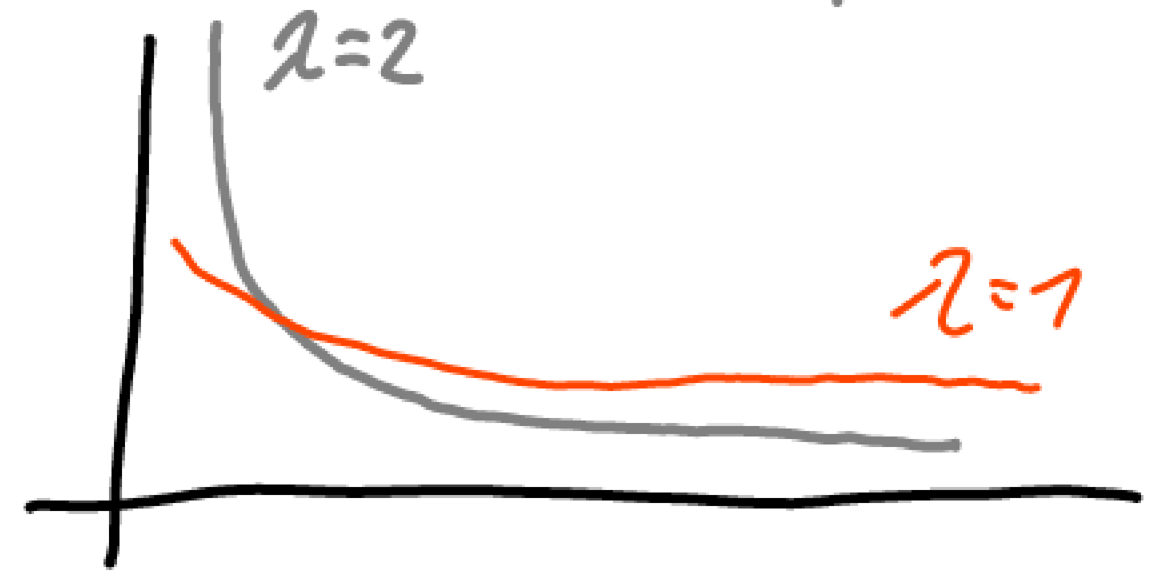
Introduction to blockchain technology.

① Exponential distribution

$X \sim Exp(\lambda)$, $f(x) = \lambda e^{-\lambda x}$

$E[X] = \frac{1}{\lambda}$, $Var[X] = \frac{1}{\lambda^2}$ $F(x) = 1 - e^{-\lambda x}$ for $\lambda > 0, x \geq 0$



Lemma 1

Exponential distribution is the only continuous distribution on $[0, \infty)$ that is memoryless:

$$X \sim Exp(\lambda) \iff (\forall_{t,s \geq 0})(Pr[X > t+s \mid X > s] = Pr[X > t])$$

it's like: I already was waiting, what's the impact on prob. that it will happen
in exp dist it doesn't matter how long i was waiting.

proof:

'→' $X \sim Exp(\lambda) \to \overbrace{(\forall_{t,s \geq 0})(Pr[X > t+s \mid X > s] = Pr[X > t])}^{MP}$

we know that • $Pr[X > t] = 1 - Pr[X \leq t] = 1 - (1 - e^{-\lambda t}) = e^{-\lambda t}$ for $t \geq 0$

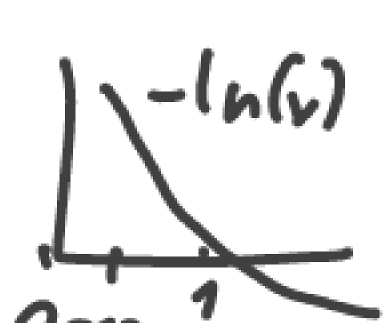
• $Pr[X > t+s \mid X > s] = \frac{Pr[X > t+s \wedge X > s]}{Pr[X > s]} = \frac{Pr[X > t+s]}{Pr[X > s]} = \frac{e^{-\lambda(t+s)}}{e^{-\lambda s}} = e^{-\lambda t}$ for $t, s \geq 0$

'←' $MP \to X \sim Exp(\lambda)$

• Let $G(x) = Pr[X > x]$, we show that $MP \to G(x) \overset{*}{=} G(1)^x \to$

$G(x) = e^{\ln(G(1)^x)} = e^{\lambda x}$

for $\lambda = -\ln G(1) > 0$

because  > 0

$\Rightarrow F(x) = 1 - e^{-\lambda x}$

and CDF uniquely determines distribution.

Now we just have to show ⊛.

⊛ proof:

$MP \rightarrow G(x) = G(1)^x$

① $(\forall t, s \geq 0)(G(t+s) = G(t)G(s))$

$$G(t+s) = Pr[X > t+s] =$$

$$= \underbrace{Pr[X > t+s \mid X > s]}_{MP} \cdot Pr[X > s] + \underbrace{Pr[X > t+s \mid X \leq s]}_{0} \cdot Pr[X \leq s]$$

$$= Pr[X > t] \cdot Pr[X > s] = G(t) \cdot G(s) \quad \triangle$$

---

② $MP \rightarrow$ ⊛ holds for $x \in \mathbb{Q}$

$\cdot\ m, n \in \mathbb{N}^+ : \quad G\left(\frac{m}{n}\right)^n = G(\underbrace{\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}}_{m})^n \overset{①}{=} \left(G\left(\frac{1}{n}\right)^m\right)^n =$

$$= \left(G\left(\frac{1}{n}\right)^n\right)^m \overset{①}{=} G(1)^m \rightarrow$$

$$\rightarrow G\left(\frac{m}{n}\right) = G(1)^{\frac{m}{n}} \quad \triangle$$

---

③ There exists sequences of rational numbers q_n and r_n such that $q_n \leq x \leq r_n$ for any $x \in \mathbb{R}$ and such that

$$\lim_{n \to \infty} q_n = x \quad \land \quad \lim_{n \to \infty} r_n = x$$

for example $q_n = \frac{\lfloor n \cdot x \rfloor}{n}$

$r_n = \frac{\lceil n \cdot x \rceil}{n}$

(4) Since $G(x) = \Pr[\mathcal{X} > x]$ is non-increasing in x,
we know that

$$
\begin{array}{ccccc}
q_n & \le & x & \le & r_n \\
G(q_n) & \ge & G(x) & \ge & G(r_n) \\
\| \text{②} & & & & \| \text{②} \\
G(1)^{q_n} & & & & G(1)^{r_n} \\
\downarrow n\to\infty & & & & \downarrow n\to\infty \\
G(1)^{x} & \ge & G(x) & \ge & G(1)^{x}
\end{array}
$$

$$\Downarrow$$

$$G(x) = G(1)^x \quad \text{for any } x \in \mathbb{R}^+$$

Lemma 2 Let $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$ be independent rand. var. such that $\mathcal{X}_i \sim Exp(\lambda_i)$.

Then (a) $\min(\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n) \sim Exp(\Lambda)$, $\Lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_n$

(b) $\Pr[\min(\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n) = \mathcal{X}_i] = \dfrac{\lambda_i}{\Lambda}$

We don't show proof we give example (nice).

Example

$T_K \sim Exp(\lambda_K)$ Miss Kasia

$T_m \sim Exp(\lambda_m)$ Miss Monika

$T_u \sim Exp(\lambda_u)$ Miss Ula

- first person, we think only about him.

a) how long a first person will wait: $\min(T_K, T_m, T_u) \sim Exp(\lambda_K + \lambda_m + \lambda_u)$

b) what is the chance that the first person will go to miss Ula $\Pr[\min(T_K, T_m, T_u) = T_u] = \dfrac{\lambda_u}{\lambda_K + \lambda_m + \lambda_u}$

II Poisson distribution

- $Y \sim Poiss(\mu)$, $\mu > 0$: $\underline{Pr[Y=j] = \frac{e^{-\mu}\mu^{j}}{j!} \text{ for } j=0,1,2,\dots}$

- $E[Y] = \mu$

- $Var[Y] = \mu$

<u>Lemma 3</u> Let $X_n \sim \overset{\text{Binomial distribution}}{Bin}(n, p_n)$ and $\lim\limits_{n\to\infty} n \cdot p_n = \mu > 0$

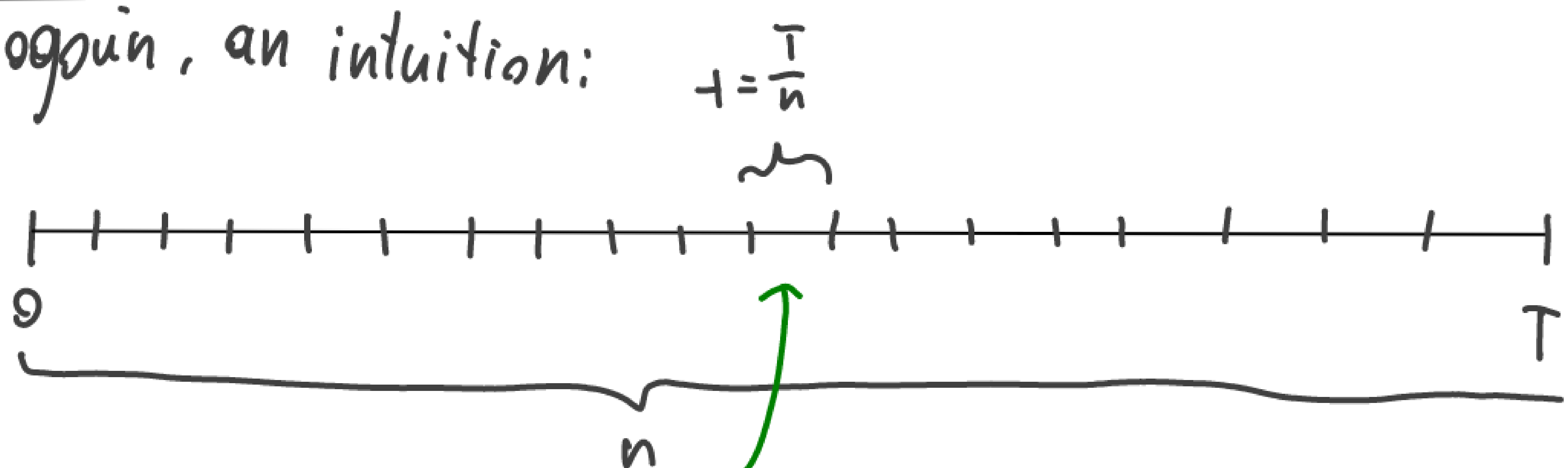
Then $(\forall_j \in \mathbb{N})$ we have $\lim\limits_{n\to\infty} Pr[X_n = j] = \frac{e^{-\mu}\mu^{j}}{j!}$

<u>proof</u> (ex)

⋮

---

once again, an intuition:



simple Bernoulli trial B_i

$Pr[B_i = 1] = t \cdot \lambda \longrightarrow \begin{cases} Pr[B_i = 0] = 1 - t\lambda \\ Pr[B_i \geq 2] = 0 \end{cases}$

- $X_{T,n} = B_1 + B_2 + \dots + B_n$, $X_{T,n} \sim Bin(n, \lambda t)$

- $\lim\limits_{n\to\infty} n \cdot \lambda t = \lim\limits_{n\to\infty} n \cdot \lambda \frac{T}{n} = \lambda \cdot T > 0 \longrightarrow n \to \infty : X_{T,n} \sim Poiss(\lambda t)$

III Stochastic processes

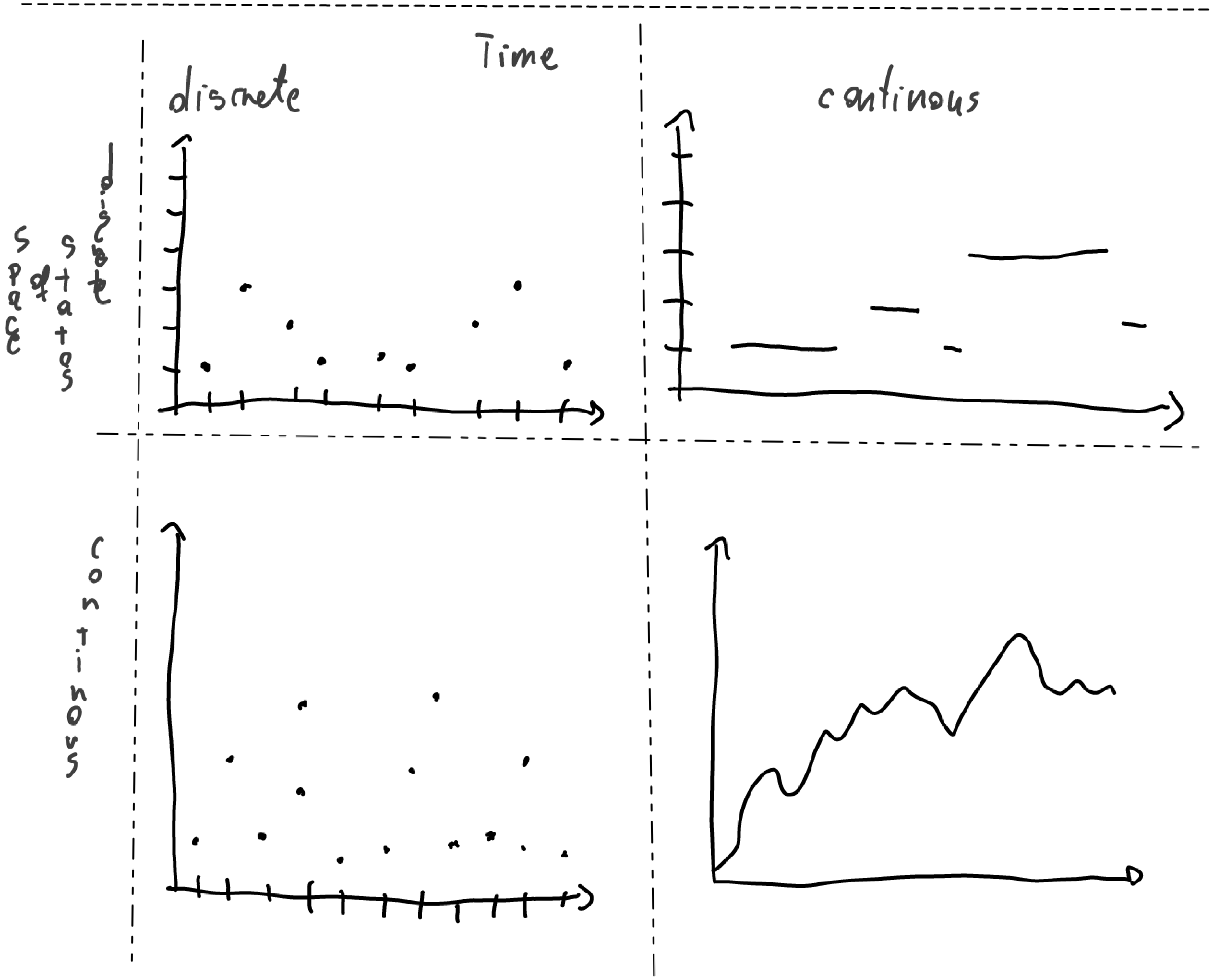
<u>Def</u> stochastic process is a family of random variables

$$\mathcal{X} = \{ X_t : t \in T \}$$

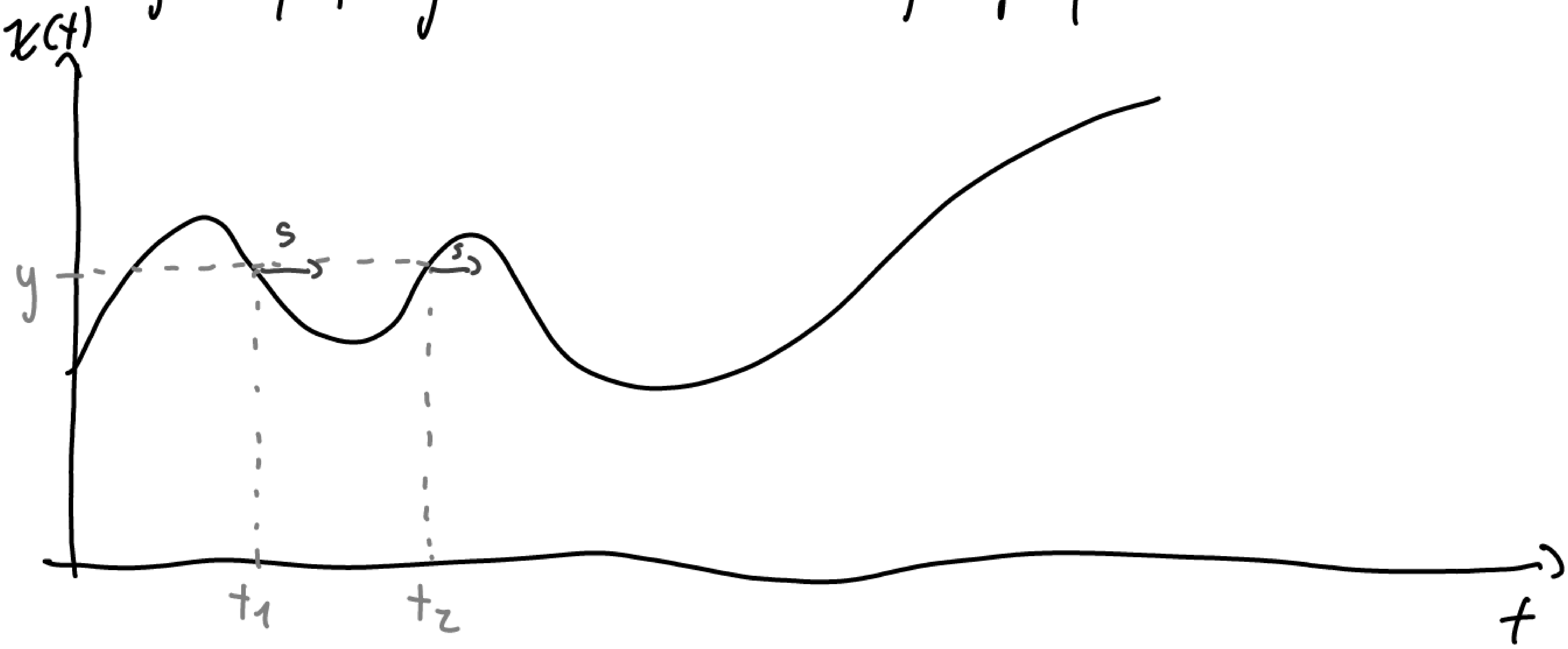
we try to model how random variable changes in time.

- Index t often represents time, e.g. $T = \mathbb{N}$ (SP with discrete time) X_t - discrete time
  $T = \mathbb{R}^+$ (SP with continues time) $X(t)$ - continues time

- Space of states for all variable X_i is usually common and can be discrete or continues.



Memoryless property and time-homogenity for stochastic processes



- MP in this context means that only current value matters for $\xrightarrow{s}$, so future prediction
- time-homogenity means that if $X(t_1) = X(t_2)$ "$(y = y)$" then $t_1 = t_2$, same moments in time.

$$Pr[X(t_1+s) = x \mid \underbrace{X(u),\ 0 \leq u \leq t_1}_{\text{we know all values before } t_1}] \underset{MP}{=} Pr[X(t_1+s) = x \mid X(t_1) = y]$$

$$\underset{\text{time-hom}}{=} Pr[X(t_2+s) = x \mid X(t_2) = y)$$