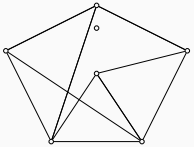
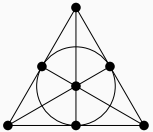
Radboud University

Introduction to Finite Affine Geometry, with an application to Cryptography

Vahid Jahandideh, Jan Schoone, Lejla Batina
Radboud University (The Netherlands)
ESCADA meeting
21 March 2025





Euclidean Geometry example

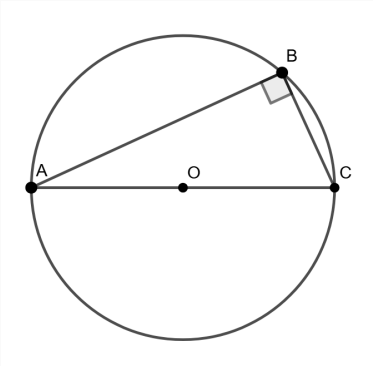


Figure: Thales' Theorem.

Euclidean Geometry

- (Mostly) planar geometry concerning points, lines and circles;
- Based on postulates:

(I): There is a line between any two points;
(II): Any line can be extended infinitely long;
(III): There is a circle for each center and radius;
(IV): All right angles are equal;
(V): (Parallel postulate) Given a line and a point not on the line, there is a line parallel to it through that point.[1]

[1] This is actually Playfair's axiom, which is equivalent.

- (Mostly) planar geometry concerning points and lines;
- Based on postulates:

(I): For any two distinct points, there is a line containing both;
(II): ~~Any line can be extended infinitely long;~~
(III): ~~There is a circle for each center and radius;~~
(IV): ~~All right angles are equal;~~
(V): (Playfair's axiom) Given a line ℓ and a point p not on ℓ, there exists a line ℓ' such that $\ell \cap \ell' = \emptyset$ and $p \in \ell'$.

Trivial examples

Definition (Finite Pre-Affine plane)

A finite pre-affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V).

Example

Let $P = \emptyset$ and $L = \emptyset$. Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Example

Let $P = \{x_1 \ldots, x_n\}$ and $L = \{P\}$ (the line contains all points in P). Then (P, L) satisfies (I) and (V) and thus is a finite pre-affine plane.

Non-example and non-trivial example

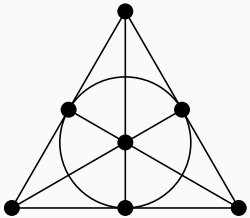
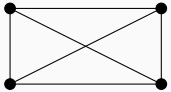


Figure: Fano plane.

The Fano plane has 7 points and 7 lines, where each line contains 3 points, each point lies on 3 lines and all lines intersect. It is actually an example of a projective plane.



This finite pre-affine plane has 4 points, 6 lines,and satisfies postulates (I) and (V).

Definition

A finite affine plane consists of a set of points P and a set of lines L such that it satisfies the postulates (I) and (V) and additionally that there is a set of four points in P such that no three of them are on the same line.

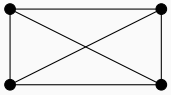


Figure: Affine plane of order 2.

Properties of finite affine planes

- All lines in a finite affine plane have the same number of points;
- All points in a finite affine plane are on the same number of lines;
- The number of points per line in a finite affine plane is called the order of the affine plane.
- Let $A = (P, L)$ be an affine plane of order k.
  - Every point is on $k + 1$ lines.
  - A has k^2 points.
  - For any line ℓ there are k lines that are parallel to ℓ.
  - A has $k^2 + k$ lines.

Construction (Coordinatization)

Let $\mathbb{F}$ be a field and consider $P := \mathbb{F} \times \mathbb{F}$. Furthermore, let $a, b, s \in \mathbb{F}$ and define $\ell_{s,b} := \{(x, y) \mid y = sx + b\}$ and $\ell_a := \{(a, y) \mid y \in \mathbb{F}\}$. Set $L = \{\ell_{s,b}\} \cup \{\ell_a\}_{a \in \mathbb{F}}$. Then (P, L) is an affine plane of order $\#\mathbb{F}$.

Example (Affine plane of order 2)

Let $P := \{(0,0), (0,1), (1,0), (1,1)\}$.

$\ell_0 := \{(0,0), (0,1)\}$; $\ell_1 := \{(1,0), (1,1)\}$;
$\ell_{0,0} := \{(0,0), (1,0)\}$; $\ell_{0,1} := \{(0,1), (1,1)\}$;
$\ell_{1,0} := \{(0,0), (1,1)\}$; $\ell_{1,1} := \{(0,1), (1,0)\}$.

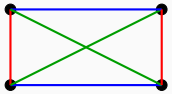


Figure: Affine plane of order 2.

Parallel lines

- Lines ℓ_a are parallel;
- Lines in $\{\ell_{s,b} \mid b \in \mathbb{F}\}$ are parallel for each slope s.
- We say that the lines ℓ_a have slope ∞.

Example

A finite affine plane of order 4. We take $\mathbb{F} := \mathbb{F}_2[X]/(X^2 + X + 1)$:

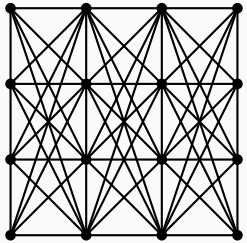


Figure: A finite affine plane of order 4.

Definition (Cluster)

Let X be a set of $n = s^2$ elements. A cluster C is a partition of X in s sets of equal size s.

Definition (MNO clusters)

Let C^1 and C^2 be two clusters of X, then they are maximally non-overlapping (MNO) if given any set $c \in C^1$ and any set $d \in C^2$, we have $|c \cap d| = 1$.

Definition (SMNO clusters)

Let $\mathfrak{C}$ be a collection of clusters. Then $\mathfrak{C}$ is called a collection of simultaneous MNO clusters if each pair of clusters in $\mathfrak{C}$ is MNO.

Maximum number of SMNO clusters

- Assume we have a finite affine plane $A = (P, L)$ of order s;
- Any set s of parallel lines is a cluster of P;
- Then any two clusters so obtained are MNO;
- Then we obtain $s + 1$ SMNO clusters.
- Known to be possible for all prime powers ($s = p^k$).

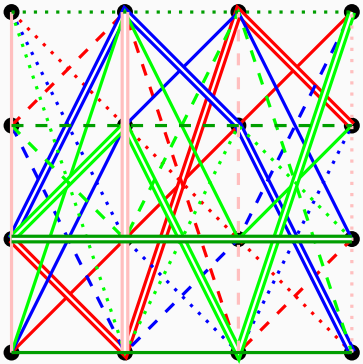


Figure: Example for $s = 4$.

To be continued...

- Masking is replaces gates like AND and XOR with gadgets;
- Gadgets are small circuits that operate on shared values and produce shared outputs;
- Gadgets typically require randomness;
- Use the clustering approach for making deterministic gadgets:
  - (uniform) AND-gadget;
  - Toffoli gadget;
  - higher-order gadgets to compute χ_5;
- Vahid will present about this two weeks from now!