]) the following result.

LEMMA 3.1.1.

$$-\sum_{\alpha\in\Gamma}\log(1-\pi_\alpha)\le\log\operatorname{Prob}(X_r=0)\le-\sum_{\alpha\in\Gamma}\operatorname{E}\frac{I_\alpha}{\sum_{\alpha\sim\beta}I_\beta}$$

and if the π_α are independent of α then

$$\log\operatorname{Prob}(X_r=0)\le-\frac{(\operatorname{E}X_r)^2}{\sum\sum_{\beta\sim\alpha}\operatorname{E}I_\alpha I_\beta}. \tag{3.1.1}$$ ∎

Suppose that for each $\alpha\in\Gamma$, there exist 0-1 random variables $\{J_{\beta\alpha},\beta\in\Gamma\}$ defined on the same probability space as $\{I_\beta,\beta\in\Gamma\}$ with

$$\mathcal{L}(J_{\beta\alpha},\beta\in\Gamma)=\mathcal{L}(I_\beta,\beta\in\Gamma|I_\alpha=1).$$

We call $\{I_\alpha,\alpha\in\Gamma\}$ *positively related* if $J_{\beta\alpha}\ge I_\beta$ and *negatively related* if $J_{\beta\alpha}\le I_\beta$ for all $\beta\ne\alpha$.

Let $d_{\mathrm{TV}}(\mathcal{L}(X),\mathrm{Po}(\lambda))$ denote the *total variation* distance between $\mathcal{L}(X)$ and $\mathrm{Po}(\lambda)$, where $\mathrm{Po}(\lambda)$ denotes the Poisson distribution with mean λ, that is,

$$d_{\mathrm{TV}}(\mathcal{L}(X),\mathrm{Po}(\lambda))=\sup_{A\subseteq\{0,1,\dots\}}|\operatorname{Prob}(X\in A)-\operatorname{Prob}(Y\in A)|=\delta$$

where Y is a Poisson random variable with mean λ. We call X are *Poisson convergent* if and only if $\delta\to0$.

Barbour, Holst and Janson give the following inequality ([3], formula (1.2)):

LEMMA 3.1.2.

$$d_{\mathrm{TV}}(\mathcal{L}(X),\mathrm{Po}(\lambda))\le\frac{1-e^{-\lambda}}{\lambda}\sum_{\alpha\in\Gamma}\operatorname{Prob}(I_\alpha=1)\operatorname{E}\Big|I_\alpha+\sum_{\beta\ne\alpha}(I_\beta-J_{\beta\alpha})\Big|. \tag{3.1.2}$$ ∎

We use the following inequality for δ ([3], Corollary 2.C.4):

LEMMA 3.1.3. *If the random variables $\{I_\alpha,\alpha\in\Gamma\}$ are positively related, then*

$$\delta\le\frac{1-e^{-\lambda}}{\lambda}\Big(\sigma^2-\lambda+2\sum_{\alpha\in\Gamma}\pi_\alpha^2\Big).$$ ∎

The following corollary is then immediate.

COROLLARY 3.1.4. *If $\{I_\alpha,\alpha\in\Gamma\}$ are positively related, then X is Poisson convergent if and only if $\sigma^2\sim\lambda$ and $\sum_{\alpha\in\Gamma}\pi_\alpha^2/\lambda\to0$.* ∎

LEMMA 3.1.5. *If $\{I_\alpha,\alpha\in\Gamma\}$ are positively or negatively related, then*

$$d_{\mathrm{TV}}(\mathcal{L}(X),\mathrm{Po}(\lambda))\le\frac{1-e^{-\lambda}}{\lambda}\sum_{\alpha\in\Gamma}\Big((\operatorname{Prob}(I_\alpha=1))^2+\sum_{\beta\ne\alpha}|\operatorname{Cov}(I_\alpha,I_\beta)|\Big). \tag{3.1.3}$$

P r o o f. Since $\operatorname{Prob}(I_\alpha=1)\operatorname{E}(J_{\beta\alpha}-I_\alpha)=\operatorname{Cov}(I_\alpha,I_\beta)$, from Lemma 3.1.2 we obtain the above assertion. ∎

3.2. Normal convergence. We shall denote by

$$\widetilde{X}_n = \frac{X_n - \mathrm{E}\, X_n}{\sqrt{\mathrm{Var}\, X_n}}$$

a standardized random variable. Throughout this text the notation $\widetilde{X}_n \to \mathrm{N}(0,1)$ means that $\widetilde{X}_n$ converges in distribution to the standard normal distribution; that is,

$$\lim_{n\to\infty} \mathrm{Prob}(\widetilde{X}_n < x) = \Phi(x), \quad -\infty < x < \infty,$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-u^2/2}\, du.$$

The review paper [43] offers a broad overview of methods that are used to prove asymptotic normality in combinatorics. In this section, we present only one of them, which seems to be the most appropriate for our problems.

Janson [16] introduced a method of cumulants as the method of proving asymptotic normality. We present this method in the improved version of Mikhailov [36].

Let $\{\xi_i, i = 1, \dots, n\}$ be a family of random variables (not necessarily $0-1$ r.vs.). The *dependency graph* $\mathcal{G}$ of $\{\xi_i\}$ is a graph on the set of vertices $\{1, \dots, n\}$. Let $V \cap W = \emptyset$. If there is no edge between V and W, then $\{X_j, j \in V\}$ and $\{X_j, j \in W\}$ are independent. The maximum degree Δ of $\mathcal{G}$ is defined as usual, except that it is defined to be 1 for an empty graph. For every $V \subseteq \{1, \dots, n\}$ define

$$L(V) = V \cup \{i : \text{there exists an edge from } i \text{ to } V\}.$$

Mikhailov [36] proved the following generalization of Janson's theorem [16].

THEOREM 3.2.1. *Let $\{\xi_{ni}, i = 1, \dots, N_n\}$ be an array of random variables such that for all n*

$$\sum_{i \in L(V)} \mathrm{E}\,(|\xi_{ni}| \mid \mathcal{F}(V)) \le C_{|V|} Q \quad \textit{a.s.},$$

where $C_{|V|}$ is not dependent on n and Q is not dependent on $|V|$. $\mathrm{E}\,(\cdot|\mathcal{F}(V))$ is the conditional expectation with respect to the σ-field generated by the family of random variables $\{\xi_{ni}, i \in V\}$. Let $S_n = \sum_{i=1}^{N_n} \xi_{ni}$ and $M_n = \sum_{i=1}^{N_n} \mathrm{E}\,\xi_{ni}$. If

$$\exists_{0<\alpha\le 2/3} \left(\frac{M_n}{Q}\right)^{\alpha} \frac{Q^2}{\sqrt{\mathrm{Var}\, S_n}} \to 0 \tag{3.2.1}$$

then $\widetilde{S}_n \to \mathrm{N}(0,1)$. ∎

From Theorem 3.2.1 one can obtain Janson's original results:

THEOREM 3.2.2. *Let $\{\xi_{ni}, i = 1, \dots, N_n\}$ be an array of random variables such that $|\xi_{ni}| \le A_n < \infty$ a.s, for $i = 1, \dots, N_n$. If*

$$\exists_{0<\alpha\le 2/3} \left(\frac{N_n}{\Delta_n}\right)^{\alpha} \frac{\Delta_n^2 A_n^2}{\sqrt{\mathrm{Var}\, S_n}} \to 0, \tag{3.2.2}$$

then $\widetilde{S} \to \mathrm{N}(0,1)$. ∎

If the ξ_{ni} are indicator random variables, Ruciński [43] improved Theorem 3.2.2 to the following form.

THEOREM 3.2.3. *Let b_n be an upper bound for* $\mathrm{Prob}(\xi_{ni}=1)$. *If*

$$N_n b_n \Delta_n^{m-1}\sigma_n^{-m} \to 0, \tag{3.2.3}$$

then $\widetilde{S} \to \mathrm{N}(0,1)$.

This result is weaker (but easier to apply) than the result of Mikhailov. However, if $p \to c > 0$, then both criterions are equivalent.

3.3. Markov processes on finite lattices. Let $\mathcal{L} = (E, \leq)$ be a finite lattice with minimal element $\mathbf{0}$ and maximal element $\mathbf{1}$.

Define a Markov process $\xi(t)$ on $\mathcal{L}$ with infinitesimal matrix $[\mu_{rs}]$ (see [20], p. 225). Assume that if $r \neq s$ and $\mu_{rs} > 0$, then $r \lessdot s$. Let

$$\mu_s = \sum_{r \gtrdot s} \mu_{sr}. \tag{3.3.1}$$

Then we have the forward Kolmogorov equations

$$P_s'(t) = -\mu_s P_s(t) + \sum_{r \lessdot s} P_r(t)\mu_{rs}.$$

Assume that $\mu_{\mathbf{0}} > \mu_{s_1} > \ldots > \mu_{s_k} > \ldots > \mu_{\mathbf{1}} = 0$ for any sequence $\mathbf{0} < s_1 < \ldots < s_k < \ldots < \mathbf{1}$. Let $\mathbf{0} \lessdot s_1 \lessdot s_2 \lessdot \ldots \lessdot s_k = s$, and let τ_ω be the moment of achieving $\mathbf{1}$ along the trajectory $\omega = (\mathbf{0}, s_1, s_2, \ldots, \mathbf{1})$. Then τ_ω is the sum of waiting times in states s_i, each from the exponential distribution with parameter μ_{s_i}. The distribution function of τ_ω is the convolution $F(t) = \mathrm{Prob}(\tau_\omega < t) = F_1(t) * \ldots * F_{k-1}(t)$, $F_i(t) = 1 - e^{\mu_{s_i} t}$.

Below we present two simple properties of exponential distributions and Markov chains. The first one was presented in [35].

LEMMA 3.3.1. *If $F_i(t) = 1 - e^{-\lambda_i t}$ for $i = 1, 2, \ldots, n$ and $\lambda_1 > \lambda_2 > \ldots > \lambda_n$ then*

$$F(t) = \sum_{k=1}^{n} (1 - e^{-\lambda_k t}) \prod_{j \neq k} \frac{\lambda_j}{\lambda_j - \lambda_k}. \tag{3.3.2}$$

P r o o f. Denoting by $F^*(s)$ the Laplace transform of the distribution function $F(t)$, we have $F_i^*(s) = \lambda_i/(\lambda_i + s)$ and

$$F^*(s) = \prod_{k=1}^{n} \frac{\lambda_k}{\lambda_k + s} = \sum_{k=1}^{n} \frac{A_k}{\lambda_k + s}.$$

Since

$$A_m = \frac{\prod_{j=1}^{n} \lambda_j}{\prod_{j \neq m} (\lambda_j - \lambda_m)}$$

it follows that

$$F^*(s) = \sum_{k=1}^{n} \frac{\lambda_k}{\lambda_k + s} \prod_{j \neq k} \frac{\lambda_j}{\lambda_j - \lambda_k}$$

and we obtain assertion (3.3.2). ∎

LEMMA 3.3.2. *Let X_t and Y_t be two finite Markov processes on the same space S. Assume that both X_t and Y_t have the same embedded Markov chains $[p_{ij}]$, $i,j \in S$ and $\mu'_i \geq \mu''_i$ for all $i \in S$ where μ'_i and μ''_i are the parameters given by* 3.3.1 *for state $i \in S$ for X_t and Y_t, respectively. Let τ_X and τ_Y be the times of achieving state s'' starting from state s' for X_t and Y_t, respectively. We have*

$$\text{Prob}(\tau_X < t) > \text{Prob}(\tau_Y < t). \tag{3.3.3}$$

P r o o f. Let p_ω denote the probability that s'' is achieved from s' along $\omega = (s' = s_1, s_2, \ldots, s'')$. Hence

$$\text{Prob}(\tau < t) = \sum_\omega p_\omega \,\text{Prob}(\tau_\omega < t)$$

where τ is either τ_X or τ_Y. The sum is taken over all the trajectories from s' to s''. If the graph of transitions of the embedded Markov chain is acyclic, then this sum has a finite number of summands. Since the probability that X_t is in state s for a time shorter than x is greater than the probability that Y_t is in state s for a time shorter than x, we obtain assertion (3.3.3). ∎

If the trajectory $\omega = (\mathbf{0}, s_1, s_2, \ldots, \mathbf{1})$ is fixed then

$$P_\omega(t) = \text{Prob}(\tau_\omega < t) = \sum_{j=0}^{k-1} (1 - e^{-\mu_{s_j} t}) \prod_{i \neq j} \frac{\mu_{s_i}}{\mu_{s_i} - \mu_{s_j}}.$$

The same considerations will be valid for the reverse inequalities. Thus from the Lemmas 3.3.1 and 3.3.2, we immediately obtain the following result which generalizes Theorem 1 from [35].

THEOREM 3.3.3. *Let $\mathcal{L}$ be a lattice with the Jordan–Dedekind property and with rank function ϱ. Let $\varrho(\mathbf{1}) = k$, $m'_i = \min_{\varrho(r)=i} \mu_r$ and $m''_i = \max_{\varrho(r)=i} \mu_r$. Then*

$$\sum_{j=0}^{k-1} (1 - e^{-t m'_j}) \prod_{i \neq j} \frac{m'_i}{m'_i - m'_j} \leq \text{Prob}(\tau < t) \leq \sum_{j=0}^{k-1} (1 - e^{-t m''_j}) \prod_{i \neq j} \frac{m''_i}{m''_i - m''_j}. \tag{3.3.4}$$ ∎

4. Random matroids—general approach

4.1. Definitions. Let M be a matroid on the set E and suppose that each element of E has, independently of all other elements, probability $q = 1 - p$ of being deleted from E. We call the resulting set R a *random set* and we denote by $\omega_1(M) = M|R$ a *random matroid of the first type* and by $\omega_2(M) = M.R$ a *random matroid of the second type.*

Recall (see Section 2.1) that independent sets in the restriction $M|T$ of a matroid M to T are independent sets I in M such that $I \subseteq T$. The contraction $M.T$ satisfies the formula $M.T = (M^*|T)^*$. In fact, in almost all the sections, we consider only matroids of the first type. The only exception will be in Section 4.3. Hence, we use $\omega(M)$ rather than $\omega_1(M)$ throughout the paper (excluding Section 4.3).

If M is the projective geometry $PG(r-1, q)$, then we write ω_r instead of $\omega(M) = M|R$.

In particular applications (i.e. in reliability theory), elements of E can be selected with different probabilities. In such cases, we let $p_e = \text{Prob}(e \in R)$ and $\mathbf{p} = (p_e; e \in E)$.

In this case a random matroid is denoted by $\omega(M, \mathbf{p})$. Sometimes instead of p we shall write $1 - e^{-t}$, $t > 0$. This notation was introduced by Stepanov [44].

If the probabilities p_e are different for different $e \in E$, then we can write $p_e = e^{\lambda_e t}$, $\lambda_e > 0$ and $\lambda = (\lambda_e; e \in E)$. For $A \subseteq E$ we let $\Lambda(A) = \sum_{e \in A} \lambda_e$.

Define a *continuous random-M-process* $\{\omega(M, \Lambda, t), t \in [0, \infty)\}$ as a process which starts with the empty set at $t = 0$ and an element e arises before time t with probability $1 - e^{-\lambda_e t}$ independently of all other elements. If t is fixed, then $\omega(M, \Lambda, t)$ is a random matroid $\omega(M)$ with $p_e = 1 - e^{-\lambda_e t}$ for each $e \in E$. If $\lambda \equiv 1$ (and $\Lambda(A) = |A|$), we simply write $\omega(M, t)$ for $\omega(M, \Lambda, t)$.

Define a *discrete random-M-process* $\{\omega(n)\}_{n=0}^{|M|}$ as a Markov chain of subsets of elements of the matroid M, which starts with the empty set, and, for $n = 1, 2, \ldots, |M|$, $\omega(n)$ is obtained by the addition to $\omega(n-1)$ of a new, randomly chosen, element of M. Clearly, one may also view the random matroid $\omega(n)$ as a subset chosen at random from all the n-element subsets of the matroid M.

Let $\mathcal{A}$ be some class of matroids. Then the event that $\omega(M, p) \in \mathcal{A}$ means that $\omega(M, p)$ has *property* $\mathcal{A}$. Here $\mathcal{A}$ is simply meant as the property of a random matroid. Similarly one can define the properties of a process $\omega(M, \Lambda, t)$ or $\omega(n)$. Now we restrict ourselves to the case $p_e = p$ for all $e \in E$.

Let $\omega(M_n, p_n)$ be a sequence of random matroids. A *threshold function* for the property $\mathcal{A}$ is a function $f(n)$ such that

$$\lim_{n\to\infty} \operatorname{Prob}(\omega(M_n, p_n) \in \mathcal{A}) = \begin{cases} 0 & \text{if } \lim_{n\to\infty} p_n/f(n) = 0, \\ 1 & \text{if } \lim_{n\to\infty} p_n/f(n) = \infty. \end{cases} \tag{4.1.1}$$

For a random process $\omega(M, t)$ the threshold function $f(n)$ satisfies the relation

$$\lim_{n\to\infty} \operatorname{Prob}(\omega(M_n, t_n) \in \mathcal{A}) = \begin{cases} 0 & \text{if } \lim_{n\to\infty} t_n/f(n) = \infty, \\ 1 & \text{if } \lim_{n\to\infty} t_n/f(n) = 0. \end{cases} \tag{4.1.2}$$

Knuth [27] showed a quite different way of obtaining random matroids. In his definition of a random matroid $(E, \mathcal{F})$, where $\mathcal{F}$ is a set of flats, the set E is fixed and the family $\mathcal{F}$ is constructed step by step, starting with $\mathcal{F}_0 = \{\emptyset\}$. Then in each step of the iteration, by using a few "random sets", the family $\mathcal{F}_{r+1}$ is obtained from $\mathcal{F}_r$, where all the flats from $\mathcal{F}_r$ have rank r. When the algorithm stops, the matroid has a random rank. The detailed construction is as follows.

Algorithm 4.1.1. *Let E be a nonempty set.*

Step 1 (*Initialize*) *Let $r = 0$ and $\mathcal{F}_0 = \{\emptyset\}$.*

Step 2 (*Generate covers*)

$$\mathcal{F}_{r+1} = \{B : B = A \cap \{a\},\ A \in \mathcal{F}_r,\ a \in E \setminus A\}.$$

Step 3 (*Enlarge*) *Add additional sets to $\mathcal{F}_{r+1}$, perhaps in a "random manner", where each new set properly contains some set from $\mathcal{F}_r$.*

Step 4 (*Superpose*) *If $A, B \in \mathcal{F}_{r+1}$ but $A \cap B$ is not contained in any $C \in \mathcal{F}_r$, replace A and B in $\mathcal{F}_{r+1}$ by $A \cup B$. Repeat this operation until $A \cap B \subset C$ for some $C \in \mathcal{F}_r$ whenever $A, B \in \mathcal{F}_{r+1}$, $A \neq B$.*

STEP 5 (*Test for completion*) *If* $E \in \mathcal{F}_{r+1}$, *then stop the algorithm, otherwise increase* r *by* 1 *and go to Step* 2.

The following theorem gives the most important properties of this algorithm.

THEOREM 4.1.2.

- *The family* $\mathcal{F}$ *obtained from Algorithm* 4.1.1 *is a family of flats. Hence* $(E, \mathcal{F})$ *is a matroid for every choice of sets in Step* 3 *of Algorithm* 4.1.1.
- *The resulting matroid obtained from Algorithm* 4.1.1 *does not depend on the order of replacements in Step* 4.
- *Every matroid is obtainable by Algorithm* 4.1.1. ■

Knuth [27] gives a computer program for Algorithm 4.1.1, written in ALGOL W. An implementation rewritten in C [11] is available.

4.2. Rank. Let $P(M, \mathbf{p})$ be the probability that $\omega(M)$ has the same rank as M. In other words, $P(M, \mathbf{p})$ denotes the probability that the random set R of elements selected according to probabilities $\mathbf{p}$, contains at least one basis from $\mathcal{B}$. Let $P_k(M, \mathbf{p})$ mean that $\omega(M)$ has rank k. Therefore, $P(M, \mathbf{p}) = P_{\varrho(M)}(M, \mathbf{p})$.

It is easy to see that

$$P(M, \mathbf{p}) = \sum \prod_{e \notin A} (1 - p_e) \prod_{e \in A} p_e, \tag{4.2.1}$$

where the sum is taken over all the subsets $A \subseteq E$ which contain some basis $B \in \mathcal{B}$. Since

$$\sum_{E' \in \mathcal{J}} P(M', \mathbf{p}) \prod_{e \notin E'} (1 - p_e) = 1,$$

we have

$$P(M, \mathbf{p}) = 1 - \sum_{E \neq E' \in \mathcal{J}} P(M', \mathbf{p}) \prod_{e \notin E'} (1 - p_e). \tag{4.2.2}$$

Let $p_e = 1 - e^{\lambda_e t}$ and let $P_k(M, \Lambda, t)$ mean, as above, that $\omega(M)$ has rank k. Thus $P(M, \Lambda, t) = P_{\varrho(M)}(M, \Lambda, t)$.

Formula (4.2.2) shows the difference between the probability that a random matroid has a full rank and the probability that a random graph is connected. In the case of random matroids, it is necessary to consider all flats in M. In the case of a random graph, it is sufficient to consider only the connected subgraphs containing some fixed vertex. Hence, the probability $P(V)$ that a random graph $G = (V, E)$ is connected is equal (see [26]) to

$$1 - \sum_{a \in A \subset V} P(A) \prod_{e \in E(A)} (1 - p_e),$$

where $E(A)$ is the set of edges in a spanning graph on A in G and a is a fixed vertex. Note that a flat in a matroid of cycles of G can be a disconnected graph.

Let e be neither a loop nor a coloop of M and $p_e = p$. Then

$$P(M, p) = (1 - p)P(M^{-e}, p) + pP(M^{\times e}, p). \tag{4.2.3}$$

Hence, by Theorem 2.1.3 and by (4.2.3)

$$P(M,p) = (1-p)^{\varrho^* E} p^{\varrho(E)} T(M;1,(1-p)^{-1}). \tag{4.2.4}$$

Let $r(M,\theta) = \mathrm{E}\,(\theta^{\varrho(\omega_1(M))})$ denote the probability generating function of the rank of $\omega_1(M)$. Then

$$r(M;\theta) = (1-p)^{\varrho^* E}(p\theta)^{\varrho(E)} T\left(M; \frac{1-p}{p\theta}+1, \frac{1}{1-p}\right). \tag{4.2.5}$$

Formulae (4.2.4) and (4.2.5) were given by Oxley and Welsh [40]. Note that the above two formulae are true only for cases where each element $e \in E$ is selected to be included in a random R with the same probability p.

Example 4.2.1. Consider formulae (4.2.4) and (4.2.5) when $M = F_3$ or $M = F_4$, using the result from Example 2.1.7. After suitable substitutions we obtain the probabilities

$$\begin{aligned} P(F_3,p) &= p^3(28-77p+84p^2-42p^3+8p^4),\\ P(F_4,p) &= p^4(28-63p+49p^2-13p^3), \end{aligned}$$

and the generating functions

$$\begin{aligned} r(F_3,\theta) &= (1-p)^7 + 7(1-p)^6 p\theta - 7(3-2p)(1-p)^4 p^2\theta^2\\ &\quad + p^3(28-77p+84p^2-42p^3+8p^4)\theta^3,\\ r(F_4,\theta) &= (1-p)^7 + 7(1-p)^6 p\theta + 21(1-p)^5 p^2\theta^2\\ &\quad - 7(1-p)^3 p^3(-5+4p)\theta^3 + p^4(28-63p+49p^2-13p^3)\theta^4. \end{aligned}$$

This example shows that the Tutte polynomial is not very useful for the effective calculation of $P(M,p)$ because the evaluation of $T(M;x,y)$ has a high complexity (in fact it is $\#P$-hard). Recently, a general technique has been developed that supplies fully randomized approximation schemes for approximating the value of $T(M;x,y)$, where $M = M(G)$ for some class of graphs G. For example [1] (see also [48] and [47]) concerns the problem of the approximate evaluation of reliability, i.e. probability that the graph G is connected.

Consider a random process $\overline{\omega}(M,t)$ with values in a family of flats $\mathcal{J}$. The process $\overline{\omega}(M,t)$ will be in state $a \in \mathcal{J}$ if $\sigma(R) = A$. Assume that our process starts at time $t = 0$ from state $\emptyset$. Therefore, $\overline{\omega}(M,t)$ is a Markov process. The infinitesimal parameters are equal to

$$\mu_{AB} = \begin{cases} \Lambda(B \setminus A) & \text{if } B \succcurlyeq A,\\ 0 & \text{otherwise,} \end{cases}$$

where $A, B \in \mathcal{J}$ and $A \neq B$. Let $\mu_A = \Lambda(E \setminus A)$.

Let $P_A(t)$ denote the probability that $\overline{\omega}(M,t)$ is in state A at time t. Then the Kolmogorov equations have the form

$$\frac{d}{dt}P_B(t) = -P_B(t)\sum_{C \succcurlyeq B}(\Lambda(C \setminus B) + \sum_{A \preccurlyeq B}\Lambda(B \setminus A)P_A(t) \tag{4.2.6}$$

if $B \neq \emptyset$ and $B \neq E$, and

$$\frac{d}{dt}P_E(t) = \sum_{A \lessdot E} \Lambda(E \setminus A)P_A(t), \qquad \frac{d}{dt}P_\emptyset(t) = -P_\emptyset(t)\Lambda(E). \tag{4.2.7}$$

It follows from the last equation that $P_\emptyset(t) = e^{-\Lambda(E)t}$.

Theorem 3.3.3 immediately gives the following result.

THEOREM 4.2.1. *Let* $\varrho(M) = k$, $m'_i = \min_{\varrho(A)=i} \mu_A$ *and* $m''_i = \max_{\varrho(A)=i} \mu_A$. *We have*

$$\sum_{j=0}^{k-1}(1 - e^{-tm'_j}) \prod_{i \neq j} \frac{m'_i}{m'_i - m'_j} \leq P_E(t) \leq \sum_{j=0}^{k-1}(1 - e^{-tm''_j}) \prod_{i \neq j} \frac{m''_i}{m''_i - m''_j}. \quad \blacksquare \tag{4.2.8}$$

Lomonosov [35] proved this theorem in a different and more complicated way. In fact, his result gives only the lower bound for $P_E(t)$. He also obtained another upper bound for $P_E(t)$, using the particular properties of circuits of matroids. This is the following result.

THEOREM 4.2.2. *Let the family of cocircuits* $\mathcal{C} = \{C_1, \ldots, C_r\}$ *of the matroid* M, *where* $\varrho(M) = r$, *be generated by a basis. Then*

$$P(M, \mathbf{p}) \leq \prod_{i=1}^{r} \Big(1 - \prod_{e \in C_i} (1 - p)_e\Big). \quad \blacksquare$$

4.3. Duality. Let S be a clutter. Suppose that each element of E is, independently of all other elements, painted white with probability p or painted black with probability $q = 1 - p$. This defines the probability space Ω of possible realizations and we call this space a *percolation model* on S. For given S and p we define the *percolation probability* $P(S, p)$ to be the probability that a member of $\mathcal{P}$ has all its members painted white.

In terms of reliability theory we view the white elements as those that work and the black elements as those which fail. Thus the probability $P(S, p)$ is the probability that the system works (see [5]).

It is easy to see that

$$P(S, p) = \sum p^{|A|} q^{|E \setminus A|}$$

where the sum is taken over all the subsets A of E which contain some member of $\mathcal{P}$. It is well known that

$$P(S, p) = 1 - P(\overline{S}, q). \tag{4.3.1}$$

The relation (4.3.1), which is natural and intuitive, combines combinatorial and probabilistic notions. For a matroid M and its dual M^*, such exact probabilistic relationships generally do not exist. However, under certain conditions, we can derive certain relationships between duality in the combinatorial and probabilistic sense.

According to Lemma 2.1.2 we have

$$P(M^*, (1 - p)) = (1 - p)^{\varrho^*(E)} p^{\varrho(E)} T(M; p^{-1}, 1). \tag{4.3.2}$$

and

$$r(M^*; \theta) = (1 - p)^{\varrho(E)} (p\theta)^{\varrho^*(E)} T\left(M; \frac{1}{1 - p}, \frac{1 - p}{p\theta} + 1\right). \tag{4.3.3}$$

Let us write r for $\varrho(M)$ and r^* for $\varrho(M^*) = |E| - \varrho(E)$. For a random subset R of the set E,

$$\varrho(R) = r \Leftrightarrow \exists_{B\in\mathcal{B}} B \subseteq R, \tag{4.3.4}$$

$$\varrho^*(R) = r^* \Leftrightarrow \exists_{B\in\mathcal{B}} E \setminus R \subseteq B. \tag{4.3.4*}$$

Let

$$P_1(M,p) = \mathrm{Prob}(\varrho(\omega_1(M)) = \varrho(M) \text{ and } R \notin \mathcal{B}(M)), \tag{4.3.5}$$

$$P_0(M,p) = \mathrm{Prob}(\varrho(\omega_1(M)) < \varrho(M) \text{ and } R \in \mathcal{I}(M)), \tag{4.3.6}$$

$$P_{1*}(M,p) = \mathrm{Prob}(R \in \mathcal{B}(M)), \tag{4.3.7}$$

$$P_{0*}(M,p) = \mathrm{Prob}(\varrho(\omega_1(M)) < \varrho(M) \text{ and } R \notin \mathcal{I}(M)). \tag{4.3.8}$$

Thus according to (4.3.4) and (4.3.4*) we have the following results.

Proposition 4.3.1.

$$P_{1*}(M,p) = P_{1*}(M^*,(1-p)), \quad P_1(M,p) = P_0(M^*,(1-p)),$$
$$P_{0*}(M,p) = P_{0*}(M^*,(1-p)), \quad P_0(M,p) = P_1(M^*,(1-p)). \ \blacksquare$$

Proposition 4.3.2.

$$P(M,p) = P_1(M,p) + P_{1*}(M,p), \quad 1 - P(M,p) = P_0(M,p) + P_{0*}(M,p). \ \blacksquare$$

In several situations, the probabilities P_{1*} tend to zero. Let us consider the following well-known example.

Let $M = M(K_n)$ be the cycle matroid of the complete graph K_n. Since $|\mathcal{B}(M)| = n^{n-2}$,

$$P_{1*}(M,p) = n^{n-2}p^{n-1}(1-p)^{\binom{n}{2}-n+1}.$$

If $n \to \infty$ and $p \to 0$ in such a way that $np = o(n)$, then

$$(np)^{n-1}(1-p)^{\binom{n}{2}-1+1}n^{-1} = o(n).$$

It is well known that if

$$p \sim \frac{\ln n + x + o(n)}{n}, \tag{4.3.9}$$

then $P(M,p) \to e^{-e^{-x}}$ and a random graph has one giant component with at least one cycle a.s. Hence, $P_0(M,p) = o(1)$ if p is given by (4.3.4) and $P_{0*}(M,p) \to 1 - e^{-e^{-x}}$.

Therefore from Propositions 4.3.1 and 4.3.2, for the matroid M^* dual to $\mathcal{M}(K_n)$ we obtain

$$1 - P(M^*,(1-p)) = P_0(M^*,(1-p)) + P_{0*}(M^*,(1-p)) = P_1(M,p) + P_{0*}(M,p).$$

Thus we simply obtain

$$P(M,(1-p)) = o(n)$$

provided p is given by (4.3.9).

If $R \in \mathcal{I}(M)$, then R is a forest. It is well known that the probability of such an event tends to $(1-x)^{1/2}\exp(x/2 + x^2/4)$ as $np \to x$, $0 < x < 1$. Thus if $np \to x$, then

$$P_0(M,p) \to (1-x)^{1/2}\exp(x/2 + x^2/4)$$

and $P_{0*}(M,p) = o(1)$. Since $P_0(M,p) = P_1(M^*,(1-p))$, if $n(1-p) \to x$, then

$$P(M^*,p) \to (1-x)^{1/2}\exp(x/2 + x^2/4).$$

Let C_n be a cycle on the set $\{v_1,\dots,v_n\}$ of vertices (the edges are of the form (v_i,v_{i+1}), $i = 1,\dots,n-1$ and (v_n,v_1)). By a *wheel* W_n, we mean a graph on the set of vertices $\{v_0,\dots,v_n\}$, where $\{v_1,\dots,v_n\}$ forms a cycle C_n and the vertex v_0 is joined to all other vertices of C_n. Let M'_n be the matroid of cycles of W_n. The matroid M''_n, which is called a *whirl*, is obtained (see [14]) by the deletion of the greatest cycle C_n from W_n and by the addition of n cycles of the form $C_n \cup \{e_i\}$, where $e_i = (v_0,v_i)$. Both M'_n and M''_n have rank n.

The following result is a corollary of Theorem 5.5 from [29].

PROPOSITION 4.3.3. *Let $f(n) \to \infty$ as $n \to \infty$. If M is M'_n or M''_n, then*

$$P(M,p) \to \begin{cases} 0 & \text{if } p = 1-(f(n)/n)^{1/3}, \\ e^{-x} & \text{if } p = 1-(x/n)^{1/3}, \\ 1 & \text{if } p = 1-(f(n)/n)^{-1/3}. \end{cases} \blacksquare$$

As in the previous example, $P_0(M,p) = o(1)$ and $P_{1*}(M,p) = o(1)$. From Proposition 4.3.3, we obtain the following result.

COROLLARY 4.3.4. *Let $P_n^{(c)}$ denote the probability that M has exactly one circuit. Then*

$$P_n^{(c)}(M,p) \to \begin{cases} 1 & \text{if } p = 1-(f(n)/n)^{1/3}, \\ 1-e^{-x} & \text{if } p = 1-(x/n)^{1/3}, \\ 0 & \text{if } p = 1-(f(n)/n)^{-1/3}, \end{cases}$$

where $f(n) \to \infty$ as $n \to \infty$ and M is M'_n or M''_n. $\blacksquare$

On the other hand, the assertion of Corollary 4.3.4 is not surprising because it is well-known that M^* is isomorphic to M, (M is M'_n or M''_n). Then the M's have full rank if and only if the M^*'s have no circuits (cocircuits in the M's).

Now let us consider another example (see Ruciński [40]). Let $L_n^{(3)}$ denote the graph on n vertices arising from a tetrahedron by placing on each region a triangular lattice and let $L_m^{(6)} = (L_n^{(3)})^*$.

Let $L_{n,1}^{(4)}$ denote the graph on n vertices arising from a cube by placing on each region a square lattice and let $L_{m,2}^{(4)} = (L_{n,1}^{(4)})^*$. Note that $L_m^{(6)}$ and $L_{m,2}^{(4)}$ are also graphs (more precisely, $L_m^{(6)}$ and $L_{m,2}^{(4)}$ are graphic matroids).

A sequence of graphs G_n is called *almost d-regular* if the maximal degree of G_n is equal to d and the number of vertices whose degree is not equal to d is $o(n)$. Note that $L_n^{(3)}$ is almost 6-regular, $L_{n,1}^{(4)}$ and $L_{n,2}^{(4)}$ are almost 4-regular and $L_n^{(6)}$ is almost 3-regular. Moreover, $L_n^{(3)}$ has all faces of size 3, $L_{n,1}^{(4)}$ has all (and $L_{n,2}^{(4)}$ almost all) faces of size 4, and $L_n^{(6)}$ has almost all faces of size 6.

The following result is a corollary of Theorem 7 from [40] and is a slightly modified version of Corollary 2 from [40].

PROPOSITION 4.3.5. *Let $f = f(n) \to \infty$ as $n \to \infty$. Then*

$$P(M^{(i)}, p) \to \begin{cases} 0 & \text{if } p = 1 - fn^{-1/d_i}, \\ \exp(-x^{d_i}) & \text{if } p = 1 - xn^{-1/d_i}, \\ 1 & \text{if } p = 1 - f^{-1}n^{-1/d_i}, \end{cases}$$

where $i = 3, 4, 6$, $M^{(3)} = L_n^{(3)}$, $M^{(4)} = L_{n,1}^{(4)}$ or $M^{(4)} = L_{n,2}^{(4)}$, $M^{(6)} = L_n^{(6)}$, $d_3 = 6$, $d_4 = 4$, $d_6 = 3$. ∎

As in the previous example, $P_0(M^{(i)}, p) = o(1)$ and $P_{1*}(M^{(i)}, p) = o(1)$. From Proposition 4.3.5, we obtain the following result.

COROLLARY 4.3.6. *Let $P_n^{(i)}$ denote the probability that $M^{(i)}$ has at least one circuit (i.e. $L_n^{(3)}$, $L_{n,1}^{(4)}$, $L_{n,2}^{(4)}$ or $L_n^{(6)}$ has at least one cycle) and $f = f(n) \to \infty$ as $n \to \infty$. Then*

$$P_n^{(i)} \to \begin{cases} 1 & \text{if } p = 1 - fn^{-1/d_i}, \\ 1 - \exp(-x^{d_i}) & \text{if } p = 1 - xn^{-1/d_i}, \\ 0 & \text{if } p = 1 - f^{-1}n^{-1/d_i}, \end{cases}$$

where i, $M^{(i)}$ and $L^{(i)}$ are as in Proposition 4.3.5. ∎

Now let us consider random matroids of the second type. Since $M.R = (M^*|R)^*$,

$$((\varrho^*)_R)^*(R) = \varrho(M.R),$$

where f_A denotes the function f restricted to the domain A. Therefore

$$((\varrho^*)_R)^*(R) = |R| - \varrho^*(R) = \varrho(E) - \varrho(E \setminus R)$$

and for $R' = E \setminus R$,

$$\varrho(M.R) = 0 \Leftrightarrow \varrho(E) = \varrho(E \setminus R) \Leftrightarrow \varrho(R') = r.$$

Therefore, if $\mathrm{Prob}(e \in R) = p$ for every $e \in E$, then

$$\mathrm{Prob}(\varrho(\omega_2) = 0) = P(M, 1 - p).$$

5. Random projective geometries—combinatorial results

5.1. Distribution of rank. The results in this section are mostly from [30].

Let M_r denote $PG(r-1, q)$. We consider two different random variables X_r and Y_r defined as follows: $X_r = k \Leftrightarrow \varrho(\omega_r) = k$ and $Y_r = k \Leftrightarrow \varrho(\omega_r) = r - k$. Let $P^{(r)}$ denote the probability that ω_r has full rank, i.e.

$$P^{(r)} = \mathrm{Prob}(X_r = r).$$

Obviously we have

$$\mathrm{Prob}(X_r = k) = \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)}, \qquad \mathrm{Prob}(Y_r = k) = \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[r-k]} P^{(r-k)},$$

where $k = 0, 1, \ldots, r$. If we formally take $q \to 1$, then both X_r and Y_r have a binomial distribution.

If $p = 1 - e^{-t}$, then we write $P^{(r)}(t)$ for $P^{(r)}$. Now, by $\tau(r)$ we denote the moment at which ω_r obtains full rank. Therefore

$$\tau(r) = \min\{t : X_r = r\} \quad \text{and} \quad \operatorname{Prob}(\tau(r) < t) = P^{(r)}(t).$$

The Laplace transform of $\tau(r)$ has the form

$$\overline{P}(s) = \mathrm{L}\{P^{(r)}(t)\} = \int_0^\infty e^{-st}\, dP^{(r)}(t) = Ee^{-s\tau(r)}$$

and

$$\mathrm{E}\,\tau(r) = -\frac{d\overline{P}^{(r)}(s)}{ds}\bigg|_{s=0}, \qquad \mathrm{E}\,(\tau(r))^2 = \frac{d^2\overline{P}^{(r)}(s)}{ds^2}\bigg|_{s=0}.$$

Let S_k be any fixed subspace of rank k. Then

$$|\{e : e \notin S_k, e \in M_r\}| = [r] - [k].$$

Since

$$\sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)} = 1, \tag{5.1.1}$$

it follows that

$$P^{(r)} = 1 - \sum_{k=0}^{r-1} \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)} \tag{5.1.2}$$

(see Section 4, formula (4.2.2)). If $\varrho(\omega_r) \le r-1$, then $\sigma(\omega_r) \subseteq H$ or $\varrho(H \cap \sigma\omega_r) \le r-2$, where $\sigma(\omega_r)$ denotes the span of ω_r in $PG(r-1,q)$ and H is a hyperplane in M_r. Since

$$\operatorname{Prob}(\sigma(\omega_r) \subseteq H) = (1-p)^{q^{r-1}}$$

and for a fixed subspace $S_k \subseteq M_r$,

$$\operatorname{Prob}(\sigma(\omega_r) = S_k) = (1-p)^{[r]-[k]} P^{(k)}$$

it follows that

$$(1-p)^{q^{r-1}} + \sum_{k=1}^{r} \begin{bmatrix} r-1 \\ k-1 \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)} = 1.$$

Hence

$$P^{(r)} = 1 - (1-p)^{q^{r-1}} - \sum_{k=1}^{r-1} \begin{bmatrix} r-1 \\ k-1 \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)}. \tag{5.1.3}$$

Now let $p = 1 - e^{-t}$, $t > 0$. If $\varrho(\omega_r) = r$ at time $t+h$, then at time t we have either $\varrho(\omega_r) = r-1$ and in $[t, t+h]$ one new element $e \in \sigma(\omega_r)$ is added or $\varrho(\omega_r) = r$ at time t. Hence

$$P^{(r)}(t+h) = P^{(r)}(t) + [r]q^{r-1}e^{-tq^{r-1}} P^{(r-1)}(t)h + o(h).$$

Therefore

$$\frac{dP^{(r)}(t)}{dt} = [r]q^{r-1}e^{-tq^{r-1}} P^{(r-1)}(t), \tag{5.1.4}$$

$P^{(i)}(0) = 0$ for $i > 0$, $P^{(0)}(t) = 1$ and

$$\frac{dP^{(1)}(t)}{dt}\bigg|_{t=0} = 1.$$

Substituting $t = -\ln(1-p)$, from (5.1.4) we obtain

$$\frac{dP^{(r)}}{dp} = [r]q^{r-1}(1-p)^{q^{r-1}-1}P^{(r-1)} \tag{5.1.5}$$

(see Section 4, formula (4.2.8)).

From formula (5.1.2) or (5.1.3), for $q = 2$ we have

$$P^{(1)} = p = 1 - e^{-t}, \quad P^{(2)} = 3p^2 - 2p^3 = 1 - 3e^{-t} + 2e^{-3t}.$$

Now we use formula (2.2.5). If we rewrite (5.1.1) in the form

$$(1-p)^{-[r]} = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{-[k]} P^{(k)}$$

then we can substitute $b_k = (1-p)^{-[k]}$ and $a_k = (1-p)^{-[k]}P^{(k)}$. Therefore,

$$(1-p)^{-[r]}P^{(r)} = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} (-1)^{r-k} q^{\binom{r-k}{2}} (1-p)^{-[k]}$$

and after simple computations we obtain

$$P^{(r)} = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} (-1)^{k} q^{\binom{k}{2}} (1-p)^{[r]-[r-k]}. \tag{5.1.6}$$

Consider the process $\overline{\omega}_r(t)$ defined as $\overline{\omega}(M_r, t)$. Since every trajectory from $\emptyset$ to E is equally likely, from Theorem 4.2.1 we have $m'_i = m''_i$, for all i. Therefore the left and right sides in (4.2.8) are equal and we have the following formula:

$$P^{(r)}(t) = \sum_{j=0}^{r-1} (1 - e^{-t([r]-[j])}) \prod_{i \neq j} \frac{[r]-[i]}{[j]-[i]}.$$

Let

$$l(r,k) = \prod_{i \neq k} \frac{[r]-[i]}{[k]-[i]}.$$

Since

$$l(r,k) = \frac{\prod_{i=0}^{r-1}([r]-[i])}{([r]-[k])\prod_{i=0}^{k-1}([k]-[i])\prod_{i=k+1}^{r-1}([k]-[i])}$$

and

$$\prod_{i=k+1}^{r-1} ([k]-[i]) = (-1)^{r-k-1} q^{k(r-k-1)} [r-k-1]!$$

and

$$\prod_{i=0}^{r-1} ([r]-[i]) = q^{\binom{r}{2}} [r]!\,,$$

it follows that

$$l(r,k) = q^{\binom{r-k}{2}} (-1)^{r-k-1} \begin{bmatrix} r \\ k \end{bmatrix}.$$

Hence

$$P^{(r)}(t) = \sum_{j=0}^{r-1} \begin{bmatrix} r \\ j \end{bmatrix} (-1)^{r-j-1} q^{\binom{r-j}{2}} (1 - e^{-t([r]-[j])})$$

or

$$P^{(r)} = \sum_{j=0}^{r-1} \begin{bmatrix} r \\ j \end{bmatrix} (-1)^{r-j-1} q^{\binom{r-j}{2}} (1 - (1-p)^{[r]-[j]}). \tag{5.1.7}$$

Formulae (5.1.2), (5.1.3), (5.1.6) or (5.1.7) may be used to calculate the value of $P^{(r)}$.

Finally, note that from Lemma 3.1.1 we can obtain a simple lower bound for $P^{(r)}$. Let $I_\alpha = 1$ if $\omega_r \setminus H_\alpha = \emptyset$, where H_α is a hyperplane, and $I_\alpha = 0$ otherwise. Defining $Z_r = \sum_\alpha I_\alpha$, we obtain $P^{(r)} = \mathrm{Prob}(Z_r = 0)$. Thus

$$P^{(r)} \geq (1 - (1-p)^{q^{r-1}})^{[r]}.$$

It is easy to see that if we formally take $q \to 1$, then the right-hand side of (5.1.6) tends to

$$\sum_{k=0}^{r} \binom{r}{k} (-1)^k (1-p)^k = p^r$$

and the right-hand side of (5.1.7) tends to

$$\sum_{j=0}^{r-1} \binom{r}{j} (-1)^{r-j-1} (1 - (1-p)^{r-j}) = p^r.$$

Numerical values of $P^{(r)}$ for small values of r and for $q = 2, 3, 4, 5, 7, 8$ and 9 are given in the Appendix (Table 2).

To obtain the properties of $\tau(r)$, we calculate the function $\overline{P}^{(r)}(s) = \mathrm{L}\{\tau(r)\}$.

Lemma 5.1.1. *For $r \geq 1$ we have*

$$\overline{P}^{(r)}(s) = q^{\binom{r}{2}} [r]! \prod_{k=1}^{r} (s + q^{r-k}[k])^{-1}. \tag{5.1.8}$$

P r o o f. Taking the Laplace transformation of both sides of equation (5.1.4), we obtain

$$s\overline{P}^{(r)}(s) = [r] q^{r-1} \, \mathrm{L}\{e^{-tq^{r-1}} P^{(r-1)}(t)\}$$

for $r \geq 2$. Thus,

$$s\overline{P}^{(r)}(s) = [r] q^{r-1} \overline{P}^{(r-1)}(s + q^{r-1}). \tag{5.1.9}$$

If $r = 1$, then $\overline{P}^{(1)}(s) = 1/(s+1)$ and (5.1.2) is fulfilled.

If $r \geq 2$, we assume that (5.1.8) is true for some r and prove (5.1.8) for $r+1$. Note that

$$q^{r-k}[k] + q^r = q^{(r+1)-(k+1)}[k+1].$$

Therefore using (5.1.9), we have

$$\begin{aligned} \overline{P}^{(r+1)}(s) &= \frac{1}{s} q^r [r+1] q^{\binom{r}{2}} \prod_{k=1}^{r} (s + q^r + q^{r-k}[k])^{-1} \\ &= q^{\binom{r+1}{2}} [r+1] \prod_{k=1}^{r+1} (s + q^{r+1}[k])^{-1}, \end{aligned}$$

and thus we obtain the assertion. ∎

The next step in our investigations of $\tau(r)$ is to give formulae for $\mathrm{E}\,\tau(r)$ and $\mathrm{Var}\,\tau(r)$. We have the following results.

THEOREM 5.1.2.

$$\mathrm{E}\,\tau(r) = q^{-r}\sum_{k=1}^{r}\frac{q^k}{[k]}, \tag{5.1.10}$$

$$\mathrm{Var}\,\tau(r) = q^{-2r}\sum_{k=1}^{r}\frac{q^{2k}}{[k]^2}. \tag{5.1.11}$$

P r o o f. From Lemma 5.1.1, we calculate the first two derivatives of $\overline{P}^{(r)}(s)$. First we calculate

$$\frac{d}{ds}\prod_{k=1}^{r}(s+q^{r-k}[k]) = \sum_{k=1}^{r}\prod_{j\neq k}(s+q^{r-k}[k]).$$

Hence

$$\frac{d\overline{P}^{(r)}(s)}{ds} = -q^{\binom{r}{2}}[r]!\,\frac{\displaystyle\sum_{k=1}^{r}\frac{1}{s+q^{r-k}[k]}}{\prod_{k=1}^{r}(s+q^{r-k}[k])} \tag{5.1.12}$$

and

$$\frac{d^2\overline{P}^{(r)}(s)}{ds^2} = -q^{\binom{r}{2}}[r]!\,\frac{\displaystyle\sum_{k=1}^{r}\frac{1}{s+q^{r-k}[k]} + \Big(\sum_{k=1}^{r}\frac{1}{s+q^{r-k}[k]}\Big)^2}{\displaystyle\prod_{k=1}^{r}(s+q^{r-k}[k])}. \tag{5.1.13}$$

Substituting $s=0$ into formulae (5.1.12) and (5.1.13), we obtain (5.1.10) and the second moment:

$$\mathrm{E}\,\tau^2(r) = q^{-2r}\Big(\sum_{k=1}^{r}\frac{q^{2k}}{[k]^2} + \Big(\sum_{k=1}^{r}\frac{q^k}{[k]}\Big)^2\Big).$$

Therefore

$$\mathrm{Var}\,\tau(r) = \mathrm{E}\,\tau^2(r) - (\mathrm{E}\,\tau(r))^2 = q^{-2r}\sum_{k=1}^{r}\frac{q^{2k}}{[k]^2}$$

and (5.1.11) is proved. ∎

5.2. Full subspaces—expectation and variance. The results in this section are from [31]. If M' is a submatroid of $PG(r-1,q)$ and M'' is a submatroid of M' such that $M'' \sim PG(d-1,q)$ for some d, we say that M'' is a *full subspace* of M' (more precisely a full subspace of rank d of M'). Note that by a subspace of $PG(r-1,q)$ we always mean a full subspace, i.e. a flat of $PG(r-1,q)$. Let Γ be the set of all $PG(d-1,q)$ in $PG(r-1,q)$ for some fixed d.

Let

$$I_\alpha = \begin{cases} 1 & \text{if } V_\alpha \text{ is a maximal full } PG(d-1,q) \text{ in } \omega_r,\\ 0 & \text{otherwise,}\end{cases}$$

where $\alpha \in \Gamma$ and $V_\alpha = \alpha \cap \omega_r$. Then $X_r(d) = \sum_\alpha I_\alpha$. Since $\mathrm{E}\, I_\alpha = p^{[d]}(1-p^{q^d})^{[r-d]}$ we have

$$\mathrm{E}\, X_r(d) = \begin{bmatrix} r \\ d \end{bmatrix} p^{[d]}(1-p^{q^d})^{[r-d]}.$$

From the upper bound (2.2.1) we obtain

$$\mathrm{E}\, X_r(d) \le q^{dr} p^{[d]}.$$

Now we calculate the variance of $X_r(d)$. In the case of random graphs, one can apply the lemma of Kalbfleish [19] (see [4], where $X_n(d)$ is the number of cliques of size d in the random complete graphs $K_{n,p}$). Because a counterpart to bipartite graphs does not exist for projective geometries, we have to calculate the variance directly. The calculations presented below are fairly similar to those from [4].

Lemma 5.2.1.

(5.2.1) $\mathrm{Var}\, X_r\,(d)$

$$\begin{aligned} &= \sum_{s=0}^{d} \Bigg(\begin{bmatrix} r \\ d \end{bmatrix} \begin{bmatrix} r-d \\ d-s \end{bmatrix} \begin{bmatrix} d \\ s \end{bmatrix} q^{(d-s)^2} p^{2[d]-[s]} (1 - 2p^{q^d} + p^{q^{2d-s}})^{[r-2d+s]} P_2(d,s) \\ &\quad - (p^{[d]}(1-p^{q^d})^{[r-d]})^2 \Bigg) \\ &= \sum_{s=0}^{d} A_s \end{aligned}$$

where

$$P_2(d,s) = \sum_{k=s}^{2d-s} (-1)^{k-s} \sum_{l=s}^{k} \begin{bmatrix} d-s \\ k-l \end{bmatrix} \begin{bmatrix} d-s \\ l-s \end{bmatrix} p^{q^d([k-l]+[l-s])-q^s[k-s]}. \tag{5.2.2}$$

Proof. Note that

$$\mathrm{Var}\, X_r(d) = \sum_\alpha \sum_\beta \mathrm{Cov}(I_\alpha, I_\beta) = \sum_\alpha \sum_\beta \mathrm{Prob}(I_\alpha, I_\beta = 1) - \mu_r^2.$$

Let the rank $\varrho(V_\alpha \cap V_\beta) = s \le d$ and $\sigma(V_\alpha \cap V_\beta)$ be the span defined by (2.1.1). Then

$$\mathrm{Prob}(I_\alpha I_\beta = 1) = p^{2[d]-[s]} P_1(d,s) P_2(d,s),$$

where the first factor gives the probability that V_α and V_β are full, $P_1(d,s)$ is the probability that no subspace $PG(d,q)$ contains V_α or V_β and is not contained in $\sigma(V_\alpha \cup V_b)$, $P_2(d,s)$ is the probability that there is no larger full subspace in $\sigma(V_\alpha \cup V_\beta)$ which contains either V_α or V_β.

First we find P_1. The submatroids V_α and V_β are maximal full if A does not occur, where A is defined as

$$A = \{V_\alpha \text{ is contained in some } PG(d,q) \text{ or } V_\beta \text{ is contained in some } PG(d,q)\}.$$

Thus,

$$\begin{aligned} \mathrm{Prob}(A) = {} & \mathrm{Prob}(V_\alpha \subset PG(d,q)) + \mathrm{Prob}(V_\beta \subset PG(d,q)) \\ & - \mathrm{Prob}(V_\alpha \cup V_\beta \subset PG(2d-s,q)) \\ = {} & 2p^{q^d} - p^{q^{2d-s}}. \end{aligned}$$

There are $[r-2d+s]$ subspaces of rank $2d-s+1$ containing $\sigma(V_\alpha \cup V_\beta)$, so

$$P_1(d,s) = (1-2p^{q^d}+p^{q^{2d-s}})^{[r-2d+s]}.$$

Now we find P_2. Let $V_\alpha \subseteq V'_\alpha$, $V_\beta \subseteq V'_\beta$. Letting

$$S_k = \sum_{\varrho(V'_\alpha \cap V'_\beta)=k} \text{Prob}(V'_\alpha \text{ is full, } V'_\beta \text{ is full})$$

we obtain

$$P_2(d,s) = \sum_{k=s}^{2d-s} (-1)^{k-s} S_k$$

from the inclusion-exclusion formula. Let $k = \varrho(V'_\alpha \cap V'_\beta),\ l = \varrho(V'_\alpha \cap V_\beta),\ k-l+s = \varrho(V_\alpha \cap V'_\beta)$. Then

$$\varrho(V'_\beta) = d+k-l, \qquad \varrho(V'_\alpha) = d+l-s.$$

If $V'_\alpha \supseteq V_\alpha$ and $V'_\beta \supseteq V_\beta$ are fixed, then

$$\begin{aligned} |V'_\alpha \cup V'_\beta| \setminus |V_\alpha \cup V_\beta| &= |V'_\alpha t| + |V'_\beta| - |V'_\alpha \cap V'_\beta| - |V_\alpha| - |V_\beta| + |V_\alpha \cap V_\beta| \\ &= [d+k-l] + [d+l-s] - [k] - 2[d] + [s] \\ &= q^d([k-l]+[l-s]) - q^s[k-s]. \end{aligned}$$

Hence,

$$S_k = \sum_{l=s}^{k} \begin{bmatrix} d-s \\ k-l \end{bmatrix} \begin{bmatrix} d-s \\ l-s \end{bmatrix} p^{q^d([k-l]+[l-s])-q^s[k-s]}$$

and finally we obtain (5.2.2). Therefore, if $|\alpha \cap \beta| = s$ then

$$\text{(5.2.3)}\quad \text{Cov}(I_\alpha, I_\beta) = \sum_{s=0}^{d} p^{2[d]-[s]}(1-2p^{q^d}+p^{q^{2d-s}})^{[r-2d+s]} P_2(d,s) - p^{2[d]}(1-p^{q^d})^{2[r-d]}$$

and

$$\begin{aligned} \text{Var}\, X_r(d) = &\sum_{s=0}^{d} \begin{bmatrix} r \\ d \end{bmatrix} \begin{bmatrix} r-d \\ d-s \end{bmatrix} \begin{bmatrix} d \\ s \end{bmatrix} q^{(d-s)^2} p^{2[d]-[s]} (1-2p^{q^d}+p^{q^{2d-s}})^{[r-2d+s]} P_2(d,s) \\ &- \left(\begin{bmatrix} r \\ d \end{bmatrix} p^{[d]} (1-p^{q^d})^{[r-d]} \right)^2. \end{aligned}$$

Hence, from (2.3.2) we obtain (5.2.1). ∎

In the next section, we will only need the exact values of $P_2(d,s)$ for $s=d$, $s=d-1$ and $s=d-2$. From formula (5.2.2), we immediately get $P_2(d,d)=1$ and $P_2(d,d-1) = 1-p^{q^{d-1}(d-1)}$. Now we calculate $P_2(d,d-2)$ for $d \geq 2$. After simple computations we obtain from (5.2.2):

$$\begin{aligned} P_2(d,d-2) &= 1 - 2[2]p^{q^d-q^s[2]} + 2p^{q^d[2]-q^s[2]} \\ &\quad + [2]p^{2q^d-q^s[2]} - 2[2]p^{q^d([1]+[2])-q^s[3]} + p^{2q^d[2]-q^s[4]} \\ &= 1 - 2(q+1)p^{q^{d-2}(q^2-1)} + (q+1)p^{q^{d-2}(2q^2-q-1)} \\ &\quad + (2q+1)p^{q^{d-2}(q^3+q^2-q-1)}. \end{aligned}$$

5.3. Submatroids of a given type. In this section, we give a brief review of results concerning the existence of circuits, independent sets, bases and flats in random projective geometries. Those results were given by Kelly and Oxley in [23].

Let $C_{r,k}$ and $I_{r,k}$ denote the number of circuits and independent sets with k elements, respectively, in ω_r. By (2.3.6) and (2.3.5) we have

THEOREM 5.3.1.

$$\mathrm{E}\, C_{r,k} = p^k \left|\mathcal{C}\right|_{r,k} = \frac{p^k q^{\binom{k-1}{2}}}{k!}(q-1)^{k-2}[r]_{k-1} \quad \textit{for } 0 \le k \le r+1, \tag{5.3.1}$$

$$\mathrm{E}\, I_{r,k} = p^k \left|\mathcal{I}_{r,k}\right| = \frac{p^k q^{\binom{k}{2}}}{k!}[r]_k \quad \textit{for } 0 \le k \le r. \ \blacksquare \tag{5.3.2}$$

Let B_r and $F_{r,k}$ denote the number of bases and flats of rank k in ω_r. The result below gives the expected values of B_r and $F_{r,k}$ in terms of Tutte polynomials (see Section 2). The projective geometry $PG(r-1,q)$ will be denoted by M_r.

THEOREM 5.3.2.

$$\mathrm{E}\, B_r = \sum_{i=0}^{r} \frac{p^{2i}}{i!}(1-p)^{[r]-i} q^{\binom{i}{2}} [r]_i T(M_i; 1, (1-p)^{-1}), \tag{5.3.3}$$

$$\mathrm{E}\, F_{r,k} = \begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[k]-k} p^k T(M_k; 1, (1-p)^{-1}). \tag{5.3.4}$$

P r o o f. Note that

$$\mathrm{E}\, B_r = \sum_{i=0}^{r} \mathrm{E}\,(B_r | \varrho(\omega_r) = i) \,\mathrm{Prob}(\varrho(\omega_r) = i)$$

and $\mathrm{E}\,(B_r|\varrho(\omega_r) = i) = \mathrm{E}\, I_{i,i}$ which is given by (5.3.2). From (4.2.4) we have

$$\mathrm{Prob}(\varrho(\omega_r) = i) = \begin{bmatrix} r \\ i \end{bmatrix} p^i (1-p)^{[r]-i} T(M_i; 1, (1-p)^{-1}).$$

Hence, we obtain (5.3.3). From (4.2.4), we immediately obtain (5.3.4). ∎

6. Random projective geometries—limit theorems

6.1. Rank of random subspaces. First we consider the convergence of random variables X_r defined in 5 as $r \to \infty$. Recall that $X_r = k \Leftrightarrow \varrho(\omega_r) = k$. Most results in this subsection are given in [30] and [33].

Kelly and Oxley [24] proved that a threshold function for the property that $\varrho(\omega_r) \ge k$ ($\varrho(\omega_r) \ge r-k$), where k is fixed, is equal to q^{-r} (rq^{-r}, respectively). Hence, from now on we shall consider only the case $p = O(rq^{-r})$.

Now we investigate how $P^{(k)}$ changes if k is fixed and p tends to zero as r tends to infinity. We have the following result.

LEMMA 6.1.1. *If $p = o(1)$ and k is a fixed number then*

$$P^{(k)} = \frac{p^k [k]! q^{\binom{k}{2}}}{k!}(1 + o(1)).$$

P r o o f. First we prove that

$$P^{(k)} = w_k p^k (1 + v_k(p)) \tag{6.1.1}$$

where w_k is a function of k and $v_k(p)$ is a polynomial whose degree is a function of k and whose free term is equal to zero. If $k = 1$, the result is obvious if we take $v_1(p) \equiv 0$, then $P^{(1)} = p$.

Now suppose that (6.1.1) is true for $k-1$, i.e.

$$P^{(k-1)} = w_{k-1} p^{k-1} (1 + v_{k-1}(p)).$$

Integrating (5.1.5) we obtain

$$\begin{aligned} P^{(k)} &= [k]q \int_0^p (1-v)^{q^{k-1}} w_{k-1} v^{k-1} (1 + v_{k-1}(v))\, dv \\ &= [k]q^{k-1} w \int_0^p \Big(1 + \sum_{i=1}^{q^{k-1}-1} (-v)^i\Big)(1 + v_{k-1}(v)) v^{k-1}\, dv \\ &= [k]q^{k-1} w_{k-1} \left(\frac{p^k}{k} + \frac{p^k v_k}{k}\right). \end{aligned}$$

Hence, we obtain the assertion. ∎

Theorem 6.1.2. *If*

$$p = \frac{\lambda + o(1)}{[r]}$$

and $0 < \lambda = \text{const}$, *then*

$$p_k = \text{Prob}(X_r = k) \to e^{-\lambda} \frac{\lambda^k}{k!},$$

as $r \to \infty$.

P r o o f. It is obvious that $p_0 \to e^{-\lambda}$. Now we calculate the quotient

$$\frac{p_{k+1}}{p_k} = \frac{\begin{bmatrix} r \\ k+1 \end{bmatrix} (1-p)^{[r]-[k+1]} P^{(k+1)}}{\begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[k]} P^{(k)}}.$$

From Lemma 5.1.1, we have

$$\begin{aligned} \frac{p_{k+1}}{p_k} &\sim \frac{\begin{bmatrix} r \\ k+1 \end{bmatrix} (1-p)^{[r]-[k+1]} p^{k+1} [k+1]! q^{\binom{k+1}{2}} k!}{\begin{bmatrix} r \\ k \end{bmatrix} (1-p)^{[r]-[k]} p^k [k]! q^{\binom{k}{2}} (k+1)!} \\ &\sim \frac{[r-k]}{[k+1]} \frac{1}{(1-p)^{q^k}} p[k+1] q^k \frac{1}{k+1} \sim \frac{q^{r-k}-1}{k+1} q^{k-r} \lambda \sim \frac{\lambda}{k+1}. \end{aligned}$$

Hence we obtain the assertion. ∎

Let us consider a random-$PG(r-1,q)$-process $\{\omega_r(n)\}_{n=0}^{[r]}$ (see Section 4.1). First we show that for large r, typically the rank of $\varrho(\omega_r(n))$ does not differ from $|n|$ very much.

Kelly and Oxley [24] proved that if $k(r)$, $0 \le k(r) \le r$, is a function of r for which $\liminf_{n\to\infty} k(r)/r > 0$ and $p'(r)/rq^{-r} \to \infty$, then a.s. $\varrho(\omega_r(p'(r))) \ge k(r)$, whereas for $p''(r)/rq^{-r} \to 0$, a.s. we have $\varrho(\omega_r(p''(r))) \le k(r)$. We shall give a simple argument which shows that a much stronger result holds.

Let us define $\{\widehat{\omega}_r(n)\}_{n=0}^{\infty}$ as a nondecreasing sequence of subsets of $PG(r-1,q)$, which starts with the empty set and at each step we add to $\widehat{\omega}_r(n)$ an element randomly chosen from $PG(r-1,q)$. It may happen that the new added element has already been added at some earlier step of this sequence.

LEMMA 6.1.3. *A.s.* $|\widehat{\omega}_r(i)| = i$ *for every* $i \le 2r$.

Proof. In this case it may happen that $\widehat{\omega}_r(n) = \widehat{\omega}_r(n+1)$. Clearly, $\widehat{\omega}_r(n)$ might be identified with $\omega_r(n)$ whenever $|\widehat{\omega}_r(n)| = n$. Hence the probability that $|\widehat{\omega}_r(2r)| < 2r$ is less than $r^2(q-1)/(q^r-1) \to 0$. ∎

THEOREM 6.1.4. *If* $r - n(r) \to \infty$ *as* $r \to \infty$, *then a.s.* $\varrho(\omega_r(n)) = n$, *i.e.* $\omega_r(n)$ *is a.s. a free matroid.*

Proof. From Lemma 6.1.3, the asymptotic properties of the first $2r$ stages of a random $PG(r-1,q)$-process $\{\omega_r(n)\}_{n=0}^{(q^r-1)/(q-1)}$ are identical to those of $\{\widehat{\omega}_r(n)\}_{n=0}^{\infty}$.

Let $1 \le n \le r$. The probability that $|\widehat{\omega}_r(n)| = n$, i.e. that each new point is picked outside the subspace generated by the already chosen point, is given by

$$\prod_{k=1}^{n}\left(1-\frac{[k]}{[r]}\right) = \prod_{k=1}^{n}\left(1-\frac{q^k-1}{q^r-1}\right) = \prod_{k=1}^{n}(1-q^{k-r}+O(q^{-r}))$$
$$= (1+O(nq^{-r}))\prod_{k=1}^{n}(1-q^{k-r}).$$

Moreover, if we assume that $r - n \to \infty$ then

$$\prod_{k=1}^{n}(1-q^{k-r}) = \exp\Big(-\sum_{k=1}^{n}(q^{k-r}+O(q^{2k-2r}))\Big)$$
$$= \exp\left(-q^{-r}\frac{q^{n+1}-1}{q-1}+O(q^{2n+2-2r})\right) \to 1.$$

Hence a.s. $\varrho(\widehat{\omega}_r(n)) = n$ and due to Lemma 6.1.3, a.s. $\varrho(\omega_r(n)) = n$. ∎

Note that Theorems 6.1.2 and 6.1.4 are closely related. If p is small, then the number of existing elements is small having a Poisson distribution and being equal to the rank of ω_r.

Now let us look at the value of $\varrho(\omega_r(n))$ when n approaches r. More precisely, let m_r denote the minimal value of n for which $\varrho(\omega_r(n)) = r$ and set $u_r = r - m_r$. Again, instead of studying u_r, we shall consider the corresponding random variable $\widehat{u}_r$ defined according to $\{\widehat{\omega}_r(n)\}_{n=0}^{\infty}$.

To find the distribution of $\widehat{u}_r$, it is enough to notice that this is the sum of the random variables $\widehat{u}_r^{(k)}$ which count the number of points picked in the subspace generated by the points already chosen, when the rank of this subspace equals k. Each $\widehat{u}_r^{(k)}$ has a geometric distribution, thus, for example, for the expectation of $\widehat{u}_r$ we have

$$\mathrm{E}\,\widehat{u}_r = \mathrm{E}\sum_{k=1}^{r-1}\widehat{u}_r^{(k)} = \sum_{k=1}^{r-1}\frac{(q^k-1)/(q^r-1)}{1-(q^k-1)/(q^r-1)} = (1+o(1))\sum_{i=1}^{\infty}\frac{q^{-i}}{1-q^{-i}}\,.$$

From the above result and the Markov inequality, it immediately follows that $\widehat{u}_r$ (and, due to Lemma 6.1.3, also u_r) is bounded in probability.

PROPOSITION 6.1.5. *Let $\gamma(r) \to \infty$. Then both $\widehat{u}_r$ and u_r are less than $\gamma(r)$ a.s.* ∎

Since the generating function of $\widehat{u}_r^{(k)}$ equals $(1-q^{-k})/(1-sq^{-k})$, the generating function of $\widehat{u}_r$ is given by

$$g(s) = \prod_{k=1}^{r-1} \frac{1-q^{-k}}{1-sq^{-k}} = (1+O(sq^{-r}))\beta \prod_{k=1}^{\infty} (1-sq^{-k})^{-1} ,$$

where we set $\beta = \prod_{k=1}^{\infty}(1-q^{-k})$.

The well known Euler formula (see [2], p. 19, Corollary 2.2) says that

$$\prod_{k=0}^{\infty}(1-st^k)^{-1} = 1 + \sum_{k=1}^{\infty} \frac{s^k}{(1-t)(1-t^2)\dots(1-t^k)}$$

for $|s|<1$ and $|t|<1$, so for $g(s)$, we immediately obtain

$$g(s) = \beta(1+O(q^{-r}))\Big[1 + \sum_{k=1}^{\infty} \frac{s^k q^{-k}}{\prod_{i=1}^{k}(1-q^{-i})}\Big].$$

Thus, we arrive at the following formula for the limit distributions of $\widehat{u}_r$ and u_r:

$$\begin{aligned} \lim_{r\to\infty} \operatorname{Prob}\{u_r = k\} &= \lim_{r\to\infty} \operatorname{Prob}\{\widehat{u}_r = k\} \\ &= \begin{cases} \beta & \text{if } k = 0, \\ \beta q^{-k} / \prod_{i=1}^{k}(1-q^{-i}) & \text{if } k \geq 1. \end{cases} \end{aligned} \tag{6.1.2}$$

Clearly, the above results and the model are much more precise than those used by Kelly and Oxley in [24]. For instance, the limit value of the probability that $X_r = r$ follows easily from Theorem 6.1.4, Proposition 6.1.5 and the fact that the number of points which belong to $\omega_r(p)$ is binomially distributed. Then, as an easy consequence, we have the following result.

COROLLARY 6.1.6. *Let x be a real number and $p(r) = (r + x\sqrt{r})/[r]$. Then*

$$\lim_{r\to\infty} \operatorname{Prob}\{\varrho(\omega_r(p)) = r\} = \Phi(x),$$

where $\Phi(x)$ is the standard normal distribution function.

Proof. Let $X = |\omega_r(p)|$. Then X has a binomial distribution and $\operatorname{Prob}(X - r > \gamma(r)) \to \Phi(x)$, where $\gamma(r) \to \infty$, but $\gamma(r) = o(\sqrt{r})$. Hence, due to Proposition 6.1.5, $\operatorname{Prob}(\varrho(\omega_r(p)) = r) = \Phi(x)$. ∎

Finally, we should point out that the only property of projective spaces used in our argument is the fact that the subspaces of $PG(r-1,q)$ form a lattice with the Jordan–Dedekind property, in which for each element e of rank k there exist roughly q^{k-1} atoms a such that $a \leq e$.

Now, let us return to formula (6.1.2). Note that this formula defines the distribution of some discrete random variable X, after substituting x for q^{-1}, where $0 < x < 1$. Then the formula

$$p_k(x) = \operatorname{Prob}(X = k) = \begin{cases} \beta & \text{if } k = 0, \\ \beta x^k / \beta_k & \text{if } k \geq 1, \end{cases} \tag{6.1.3}$$

defines the discrete distribution for all x, where $\beta_k = \prod_{i=1}^{k}(1-x^k)$ and $\beta = \lim_{k\to\infty}\beta_k$. The graphs of the family of functions $p_k(x)$ defined by (6.1.3) are shown in Figure 6.1.1. The values of the expectation, variance, standard deviation and variance coefficients are given in the Appendix (Table 3).

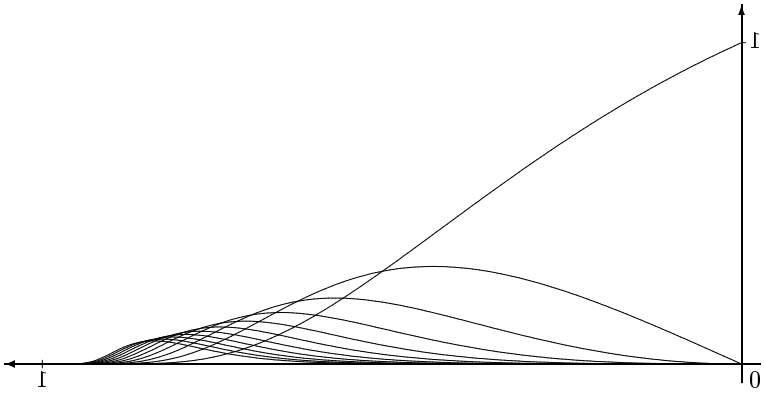

Fig. 6.1.1. The family of functions $p_k(x)$ defined by 6.1.3

Now let us return to the random variable $\tau(r)$, where $p = e^{-t}$, described in Section 5, as $r \to \infty$. Using Theorem 5.1.2, we obtain the following results.

THEOREM 6.1.7. *If $q \neq 1$, then*

$$\mathrm{E}\,\tau(r) \sim \frac{r}{[r]}, \tag{6.1.4}$$

$$\mathrm{Var}\,\tau(r) \sim \frac{r}{[r]^2}. \tag{6.1.5}$$

P r o o f. For $q \neq 1$ we have

$$\mathrm{E}\,\tau(r) = (q-1)q^r \sum_{k=1}^{r} \frac{q^k}{q^k-1} = (q-1)q^{-r}\left(r + \sum_{k=1}^{r}\frac{1}{q^k-1}\right).$$

Since for $q \neq 1$,

$$\sum_{k=1}^{\infty}\frac{1}{q^k-1} < \infty,$$

we obtain (6.1.4). In the same manner one can obtain (6.1.5), thereby completing the proof. ∎

If $q = 1$, then $\tau(r)$ is the maximal order statistic for the exponential distribution and it is well known that

$$\mathrm{E}\,\tau(r) = \sum_{k=1}^{r}\frac{1}{k} \sim \ln r + C,$$

where $C = 0.577\ldots$ is the Euler constant and $\mathrm{Var}\,\tau(r) < \infty$.

By substituting $s = -iu$, the characteristic function $\varphi(u)$ of $\tau(r)$ can be obtained. Thus, $\varphi(u) = \overline{P}^{(r)}(-iu)$ and $\tau(r) - \ln r$ has a characteristic function equal to

$$\overline{P}(-iu)e^{-iu\ln r} = r!\prod_{k=1}^{r}(-iu+k)^{-1}r^{-iu} \sim iu\Gamma(-iu) = \Gamma(-iu+1).$$

Here $\Gamma(x)$ denotes the gamma-function.

The above function is the characteristic function of a double exponential distribution. Hence, as is well known,

$$\operatorname{Prob}(\tau(r) - \ln r < x) \sim e^{-e^{-x}}.$$

If $q \neq 1$, then both $\operatorname{E}\tau(r)$ and $\operatorname{Var}\tau(r)$ tend to zero. Hence we have the following problem. Is it possible to obtain a limiting distribution of $(\tau(r) - \operatorname{E}\tau(r))/\sqrt{\operatorname{Var}\tau(r)}$ for $q \neq 1$ by using a similar method?

6.2. Small submatroids. Let I_α be an indicator 0–1 random variable such that

$$I_\alpha = \begin{cases} 1 & \text{if } M_\alpha \text{ appears in } \omega_r, \\ 0 & \text{otherwise,} \end{cases}$$

where $\{M_\alpha\}_{\alpha\in\Gamma}$ is the set of copies of a fixed matroid M in ω_r.

Let $X_r = \sum_{\alpha\in\Gamma} I_\alpha$, $\lambda_r = \operatorname{E}X_r$, $\sigma_r^2 = \operatorname{Var}X_r$ and $\pi_\alpha = \operatorname{Prob}(I_\alpha = 1) = p^{|M|}$. Let us write $\alpha \div \beta$ if $M_\alpha \cap M_\beta \neq \emptyset$, but $\alpha \neq \beta$. Thus we can define the dependency graph $\mathcal{G}$ with the set of vertices Γ and relation "$\div$" defined above.

It is known (see for example [6], [42]) that

$$\operatorname{Prob}(X_r > 0) \to \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \quad \text{if } rp^{\gamma(M)} \to \begin{Bmatrix} \infty \\ 0 \end{Bmatrix}$$

in the case when $\omega(M) = K(n,p)$, $r = n-1$, and (see [38])

$$\operatorname{Prob}(X_r > 0) \to \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \quad \text{if } q^r p^{\gamma(M)} \to \begin{Bmatrix} \infty \\ 0 \end{Bmatrix}$$

in the case when $\omega(M) = PG(r-1,q)$. It can be seen at once that there is a big difference between these properties. In the first one, $r = n-1 = \varrho(K_n)$ (we treat K_n as the matroid of circuits) is the rank of K_n, but

$$q^r \asymp |PG(r-1,q)| = \frac{q^r-1}{q-1} = [r]$$

is the number of elements of $PG(r-1,q)$.

For a strictly balanced M and $M(r) = \omega_r$, Oxley [38] proved that X_r has a Poisson distribution with expectation λ if

$$q^r p^{\gamma(M)} \to c > 0$$

and

$$\lambda = \nu c^{|M|}\begin{bmatrix} r \\ k \end{bmatrix} q^{-rk}$$

where ν denotes the number of copies of M in $PG(k-1,q)$.

The above results of Oxley have very complicated proofs. Later in this section, we shall give simple proofs based on more recent methods such as exponential bounds (the Janson–L uczak–Ruciński Lemma) for the threshold, the Stein–Chen method for the Poisson approximation and the Janson semiinvariants method for normal convergence.

In 1960 Erdős and Rényi gave the first threshold theorem for the existence of small balanced graphs in a random graph. Bollobás [6] generalized this theorem for arbitrary graphs. At present several different proofs are known (see [42]). In order to generalize to the calculation of thresholds for exponentially growing random matroids, it seems that the proof, based on the exponential bound from [18], is the most appropriate. Reference [32] gives the following results.

THEOREM 6.2.1. *If $M(r)$ is exponentially growing, then*

$$\lim_{r\to\infty} \operatorname{Prob}(M \subset \omega(M)) = \begin{cases} 0 & \text{if } g_r p^{\gamma(M)} \to 0, \\ 1 & \text{if } g_r p^{\gamma(M)} \to \infty. \end{cases}$$

P r o o f. If $p \to c < 1$, then

$$\operatorname{Var} X_r \asymp \sum_{\emptyset \neq T \subseteq M} g_r^{2\varrho(M)-\varrho(T)} p^{|M|-|T|}.$$

We call T a *leading overlap* of M if $T \subseteq M$, $|T| > 0$ and

$$\operatorname{Var} X_r = O(g_r^{2\varrho(M)-\varrho(T)} p^{2|M|-|T|}).$$

Now we use Lemma 3.1.1. The argument below is similar to the proof of formula (2.3) in [17]. It is given here for completeness.

If $T \subseteq M$, let us denote by $n(T, M)$ the number of copies of M in $M(r)$. There are $N(r, M)n(T, M)$ pairs (T', M') with $T' \subseteq M' \subseteq M(r)$, where T' and M' are copies of T and M, respectively. Each copy of T is contained in $\xi = N(r, M)n(T, M)/N(r, T)$ copies of M. Thus if T' is one of them, there are at most ξ^2 pairs (α, β) with $M_\alpha \cap M_\beta = T'$. Since for any such pair (α, β) we have $\operatorname{E} I_\alpha I_\beta = p^{2|M|-|T|}$, then denoting by $X_r(T)$ the number of copies of T in $\omega(M(r))$ we have

$$\begin{aligned} \sum_{\alpha \doteqdot \beta} \sum \operatorname{E} I_\alpha I_\beta &\le \sum_{\emptyset \neq T \subseteq M} N(r, T)\xi^2 p^{2|M|-|T|} \\ &= \sum_{\emptyset \neq T \subseteq M} \frac{\lambda_r^2}{\operatorname{E} X_r(T)} n(T, M), \end{aligned} \tag{6.2.1}$$

where we sum over all the pairwise disjoint nonisomorphic nonempty submatroids of M.

Collecting (3.1.2) and (6.2.1) we obtain

$$\log \operatorname{Prob}(X_r = 0) \le \left(\sum_{\emptyset \neq T \subseteq M} \frac{1}{\operatorname{E} X_r(T)} n(T, M) \right)^{-1}.$$

Thus, if T is a leading overlap of M, then

$$\exp\{-c_1 \operatorname{E} X_r(T)\} \le \operatorname{Prob}(X_r = 0) \le \exp\{-c_2 \operatorname{E} X_r(T)\}.$$

Call $T \subseteq M$ *extreme* in M if $d(T) = \gamma(M)$. If $g_r p^{\gamma(M)} \to \infty$ (0) arbitrarily slowly then the smallest (largest) extreme submatroid is leading and $\operatorname{E} X_r(T) \to \infty$ (0). This completes the proof. ∎

THEOREM 6.2.2. *Let X_r be the number of submatroids of an exponentially growing $\omega(M(r))$ isomorphic to a given matroid M. Then X_r is Poisson convergent if and only if*

$$g_r p^{d(M)} \to 0 \quad \text{or} \quad g_r p^{\eta(M)} \to 0.$$

P r o o f. Since $\operatorname{Cov}(I_\alpha, I_\beta) = \operatorname{E}(I_\alpha I_\beta) - \pi_\alpha^2$ and

$$\sigma_r^2 = \sum_{\alpha,\beta} \operatorname{Cov}(I_\alpha, I_\beta) = \sum_{\alpha} (\pi_\alpha - \pi_\alpha^2) + \sum_{\alpha \neq \beta} \operatorname{Cov}(I_\alpha, I_\beta),$$

it remains to show that $\sum_{\alpha \doteqdot \beta} \operatorname{E}(I_\alpha I_\beta) = o(\lambda_r)$. But

$$\begin{aligned}
\sum_{\alpha \doteqdot \beta} \operatorname{E}(I_\alpha I_\beta) &\asymp \sum_{\emptyset \neq T \subseteq M} f_r^{(2\varrho(M) - \varrho(T))} p^{2|M| - |T|} \\
&= f_r^{(\varrho(M))} p^{|M|} \sum_{\emptyset \neq T \subseteq M} f_r^{(\varrho(M) - \varrho(T))} p^{|M| - |T|} \\
&= ((f_r^{(\varrho(M))})^{1/\varrho(M)} p^{d(M)})^{\varrho(M)} \sum_{\emptyset \neq T \subseteq M} ((f_r^{(\varrho(M) - \varrho(T))})^{1/(\varrho(M) - \varrho(T))} p^{\eta(M)})^{|M| - |T|} \\
&= O\Big(g_r p^{d(M)} \sum_{\emptyset \neq T \subseteq M} (g_r p^{\eta(M)})^{|M| - |T|} \Big).
\end{aligned}$$

From the fact that

$$\operatorname{E} X_r \asymp f_r^{(\varrho(M))} p^{|M|} = ((f_r^{\varrho(M)})^{1/\varrho(M)} p^{|M|/\varrho(M)})^{\varrho(M)} = O(g_r p^{d(M)})^{\varrho(M)}$$

we obtain

$$\sum_{\alpha \doteqdot \beta} \operatorname{E}(I_\alpha I_\beta) = o(\lambda_r),$$

provided $g_r p^{d(M)} \to 0$ or $g_r p^{\eta(M)} \to 0$. ∎

COROLLARY 6.2.3. *Let X_r be the number of submatroids of ω_r isomorphic to a given matroid M. Then X_r is Poisson convergent if and only if $q^r p^{d(M)} \to 0$ or $q^r p^{\eta(M)} \to 0$ as $r \to 0$.* ∎

COROLLARY 6.2.4. *Let X_r be the number of submatroids of $M(r,p) = M(K(n,p))$, $r = n - 1$, isomorphic to a given graphic matroid M. Then X_r is Poisson convergent if and only if $rp^{d(M)} \to 0$ or $rp^{\eta(M)} \to 0$ as $r \to 0$.* ∎

REMARK 6.2.1. Corollary 6.2.3 extends Theorem 2 from [28] when $|M| = \text{const}$.

REMARK 6.2.2. Corollary 6.2.4 and Theorem 1 from [41] are not equivalent. This is an easy consequence of the fact that two isomorphic matroids may be obtained from two nonisomorphic graphs. For example, let G_1 and G_2 be the nonisomorphic graphs of Figure 6.2.1.

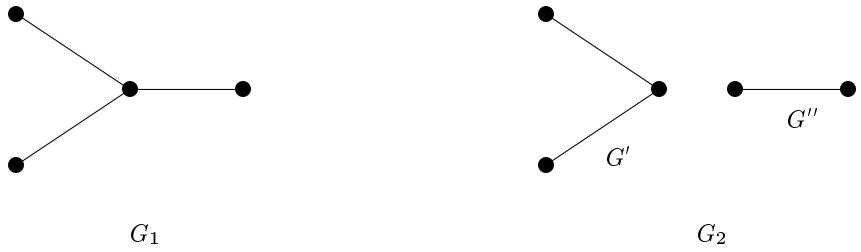

Fig. 6.2.1. Graphs G_1 and G_2

From these graphs, we obtain two isomorphic matroids M_1 and M_2, where $M_i = M(G_i)$. Note that G_2 is strictly balanced as a graph. Since $G_1 = G' \cup G''$ and $\overline{d}(G') = 2/3$, $\overline{d}(G'') = 1/2$ but $\overline{d}(G_2) = 3/5$, it follows that G_2 is not balanced. However, $M(G_1)$ and $M(G_2)$ are both balanced, $d(M(G_i)) = 1$, but not strictly balanced. Thus the number of copies of G_2 in $K(n,p)$ has a nontrivial Poisson distribution, but this is not true for $M(G_1)$.

Remark 6.2.3. Given $K(n,p)$, if $n^2(1-p) \to c > 0$, then $-X'_n \to \widetilde{\mathrm{Po}}(c/2)$, where X'_n denotes the number of subgraphs isomorphic to a given graph G and $\widetilde{\mathrm{Po}}(\lambda)$ denotes the distribution of $(X-\lambda)/\lambda$, where X has Poisson distribution $\mathrm{Po}(\lambda)$.

Note that the proofs of Theorems 6.2.1 and 6.2.2 avoid a detailed analysis of the behavior of the variance and leading overlaps which was necessary in [41].

Now we will prove the asymptotic normality of X_r, with $\lambda_r = \mathrm{E}\, X_r$, $\sigma_r^2 = \mathrm{Var}\, X_r$.

Lemma 6.2.5. *If there exists a natural number $n > 3$ such that*

$$J_M = |\Gamma|\, p^{|M|+n-1} \Delta_r \sigma_r^{-n} \to 0 \tag{6.2.2}$$

where Δ_r is the maximal degree of the vertices in the dependency graph $\mathcal{G}$, then $X_r \to \mathrm{N}(0,1)$.

P r o o f. Mikhailov [36] proved a refined version of Janson's Theorem 2 from [16]. For indicator random variables I_α, we can formulate this result in the following form. Let

$$\Gamma(V) = \{\beta : \alpha \sim \beta,\ \alpha \in V \subset \Gamma_r\}.$$

If there exist positive constants $C_{|V|}$ (not depending on $|\Gamma|$) and Q_r (not depending on $|V|$) such that

$$\sum_{\alpha \in \Gamma(V)} \mathrm{E}\,(I_\alpha | \mathcal{F}(V)) \le C_{|V|} Q_r, \tag{6.2.3}$$

where $\mathcal{F}(V)$ is the σ-field generated by $\{I_\alpha, \alpha \in V\}$ and if there exists an integer $n \ge 3$ such that

$$J = \lambda_r Q_r^{n-1} \sigma_r^{-n} \to 0,$$

then $X_r \to \mathrm{N}(0,1)$. In our case,

$$\sum_{\alpha \in \Gamma(V)} \mathrm{E}\,(I_\alpha | \mathcal{F}(V)) = \sum_{\alpha \in V} \pi_\alpha + \sum_{\alpha \in \Gamma(V) \setminus V} \mathrm{E}\,(I_\alpha | \mathcal{F}(V)),$$

and if $\alpha \notin V$ then

$$\mathrm{E}\,(I_\alpha|\mathcal{F}(V)) \le \mathrm{E}\,(I_\alpha|I_\beta = 1, \beta \in V) = \frac{\mathrm{Prob}(I_\alpha = 1, I_\beta = 1, \beta \in V)}{\mathrm{Prob}(I_\beta = 1, \beta \in V)} < p.$$

Since for positively related I_α's, we have $p \ge \pi_\alpha$, it follows that

$$\sum_{\alpha \in \Gamma(V)} \mathrm{E}\,(I_\alpha|\mathcal{F}(V)) \le C'_V\,|\Gamma(V)|\,\Delta_r p,$$

where C'_V depends only on V. Thus (6.2.3) gives $C_{|V|} = C'_V\,|\Gamma(V)|$ and $Q_r = \Delta_r p$. ∎

THEOREM 6.2.6. *Let X_r be the number of submatroids of an exponentially growing $\omega(M(r))$ isomorphic to a given matroid M. Then $X_r \to \mathrm{N}(0,1)$ if and only if $g_r p^{\gamma(M)} \to \infty$ and $g_r(1-p) \to \infty$.*

Proof. We split the proof of sufficiency into 3 cases according to the value of $c = \lim_{r\to\infty} p(r)$: $0 < c < 1$, $c = 0$ and $c = 1$. Note that

$$\begin{aligned} |\Gamma_r| &\asymp g_r^{\varrho(M)}, \\ \Delta_r &\asymp g_r^{\varrho(M)-1}, \\ \mathrm{Var}\,X_r &\asymp \sum_{\emptyset \ne T \subseteq M} g_r^{2\varrho(M)-\varrho(T)} p^{2|M|-|T|}(1-p^{|T|}). \end{aligned}$$

CASE 1: $p \to c$, $0 < c < 1$. In this case,

$$\mathrm{Var}\,X_r \asymp g_r^{2\varrho(M)-1}.$$

Hence, condition (6.2.2) is equivalent to

$$J_M \asymp g_r^{\varrho(M)-(2\varrho(M)-1)n/2+(\varrho(M)-1)(n-1)} = g_r^{1-n/2}$$

and $J_M \to 0$ for $n \ge 3$.

CASE 2: $p \to 1$. Now,

$$J_M \asymp g_r^{\varrho(M)-(2\varrho(M)-1)n/2+(\varrho(M)-1)(n-1)}(1-p)^{-n/2} \asymp (g_r^{(-n/2+1)}(1-p))^{-n/2}$$

and $J_M \to 0$ for sufficiently large n.

CASE 3: $p \to 0$. Because of (2.4.1),

$$\begin{aligned} \mathrm{Var}\,X_r &\asymp \sum_{\emptyset \ne T \subseteq M} g_r^{2\varrho(M)-\varrho(T)} p^{2|M|-|T|} \\ &\ge (g_r p^{d(M)})^{\varrho(M)} \sum_{\emptyset \ne T \subseteq M} (g_r p^{\gamma(M)})^{\varrho(M)-\varrho(T)} \end{aligned}$$

and

$$\begin{aligned} J_M &\le \frac{g_r^{2\varrho(M)-1} p^{|M|+n-1}}{(g_r p^{d(M)})^{n\varrho(M)/2} (\sum_{\emptyset \ne T \subseteq M} (g_r p^{\gamma(M)})^{\varrho(M)-\varrho(T)})^{n/2}} \\ &\le \frac{g_r^{\varrho(M)} (g_r p^{d(M)})^{\varrho(M)} p^{n-1}}{(g_r p^{d(M)})^{n\varrho(M)/2} (\sum_{\emptyset \ne T \subseteq M} (g_r p^{\gamma(M)})^{\varrho(M)-\varrho(T)})^{n/2}} \\ &\le (g_r p^{\gamma(M)})^{\varrho(M)(1-n/2)} \Big(\sum_{\emptyset \ne T \subseteq M} (g_r p^{\gamma(M)})^{\varrho(M)-\varrho(T)} \Big)^{-n/2} g_r^{\varrho(M)} p^{n-1}. \end{aligned}$$

Thus $J_M \to 0$, provided $n \ge 3$. ∎

Corollary 6.2.7. *Let X_r be the number of submatroids of ω_r isomorphic to a given matroid M. Then $X_r \to \mathrm{N}(0,1)$ if and only if $q^r p^{\gamma(M)} \to \infty$ and $q^r(1-p) \to \infty$.*

Corollary 6.2.8. *Let X_r be the number of submatroids of $\omega(M(K(n,p)))$, $r = n-1$, isomorphic to a given graphic matroid M. Then $X_r \to \mathrm{N}(0,1)$ if and only if $rp^{\gamma(M)} \to \infty$ and $n^2(1-p) \to \infty$.*

6.3. Full subspaces. The results in this section are mostly from [31]. Let X_r denote the number of full subspaces of rank d in ω_r. First we investigate the asymptotic behavior of the expectation $\mathrm{E}\, X_r$.

Lemma 6.3.1. *Let*

$$[r]p^{q^d} = r(dq^d - [d])\log q + [d]\log r + \lambda_r. \tag{6.3.1}$$

Then $\mathrm{E}\, X_r \to \left\{ {0 \atop \infty} \right\}$ iff $\lambda_r \to \left\{ {\infty \atop -\infty} \right\}$.

Proof. Note that $\mathrm{E}\, X_r \to \left\{ {0 \atop \infty} \right\}$ iff the following formulae hold:

$$q^{rd} p^{[d]} (1-p^{q^d})^{[r-d]} \to \left\{ {0 \atop \infty} \right\},$$

$$q^{rd} p^{[d]} \exp(-[r-d]p^{q^d}) \to \left\{ {0 \atop \infty} \right\},$$

$$rd\log q + [d]\log p - [r]q^{-d}p^{q^d} \to \left\{ {-\infty \atop \infty} \right\},$$

$$[r]q^{-d}p^{q^d} = rd\log q + [d]\log p + \lambda_r, \tag{6.3.2}$$

where $\lambda_r \to \left\{ {\infty \atop -\infty} \right\}$.

Now, one can calculate p from (6.3.2):

$$p = \left(\frac{rd\log q + [r]\log p + \lambda_r}{[r]q^{-d}} \right)^{q^{-d}}$$

and

$$\log p \asymp q^{-d}(\log r - \log[r]).$$

Therefore, returning to (6.3.2),

$$[r]q^{-d}p^{q^d} = rd\log q + [d]q^{-d}(\log r - \log[r]) + \lambda_r.$$

Since $\lambda_r \to \left\{ {\infty \atop -\infty} \right\}$, one can omit all bounded terms on the right-hand side of (6.3.2). Hence we obtain the assertion of our lemma. ∎

For $0 \le s < d-2$, we have

$$\begin{aligned} P_2(d,s) = 1 &- 2[d-s]p^{q^d-q^s} + [d-s]^2 p^{2q^d-[2]q^s} \\ &+ 2\begin{bmatrix} d-s \\ 2 \end{bmatrix} p^{[2](q^d-q^s)} + O(p^{q^d([1]+[2])-q^s[3]}). \end{aligned} \tag{6.3.3}$$

The last summand is equal to

$$O(p^{q^s(q^{d-s+1}+2q^{d-s}-q^2-q-1)}).$$

LEMMA 6.3.2. *Let* $pq^{rd/[d]} > c > 0$ *and* $[r]p^{q^d} = O(r)$. *Then*

$$\operatorname{Var} X_r = \operatorname{E} X_r + O(q^{-r}(\operatorname{E} X)^2).$$

P r o o f. Using (5.2.1) and (6.3.3), we have

$$A_0 = \begin{bmatrix} r \\ d \end{bmatrix} \begin{bmatrix} r-d \\ d \end{bmatrix} q^{d^2} p^{2[d]} (1 - 2p^{q^d} + p^{q^{2d}}) P_2(d,0) \tag{6.3.4}$$
$$- (p^{[d]}(1-p^{q^d})^{[r-d]})^2 = (\operatorname{E} X_r)^2 (2[d]p^{q^d-1} + O(p^{q^d})),$$

$$A_s = O(q^{r(2d-s)} p^{2[d]-[s]} e^{-2q^d[r]}) = O(q^{-r} p^{-1} (\operatorname{E} X_r)^2), \tag{6.3.5}$$

where $s = 1, 2, \ldots, d-1$,

$$A_d = \operatorname{E} X_r (1 - \operatorname{E} I_\alpha) = \operatorname{E} X_r + O(q^{-r}(\operatorname{E} X_r)^2). \tag{6.3.6}$$ ∎

THEOREM 6.3.3. *For fixed* $d \geq 1$, *as* $r \to \infty$ *we have*

(a) *if* $pq^{rd/[d]} \to 0$, *then* $\operatorname{Prob}(X_r = 0) \to 1$,
(b) *if* $pq^{rd/[d]} \to \infty$ *and* $\lambda_r \to -\infty$, *then* $\operatorname{Prob}(X_r = 0) \to 0$,
(c) *if* $\lambda_r \to \infty$, *then* $\operatorname{Prob}(X_r = 0) \to 1$.

P r o o f. If conditions (a) or (c) hold, then $\operatorname{E} X_r \to 0$. In case (b) the Chebyshev Inequality implies that

$$\operatorname{Prob}(X_r = 0) \leq \frac{\operatorname{Var} X_r}{(\operatorname{E} X_r)^2} = O\left(\frac{1}{\operatorname{E} X_r} + q^{-r}\right).$$

The conditions in case (b) are equivalent to $\operatorname{E} X_r \to \infty$ or $\operatorname{Var} X_r \to \infty$. Hence, $\operatorname{Prob}(X_r = 0) \to 0$. ∎

Now, we investigate the conditions leading to the Poisson convergence of X_r. First we present an auxiliary result which is a simple corollary of Theorem 2.A from [3].

Note that from the proof of Lemma 6.3.2 (the formulae (6.3.4) and (6.3.2)) we immediately obtain

$$\sum_{\alpha \neq \beta} |\operatorname{Cov}(I_\alpha, I_\beta)| = O(q^{-r}(\operatorname{E} X)^2).$$

Hence, we have to investigate the asymptotic behavior of $q^{-r} \operatorname{E} X_r$. If $d = 1$, then $q^{-r} \operatorname{E} X_r \to 0$ for all $p < 1$. For $d > 1$, we have the following result.

LEMMA 6.3.4. *Let*

$$[r]p^{q^d} = r(q^d(d-1) - [d]) \log q + [d] \log r + \theta_r. \tag{6.3.7}$$

Then $q^{-r} p^{-1} \operatorname{E} X_r \to 0$ *iff* $q^{r(d-1)/([d]-1)} p \to 0$ *or* $\theta_r \to \infty$ *in* (6.3.7).

P r o o f.

$$q^{-r} \operatorname{E} X_r = q^{-r} \begin{bmatrix} r \\ d \end{bmatrix} p^{[d]} (1 - p^{q^d})^{[r-d]} \tag{6.3.8}$$

$$\asymp q^{(d-1)r} p^{[d]} \exp\{-q^{-d}([r] - [d]) p^{q^d}\}. \tag{6.3.9}$$

Consider under what circumstances the last term of the above expression tends to zero. It is true for $d > 1$ iff the subsequent formulae hold, where $\theta_r \to \infty$:

$$(d-1)r\log q + [d]\log p - q^{-d}([r]-[d])p^{q^d} = -\theta_r,$$
$$\theta_r = q^{-d}([r]-[d])p^{q^d} - (d-1)r\log q - [d]\log p.$$

Calculating p from the above formula we obtain

$$p \asymp (q^{-(r-d)}(q-1)(d-1)r\log q)^{q^{-d}}$$

and

$$\log p \asymp q^{-d}(\log r - r\log q).$$

Hence

$$\theta_r = q^{-d}[r]p^{q^d} - (d-1)r\log q - [d]\{q^{-d}(\log r - r\log q)\}$$

and $\theta_r \to \infty$ or

$$\theta_r = [r]p^{q^d} - (q^d(d-1) - [d])r\log q - [d]\log r$$

and $\theta_r \to \infty$. ∎

THEOREM 6.3.5. *Let* $\mu_r = \mathrm{E}\, X_r$ *and* $r \to \infty$.

(i) *If* $d \geq 2$, *then*
  (a) *if* $pq^{r(d-1)/([d]-1)} \to 0$ *then* $d_{\mathrm{TV}}(\mathcal{L}(X_r), Po(\mu_r)) \to 0$,
  (b) *if*

$$[r]p^{q^d} = (q^d(d-1) - [d])r\log q + [d]\log r + \theta_r$$

  where $\theta_r \to \infty$, *then* $d_{\mathrm{TV}}(\mathcal{L}(X_r), Po(\mu_r)) \to 0$.

(ii) *If* $d = 1$ *and* $0 < p < 1$, *then* $d_{\mathrm{TV}}(\mathcal{L}(X_r), Po(\mu_r)) \to 0$.

Proof. Let $\delta_r = d_{\mathrm{TV}}(\mathcal{L}(X_r), \mathrm{Po}(\mu_r)))$. If $\mathrm{E}\, X_r \to 0$, then obviously $\delta_r \to 0$. Note that, if $pq^{r(d-1)/[d]} \to 0$, then $q^{-r}\,\mathrm{E}\, X_r \to 0$. Applying Lemma 3.1.5 we get

$$\delta_r = O\Big(\frac{1-e^{-\mu_r}}{\mu_r}\Big(\sum_{\alpha\in\Gamma}(\mathrm{Prob}(I_\alpha = 1))^2 + O(q^{-r}\mu_r^2)\Big)\Big).$$

Since

$$\sum_{\alpha\in\Gamma}(\mathrm{Prob}(I_\alpha = 1))^2/\mu_r = \mathrm{Prob}(I_\alpha = 1) = p,$$

it follows that either $p \to 0$ or $1 - e^{-\mu_r} \to 0$ and if $pq^{r(d-1)/[d]} \to 0$ or $\theta_r \to \infty$, then $\delta_r \to 0$. ∎

Finally, let us point out the related result given by Kelly and Oxley [23]. For $k = 1, 2, \ldots$, let K_r be the rank of the largest full subspace of ω_r. We define b to be the positive real number satisfying $b^{q-1} = p^{-1}$. For any $\varepsilon \geq 0$, define

$$d_{r,\varepsilon} = \Big(\log_q\Big(\frac{r\log_q r}{\log_q b}\Big) + \varepsilon\Big).$$

THEOREM 6.3.6. *If* $0 \leq \varepsilon \leq 1$ *then* $\mathrm{Prob}(K_r \in \{d_{r,0}, d_{r,\varepsilon}\}) \to 1$ *for* $r \to \infty$. ∎

A complete proof of this theorem is given in [23].

6.4. Related results. In this section we give some results related to those in the previous sections, such as the asymptotic behavior of random projective geometries. It is easy to see that these results can also be formulated, in most cases, for exponentially growing matroids.

We present some corollaries of the results of Section 6 and additional results from the papers of Kelly and Oxley [23] and [38] and from [28] for strictly balanced submatroids in random projective geometries.

Let $Y_r(k)$ be the number of k-element cycles. Since any cycle is a strictly balanced submatroid in ω_r, from Theorems 6.2.1, 6.2.2 and 6.2.6 we have the following results.

THEOREM 6.4.1. *Fix $k \geq 2$, let $Y_r = Y_r(k)$ and $\mu_r = \mathrm{E}\, Y_r$, $p = p(r)$. Then, as $r \to \infty$,*

(a) *Threshold: if $pq^{r(k-1)/k} \to \{{}^{0}_{\infty}\}$, then $\mathrm{Prob}(Y_r = 0) \to \{{}^{1}_{0}\}$;*

(b) *Poisson approximation: if $pq^{r(k/(k-1))} \to 0$, then $d_{\mathrm{TV}}(\mathcal{L}(Y_r), \mathrm{Po}(\mu_r)) \to 0$;*

(c) *Normal approximation: if $pq^{r(k-1)/k} \to \infty$ and $q^r(1-p) \to \infty$, then $\widetilde{Y}_r \to \mathrm{N}(0,1)$;*

where $\mu_r = \mathrm{E}\, C_{r,k}$ is given by (5.3.1). ∎

Now, let Y_r be the number of full $PG(d-1,q)$ in ω_r. As above, we have the following results.

THEOREM 6.4.2. *Fix $d \geq 2$, let $Y_r = Y_r(d)$ and $\mu_r = \mathrm{E}\, Y_r$, $p = p(r)$. Then, as $r \to \infty$,*

(a) *Threshold: if $pq^{rd/[d]} \to \{{}^{0}_{\infty}\}$, then $\mathrm{Prob}(Y_r = 0) \to \{{}^{1}_{0}\}$;*

(b) *Poisson approximation: if $pq^{r(d/[d]-1/[d]^2)} \to 0$, then $d_{\mathrm{TV}}(\mathcal{L}(Y_r), \mathrm{Po}(\mu_r)) \to 0$;*

(c) *Normal approximation: if $pq^{rd/[d]} \to \infty$ and $q^r(1-p) \to \infty$, then $\widetilde{Y}_r \to \mathrm{N}(0,1)$;*

where

$$\mu_r = \mathrm{E}\, Y_r = \begin{bmatrix} r \\ d \end{bmatrix} p^{[d]}. \quad ∎$$

The first two statements of Theorem 6.4.1 were proved (although in quite different terminology) by Voigt [45].

Kelly and Oxley proved [23] the following results.

LEMMA 6.4.3. *Let $(X_1, X_2, \ldots)$ be a sequence of random variables with $\mathrm{E}\, X_n = \mu_n$ and $\mathrm{Var}\, X_n = \sigma_n^2$ for $n = 1, 2, \ldots$ If $\sum_{n=1}^{\infty} \sigma_n^2/\mu_n^2$ is convergent, then*

$$\mathrm{Prob}(\lim_{n\to\infty} X_n/\mu_n = 1) = 1. \quad ∎$$

THEOREM 6.4.4. *Let $C_{r,k}$ and $I_{r,k}$ denote the number of circuits and independent sets with k elements, respectively, in ω_r. Let $k = k_r$ be a fixed sequence of nonnegative integers. If $3 \leq k \leq r+1$ for all r, then*

$$\mathrm{Prob}(\lim_{r\to\infty} C_{r,k}(\mathrm{E}\, C_{r,k}) = 1) = 1$$

and if $0 \leq k \leq r$ for all r, then

$$\mathrm{Prob}(\lim_{r\to\infty} I_{r,k}(\mathrm{E}\, I_{r,k}) = 1) = 1. \quad ∎$$

THEOREM 6.4.5. *For every sequence $\{k_r\}$ of nonnegative integers, if $3 \leq k_r \leq r+1$ for all r, then ω_r has a k_r-element cycle a.s.* ∎

Theorems 6.4.4 and 6.4.5 follow from Lemmas 6.4.3 and 2.3.6 (see [23] for details).

Now, we extend some results from Section 6 to the case where the rank of a "small" submatroid depends on r and tends slowly to infinity. We assume that all such matroids are submatroids of $PG(r-1,q)$.

Let Y_r denote the number of matroids isomorphic to a matroid from the family of matroids $\mathcal{B}$. Let $b(\mathcal{B})$ be the number of all matroids of rank isomorphic to a matroid from $\mathcal{B}$. Reference [28] gives the following two theorems.

THEOREM 6.4.6. *If $\mathcal{B}$ is a family of balanced matroids, each of which has m elements and rank k, then*

$$d_{\mathrm{TV}}(Y_r, \mathrm{Po}(\alpha^*(r))) \le 2p^m + \frac{4}{\alpha^*(r)} \sum_{k \le l \le 2k-1} \begin{bmatrix} r \\ l \end{bmatrix} \left\{ \begin{bmatrix} l \\ k \end{bmatrix} b(\mathcal{B}) \right\}^2 p^{lm/k+\varepsilon(\mathcal{B})}, \tag{6.4.1}$$

where

$$\alpha^*(n) = \begin{bmatrix} r \\ k \end{bmatrix} b(\mathcal{B}) p^m. \ \blacksquare$$

To prove that Y_r is Poisson convergent one has to find when the right-hand side of inequality (6.4.1) tends to zero as $r \to \infty$.

We write

$$\begin{aligned} \alpha(r) &= p^m q^{rk} b(\mathcal{S}) ([k]_k (q-1)^k q^{\binom{k}{2}})^{-1}, \\ \eta &= \max\{1, b(\mathcal{S})\} ([k]_k (q-1)^k q^{\binom{k}{2}})^{-1}, \end{aligned} \tag{6.4.2}$$

where $\mathcal{S}$ is a family of strictly balanced matroids each of which has m elements and rank k. In the following theorem, m can depend on n.

THEOREM 6.4.7. *If $\alpha(r) \to \lambda$, where λ is some positive constant and*

$$\eta q^{4k^2 - r\varepsilon(\mathcal{S})/m} = o(1),$$

or $\alpha(r) \to \infty$ and

$$\alpha(r) = o(\eta^{-1} 1^{-4k^2 + r\varepsilon(\mathcal{S})/m}),$$

then Y_r is Poisson convergent. $\blacksquare$

Theorem 6.4.7 generalizes some results from [38]. The proofs of Theorems 6.4.6 and 6.4.7 use Lemma 2.4.1. Theorem 6.4.6 is a matroid counterpart to Theorem 2.7 in [21]. The first statement of Theorem 6.4.7 is an extension of Theorems 3.1 and 3.12 in [38]. These results are obtained from Theorem 6.4.7 by substituting $p \sim cq^{-rk/m}$, where c is an arbitrary positive constant and k and m are fixed or $\alpha(r) \sim \lambda$ for some positive constant λ, and $km^2 = o(r)$. Theorem 6.4.7 is also a matroid counterpart of Theorems 2.8 – 2.10 in [21]. Two further theorems from [38] are given below.

THEOREM 6.4.8. *Let $\alpha(r)$ be given by* (6.4.2). *M is strictly balanced and $\mathcal{B} = \{M\}$. Let W_r denote the number of pairwise disjoint flats of ω_r which are isomorphic to M. If $\alpha(r) \to \lambda$, where λ is a positive constant, then W_r is Poisson convergent.* $\blacksquare$

THEOREM 6.4.9. *Let $M_1, M_2, \ldots$ be fixed strictly balanced matroids. Suppose that M_i has rank k_i and has m_i elements and that, for all i, m_i/k_i equals a fixed constant d. Let $Z_{r,i}$ and ν_i denote the numbers of submatroids of ω_r and $PG(k-1,q)_i$, respectively, which are isomorphic to M_i. Let $\alpha_i(r) \to \lambda$, where λ is a positive constant, and $\alpha_i(r)$ is*

given by (6.4.2) *with* $k = k_i$ *and* $m = m_i$. *Then, whenever* $s, n_1, n_2, \ldots, n_s$ *are natural numbers*,

$$\operatorname{Prob}(Z_{r,k} = n_i, i = 1, 2, \ldots, s) \sim \prod_{i=1}^{s} e^{-\alpha_i(r)} \alpha_i(r)^{n_i} / n_i! \,.$$

Moreover, if

$$Z_r = \sum_{i=1}^{s} Z_{r,i} \quad \textit{and} \quad \lambda = \sum_{i=1}^{s} \alpha_i(r),$$

then for every natural number n,

$$\operatorname{Prob}(Z_r = n) \sim e^{-\lambda} \lambda^n / n! \,. \ \blacksquare$$

To end this section, we present a brief sketch of the results from the paper of Kelly and Oxley [25].

Kelly and Oxley consider a column dependence matroid M_r of an $r \times n$ matrix whose elements are chosen independently and at random from $GF(q)$. Let $n = n_r$ and $r \to \infty$. If there exists a random integer R such that a given property $A(r)$ holds for all $r \geq R$, then $A(r)$ holds *eventually*. The following two theorems are directly comparable to Theorem 6.1.4.

THEOREM 6.4.10. *Suppose that eventually* $n_r \leq r$. *Then*

$$\sum_r \operatorname{Prob}(\varrho(M_r) < n_r) < \infty \quad \textit{if and only if} \quad \sum_r q^{(r-n)} < \infty.$$

In particular, if eventually

$$n_r \leq r - \log_q r - (1 + \delta) \log_q \log_q r$$

for some $\delta > 0$, *then* $\sum_r (\varrho(M_r) < n_r) < \infty$, *and so a.s., eventually* M_r *is the free matroid on* n_r *elements. If eventually*

$$n_r \geq r - \log_q r - \log_q \log_q r,$$

then $\sum_r (\varrho(M_r) < n_r)$ *diverges.* $\blacksquare$

THEOREM 6.4.11. *Suppose that eventually* $n_r \geq r$. *Then*

$$\sum_r \operatorname{Prob}(\varrho(M_r) < r) < \infty \quad \textit{if and only if} \quad \sum_r q^{(n-r)} < \infty.$$

In particular, if eventually

$$n_r \geq r + \log_q r + (1 + \delta) \log_q \log_q r$$

for some $\delta > 0$, *then* $\sum_r (\varrho(M_r) < r) < \infty$, *and so a.s., eventually* M_r *has a full rank. If eventually*

$$n_r \leq r + \log_q r + \log_q \log_q r,$$

then $\sum_r (\varrho(M_r) < n_r)$ *diverges.* $\blacksquare$

The remaining results from [25] are not directly comparable to the theorems presented in the previous sections. Kelly and Oxley consider the connectivity and vertical connectivity of M_r and the existence of k_r-cycles.

7. Problems and conclusions

In this final section we describe some open problems:

1. Find an effective method to calculate the likelihoods of some characteristics of random matroids in finite cases. It is relatively easy to compute the probability $P^{(r)}$ that a random submatroid of $PG(r-1,q)$ has full rank, but for other characteristics this is still an unsolved problem. Note, however, that the probability $P^{(r)}$ may be very hard to compute for small p and large r, such that $P^{(r)}$ is bounded away from 1. This problem is more difficult for matroids than for graphs because $\begin{bmatrix} r \\ k \end{bmatrix}$ tends to infinity faster than $\binom{r}{k}$.

2. Find a method of generating ω_r. Is it possible to generate ω_r using Algorithm 4.1.1? How should other random matroids be generated?

3. Investigate normal convergence for maximal full subspaces in ω_r. Barbour, Janson, Karoński and Ruciński [4] prove normality using several methods, but it seems that these methods are not applicable in the case of random matroids. An interesting goal would be to adapt or extend the method of cumulants to the case of matroids.

Since every graph is a matroid, almost all problems which can be stated in terms of cycles, trees etc. can be treated as matroid problems. Thus we have this "general" problem: which of the random graph problems can be translated in an interesting way into problems of random matroids? For what class of matroids is it possible? In fact, from the known matroids only ω_r and closely related random matroids (such as exponentially growing matroids) are sufficiently nontrivial to be worth further investigation.

Appendix: Tables

1. Gaussian coefficients. This table contains the Gaussian coefficients $\begin{bmatrix} n \\ m \end{bmatrix}$ for $q = 2, 3, 4, 5, 7$ and 9.

$q=2$							
1							
1	1						
1	3	1					
1	7	7	1				
1	15	35	15	1			
1	31	155	155	31	1		
1	63	651	1395	651	63	1	
1	127	2667	11811	11811	2667	127	1

$q=3$							
1							
1	1						
1	4	1					
1	13	13	1				
1	40	130	40	1			
1	121	1210	1210	121	1		
1	364	11011	33880	11011	364	1	
1	1093	99463	925771	925771	99463	1093	1

$q = 4$						
1						
1	1					
1	5	1				
1	21	21	1			
1	85	357	85	1		
1	341	5797	5797	341	1	
1	1365	93093	376805	93093	1365	1

$q = 5$						
1						
1	1					
1	6	1				
1	31	31	1			
1	156	806	156	1		
1	781	20306	20306	781	1	
1	3906	508431	2558556	508431	3906	1

$q = 7$					
1					
1	1				
1	8	1			
1	57	57	1		
1	400	2850	400	1	
1	2801	140050	140050	2801	1

$q = 8$					
1					
1	1				
1	9	1			
1	73	73	1		
1	585	4745	585	1	
1	4681	304265	304265	4681	1

$q = 9$					
1					
1	1				
1	10	1			
1	91	91	1		
1	820	7462	820	1	
1	7381	605242	605242	7381	1

2. Probabilities $P^{(r)}$. This table contains probabilities $P^{(r)}$ (see Section 5.1) calculated from formula (5.1.2) for $q = 2, 3, 4, 5, 7$ and 9.

$q = 2$

p	$r=2$	3	4	5	6	7	8
0.05	0.0073	0.0030	0.0035	0.0101	0.0527	0.2991	0.8482
0.10	0.0280	0.0211	0.0379	0.1245	0.4497	0.9149	0.9997
0.15	0.0608	0.0614	0.1279	0.3716	0.8246	0.9966	1.0000
0.20	0.1040	0.1251	0.2679	0.6348	0.9637	0.9999	1.0000
0.25	0.1563	0.2090	0.4328	0.8238	0.9945	1.0000	
0.30	0.2160	0.3076	0.5941	0.9279	0.9993	1.0000	
0.35	0.2818	0.4141	0.7318	0.9746	0.9999	1.0000	
0.40	0.3520	0.5220	0.8365	0.9923	1.0000		
0.45	0.4253	0.6252	0.9084	0.9980	1.0000		
0.50	0.5000	0.7188	0.9531	0.9995	1.0000		
0.55	0.5748	0.7993	0.9783	0.9999	1.0000		
0.60	0.6480	0.8650	0.9911	1.0000			
0.65	0.7183	0.9155	0.9968	1.0000			
0.70	0.7840	0.9518	0.9990	1.0000			
0.75	0.8438	0.9756	0.9998	1.0000			
0.80	0.8960	0.9896	1.0000				
0.85	0.9393	0.9966	1.0000				
0.90	0.9720	0.9993	1.0000				
0.95	0.9928	1.0000					

$q = 3$

p	$r=2$	3	4	5	6
0.05	0.0140	0.0206	0.1075	0.6414	0.9990
0.10	0.0523	0.1152	0.4983	0.9862	1.0000
0.15	0.1095	0.2720	0.8118	0.9998	1.0000
0.20	0.1808	0.4509	0.9473	1.0000	
0.25	0.2617	0.6178	0.9883	1.0000	
0.30	0.3483	0.7536	0.9979	1.0000	
0.35	0.4370	0.8528	0.9997	1.0000	
0.40	0.5248	0.9186	1.0000		
0.45	0.6090	0.9586	1.0000		
0.50	0.6875	0.9808	1.0000		
0.55	0.7585	0.9920	1.0000		
0.60	0.8208	0.9971	1.0000		
0.65	0.8735	0.9991	1.0000		
0.70	0.9163	0.9998	1.0000		

$q = 3$ (continued)

p	$r=2$	3
0.75	0.9492	1.0000
0.80	0.9728	1.0000
0.85	0.9880	1.0000
0.90	0.9963	1.0000
0.95	0.9995	1.0000

$q = 4$

p	$r = 2$	3	4
0.05	0.0226	0.0742	0.5601
0.10	0.0815	0.3183	0.9604
0.15	0.1648	0.5880	0.9983
0.20	0.2627	0.7871	1.0000
0.25	0.3672	0.9037	1.0000
0.30	0.4718	0.9615	1.0000
0.35	0.5716	0.9864	1.0000
0.40	0.6630	0.9957	1.0000
0.45	0.7438	0.9988	1.0000
0.50	0.8125	0.9997	1.0000
0.55	0.8688	0.9999	1.0000
0.60	0.9130	1.0000	
0.65	0.9460	1.0000	
0.70	0.9692	1.0000	
0.75	0.9844	1.0000	
0.80	0.9933	1.0000	
0.85	0.9978	1.0000	
0.90	0.9995	1.0000	
0.95	1.0000		

$q = 5$

p	$r = 2$	3	4
0.05	0.0328	0.1816	0.9384
0.10	0.1143	0.5761	0.9998
0.15	0.2235	0.8389	1.0000
0.20	0.3446	0.9510	1.0000
0.25	0.4661	0.9876	1.0000
0.30	0.5798	0.9974	1.0000
0.35	0.6809	0.9995	1.0000
0.40	0.7667	0.9999	1.0000
0.45	0.8364	1.0000	
0.50	0.8906	1.0000	
0.55	0.9308	1.0000	
0.60	0.9590	1.0000	
0.65	0.9777	1.0000	
0.70	0.9891	1.0000	
0.75	0.9954	1.0000	
0.80	0.9984	1.0000	
0.85	0.9996	1.0000	
0.90	0.9999	1.0000	
0.95	1.0000		

$q = 7$

p	$r = 2$	3
0.05	0.0572	0.5208
0.10	0.1869	0.9209
0.15	0.3428	0.9922
0.20	0.4967	0.9994
0.25	0.6329	1.0000
0.30	0.7447	1.0000
0.35	0.8309	1.0000
0.40	0.8936	1.0000
0.45	0.9368	1.0000
0.50	0.9648	1.0000
0.55	0.9819	1.0000
0.60	0.9915	1.0000
0.65	0.9964	1.0000
0.70	0.9987	1.0000
0.75	0.9996	1.0000
0.80	0.9999	1.0000
0.85	1.0000	

$q = 8$

p	$r = 2$	3
0.05	0.0712	0.6904
0.10	0.2252	0.9765
0.15	0.4005	0.9990
0.20	0.5638	1.0000
0.25	0.6997	1.0000
0.30	0.8040	1.0000
0.35	0.8789	1.0000
0.40	0.9295	1.0000
0.45	0.9615	1.0000
0.50	0.9805	1.0000
0.55	0.9909	1.0000
0.60	0.9962	1.0000
0.65	0.9986	1.0000
0.70	0.9996	1.0000
0.75	0.9999	1.0000
0.80	1.0000	

$q = 9$

p	$r = 2$	3
0.05	0.0861	0.8226
0.10	0.2639	0.9945
0.15	0.4557	0.9999
0.20	0.6242	1.0000
0.25	0.7560	1.0000
0.30	0.8507	1.0000
0.35	0.9140	1.0000
0.40	0.9536	1.0000
0.45	0.9767	1.0000
0.50	0.9893	1.0000
0.55	0.9955	1.0000
0.60	0.9983	1.0000
0.65	0.9995	1.0000
0.70	0.9999	1.0000
0.75	1.0000	

3. Parameters of X. This table contains the parameters of X (see Section 6.1) calculated from formula (6.1.3) for $x \in [0.02 \ldots 0.92]$, namely $\mathrm{E}\,X$, $\mathrm{Var}\,X$, σ and a variation coefficient.

x	$\mathrm{E}\,X$	$\mathrm{Var}\,X$	σ	$\sigma/\mathrm{E}\,X$
0.02	0.0208	0.0212	0.1457	7.0000
0.04	0.0433	0.0451	0.2123	4.8991
0.06	0.0677	0.0718	0.2679	3.9585
0.08	0.0940	0.1016	0.3187	3.3919
0.10	0.1223	0.1348	0.3671	3.0012
0.12	0.1529	0.1718	0.4144	2.7097
0.14	0.1860	0.2129	0.4614	2.4809
0.16	0.2216	0.2586	0.5086	2.2945
0.18	0.2601	0.3095	0.5563	2.1385
0.20	0.3017	0.3660	0.6050	2.0051
0.22	0.3467	0.4289	0.6549	1.8892
0.24	0.3953	0.4990	0.7064	1.7869
0.26	0.4479	0.5770	0.7596	1.6958
0.28	0.5050	0.6640	0.8149	1.6136
0.30	0.5669	0.7612	0.8724	1.5391
0.32	0.6341	0.8698	0.9326	1.4708
0.34	0.7072	0.9916	0.9958	1.4080
0.36	0.7869	1.1282	1.0622	1.3498
0.38	0.8739	1.2819	1.1322	1.2956
0.40	0.9690	1.4552	1.2063	1.2449
0.42	1.0732	1.6511	1.2849	1.1973
0.44	1.1876	1.8732	1.3686	1.1524
0.46	1.3136	2.1257	1.4580	1.1099
0.48	1.4527	2.4139	1.5537	1.0695
0.50	1.6067	2.7440	1.6565	1.0310
0.52	1.7777	3.1238	1.7674	0.9942
0.54	1.9683	3.5626	1.8875	0.9589
0.56	2.1815	4.0722	2.0180	0.9250
0.58	2.4210	4.6673	2.1604	0.8923
0.60	2.6914	5.3666	2.3166	0.8607
0.62	2.9981	6.1940	2.4888	0.8301
0.64	3.3481	7.1801	2.6796	0.8003
0.66	3.7499	8.3657	2.8924	0.7713
0.68	4.2145	9.8046	3.1312	0.7430
0.70	4.7562	11.5699	3.4015	0.7152
0.72	5.3935	13.7624	3.7098	0.6878

x	$\mathrm{E}\,X$	$\mathrm{Var}\,X$	σ	$\sigma/\mathrm{E}\,X$
0.74	6.1512	16.5241	4.0650	0.6608
0.76	7.0630	20.0602	4.4789	0.6341
0.78	8.1758	24.6750	4.9674	0.6076
0.80	9.5571	30.8361	5.5530	0.5810
0.82	11.3064	39.2896	6.2681	0.5544
0.84	13.5774	51.2846	7.1613	0.5274
0.86	16.6182	69.0383	8.3089	0.5000
0.88	20.8560	96.7898	9.8382	0.4717
0.90	27.0865	143.4747	11.9781	0.4422
0.92	36.9666	230.4346	15.1801	0.4106

Bibliography

[1] N. Alon, A. Frieze, and D. J. A. Welsh, *Polynomial time randomized approximation scheme for Tutte–Gröthendieck invariants: the dense case*, Random Structures Algorithms 6 (1995), 459–478.

[2] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading, Mass., 1976.

[3] A. D. Barbour, L. Holst, and S. Janson, *Poisson approximation*, Clarendon Press, Oxford, 1992.

[4] A. D. Barbour, S. Janson, M. Karoński, and A. Ruciński, *Small cliques in random graphs*, Random Structures Algorithms 1 (1990), 403–434.

[5] R. E. Barlow and F. Proshan, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, New York, 1975.

[6] B. Bollobás, *Threshold functions for small subgraphs*, Math. Proc. Cambridge Philos. Soc. 90 (1981), 197–206.

[7] —, *Random Graphs*, Academic Press, London, 1985.

[8] P. A. Catlin, J. W. Grossman, A. M. Hobbs, and H.-J. Lai, *Fractional arboricity, strength, principal partitions in graphs and matroids*, Combinatorics & optimization, res. report corr. 89–13, 1989.

[9] W. H. Cunnigham, *Optimal attack and reinforcement of a network*, J. Assoc. Comput. Mach. 32 (1985), 549–561.

[10] P. Erdős and A. Reńyi, *On the evolution of random graphs*, Publ. Math. Inst. Hungar. Acad. Sci. 5 (1960), 17–61.

[11] M. Filipkowska, *Matroid generating procedures in C*, Master's thesis, Technical University, Wrocław, 1993.

[12] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, Wiley, 1983.

[13] R. L. Graham, M. Grötschel, and L. Lovász (eds.), *Handbook of Combinatorics*, Elsevier, Amsterdam, 1995.

[14] F. Harary, *Graph Theory*, Addison-Wesley, Reading, Mass., 1971.

[15] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[16] S. Janson, *Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs*, Ann. Probab. 16 (1988), 305–312.
[17] S. Janson, *Poisson approximation for large deviation*, Random Structures Algorithms 1 (1990), 221–229.
[18] S. Janson, T. Łuczak, and A. Ruciński, *An exponential bound for the probability of nonexistence of a specified subgraphs in a random graph*, in: Random Graphs, Proc., Poznań 1987, Wiley, 73–87.
[19] J. G. Kalbfleisch, *Complete subgraphs of random hypergraphs and bipartite graphs*, in: Proc. 3rd S–E Conf. on Combinatorics, Graph Theory and Computing, Florida Atlantic Univ., Boca Raton, 1972, 297–304.
[20] S. Karlin, *A First Course in Stochastic Processes*, Academic Press, 1969.
[21] M. Karoński, *Balanced Subgraphs of Large Random Graphs*, Adam Mickiewicz University Press, Poznań, 1984.
[22] —, *Random matroids*, in: Handbook of Combinatorics, L. Lovász, R. L. Graham, M. Grötschel (eds.), Elsevier, Amsterdam, 1995.
[23] D. G. Kelly and J. G. Oxley, *Asymptotic properties of random subsets of projective spaces*, Math. Proc. Cambridge Philos. Soc. 91 (1982), 119–130.
[24] —, —, *Threshold functions for some properties of random subsets of projective spaces*, Quart. J. Math. Oxford 33 (1982), 463–469.
[25] —, —, *On random representable matroids*, Stud. Appl. Math. 71 (1984), 181–205.
[26] A. K. Kelmans, *Some problems of the analysis of reliability of nets*, Automat. Remote Control 26 (1965).
[27] D. Knuth, *Random matroids*, Discrete Math. 12 (1975), 341–358.
[28] W. Kordecki, *Strictly balanced submatroids in random subsets of projective geometries*, Colloq. Math. 55 (1988), 371–375.
[29] —, *Random subgraphs of the n-cycle and the n-wheel*, Discrete Math. 93 (1991), 35–53.
[30] —, *On the rank of a random submatroid of projective geometry*, in: Random Graphs, Proc. Poznań 1989, Vol. 2, Wiley, 151–163.
[31] —, *Maximal full subspaces in random projective spaces—thresholds and Poisson approximation*, Random Structures Algorithms 6 (1995), 297–305.
[32] —, *Small submatroids in random matroids*, Combin. Probab. Comput. 5 (1996), 1–10.
[33] W. Kordecki and T. Łuczak, *On random subsets of projective spaces*, Colloq. Math. 57 (1991), 353–356.
[34] W. Lipski and W. Marek, *Combinatorial Analysis*, PWN, Warszawa, 1986 (in Polish).
[35] M. V. Lomonosov, *Bernoulli scheme with closure*, Problems Inform. Transmission 10 (1974), 73–81.
[36] V. G. Mikhaĭlov, *On a Janson's theorem*, Teor. Veroyatn. i Primenen. 36 (1991), 168–170 (in Russian).
[37] H. Narayanan and N. Vartak, *On molecular and atomic matroids*, in: Combinatorics and Graph Theory, S. B. Rao (ed.), Lecture Notes in Math. 885, Springer, New York, 1981, 358–364.
[38] J. G. Oxley, *Threshold distribution function for some random representable matroids*, Math. Proc. Cambridge Philos. Soc. 95 (1984), 335–346.
[39] —, *Matroid Theory*, Oxford Univ. Press, Oxford, 1992.
[40] J. G. Oxley and D. J. A. Welsh, *The Tutte polynomial and percolation*, in: Graph Theory and Related Topics, Academic Press, New York, 1979, 329–339.

[41] A. Ruciński, *Random graphs of binomial type with sparsely-edged initial graphs*, Acta Math. Hungar. 47 (1986), 81–87.
[42] —, *Small subgraphs of random graphs—a survey*, in: Random Graphs, Proc. Poznań 1987, Wiley, 283–303.
[43] —, *Proving normality in combinatorics*, in: Random Graphs, Proc. Poznań 1989, Vol. 2, Wiley, 215–231.
[44] V. E. Stepanov, *Combinatorial algebra and random graph*, Theory Probab. Appl. 14 (1969), 373–399.
[45] B. Voigt, *On the evolution of finite affine and projective spaces*, Math. Oper. Res. 49 (1986), 313–327.
[46] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.
[47] —, *Complexity: Knots, Colourings and Counting*, London Math. Soc. Lecture Note Ser. 186, Cambridge Univ. Press, 1993.
[48] —, *Randomized approximation schemes for Tutte–Gröthendieck invariants*, in: Discrete Probability and Algorithms, D. Aldous, P. Diaconis, J. Spencer, and J. M. Steele (eds.), IMA Vol. Math. Appl. 72, Springer, New York, 1995, 133–148.
[49] N. White (ed.), *Theory of Matroids*, Encyclopedia Math. Appl., Cambridge Univ. Press, Cambridge, 1986.
[50] —, *Matroid Applications*, Encyclopedia Math. Appl. 40, Cambridge Univ. Press, Cambridge, 1992.
[51] —, *Combinatorial Geometries*, Encyclopedia Math. Appl. 29, Cambridge Univ. Press, Cambridge, 1993.