Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Combinatorial Theory, Series A 111 (2005) 1–23
Journal of Combinatorial Theory Series A
www.elsevier.com/locate/jcta

Sieve methods in combinatorics

Yu-Ru Liu[a,1], M. Ram Murty[b,1]

[a] *Department of Pure Mathematics, University of Waterloo, Waterloo, Ont., Canada, N2L 3G1*
[b] *Department of Mathematics and Statistics, Queen's University, Kingston, Ont., Canada, K7L 3N6*

Received 16 August 2004

Communicated by A.M. Odlyzko
Available online 11 January 2005

Abstract

We develop the Turán sieve and a 'simple sieve' in the context of bipartite graphs and apply them to various problems in combinatorics. More precisely, we provide applications in the cases of characters of abelian groups, vertex-colourings of graphs, Latin squares, connected graphs, and generators of groups. In addition, we give a spectral interpretation of the Turán sieve.

MSC: 05A05; 11N35

Keywords: Turán sieve; Simple sieve; Combinatorial sieve

1. A combinatorial Turán sieve

In 1934, Turán [18] gave a very simple proof of a celebrated result of Hardy and Ramanujan [8] that the normal order of distinct prime factors of a natural number n is $\log\log n$. If $\omega(n)$ denotes the number of distinct prime factors of n, Turán proved that

$$\sum_{n\leqslant x}(\omega(n)-\log\log x)^2 \ll x\log\log x,$$

from which the normal order of $\omega(n)$ is easily deduced. Turán's original derivation of the Hardy–Ramanujan theorem was essentially probabilistic and concealed in it an elementary

E-mail addresses: yrliu@math.uwaterloo.ca (Y.-R. Liu), murty@mast.queensu.ca (M.R. Murty).

[1] Partially supported by an NSERC Discovery Grant.

0097-3165/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2004.11.004

sieve method. This method has appeared in various formulations in several places. Most notable is the monograph of Erdös and Spencer [5, Section 16] and Lovász [12, problem 19, Section 2]. However, the sieve principle seems to be best emphasized in paper [11], where the authors introduced the Turán sieve method and applied it to probabilistic Galois theory problems.

In this paper, we formulate the Turán sieve method in a slightly general context, namely to that of bipartite graphs. Formulating it thus allows us the freedom to search for new applications of the method. To illustrate, we consider the problem of obtaining a non-trivial upper bound for the number of proper (vertex) colourings of a graph. We also consider related examples.

The extension of sieve methods to a combinatorial setting has been attempted before. For example, Wilson [19] and Chow [3] have formulated the Selberg sieve in a combinatorial context (see also Section 2 of [12]). However, due to the fact that the Möbius function of a lattice is difficult to compute in the abstract setting, it is not clear how one can apply the Selberg sieve to general combinatorial problems. This obstruction is somewhat eliminated by the Turán sieve.

Let X be a bipartite graph with finite partite sets (A, B). For $a \in A, b \in B$, we write $a \sim b$ if there is an edge that joins a and b. For $b \in B$, we define the *degree* of b to be

$$\deg b := \#\{a \in A,\ a \sim b\}.$$

For $b_1, b_2 \in B$, the *number of common neighbours* $n(b_1, b_2)$ of b_1 and b_2 is defined by

$$n(b_1, b_2) := \#\{a \in A, a \sim b_1 \text{ and } a \sim b_2\}.$$

Thus, if $b_1 = b_2 = b$, $n(b_1, b_2) = \deg b$.

For each $a \in A$, we define

$$\omega(a) := \#\{b \in B, a \sim b\} = \#\text{ of elements in } B \text{ that join } a.$$

Notice that

$$\sum_{a\in A} \omega(a) = \sum_{a\in A} \sum_{\substack{b\in B\\ a\sim b}} 1 = \sum_{b\in B} \sum_{\substack{a\in A\\ a\sim b}} 1 = \sum_{b\in B} \deg b.$$

Thus, the 'expected value' of $\omega(a)$ is

$$\frac{1}{|A|} \sum_{b\in B} \deg b,$$

where $|A|$ is the cardinality of A. To measure the difference between $\omega(a)$ and $\frac{1}{|A|} \sum_{b\in B} \deg b$, we consider the second moment of their difference, namely,

$$\sum_{a\in A} \left(\omega(a) - \frac{1}{|A|} \sum_{b\in B} \deg b \right)^2.$$

We have

$$\begin{aligned}
&\sum_{a\in A}\left(\omega(a)-\frac{1}{|A|}\sum_{b\in B}\deg b\right)^2\\
&\quad=\sum_{a\in A}\omega^2(a)-2\sum_{a\in A}\omega(a)\left(\frac{1}{|A|}\sum_{b\in B}\deg b\right)+\sum_{a\in A}\left(\frac{1}{|A|}\sum_{b\in B}\deg b\right)^2\\
&\quad=\sum_{a\in A}\omega^2(a)-\frac{2}{|A|}\left(\sum_{b\in B}\deg b\right)^2+\frac{1}{|A|}\left(\sum_{b\in B}\deg b\right)^2.
\end{aligned}$$

The last equality follows from the previous calculation of $\sum_{a\in A}\omega(a)$. It now remains to consider $\sum_{a\in A}\omega^2(a)$. By the definition of $\omega(a)$, we have

$$\sum_{a\in A}\omega^2(a)=\sum_{a\in A}\sum_{\substack{b_1,b_2\in B\\ a\sim b_1\\ a\sim b_2}}1=\sum_{b_1,b_2\in B}\sum_{\substack{a\in A\\ a\sim b_1\\ a\sim b_2}}1=\sum_{b_1,b_2\in B}n(b_1,b_2).$$

Combining the above results, we obtain the following theorem.

Theorem 1.

$$\sum_{a\in A}\left(\omega(a)-\frac{1}{|A|}\sum_{b\in B}\deg b\right)^2=\sum_{b_1,b_2\in B}n(b_1,b_2)-\frac{1}{|A|}\left(\sum_{b\in B}\deg b\right)^2.$$

Notice that

$$\#\{a\in A,\ \omega(a)=0\}\cdot\left(\frac{1}{|A|}\sum_{b\in B}\deg b\right)^2\leqslant\sum_{a\in A}\left(\omega(a)-\frac{1}{|A|}\sum_{b\in B}\deg b\right)^2.$$

Combining this inequality with Theorem 1, we obtain the following corollary.

Corollary 1 (*The Turán sieve*).

$$\#\{a\in A,\ \omega(a)=0\}\leqslant|A|^2\cdot\frac{\displaystyle\sum_{b_1,b_2\in B}n(b_1,b_2)}{\left(\displaystyle\sum_{b\in B}\deg b\right)^2}-|A|.$$

Example 1. We can apply Corollary 1 to obtain an upper bound for the inclusion-exclusion principle. Let A be a finite set and $\{A_1,A_2,\ldots,A_k\}$ be a collection of subsets of A. We construct a bipartite graph with B consisting of the sets A_i's. For $a\in A$, $b=A_b\in B$,

we will say

$$a \sim A_b \quad \text{if} \quad a \in A_b.$$

Thus,

$$\omega(a) = 0 \quad \text{if and only if} \quad a \notin A_i \text{ for all } 1 \leqslant i \leqslant k.$$

For $b, b_1, b_2 \in B$, notice that

$$\deg b = |A_b| \quad \text{and} \quad n(b_1, b_2) = |A_{b_1} \cap A_{b_2}|.$$

By Corollary 1, we have

$$\#\{a \in A : a \notin A_i \text{ for all } i,\ 1 \leqslant i \leqslant k\} \leqslant |A|^2 \cdot \frac{\sum_{i,j=1}^{k} |A_i \cap A_j|}{\sum_{i=1}^{k} |A_i|^2} - |A|.$$

We thus obtain an inequality for the standard inclusion-exclusion principle.

Example 2. From Theorem 1, we can derive the classical Turán theorem. For $b_1, b_2 \in B, b_1 \neq b_2$, we assume that

$$n(b_1, b_2) = \frac{\deg b_1 \cdot \deg b_2}{|A|} + e(b_1, b_2),$$

where we view $e(b_1, b_2)$ to be an 'error term' if we were to think of the events $a \sim b_1$ and $a \sim b_2$ as 'independent'. Putting it into Theorem 1, we have

$$\sum_{a \in A} \left(\omega(a) - \sum_{b \in B} \frac{\deg b}{|A|} \right)^2 = \sum_{b_1 \neq b_2} e(b_1, b_2) + \sum_{b \in B} \deg b \left(1 - \frac{\deg b}{|A|} \right).$$

This example is motivated by the classical number theory setting that inspired Turán's theorem stated at the outset of this paper. Indeed, let A denote the set of natural numbers $\leqslant x$ and B the set of primes $\leqslant x^{1/2}$. For $a \in A, b \in B$, we will say

$$a \sim b \quad \text{if} \quad b | a.$$

Thus,

$$\omega(a) = \#\text{ of distinct primes divisors of } n \text{ which are } \leqslant x^{1/2}.$$

Also, we have

$$\sum_{b \in B} \deg b \leqslant \sum_{b \leqslant \sqrt{x}} \left[\frac{x}{b} \right] = x \log\log x + O(x),$$

by a classical theorem of Mertens [13]. Moreover, if $b_1 \neq b_2$,

$$n(b_1, b_2) = \left[\frac{x}{b_1 b_2}\right] = \frac{x}{b_1 b_2} + O(1) = \frac{\deg b_1 \cdot \deg b_2}{|A|} + O(1),$$

so that $e(b_1, b_2) = O(1)$. It follows that

$$\sum_{a \leqslant x} (\omega(a) - \log\log x)^2 = O(x \log\log x),$$

which is Turán's theorem as for each $a \in A$, there is at most 1 prime divisor of a which is $> x^{1/2}$.

Corollary 1 provides an upper bound for the quantity

$$\#\{a \in A,\ \omega(a) = 0\}.$$

To get a lower bound for it, observe that

$$\{a \in A,\ \omega(a) = 0\} = A \setminus \bigcup_{b \in B} \{a \in A, a \sim b\}.$$

Since the union $\bigcup_{b \in B} \{a \in A, a \sim b\}$ is not necessarily disjoint, by the definition of $\deg b$, we have

Proposition 1 (*The simple sieve*).

$$\#\{a \in A,\ \omega(a) = 0\} \geqslant |A| - \sum_{b \in B} \deg b.$$

In Sections 2 and 3, we apply Corollary 1 and Proposition 1 to problems on characters of abelian groups and vertex-colourings of graphs. In particular, we obtain improvements of the Rédei Trägheitsatz [16,17] for some abelian groups. In Section 4, we apply Corollary 1 to obtain an upper bound for the number of Latin squares of order n. In Sections 5 and 6, we apply Proposition 1 to get lower bounds for the number of connected graphs and the number of n-tuples of elements of a group G which generate G. We conclude this paper by discussing a spectral interpretation of the Turán sieve method in Section 7.

2. Characters of abelian groups

In this section, we apply Corollary 1 and Proposition 1 to a problem about characters of abelian groups.

Let G be a finite abelian group and $\{H_1, H_2, \ldots, H_k\}$ a collection of subgroups of G. For an n-tuple $\chi = (\chi_1, \chi_2, \ldots, \chi_n)$ of characters of G, we say χ *distinguishes* $\{H_1, H_2, \ldots, H_k\}$, if for every H_j, there exists a character χ_i such that χ_i restricted to H_j is not the trivial

character. Thus, if the set $\{H_1, H_2, \ldots, H_k\}$ contains all non-trivial subgroups of G, χ distinguishes all subgroups of G except the identity. We are interested in the number of n-tuples of characters of G which distinguish $\{H_1, H_2, \ldots, H_k\}$.

Let A be the set of all n-tuples $\chi = (\chi_1, \chi_2, \ldots, \chi_n)$ of characters of G and B the set of all H_i's. For $a = \chi_a = (\chi_{a,1}, \chi_{a,2}, \ldots, \chi_{a,n}) \in A$, $b = H_b \in B$, we will say

$$a \sim b \quad \text{if} \quad \chi_{a,i} \text{ restricted to } H_b \text{ is trivial for all } i.$$

Thus, we have

$$\omega(a) = 0 \quad \text{if and only if} \quad \chi_a \text{ distinguishes } \{H_1, H_2, \ldots, H_k\}.$$

Notice that

$$|A| = |G|^n.$$

Let $b = H_b \in B$ and $a = \chi_a \sim b$. Since $\chi_{a,i}$ restricted to H_b is trivial, it can be thought of as a character of the quotient group G/H_b. Thus,

$$\deg b = (|G|/|H_b|)^n.$$

It follows that

$$\sum_{b \in B} \deg b = |G|^n \cdot \sum_{j=1}^{k} \frac{1}{|H_j|^n}.$$

For $b_1 = H_{b_1}, b_2 = H_{b_2} \in B$, we denote by $H_{b_1} \vee H_{b_2}$, the *join* of H_{b_1} and H_{b_2}, which is the smallest subgroup of G containing both H_{b_1} and H_{b_2}. For $a = \chi_a \in A$, if $a \sim b_1$ and $a \sim b_2$, the character χ_a vanishes at both H_{b_1} and H_{b_2}. Thus, it vanishes at $H_{b_1} \vee H_{b_2}$ and defines a character of the quotient group $G/(H_{b_1} \vee H_{b_2})$. It follows that

$$\sum_{b_1, b_2 \in B} n(b_1, b_2) = |G|^n \cdot \sum_{j_1, j_2 = 1}^{k} \frac{1}{|H_{j_1} \vee H_{j_2}|^n}.$$

Hence, by Corollary 1, we obtain that

Theorem 2. *Let $\{H_1, H_2, \ldots, H_k\}$ be a collection of subgroups of a finite abelian group G. We denote by $D_G(n, H_1, H_2, \ldots, H_k)$ the number of n-tuples $\chi = (\chi_1, \ldots, \chi_n)$ of characters of G distinguishing $\{H_1, H_2, \ldots, H_k\}$. We have*

$$D_G(n, H_1, H_2, \ldots, H_k) \leqslant |G|^n \cdot \left\{ \frac{\displaystyle\sum_{j_1, j_2 = 1}^{k} \frac{1}{|H_{j_1} \vee H_{j_2}|^n}}{\left(\displaystyle\sum_{j=1}^{k} \frac{1}{|H_j|^n} \right)^2} - 1 \right\}.$$

Also, by Proposition 1, we have

Theorem 3. *Let $\{H_1, H_2, \ldots, H_k\}$ be a collection of subgroups of a finite abelian group G. We denote by $D_G(n, H_1, H_2, \ldots, H_k)$ the number of n-tuples $\chi = (\chi_1, \ldots, \chi_n)$ of characters of G distinguishing $\{H_1, H_2, \ldots, H_k\}$. We have*

$$D_G(n, H_1, H_2, \ldots, H_k) \geqslant |G|^n \cdot \left\{ 1 - \sum_{j=1}^{k} \frac{1}{|H_j|^n} \right\}.$$

Let L be a lattice with a unique minimal element $\hat{0}$. An *order function* v on L is a function defined on pairs of elements x, y (with $x \preceq y$) in L such that $v(x, y) = v(x, z)v(z, y)$. We say L is *locally finite* if for every positive integer n, the number of elements $y \in L$ such that $v(x, y) = n$ is finite. The *Rédei zeta function* of a locally finite lattice L is defined by

$$\rho(s; L) = \sum_{x \in L} \mu(\hat{0}, x) v(\hat{0}, x)^{-s},$$

where μ is the Möbius function of L. By the finiteness assumption, the summation on the right is well defined as a formal Dirichlet series. Moreover, the zeros of $\rho(s; L)$ are very often combinatorially significant invariants. For example, it generalizes the chromatic polynomial of a graph, the inverse of the Dedekind zeta function of a number field, the inverse of the Weil zeta function for a variety over a finite field, etc. (For more applications of the Rédei zeta function, see [10].)

Consider the lattice $L_{\{H_1, H_2, \ldots, H_k\}}$ spanned by $\{H_1, H_2, \ldots, H_k\}$, which is a lattice containing all subgroups of G that are generated by some finite subsets of the H_i's. Partially order $L_{\{H_1, H_2, \ldots, H_k\}}$ by inclusion as the minimal element $\hat{0}$ is the identity subgroup of G. Such a lattice is locally finite with the order function

$$v(x, y) = \frac{|y|}{|x|}.$$

Thus, the Rédei zeta function associated to $L_{\{H_1, H_2, \ldots, H_n\}}$ is

$$\rho(s, H_1, H_2, \ldots, H_k) := \rho(s; L_{\{H_1, H_2, \ldots, H_n\}}) = \sum_{\hat{0} \preceq H} \mu(\hat{0}, H) \frac{1}{|H|^s},$$

where H runs through all elements of $L_{\{H_1, H_2, \ldots, H_k\}}$. It was proved in [10, Theorem 10] that

$$D_G(n, H_1, H_2, \ldots, H_k) = |G|^n \cdot \rho(n, H_1, H_2, \ldots, H_k),$$

from which we can derive that

$$0 \leqslant \rho(n, H_1, H_2, \ldots, H_k) \leqslant 1 \tag{1}$$

since $D_G(n, H_1, H_2, \ldots, H_k) \leqslant |G|^n$. This result was first proved by Rédei and is known as Rédei's Trägheitsatz [16,17].

Combining Rédei's result with Theorems 2 and 3, we conclude that

$$\max\left\{0, 1-\sum_{j=1}^{k}\frac{1}{|H_j|^n}\right\} \leqslant \rho(n, H_1, H_2, \ldots, H_k) \leqslant \min\left\{1, \frac{\displaystyle\sum_{j_1,j_2=1}^{k}\frac{1}{|H_{j_1}\vee H_{j_2}|^n}}{\left(\displaystyle\sum_{j=1}^{k}\frac{1}{|H_j|^n}\right)^2}-1\right\}.$$

The above inequality provides better upper and lower bounds than (1) for $\rho(n, H_1, H_2, \ldots, H_k)$ in many cases. For example, for all primes $p\leqslant x$, consider the abelian group G and its subgroups $\{H_p,\ p\leqslant x\}$ which are defined as follows:

$$G=\prod_{p\leqslant x}\mathbb{Z}/p\mathbb{Z} \quad H_p\cong\mathbb{Z}/p\mathbb{Z} \quad \text{for all } p\leqslant x.$$

In the case $n=1$, by Theorem 2 and Mertens' theorem, we obtain

$$\rho(1, H_p,\ p\leqslant x)\leqslant\frac{1}{\log\log x}+O\left(\frac{1}{(\log\log x)^2}\right).$$

In the case $n\geqslant 2$, by Theorem 3, we have

$$\rho(n, H_p,\ p\leqslant x)\geqslant 1-\sum_{p\leqslant x}\frac{1}{p^n}.$$

As

$$\sum_{p\leqslant x}\frac{1}{p^n}\to 0 \quad \text{as } n\to\infty,$$

we conclude that

$$\rho(n, H_p,\ p\leqslant x)\to 1 \quad \text{as } n\to\infty.$$

We can also apply Theorems 2 and 3 to vector spaces over a finite field. Let G' be a d-dimensional vector space over a finite field $\mathbb{F}_q$. Let $\{H_1', H_2', \ldots, H_k'\}$ be the set of all one-dimensional subspaces of G'. Thus, k is the number of one-dimensional subspaces of G' and is equal to $(q^d-1)/(q-1)$. Let $L_{\{H_1', H_2', \ldots, H_k'\}}$ be the lattice spanned by $\{H_1', H_2', \ldots, H_k'\}$. For $H'\in L_{\{H_1', H_2', \ldots, H_k'\}}$, the absolute value of the Möbius function $\mu(\hat{0}, H')$ increases rapidly as the dimension of H' increases. Thus, it is not easy to compute the value of the Rédei zeta function in this case. However, from Theorem 2, we have

$$\rho(n, H_1', H_2', \ldots, H_k')\leqslant\frac{(q-1)(q^n-1)}{q^d-1},$$

which is < 1 if $n \leqslant (d-1)$. In the case $n \geqslant d$, by Theorem 3, we have

$$\rho(n, H_1', H_2', \ldots, H_k') \geqslant 1 - \frac{(q^d - 1)}{q^n(q-1)} > 0.$$

Remark. As we can see from the above two examples, it seems that Corollary 1 and Proposition 1 are complementary. When Corollary 1 provides a non-trivial upper bound, Proposition 1 usually fails to give a meaningful lower bound. On the contrary, in the cases when Proposition 1 is valid, Corollary 1 is usually not useful. We will see the same situation happens again later in Theorems 4 and 5.

3. Vertex-colourings of graphs

We now consider a graph colouring problem. Let $X = (V, E)$ be a simple graph, where V is the vertex set of X and E the edge set. We denote by v and e the cardinalities of V and E, respectively. For $\lambda \in \mathbb{N}$, $\lambda \geqslant 1$, suppose we use λ colours to colour the vertex set V of X. A *λ-colouring* C can be viewed as a map from V to $\{1, 2, \ldots, \lambda\}$. We say C is *proper* if no two adjacent vertices have the same value(colour). Our goal is to count the number of proper colourings of X.

Let A be the set of all colourings of X and B the edge set of X. For $a = C_a \in A, b = e_b \in B$, we will say

$$a \sim b \quad \text{if the two vertices joined by } e_b \text{ have the same value in } C_a.$$

Thus,

$$\omega(a) = 0 \quad \text{if and only if} \quad C_a \text{ is a proper colouring of } X.$$

Notice that

$$|A| = \lambda^v \quad \text{and} \quad |B| = e.$$

For each $b = e_b \in B$, we have

$$\deg b = \lambda^{v-1},$$

since the values of the vertices joined by e_b are the same. It follows that

$$\sum_{b \in B} \deg b = e \cdot \lambda^{v-1}.$$

Let $b_1 = e_{b_1}, b_2 = e_{b_2} \in B$. If $b_1 = b_2 = b$, then

$$n(b_1, b_2) = \deg b = \lambda^{v-1}.$$

If $b_1 \neq b_2$, there are two possibilities:

(1) e_{b_1} and e_{b_2} share one vertex; thus those three vertices joined by e_{b_1} and e_{b_2} have the same values. In this case,

$$n(b_1, b_2) = \lambda^{v-2}.$$

(2) e_{b_1} and e_{b_2} do not share any vertex; thus the vertices joined by e_{b_1} have the same values and the values of the vertices joined by e_{b_2} are the same. Thus,

$$n(b_1, b_2) = \lambda^{v-2}.$$

Hence, we conclude that if $b_1 \neq b_2$,

$$n(b_1, b_2) = \lambda^{v-2}.$$

Notice also that

$$\#\{(b_1, b_2) \in B^2, b_1 \neq b_2\} = e^2 - e.$$

It follows that

$$\begin{aligned}\sum_{b_1, b_2 \in B} n(b_1, b_2) &= \sum_{b_1 \neq b_2} n(b_1, b_2) + \sum_{b \in B} \deg b \\ &= (e^2 - e) \cdot \lambda^{v-2} + e \cdot \lambda^{v-1}.\end{aligned}$$

Hence, by Corollary 1, we obtain

Theorem 4. *Let $X = (V, E)$ be a simple graph with the vertex set V and the edge set E. Suppose we use λ colours to colour the set V. We have*

$$\#\ \textit{of proper}\ \lambda\textit{-colourings of}\ X \leqslant \lambda^v \cdot \left\{\frac{\lambda - 1}{e}\right\},$$

where $v = |V|$ and $e = |E|$.

Notice that since

$$\#\ \text{of proper}\ \lambda\text{-colourings of}\ X \leqslant \lambda^v,$$

Theorem 4 provides a non-trivial upper bound only if

$$\frac{\lambda - 1}{e} \leqslant 1, \quad \text{i.e.,}\ \lambda \leqslant (e + 1).$$

In the case when $\lambda \geqslant e$, by Proposition 1, we have

Theorem 5. *Let $X = (V, E)$ be a simple graph with the vertex set V and the edge set E. Suppose we use λ colours to colour the set V. We have*

$$\#\ \textit{of proper}\ \lambda\textit{-colourings of}\ X \geqslant \lambda^v \cdot \left\{1 - \frac{e}{\lambda}\right\},$$

where $v = |V|$ and $e = |E|$.

A graph X' is called a *subgraph* of X if it can be obtained by contracting some edges of X (thus identifying two vertices that are joined by an erased edge). Consider the lattice L_X spanned by subgraphs of X. Partially order L_X as follows: we say $X_1 \preceq X_2$ if X_1 is a subgraph of X_2. Hence, the maximal element $\hat{1}$ of L_X is X.

For $\lambda \in \mathbb{N}$, suppose we use λ colours to colour the vertex set $V(X)$ of X. The number of proper λ-colourings of X can be expressed in terms of the Möbius functions of L_X. Let $P_X(\lambda)$ denote the number of proper colourings of X using λ colours. For each colouring C of X, there exists a unique maximal subgraph X' such that C is a proper colouring of X'. Thus, we have

$$\lambda^{V(X)} = \sum_{X' \preceq \hat{1}} P_{X'}(\lambda),$$

where X' runs through all elements of L_X. Applying the Möbius inversion formula, we obtain

$$P_X(\lambda) = \sum_{X' \preceq \hat{1}} \mu(X', \hat{1}) \lambda^{V(X')},$$

which is the *chromatic polynomial* of X. In general, it is difficult to estimate $P_X(\lambda)$ due to the fact that the Möbius function $\mu(X', \hat{1})$ is hard to compute. One of the advantages of both the Turán sieve and the simple sieve is that they eliminate the use of the Möbius function. Thus, they can provide estimates of $P_X(\lambda)$ without knowing $\mu(X', \hat{1})$. Indeed, the graph colouring problem can be viewed a special case of the character problem that we mentioned in Section 2 (see [1] and [15, Proposition 5.1.2] for explanations).

4. Latin squares

A *Latin square* of order n is an $n \times n$ matrix with entries from $\{1, 2, \ldots, n\}$ such that the entries in each row and the entries in each column are distinct. Let $L(n)$ be the number of Latin squares of order n. Since there are n^{n^2} ways of filling in the n^2 positions of the matrix with entries from $\{1, 2, \ldots, n\}$, we have

$$L(n) \leqslant n^{n^2}.$$

To obtain the number of Latin squares $L(n)$ is indeed a special case of the vertex-colourings of graphs. Let $X = K_n \times K_n$, the graph whose vertex set consists of the points of an $n \times n$ matrix and in which two vertices are adjacent if and only if they lie in the same row or column. Suppose we use n colours to colour the vertex set of X. In this case, the number of proper n-colourings of X is equal to the number of Latin squares of order n. Let V and E be the vertex set and the edge set of $X = K_n \times K_n$, respectively. Notice that

$$|V| = n^2 \quad \text{and} \quad |E| = n^2(n-1).$$

Applying Theorem 4, we can improve $L(n)$ to

$$L(n) \leqslant n^{n^2} \cdot \left\{ \frac{1}{n^2} \right\}.$$

The above upper bound can be improved to

$$L(n) \leqslant (n!)^n,$$

since each entire row is chosen from the set of permutations of $\{1, 2, \ldots, n\}$ and there are $n!$ permutations. Further improvement of an upper bound of $L(n)$ can be obtained by considering derangements of $\{1, 2, \ldots, n\}$.

A *derangement* of $\{1, 2, \ldots, n\}$ is a permutation of this set which leaves no point fixed. Let $d(n)$ be the number of derangements of $\{1, 2, \ldots, n\}$. Using the principle of inclusion-exclusion, we have [2, Theorem 5.1.3]

$$d(n) = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}.$$

One can show that this is the nearest integer to $n!/e$.

Consider a Latin square of order n. The first row of it is simply a permutation of $\{1, 2, \ldots, n\}$, and there are $n!$ choices for it. Given the first row, we may (by re-labeling) assume that it is $(1, 2, \ldots, n)$; then a legitimate second row is precisely a derangement of $\{1, 2, \ldots, n\}$. Similarly, all the rows after the first are derangements of the first one. Thus, we have

$$L(n) \leqslant (n!) \cdot d(n)^{n-1},$$

which is roughly $(n!)^n/e^{n-1}$. In the following, we apply the Turán sieve method and improve this upper bound to

$$L(n) \leqslant C(n!) \cdot \frac{d(n)^{n-1}}{n^2},$$

where C is a fixed constant.

Given an $n \times n$ matrix M, suppose the first row of it is a permutation, say $(1, 2, \ldots, n)$. We consider the $(n-1) \times n$ submatrix M_0 of M obtained by deleting the first row of M. For M to be a Latin square, all the rows of M_0 must be derangements of the first one. Let A be the collection of all such M_0's, i.e., A contains all $(n-1) \times n$ matrices such that each entire row is chosen from the set of derangements of $\{1, 2, \ldots, n\}$. Thus, we have

$$|A| = d(n)^{n-1}.$$

For $a = M_a \in A$, we denote by $(M_a)_{i,j}$ the (i, j)th entry of the matrix M_a, where $2 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant n$.

Let B be the set consisting all distinct pairs $\{(i, j), (i', j)\}$ (regardless of their order) where $2 \leqslant i, i' \leqslant n$, $i \neq i'$, and $1 \leqslant j \leqslant n$. There are $\binom{n-1}{2}$ choices for the set $\{i, i'\}$ and n choices for j. Thus,

$$|B| = \frac{n(n-1)(n-2)}{2}.$$

For a matrix $a = M_a \in A$, an element $b = \{(i_b, j_b), (i'_b, j_b)\} \in B$, we will say

$$a \sim b \quad \text{if} \quad (M_a)_{i_b, j_b} = (M_a)_{i'_b, j_b}.$$

Thus,

$$\omega(a) = 0 \quad \text{if and only if} \quad M_a \text{ forms a submatrix of a Latin square.}$$

Hence, we have

$$L(n) = (n!) \cdot \#\{a \in A,\ \omega(a) = 0\}.$$

Thus, to get an upper bound for $L(n)$, it suffices to obtain an upper bound for

$$\#\{a \in A,\ \omega(a) = 0\}.$$

Fix $b = \{(i_b, j_b), (i'_b, j_b)\} \in B$. Suppose $M_a = a \sim b$. There are $d(n)$ choices of the i_bth row of M_a. Fix the i_bth row and consider the i'_bth row of M_a. Suppose $(M_a)_{i_b, j_b} = (M_a)_{i'_b, j_b} = k$. Notice that $k \neq j_b$ since the i_bth row is a derangement. There are two possibilities for the i'_bth row:

(1) If $(M_a)_{i'_b,k} \neq j_b$, consider all entries of the i'_bth row except $(M_a)_{i'_b, j_b}$. View the entry $(M_a)_{i'_b,k}$ as $(M_a)_{i'_b, j_b}$. Thus, these $(n-1)$ entries of the i'_bth row form a derangement of the set $\{1, 2, \ldots, n\} \setminus \{k\}$ and there are $d(n-1)$ choices of them. Notice that since $(M_a)_{i'_b,k}$ is identified with $(M_a)_{i'_b, j_b}$, it follows that $(M_a)_{i'_b,k} \neq j_b$.

(2) If $(M_a)_{i'_b,k} = j_b$, consider all entries of the i'_bth row except $(M_a)_{i'_b, j_b}$ and $(M_a)_{i'_b,k}$. The remaining $(n-2)$ entries form a derangement of the set $\{1, 2, \ldots, n\} \setminus \{j_b, k\}$ and there are $d(n-2)$ choices of them.

Hence, we have totally $(d(n-1) + d(n-2))$ choices of the i'_bth row. Also, there are $d(n)$ choices of each remaining $(n-3)$ rows. Thus, we have

$$\deg b = d(n)^{n-2} \cdot (d(n-1) + d(n-2)).$$

It follows that

$$\sum_{b \in B} \deg b = d(n)^{n-2} \cdot (d(n-1) + d(n-2)) \cdot \frac{n(n-1)(n-2)}{2}.$$

Let $b_1 = \{(i_{b_1}, j_{b_1}), (i'_{b_1}, j_{b_1})\}$ and $b_2 = \{(i_{b_2}, j_{b_2}), (i'_{b_2}, j_{b_2})\}$ be two elements of B. Suppose

$$\left|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}\right| = r_1 \quad \text{and} \quad \left|\{j_{b_1}\} \cap \{j_{b_2}\}\right| = r_2,$$

where $0 \leqslant r_1 \leqslant 2$ and $0 \leqslant r_2 \leqslant 1$. We denote by $M(r_1, r_2)$ the number of pairs $(b_1, b_2) \in B^2$ such that $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = r_1$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = r_2$. There are six possibilities for the pair (r_1, r_2):

(1) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 2$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 1$.

In this case, $b_1 = b_2$. From the discussion of $\deg b$, we have

$$n(b_1, b_2) = d(n)^{n-2} \cdot (d(n-1) + d(n-2))$$

and

$$M(2, 1) = \frac{n(n-1)(n-2)}{2}.$$

(2) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 1$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 1$, say $i_{b_1} = i_{b_2}$.
There are $d(n)$ choices for the $i_{b_1}(= i_{b_2})$th row of M_a and $(d(n-1) + d(n-2))^2$ choices of the i'_{b_1}th and i'_{b_2}th rows. Also, there are $d(n)$ choices of each remaining $(n-4)$ rows. Thus,

$$n(b_1, b_2) = d(n)^{n-3} \cdot (d(n-1) + d(n-2))^2.$$

There are $\binom{n-1}{1}\binom{n-2}{1}\binom{n-3}{1}$ choices for the set $\{i_{b_1}(= i_{b_2}), i'_{b_1}, i'_{b_2}\}$ and n choices for $j_{b_1}(= j_{b_2})$. Thus,

$$M(1,1) = n(n-1)(n-2)(n-3).$$

(3) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 0$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 1$.
There are $(d(n))^2$ choices of the i_{b_1}th and i_{b_2}th rows and $(d(n-1)+d(n-2))^2$ choices of the i'_{b_1}th and i'_{b_2}th rows. Also, there are $d(n)$ choices of each remaining $(n-5)$ rows. Thus,

$$n(b_1, b_2) = d(n)^{n-3} \cdot (d(n-1) + d(n-2))^2.$$

There are $\binom{n-1}{2}\binom{n-3}{2}$ choices for the sets $\{i_{b_1}, i'_{b_1}\}$ and $\{i_{b_2}, i'_{b_2}\}$ and n choices for $j_{b_1}(= j_{b_2})$. Thus,

$$M(0,1) = \frac{n(n-1)(n-2)(n-3)(n-4)}{4}.$$

(4) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 2$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 0$, say $i_{b_1} = i_{b_2}$ and $i'_{b_1} = i'_{b_2}$.
There are $d(n)$ choices for the $i_{b_1}(= i_{b_2})$th row and $(d(n-2) + 2d(n-3) + d(n-4))$ choices for the $i'_{b_1}(= i'_{b_2})$th row. Also, there are $d(n)$ choices of each remaining $(n-3)$ rows. Thus,

$$n(b_1, b_2) = d(n)^{n-2} \cdot (d(n-2) + 2d(n-3) + d(n-4)).$$

There are $\binom{n-1}{2}$ choices for the set $\{i_{b_1}(= i_{b_2}), i'_{b_1} = (i'_{b_2})\}$ and $n(n-1)$ choices for j_{b_1} and j_{b_2} . Thus,

$$M(2,0) = \frac{n(n-1)^2(n-2)}{2}.$$

(5) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 1$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 0$, say $i_{b_1} = i_{b_2}$.
There are $d(n)$ choices of the $i_{b_1}(= i_{b_2})$th row and $(d(n-1) + d(n-2))^2$ choices of the i'_{b_1}th and i'_{b_2}th rows. Also, there are $d(n)$ choices of each remaining $(n-4)$ rows. Thus,

$$n(b_1, b_2) = d(n)^{n-3} \cdot (d(n-1) + d(n-2))^2.$$

Also, there are $\binom{n-1}{1}\binom{n-2}{1}\binom{n-3}{1}$ choices for the set $\{i_{b_1}(= i_{b_2}), i'_{b_1}, i'_{b_2}\}$ and $n(n-1)$ choices for j_{b_1} and j_{b_2}. Thus,

$$M(1,0) = n(n-1)^2(n-2)(n-3).$$

(6) $|\{i_{b_1}, i'_{b_1}\} \cap \{i_{b_2}, i'_{b_2}\}| = 0$ and $|\{j_{b_1}\} \cap \{j_{b_2}\}| = 0$.
There are $d(n)^2$ choices of the i_{b_1}th and i_{b_2}th rows and $(d(n-1)+d(n-2))^2$ choices of the i'_{b_1}th and i'_{b_2}th rows. Also, there are $d(n)$ choices of each remaining $(n-5)$ rows. Thus,

$$n(b_1, b_2) = d(n)^{n-3} \cdot (d(n-1) + d(n-2))^2.$$

Also, there are $\binom{n-1}{2}\binom{n-3}{2}$ choices for the sets $\{i_{b_1}, i'_{b_1}\}$ and $\{i_{b_2}, i'_{b_2}\}$ and $n(n-1)$ choices for j_{b_1} and j_{b_2}. Thus,

$$M(0,1) = \frac{n(n-1)^2(n-2)(n-3)(n-4)}{4}.$$

Combining all the above information together, we obtain

$$\sum_{b_1,b_2\in B} n(b_1, b_2) = d(n)^{n-3}(d(n-1)+d(n-2))^2 \cdot \frac{n^3(n-1)(n-2)(n-3)}{4} + d(n)^{n-2} \cdot \tilde{d}(n) \cdot \frac{n(n-1)(n-2)}{2},$$

where

$$\tilde{d}(n) = d(n-1) + nd(n-2) + 2(n-1)d(n-3) + (n-1)d(n-4).$$

Applying the fact that

$$d(n) = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!},$$

we obtain

$$d(n-1) + d(n-2) = \frac{d(n)}{n-1}.$$

From this, we can derive

$$\begin{aligned}\tilde{d}(n) &= (d(n-1)+d(n-2)) + (n-1)(d(n-2)+d(n-3)) \\ &\quad +(n-1)(d(n-3)+d(n-4)) \\ &= d(n) \cdot \frac{(2n-3)}{(n-1)(n-2)} + d(n-2) \cdot \frac{(n-1)}{(n-2)(n-3)}.\end{aligned}$$

Thus, we have

$$\sum_{b\in B} \deg b = d(n)^{n-1} \cdot \frac{n(n-2)}{2}$$

and

$$\sum_{b_1,b_2\in B} n(b_1, b_2) = d(n)^{n-1} \cdot \frac{n(n^4 - 5n^3 + 10n^2 - 10n + 6)}{4(n-1)} + d(n)^{n-2} \cdot d(n-2) \cdot \frac{n(n-1)^2}{2(n-3)}.$$

Hence, by Corollary 1, we obtain

$$\#\{a \in A,\ \omega(a) = 0\} \leqslant d(n)^{n-1} \cdot \left\{ \frac{2(n^2-3n+3)}{n(n-1)(n-2)^2} + \frac{2d(n-2)(n-1)^2}{d(n)n(n-2)^2(n-3)} \right\}.$$

It follows that

Theorem 6. *Let $L(n)$ be the number of Latin squares of order n and $d(n)$ the number of derangements of $\{1, 2, \ldots, n\}$. We have*

$$L(n) \leqslant (n!) \cdot d(n)^{n-1} \cdot \left\{ \frac{2(n^2-3n+3)}{n(n-1)(n-2)^2} + \frac{2d(n-2)(n-1)^2}{d(n)n(n-2)^2(n-3)} \right\}.$$

Thus, we obtain

$$L(n) \leqslant \frac{2(n!)^n}{n^2 e^{n-1}} \cdot (1 + O(1/n^2)).$$

This improves the upper bound of $L(n)$ given in [2].

Remark. Computing the asymptotic formula of $L(n)$ is a major open problem. The best partial result is due to Godsil and McKay [7] who obtained an asymptotic formula for the number of $k \times n$ Latin rectangles when $k = o(n^{6/7})$.

We can further improve Theorem 6. Given an $n \times n$ matrix M, for M to be a Latin square, the first row and the first column of M are permutations of $\{1, 2, \ldots, n\}$. Without loss of generality, we can assume that the first row is $(1, 2, \ldots, n)$ and the first column is $(1, 2, \ldots, n)^T$. If M is a Latin square, the second row of M is a derangement of $\{1, 2, \ldots, n\}$ with $(M)_{2,1} = 2$. Thus, there are $d(n)/(n-1)$ many choices for it. Similarly, there are $d(n)/(n-1)$ many choices for all the rows of M after the first one. Thus, we have

$$L(n) \leqslant n! \cdot (n-1)! \cdot \left(\frac{d(n)}{n-1} \right)^{n-1} = (n!) \cdot d(n)^{n-1} \cdot \frac{(n-1)!}{(n-1)^{n-1}}.$$

Applying the Stirling's formula

$$n! = n^n e^{-n} \sqrt{2\pi n}(1 + o(1)),$$

we have

$$L(n) \leqslant \frac{(n!)^n \sqrt{2\pi(n-1)}}{e^{2(n-1)}} \cdot (1 + o(1)).$$

Fix the first row and the first column of M. Consider the $(n-1) \times (n-1)$ submatrix M_1 of M obtained by deleting the first row and the first column of M. Applying an argument similar to the proof of Theorem 6, the Turán sieve method implies that

$$L(n) \leqslant \frac{C'(n!)^n \sqrt{n}}{e^{2(n-1)} n^2},$$

where C' is a fixed constant, which provides a better upper bound for $L(n)$ than the one given in Theorem 6.

5. Connected graphs

For $n \in \mathbb{N}$, let $\Pi(n)$ be the set of all partitions of $1, 2, \ldots, n$. For example, $\pi = \{1, 2, 3\}\{4, 5\}$ is an element of $\Pi(5)$ and we say $\{1, 2, 3\}$ and $\{4, 5\}$ are *blocks* of π. A partial order of $\Pi(n)$ is defined by refinements with $\hat{0} = \{1, 2, \ldots, n\}$ as the minimal element. For example, in $\Pi(5)$, we have $\{1, 2, 3, 4, 5\} \preceq \{1, 2, 3\}\{4, 5\} \preceq \{1, 2\}\{3\}\{4, 5\}$. Notice that in the lattice $\Pi(n)$, an elements lies right above $\hat{0}$ if it contains exactly two non-empty blocks.

Let G_n be the set of all graphs of n vertices. To each $G \in G_n$, we associate a partition $\pi_G \in \Pi(n)$ that represents the connected components of G. For example, if G is a graph of 5 vertices, suppose the vertices 1, 2, 3 are connected, so are 4 and 5, but neither 4 nor 5 connect to any of 1, 2, 3. Then we associate to G the partition $\pi_G = \{1, 2, 3\}\{4, 5\}$. Notice that G is connected if and only if $\pi_G = \{1, 2, \ldots, n\}$. Our goal is to count the number of graphs in G_n that are connected.

Let $A = G_n$ and B the set of all elements of $\Pi(n)$ that contain exactly two non-empty blocks. For $a = G_a \in A$, $b = \pi_b \in B$, we will say

$$a \sim b \quad \text{if} \quad \pi_b \preceq \pi_{G_a}.$$

Thus,

$$\omega(a) = 0 \quad \text{if and only if} \quad G_a \text{ is a connected graph.}$$

Since there are $\binom{n}{2}$ possible edges of a graph of n vertices, we have

$$|A| = 2^{\binom{n}{2}}.$$

For $b \in B$, if the two blocks of π_b contain k and $(n-k)$ elements, respectively, we have

$$\deg b = 2^{\binom{k}{2}} 2^{\binom{n-k}{2}},$$

where $1 \leqslant k \leqslant (n-1)$. Since there is no distinction between the two blocks of b, without loss of generality, we can assume that $1 \leqslant k \leqslant [\frac{n}{2}]$, where $[\frac{n}{2}]$ is the largest integer $\leqslant \frac{n}{2}$. Notice that for each fixed k, we have $\binom{n}{k}$ many choices for a block of k elements. It follows that

$$\sum_{b \in B} \deg b = 2^{\binom{n}{2}} \cdot \sum_{k=1}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)}.$$

Applying Proposition 1, we have

$$\#\text{ of connected graphs in } G_n \geqslant 2^{\binom{n}{2}} \cdot \left\{ 1 - \sum_{k=1}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)} \right\}.$$

For $1 < y < [\frac{n}{2}]$, we write

$$\sum_{k=1}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)} = \sum_{k<y} \binom{n}{k} 2^{k(k-n)} + \sum_{k \geqslant y}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)}.$$

A choice of y will be made later. Notice that $2^{k(k-n)}$ is a decreasing function of k for $1 \leqslant k \leqslant [\frac{n}{2}]$. Also, the maximum value of $\binom{n}{k}$ appears when $k = [\frac{n}{2}]$ and $\binom{n}{[\frac{n}{2}]} \leqslant 2^n$. Hence, we have

$$\begin{aligned}\sum_{k \geqslant y}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)} &\leqslant 2^{y(y-n)} \binom{n}{[\frac{n}{2}]} \sum_{k \geqslant y}^{[\frac{n}{2}]} 1 \\ &\leqslant 2^{y(y-n)} \cdot 2^n \cdot n \\ &= 2^{y^2-(y-1)n} \cdot n.\end{aligned}$$

By choosing $y = 3$, we obtain

$$\sum_{k \geqslant 3}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)} \ll 2^{-n}.$$

Also, we have

$$\sum_{k<3} \binom{n}{k} 2^{k(k-n)} \leqslant n \cdot 2^{1-n} + n^2 \cdot 2^{4-2n} \ll n \cdot 2^{-n}.$$

Hence, it follows that

$$\sum_{k=1}^{[\frac{n}{2}]} \binom{n}{k} 2^{k(k-n)} \ll n \cdot 2^{-n} + 2^{-n} \longrightarrow 0,$$

as $n \to \infty$. We recover a theorem of Gilbert [6].

Theorem 7 (*Gilbert*). *For $n \in \mathbb{N}$, let G_n be the set of all graphs of n vertices. We have*

$$\#\{G \in G_n,\ G \text{ is connected}\} \geqslant |G_n| \cdot \{1 - \varepsilon(n)\},$$

where $\varepsilon(n) \to 0$ as $n \to \infty$. Thus, almost all graphs are connected.

6. Generators of finite groups

We now consider a problem about generators of groups. Let G be a finite group. A subgroup $H \subseteq G$ is called *maximal* if $H \neq G$ and whenever there exists another subgroup K such that $H \subseteq K \subseteq G$, then either $K = H$ or $K = G$. Let G^r denote the set of all r-tuples $(g_1, g_2, \ldots, g_r)$ such that $g_i \in G$ for all $1 \leqslant i \leqslant r$. We are interested in counting the number of r-tuples that generate the full group G. We use the notation $\langle g_1, g_2, \ldots, g_r \rangle$ to denote the group generated by elements $g_1, g_2, \ldots, g_r$.

Let A be the set containing all r-tuples $(g_1, g_2, \ldots, g_r)$, i.e., $A = G^r$. Let B be the set of all maximal subgroups of G. For $a = (g_{a,1}, g_{a,2}, \ldots, g_{a,r}) \in A$, $b = H_b \in B$,

we will say

$$a \sim b \quad \text{if} \quad \langle g_{a,1}, g_{a,2}, \ldots, g_{a,r} \rangle \subseteq H_b.$$

Thus,

$$\omega(a) = 0 \quad \text{if and only if} \quad \langle g_{a,1}, g_{a,2}, \ldots, g_{a,r} \rangle = G.$$

Notice that

$$|A| = |G|^r.$$

Since H_b is maximal,

$$a \sim b \quad \text{if and only if} \quad g_{a,i} \in H_b \text{ for all } i.$$

Hence, we have

$$\deg b = |H_b|^r.$$

By Proposition 1, we have

$$\#\{(g_1, g_2, \ldots, g_r) \in G^r,\ \langle g_1, g_2, \ldots, g_r \rangle = G\} \geqslant |G|^r - \sum_{b \in B} |H_b|^r.$$

For example, a folklore conjecture of Netto [14] predicted that if A_n is the alternating group on n letters, then the probability p_n that two randomly chosen elements of A_n generate A_n tends to 1 as $n \to \infty$. The simple sieve in this context was used by Dixon [4] to prove this conjecture. It turns out that the maximal subgroups of A_n can be easily classified, and this in turn, leads to a simple proof of Netto's conjecture.

7. A spectral interpretation of the Turán sieve method

Let $M = M_{a,b}$ be the $|A| \times |B|$ incidence matrix of the bipartite graph $X = (A, B)$, i.e.,

$$M_{a,b} = \begin{cases} 1 & \text{if } a \sim b, \\ 0 & \text{otherwise.} \end{cases}$$

For $\zeta = e^{2\pi i/|A|}$, define the $|A| \times |B|$ matrix $\mathfrak{M}$ as follows:

$$\mathfrak{M}_{a,b} = \frac{1}{\sqrt{|A|}} \sum_{j=1}^{|A|} \zeta^{ja} M_{jb}.$$

Let $\mathfrak{M}_0$ be the $(|A| - 1) \times |B|$ matrix obtained by deleting the last row of $\mathfrak{M}$. Also, we denote by $\mathfrak{M}_0^* := \overline{\mathfrak{M}_0^T}$ the $|B| \times (|A| - 1)$ matrix which is the complex conjugate transpose of $\mathfrak{M}_0$.

Consider the $|B| \times |B|$ Hermitian matrix $\mathfrak{M}_0^*\mathfrak{M}_0$. For $b_1, b_2 \in B$, the (b_1, b_2)th entry of $\mathfrak{M}_0^*\mathfrak{M}_0$ is

$$\begin{aligned}(\mathfrak{M}_0^*\mathfrak{M}_0)_{b_1,b_2} &= \sum_{a=1}^{|A|-1} (\mathfrak{M}_0^*)_{b_1,a}(\mathfrak{M}_0)_{a,b_2} \\ &= \frac{1}{|A|} \sum_{a=1}^{|A|-1} \left(\sum_{k=1}^{|A|} \zeta^{-ka} M_{k,b_1} \right) \left(\sum_{j=1}^{|A|} \zeta^{ja} M_{j,b_2} \right) \\ &= \frac{1}{|A|} \sum_{j,k=1}^{|A|} M_{k,b_1} M_{j,b_2} \left(\sum_{a=1}^{|A|-1} \zeta^{a(j-k)} \right).\end{aligned}$$

Notice that

$$\sum_{a=1}^{|A|-1} \zeta^{a(j-k)} = \begin{cases} |A|-1 & \text{if } j = k, \\ -1 & \text{if } j \neq k. \end{cases}$$

We obtain

$$\begin{aligned}(\mathfrak{M}_0^*\mathfrak{M}_0)_{b_1,b_2} &= \frac{1}{|A|}(|A|-1) \sum_{j=1}^{|A|} M_{j,b_1} M_{j,b_2} - \frac{1}{|A|} \sum_{\substack{j,k=1 \\ j\neq k}}^{|A|} M_{k,b_1} M_{j,b_2} \\ &= \sum_{j=1}^{|A|} M_{j,b_1} M_{j,b_2} - \frac{1}{|A|} \sum_{j,k=1}^{|A|} M_{k,b_1} M_{j,b_2} \\ &= n(b_1, b_2) - \frac{\deg b_1 \cdot \deg b_2}{|A|}.\end{aligned}$$

Thus, we can rewrite Theorem 1 as

Proposition 2. *Define $\mathfrak{M}_0$ and $\mathfrak{M}_0^*$ as before. We have*

$$\sum_{a\in A} \left(\omega(a) - \frac{1}{|A|} \sum_{b\in B} \deg b \right)^2 = \sum_{b_1,b_2\in B} (\mathfrak{M}_0^*\mathfrak{M}_0)_{b_1,b_2}.$$

Let $v = (1, 1, \ldots, 1)^t$ be a $|B| \times 1$ vector. Let $(\cdot, \cdot)$ denote the standard dot product. For any $|B| \times |B|$ matrix T, we have

$$(Tv, v) = \sum_{b_1,b_2\in B} T_{b_1,b_2}.$$

Hence, from proposition 2, we have

$$\sum_{a\in A} \left(\omega(a) - \frac{1}{|A|} \sum_{b\in B} \deg b \right)^2 = (Tv, v),$$

where $T = \mathfrak{M}_0^*\mathfrak{M}_0$.

The expression $\frac{(Tv,v)}{(v,v)}$ is known as *Rayleigh–Ritz ratio*. Let $\lambda_{\max}(T)$ and $\lambda_{\min}(T)$ be the maximum and the minimum eigenvalues of the symmetric matrix T, respectively. A theorem of Rayleigh–Ritz [9, Theorem 4.2.2] states that for any non-zero vector v, we have

$$\max_{v\neq 0} \frac{(Tv,\, v)}{(v,\, v)} = \lambda_{\max}(T) \quad \text{and} \quad \min_{v\neq 0} \frac{(Tv,\, v)}{(v,\, v)} = \lambda_{\min}(T).$$

Combining the above information with Proposition 2, we get

Proposition 3. *Let $T = \mathfrak{M}_0^*\mathfrak{M}_0$. We have*

$$\lambda_{\min}(T)\cdot|B| \leqslant \sum_{a\in A}\left(\omega(a) - \frac{1}{|A|}\sum_{b\in B}\deg b\right)^2 \leqslant \lambda_{\max}(T)\cdot|B|.$$

We now recall the following facts about the eigenvalues of Hermitian matrices:
(1) The sets of eigenvalues of $\mathfrak{M}_0^*\mathfrak{M}_0$ and $\mathfrak{M}_0\mathfrak{M}_0^*$ are equal. In particular,

$$\lambda_{\max}(\mathfrak{M}_0^*\mathfrak{M}_0) = \lambda_{\max}(\mathfrak{M}_0\mathfrak{M}_0^*),$$

which implies a dual form of our sieve inequality.
(2) Suppose $Tv = \lambda_{\max}(T)v$, where $v = (x_1, x_2, \ldots, x_{|B|})^T$. Suppose

$$|x_{b_1}| = \max_{1\leqslant i\leqslant |B|} |x_i| \neq 0.$$

Then we have

$$\sum_{b_2=1}^{|B|} T_{b_1,b_2}\cdot x_{b_2} = \lambda_{\max}(T)x_{b_1}.$$

Thus,

$$|\lambda_{\max}(T)||x_{b_1}| \leqslant \sum_{b_2=1}^{|B|} |T_{b_1,b_2}||x_{b_2}| \leqslant |x_{b_1}| \sum_{b_2=1}^{|B|} |T_{b_1,b_2}|.$$

It follows that

$$|\lambda_{\max}(T)| \leqslant \sum_{b_2=1}^{|B|} |T_{b_1,b_2}|.$$

Thus, we conclude that

$$|\lambda_{\max}(T)| \leqslant \max_{b_1} \sum_{b_2=1}^{|B|} |T_{b_1,b_2}|.$$

Remark. Suppose we assign to each element $b \in B$ a *weight function* $X_b \in \mathbb{C}$. Let $\tilde{\omega}$ be a twisted ω-function with respect to X_b. More precisely,

$$\tilde{\omega}(a) = \sum_{\substack{b \in B \\ a \sim b}} X_b.$$

Then we have

$$\begin{aligned}
&\sum_{a \in A} \left| \tilde{\omega}(a) - \sum_{b \in B} X_b \cdot \frac{\deg b}{|A|} \right|^2 \\
&\quad = \sum_{b_1, b_2 \in B} X_{b_1} \overline{X}_{b_2} n(b_1, b_2) - \frac{1}{|A|} \left| \sum_{b \in B} X_b \cdot \deg b \right|^2 \\
&\quad = \sum_{b_1, b_2 \in B} \left\{ n(b_1, b_2) - \frac{1}{|A|} \deg b_1 \deg b_2 \right\} X_{b_1} \overline{X}_{b_2} \\
&\quad = \sum_{b_1, b_2 \in B} (\mathfrak{M}_0^* \mathfrak{M}_0)_{b_1, b_2} X_{b_1} \overline{X}_{b_2},
\end{aligned}$$

where $\mathfrak{M}_0$ and $\mathfrak{M}_0^*$ are defined as before. Let $\tilde{v} = (X_1, X_2, \ldots, X_{|B|})^T$. Notice that

$$\sum_{a \in A} \left| \tilde{\omega}(a) - \sum_{b \in B} X_b \cdot \frac{\deg b}{|A|} \right|^2 = (T\tilde{v}, \tilde{v}),$$

where $T = \mathfrak{M}_0^* \mathfrak{M}_0$. As in the proof of Proposition 3, we have

$$\sum_{a \in A} \left| \tilde{\omega}(a) - \sum_{b \in B} X_b \cdot \frac{\deg b}{|A|} \right|^2 \leqslant \lambda_{\max}(T) \cdot \sum_{b \in B} |X_b|^2.$$

This upper bound is indeed the best one that we can get since there exists X_b's such that the equality holds.

We believe that the combinatorial Turán sieve will have more applications in the future. The purpose of this paper is mainly to introduce it as a viable tool to deal with questions of this kind. For instance, is it possible to show that the probability P_G that two randomly selected elements of a simple group G generate G tends to 1 as $|G| \to \infty$? Apparently (see [4]), this has been resolved in the affirmative using the full classification of finite simple groups. In another direction, can the Turán sieve be used to count the number of Latin rectangles in ranges that have not been treated previously? We hope that this will be the case and relegate to future research the scope of the Turán sieve.

Acknowledgments

This paper was completed during the first author's stay at Queen's university in 2004. She would like to thank the Mathematics and Statistics Department for its hospitality. The authors also thank David Gregory for his careful reading of the paper.

References

[1] A. Brini, Some remarks on the critical problem, in: A. Barlotti (Ed.), Matroid Theory and its Applications: III ciclo 1980, Villa Monasterp, Varenna-Como, Napoli, 1982.
[2] P. Cameron, Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, Cambridge, 1994.
[3] T.Y. Chow, The combinatorics behind number-theoretic sieves, Adv. Math. 138 (1998) 293–305.
[4] J.D. Dixon, Probabilistic group theory, C. R. Math. Acad. Sci. Canada 24 (2002) 1–15.
[5] P. Erdös, J. Spencer, Probabilistic Methods in Combinatorics, Series of Monographs and Textbooks, vol. 17, Academic Press, New York, 1974.
[6] E.N. Gilbert, Random graphs, Ann. Math. Statist. 30 (1959) 1141–1144.
[7] C.D. Godsil, B.D. McKay, Asymptotic enumeration of Latin rectangles, J. Combin. Theory Ser. B 48 (1990) 19–44.
[8] G.H. Hardy, S. Ramanujan, The normal number of prime factors of a number n, Quart. J. Pure. Appl. Math. 48 (1917) 76–97.
[9] R.A. Horn, C.A. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, 1985.
[10] J.P.S. Kung, M.R. Murty, G.-C. Rota, On the Rédei zeta function, J. Number Theory 12 (1980) 421–436.
[11] Y.-R. Liu, M.R. Murty, The Turán sieve method and some of its applications, J. Ramanujan Math. Soc. 14 (1999) 21–35.
[12] L. Lovász, Combinatorial Problems and Exercises, North-Holland, Amsterdam, 1993.
[13] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, J. Reine Angew. Math. 78 (1874) 46–62.
[14] E. Netto, Substitutionentheorie and ihre Anwendungen auf die Algebra, Teubner, Leipzig, 1882 (English transl. 1892, second ed., Chelsea, New York, 1964).
[15] J.G. Oxley, Matroid Theory, Oxford University Press, New York, 1992.
[16] L. Rédei, Zetafunktionen in der algebra, Acta. Math. Acad. Sci. Hungar. 6 (1955) 5–25.
[17] L. Rédei, Die gruppentheoretischen Zetafunktionen und der Satz von Hajós, Acta. Math. Acad. Sci. Hungar. 6 (1955) 271–279.
[18] P. Turán, On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934) 274–276.
[19] R.J. Wilson, The Selberg sieve for a lattice, in: 'Combinatorial Theory and its Applications, Balatofüred, Hungary', Colloq. Math. Soc. János Bolyai 4 (1969) 1141–1149.