# Number of points and lines in the projective plane over a finite field

Johannes Lieberherr

March 10, 2024

## 1 Projective space

Let $k$ be a field and $V$ a vector space over $k$.

**Definition 1** (Projective space)**.** *On $(V \times k) \setminus \{0\}$ we define the following equivalence relation ($v, w \in V \times k$):*

$$v \sim w : \iff \exists \lambda \in k^*, w = \lambda \cdot v$$

*The set of equivalence classes*

$$\mathrm{P}(V) := ((V \times k) \setminus \{0\}) \sim$$

*is called the projective space over $V$.*

Two points $[v], [w] \in \mathrm{P}(V)$ are identical if and only if $v, w \in (V \times k) \setminus \{0\}$ lie on the same line throug the origin in $V \times k$. Hence the projective space is the set of lines through the origin in $V \times k$.

**Definition 2** (Line in projective space)**.** *The line $g([v], [w])$ through two points $[v], [w] \in \mathrm{P}(V)$ is defined as the set of points*

$$g([v], [w]) := \{[v + t \cdot (w - v)] \mid t \in k\} \cup \{[w - v]\}$$

We have to show, that this definition is well-definied, i.e. that $g([v], [w]) = g([v'], [w'])$ holds if $[v] = [v']$ and $[w] = [w']$.

*Proof.* Let $\lambda, \mu \in k^*$ such that $v' = \lambda v$ and $w' = \mu w$.

If $\lambda = \mu$ we have directly $[v' + t(w' - v')] = [\lambda(v + t(w - v))] = [v + t(w - v)]$ and $[w' - v'] = [\lambda(w - v)] = [w - v]$.

If $\lambda \neq \mu$ the matter is a bit technical. We only show "$\subseteq$", the other direction is similar: let $[z] = [v + t(w - v)] \in g([v], [w])$. With $a := \frac{\lambda\mu}{\mu - \mu t + \lambda t}$ and $t' := \frac{\lambda t}{\mu - \mu t + \lambda t}$ we find for $\mu - \mu t + \lambda t \neq 0$ with a short calculation $az = v' + t'(w' - v')$ and hence $[z] \in g([v'], [w'])$. If $\mu - \mu t + \lambda = 0$ we have $[z] = [v + \frac{\mu}{\mu - \lambda}(w - v)] = [\frac{1}{\mu - \lambda}(\mu w - \lambda v)] = [w' - v'] \in g([v'], [w'])$ □

For every $[v] \in \mathrm{P}(V)$ there is a unique representation $[v] = [(\tilde{v}, a)] = [(\frac{1}{a}\tilde{v}, 1)]$ if $a \neq 0$ and $[v] = [(\tilde{v}, 0)]$ else. We write $(\frac{1}{a}\tilde{v} : 1)$ or $(\tilde{v} : 0)$ for this and call these the homogenous coordinates of $[v]$.

# 2 Projective plain over a finite field

**Definition 3** (Projective plain)**.** $\mathrm{P}(k^2)$ *is called the projective plane over* $k$*.*

In the following let $k = \mathbb{F}_q$ be a finite field with $q$ elements.

**Propostition 1.**

$$\mathrm{P}(\mathbb{F}_q^2) = \{(x : y : 1) \mid x, y \in \mathbb{F}_q\} \cup \{(x : 1 : 0) \mid x \in \mathbb{F}_q\} \cup \{(1 : 0 : 0)\}$$

*The set of lines in* $\mathrm{P}(\mathbb{F}_q^2)$ *consists of three types of lines:*

- *for every* $y, m \in \mathbb{F}_q$ *the line with y-axis intercept* $y$ *and gradient* $m$*:*

  $$g_{y,m} := g((0 : y : 1), (1 : y{+}m : 1)) = \{(0 : y : 1){+}t(1 : m : 1) \mid t \in \mathbb{F}_q\} \cup \{(1 : m : 0)\}$$

- *for every* $x \in \mathbb{F}_q$ *the vertical line with x-axis intercept* $x$*:*

  $$g_{x,\infty} := g((x : 0 : 1), (x : 1 : 1)) = \{(x : t : 1) \mid t \in \mathbb{F}_q\} \cup \{(0 : 1 : 0)\}$$

- *the line at infinity:*

  $$g_{\infty,\infty} := g((1 : 0 : 0), (0 : 1 : 0)) = \{(t : 1 : 0) \mid t \in \mathbb{F}_q\} \cup \{(1 : 0 : 0)\}$$

*The number of points is* $q^2 + q + 1$*.*
*The number of lines is* $q^2 + q + 1$*.*
*There are* $p + 1$ *lines containing a point.*
*There are* $q + 1$ *points contained in a line.*
*Two distinct points have exactly one line in common.*
*Two distinct lines have exactly one point in common.*

*Proof.* TODO □