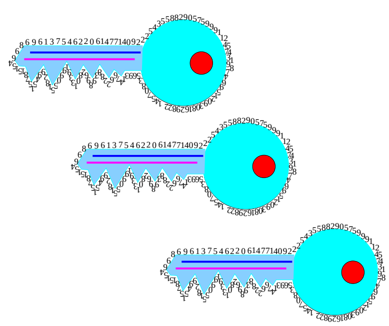
ALGEBRAIC COMBINATORICS

Aleksandar Jurišić

Laboratory for Cryptography and Computer Security
Faculty of Computer and Information Science

http://valjhun.fmf.uni-lj.si/~ajurisic



Introduction

We study an interplay between

algebra and **combinatorics**,

that is known under the name

algebraic combinatorics.

This is a discrete mathematics, where objects and structures contain some degree of regularity or symmetry.

More important areas of application of algebraic combinatorics are

- **coding theory** and error correction codes,
- **statistical design of experiments**, and
- (through finite geometries and finite fields) also **cryptography**.

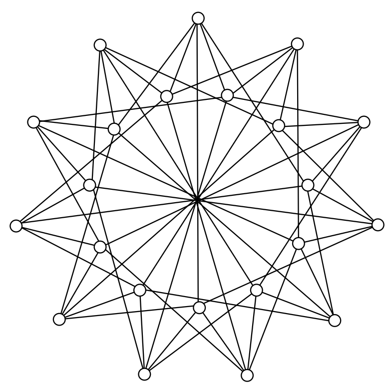
We investigate several interesting combinatorial structures. Our aim is a general introduction to algebraic combinatorics and illumination of some the important results in the past 10 years.

We will study as many topics as time permits that include:

- **algebraic graph theory and eigenvalue techniques** (specter of a graph and characteristic polynomial; equitable partitions: quotients and covers; strongly regular graphs and partial geometries, examples; distance-regular graphs, primitivity and classification, classical families),
- **associative schemes** (Bose-Mesner algebra, Krein conditions and absolute bounds; eigenmatrices and orthogonal relations, duality and formal duality, P-polynomial schemes, Q-polynomial schemes),
- **finite geometries and designs** (*projective and affine plane:* duality; *projective geometries:* spaces $\mathrm{PG}(d-1, q)$. *generalized quadrangles:* quadratic forms and a classification of isotropic spaces, classical constructions, small examples, spreads and regular points;

I. Constructions of some famous combinatorial objects

- Incidence structures
- Orthogonal Arrays (OA)
- Latin Squares (LS), MOLS
- Transversal Designs (TD)
- Hadamard matrices



Heawood's graph
the point/block incidence graph
of the unique 2-(11,5,2) design.

Incidence structures

t-(v, s, λ_t) design is

- a collection of s-subsets (**blocks**)
- of a set with v elements (**points**),
- where each t-subset of points is contained in exactly λ_t blocks.

If $\lambda_t = 1$, then the t-design is called **Steiner System** and is denoted by $S(t, s, v)$.

Let $i \in \mathbb{N}_0$, $i \leq t$ and let $\lambda_i(S)$ denotes the number of blocks containing a given i-set S. Then

(1) S is contained in $\lambda_i(S)$ blocks and each of them contains $\binom{s-i}{t-i}$ distinct t-sets with S as subset;

(2) the set S can be enlarged to t-set in $\binom{v-i}{t-i}$ ways and each of these t-set is contained in λ_t blocks:

$$\lambda_i(S)\binom{s-i}{t-i} = \lambda_t\binom{v-i}{t-i}$$

Therefore, $\lambda_i(S)$ is independent of S (so we can denote it simply by λ_i) and hence a t-design is also i-design, for $0 \leq i \leq t$.

For $\lambda_0 = b$ and $\lambda_1 = r$, when $t \geq 2$, we have

$$bs = rv \quad \text{and} \quad r(s-1) = \lambda_2(v-1)$$

or

$$r = \lambda_2 \frac{v-1}{s-1} \quad \text{and} \quad b = \lambda_2 \frac{v(v-1)}{s(s-1)}$$

A **partial linear space** is an incidence structure in which any two points are incident with at most one line. This implies that any two lines are incident with at most one point.

A **projective plane** is a partial linear space satisfying the following three conditions:

(1) Any two lines meet in a unique point.

(2) Any two points lie in a unique line.

(3) There are three pairwise noncolinear points (a *triangle*).

The **projective space** PG(d, n) (of dimension d and order q) is obtained from $[\mathrm{GF}(q)]^{d+1}$ by taking the quotient over linear spaces.

In particular, the projective space PG$(2, n)$ is the incidence structure with 1- and 2-dim. subspaces of $[\mathrm{GF}(q)]^3$ as **points** and **lines** (blocks), and **"being a subspace"** as an incidence relation.

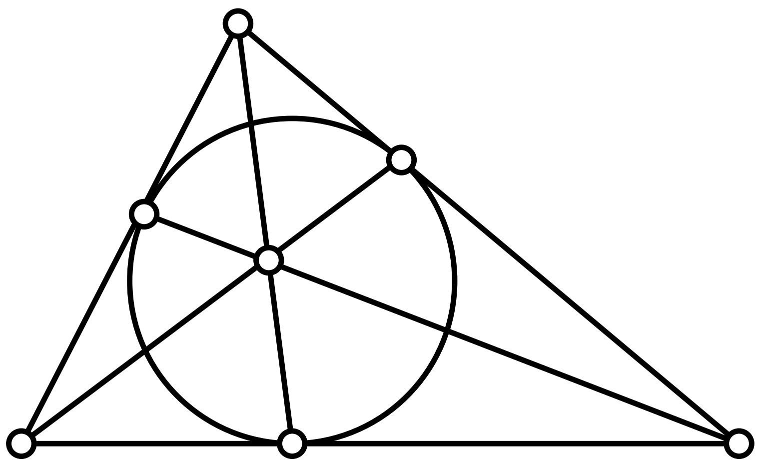
PG$(2, n)$ is a 2-$(q^2 + q + 1, q + 1, 1)$-design, i.e.,

- $v = q^2 + q + 1$ is the number of points (and lines b),
- each line contains $k = q + 1$ points
  (on each point we have $r = q + 1$ lines),
- each pair of points is on $\lambda = 1$ lines
  (each two lines intersect in a precisely one point),

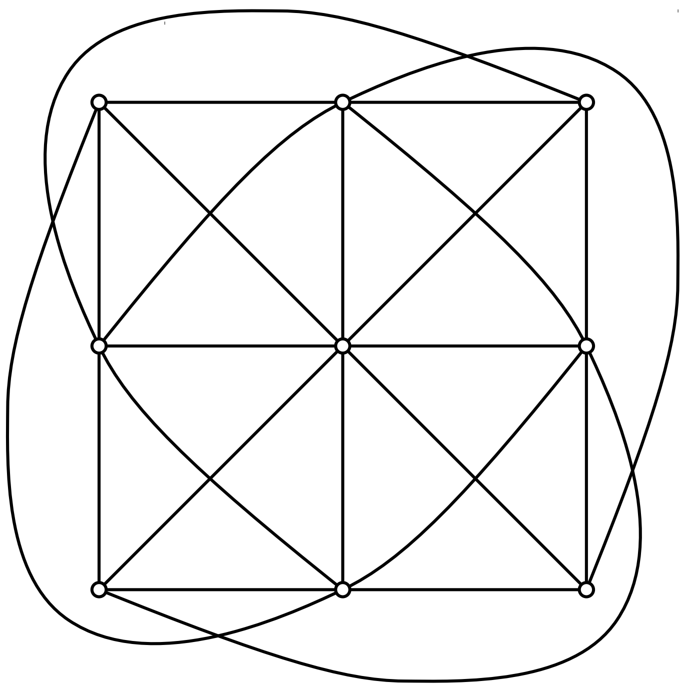
which is in turn a projective plane (see Assignment 1).

Examples:

1. The projective plane PG$(2,2)$ is also called the **Fano plane** (7 points and 7 lines).



2. PG$(2,3)$ can be obtained from 3×3 grid (or AG$(2,3)$).



3. PG$(2,4)$ is obtained from $\mathbb{Z}_{21}$:
points $= \mathbb{Z}_{21}$ and
lines $= \{S + x \mid x \in \mathbb{Z}_{21}\}$,
where S is a 5-element set $\{3,6,7,12,14\}$, i.e.,

$\{0,3,4,9,11\}$ $\{1,4,5,10,12\}$ $\{2,5,6,11,13\}$
$\{3,6,7,12,14\}$ $\{4,7,8,13,15\}$ $\{5,8,9,14,16\}$
$\{6,9,10,15,17\}$ $\{7,10,11,16,18\}$ $\{8,11,12,17,19\}$
$\{9,12,13,18,20\}$ $\{10,13,14,19,0\}$ $\{11,14,15,20,1\}$
$\{12,15,16,0,2\}$ $\{13,16,17,1,3\}$ $\{14,17,18,2,4\}$
$\{15,18,19,3,5\}$ $\{16,19,20,4,6\}$ $\{17,20,0,5,7\}$
$\{18,0,1,6,8\}$ $\{19,1,2,7,9\}$ $\{20,2,3,8,10\}$

Note: Similarly the Fano plane can be obtained from $\{0,1,3\}$ in $\mathbb{Z}_7$.