Analytic Geometry

George Țurcaș

Maths & Comp. Sci., UBB Cluj-Napoca

November 1, 2021

Digression: The Diffie-Hellman key exchange protocol (Wikipedia)

- Diffie–Hellman key exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network.
- The simplest implementation of the protocol uses the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to p–1. Here is an example of the protocol, with non-secret values in blue, and secret values in red.

- Alice and Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
- Alice chooses a secret integer $a = 4$, then sends $A = g^a \bmod p$ to Bob.

$$A = 5^4 \pmod{23} = 4$$

- Bob chooses a secret integer $b = 3$, then sends $B = g^b \bmod p$ to Alice.
- Alice computes $s = B^a \pmod{p}$

$$s = 10^4 \pmod{23} = 18.$$

- Bob computes $s = A^b \pmod{p}$, this being

$$s = 4^3 \pmod{23} = 18.$$

Now both Alice and Bob share the secret key s.

$g^a \pmod{p}$

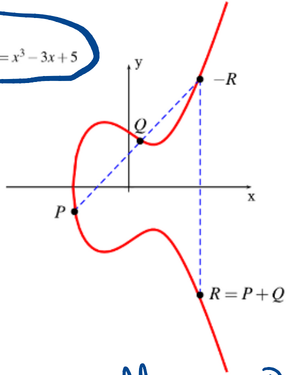
$g^b \pmod{p}$

p, g.

Use $p \approx 2048$ digits.

Get inspiration from analytic geometry

$E: y^2 = x^3 - 3x + 5$



$(x, y) \in \mathbb{R} \times \mathbb{R}$.

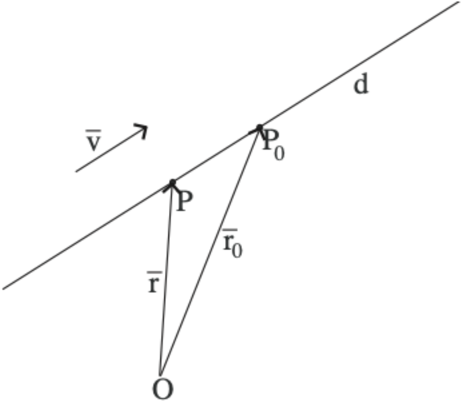
$(x, y) \in \mathbb{F}_{2^{100}} \times \mathbb{F}_{2^{100}}$.

Choose E public, $P(x_P, y_P) \in E$ public.

Alice: $a \cdot P$, Bob: $b \cdot P$

Alice & Bob can compute: $(a \cdot b) \cdot P$.

The vector language can be used to "describe" a line in a short form. Let d be a line passing through a fixed point P_0 and parallel to the fixed vector $\overline{v}$ (**director vector**). Fixing an arbitrary point O in the plane, one can characterize any point P by its *position vector*, i.e. the vector having the original point O and the terminal point P.



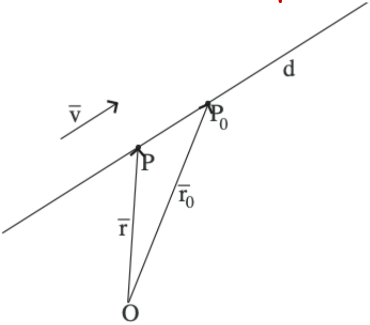
The point P belongs to the line d if and only if the vectors $\overline{P_0P}$ and $\overline{v}$ are linearly dependent. This means that there exists $t \in \mathbb{R}$, such that $\overline{P_0P} = t\overline{v}$. But $\overline{P_0P} = \overline{OP} - \overline{OP_0} = \overline{r} - \overline{r}_0$, hence $t\overline{v} = \overline{r} - \overline{r}_0$, and the *vector equation* of the line passing through P_0 and of director vector $\overline{v}$ is

$\overline{r} \overset{not}{:=} \overline{OP}$

$\overline{r_0} := \overline{OP_0}$

$$\boxed{\overline{r} = \overline{r_0} + t\overline{v}.} \qquad (1)$$

$\leftarrow$ Eq. of the line in vector form



A glimpse in the future. The line as an affine space

"Def": An affine space is a set A (points) together with $D(A)$ (vectors) that transform the points in A.

$D(A)$ - a vector space

$\dim D(A)$ is the dim. of the affine space A.

Example: $A :=$ the line d.

$D(A) = \{t \cdot \overline{v} \mid t \in \mathbb{R}\} = \langle \overline{v} \rangle$.

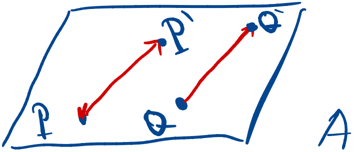
$\dim(D(A)) = 1$.

Another glimpse in the future. The plane as an affine space

Example: $A = \{$all points in a plane $\pi\}$.

Take $D(A) = \{ t_1 \cdot \overline{v}_1 + t_2 \cdot \overline{v}_2 \mid t_1, t_2 \in \mathbb{R} \}$

and $\overline{v}_1, \overline{v}_2$ are 2 linearly indep vectors in the plane π.

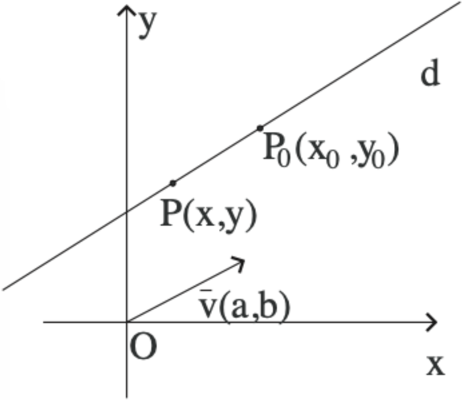


$\dim(D(A)) = 2$, so A is a 2-dim. affine space.

Parametric equation of a line

A line d can be determined by specifying a point $P_0(x_0, y_0)$ on the line and a nonzero vector $\overline{v}(a, b)$, parallel to the line (the direction of the line).

$\overline{v} \neq \overline{0}$



In the diagram above, we assume that $O(0,0)$ is the origin. Let us write the vector equation of the line d.

$$\overline{OP} = \overline{OP_0} + t \cdot \overline{v} \quad \text{for some } t \in \mathbb{R}.$$

Look at the components.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + t \cdot \begin{bmatrix} a \\ b \end{bmatrix}, \quad t \in \mathbb{R}$$

$$\therefore \begin{cases} x = x_0 + t \cdot a \\ y = y_0 + t \cdot b \end{cases}, \quad t \in \mathbb{R}.$$

Param. are not unique!

$$d: \begin{cases} x = x_0 + a\cdot(2t) \\ y = y_0 + b\cdot(2t) \end{cases}, \ t \in \mathbb{R}.$$

The line d in a 2-space, passing through the point $P_0(x_0, y_0)$ and parallel to the nonzero vector $\overline{v}(a, b)$ has the *parametric equations*

$$d : \begin{cases} x = x_0 + at \\ y = y_0 + bt \end{cases} \qquad t \in \mathbb{R}. \tag{2}$$

the parameter.

$\Leftarrow$) A point $P(x,y) \in d$ if and only if $\exists t \in \mathbb{R}$ such that $\begin{cases} x = x_0 + a\cdot t \\ y = y_0 + b\cdot t \end{cases}$.

The symmetric equation of a line

Starting with the parametric equations,

$$d : \begin{cases} x = x_0 + at \\ y = y_0 + bt \end{cases} \qquad t \in \mathbb{R}, \tag{3}$$

if $a, b \neq 0$ then, by expressing t from both equations, we see that

$$d : \frac{x - x_0}{a} = \frac{y - y_0}{b}. \tag{4}$$

This is called the "symmetric equation" of a line and $\overline{v}(a, b)$ is the director vector of the line d.

The symmetric equation of a line

Starting with the parametric equations,

$$d : \begin{cases} x = x_0 + at \\ y = y_0 + bt \end{cases} \qquad t \in \mathbb{R}, \tag{3}$$

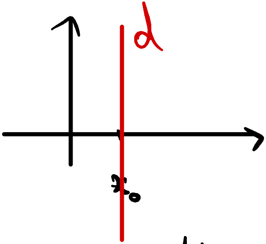
if $a, b \neq 0$ then, by expressing t from both equations, we see that

$$d : \frac{x - x_0}{a} = \frac{y - y_0}{b}. \tag{4}$$

This is called the "symmetric equation" of a line and $\overline{v}(a, b)$ is the director vector of the line d. Did you see something similar in high-school?

If $a = 0$, then

$$d : \begin{cases} x = x_0 \\ y = y_0 + t \cdot b \end{cases}, \ t \in \mathbb{R}.$$



We can choose as dir. vec. $\overline{v} = \overline{j}$.

If $b = 0$, then $d : \begin{cases} x = x_0 + t \cdot a \\ y = y_0 \end{cases}, t \in \mathbb{R}$

$d \parallel Ox$. We can choose $\overline{v} = 1 \cdot \overline{i}$.

A simple computation shows that (4) can be written in the form

$$Ax + By + C = 0, \qquad \text{with} \quad A^2 + B^2 \neq 0, \tag{5}$$

$B \neq 0.$

meaning that any line from the 2-space is characterized by a first degree equation. Suppose WLOG that $A \neq 0$. Then conversely, such of an equation represents a line, since the formula (5) is equivalent to $\dfrac{x + \frac{C}{A}}{-\frac{B}{A}} = \dfrac{y}{1}$ and this is the symmetric equation of the line passing through $P_0\left(-\dfrac{C}{A}, 0\right)$ and parallel to $\overline{v}\left(-\dfrac{B}{A}, 1\right)$. or $\overline{v}(-B, A)$.

$\perp$

(A, B)

The equation (5) is called *general equation* of the line.

Given points $P_1, P_2 \in d$, how do we write the general equation of d?

Reduced equation of lines

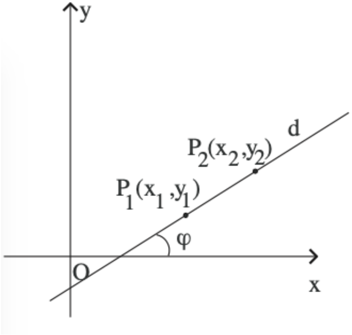
Consider a line given by its general equation $Ax + By + C = 0$, where A or B is nonzero. One may suppose that $B \neq 0$, so that the equation can be divided by B. One obtains

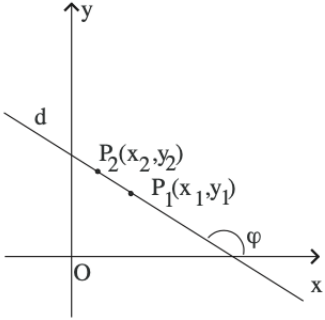
$$y = mx + n \tag{6}$$

which is said to be the *reduced equation* of the line.

Remark: If $B = 0$, then the general equation is $Ax + C = 0$, or $x = -\frac{C}{A}$, a line parallel to Oy. (In the same way, if $A = 0$, one obtains the equation of a line parallel to Ox).

Let d be a line of equation $y = mx + n$ in a Cartesian system of coordinates and suppose that the line is not parallel to Oy. Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be two different points on d and φ be the angle determined by d and Ox; $\varphi \in [0, \pi] \setminus \{\frac{\pi}{2}\}$.





The points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ belong to d, hence $\begin{cases} y_1 = mx_1 + n \\ y_2 = mx_2 + n \end{cases}$, and $x_2 \neq x_1$, since d is not parallel to Oy. Then,

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \tan\varphi. \tag{7}$$

The number $m = \tan\varphi$ is called the *angular coefficient* (or slope) of the line d.
It is immediate that the equation of the line passing through the point $P_0(x_0, y_0)$ and of the given angular coefficient m is

$$y - y_0 = m(x - x_0). \tag{8}$$

Line determined by two points

A line can be uniquely determined by two distinct points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ on the line. The line can be seen to be the line passing through the point $P_1(x_1, y_1)$ and having $\overline{P_1P_2}(x_2 - x_1, y_2 - y_1)$ as director vector, therefore its equation is

$$d : \frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}. \tag{9}$$

The equation (9) can be put in the form

$$\begin{vmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix} = 0. \tag{10}$$

Given three points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$, they are collinear if and only if

$$\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0.$$

Take home!

We saw the following ways in which one can describe a line in the plane:

- As a vector equation:
- As two parametric equations:

- Via a symmetric equation:
- A general equation:
- A reduced equation:

Intersection of two lines

Let $d_1 : a_1x + b_1y + c_1 = 0$ and $d_2 : a_2x + b_2y + c_2 = 0$ be two lines in $\mathcal{E}_2$. The solution of the system of equation

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ a_2x + b_2y + c_2 = 0 \end{cases}$$

will give the set of the intersection points of d_1 and d_2.

1) If $\dfrac{a_1}{a_2} \neq \dfrac{b_1}{b_2}$, the system has a unique solution (x_0, y_0) and the lines have a unique intersection point $P_0(x_0, y_0)$. They are *secant*.

2) If $\dfrac{a_1}{a_2} = \dfrac{b_1}{b_2} \neq \dfrac{c_1}{c_2}$, the system is not compatible, and the lines have no points in common. They are *parallel*.

3) If $\dfrac{a_1}{a_2} = \dfrac{b_1}{b_2} = \dfrac{c_1}{c_2}$, the system has infinitely many solutions, and the lines coincide. They are *identical*.

If $d_i : a_i x + b_i y + c_i = 0$, $i = \overline{1,3}$ are three lines in $\mathcal{E}_2$, then they are concurrent if and only if

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = 0. \tag{11}$$

The problem set for this week will be posted soon. Ideally you would think about it before the seminar on Friday.

Thank you very much for your attention!