

Kontinuální učení

aneb jak doučit model na nových datech?

Michaela Mašková

Fakulta jaderná a fyzikálně inženýrská
České vysoké učení technické

May 4, 2021

Obsah

1. Úvod - úloha strojového učení
2. VAE
3. Detekce anomálií pomocí VAE
4. Kontinuální učení - Deep Generative Replay

Úloha strojového učení má několik částí:

- získání dat,
- rozdelení dat na trénovací, validační a testovací,
- implementace modelu,
- natrénování modelu,
- validace modelu, testování, úpravy,
- ... nasazení do produkce atd.

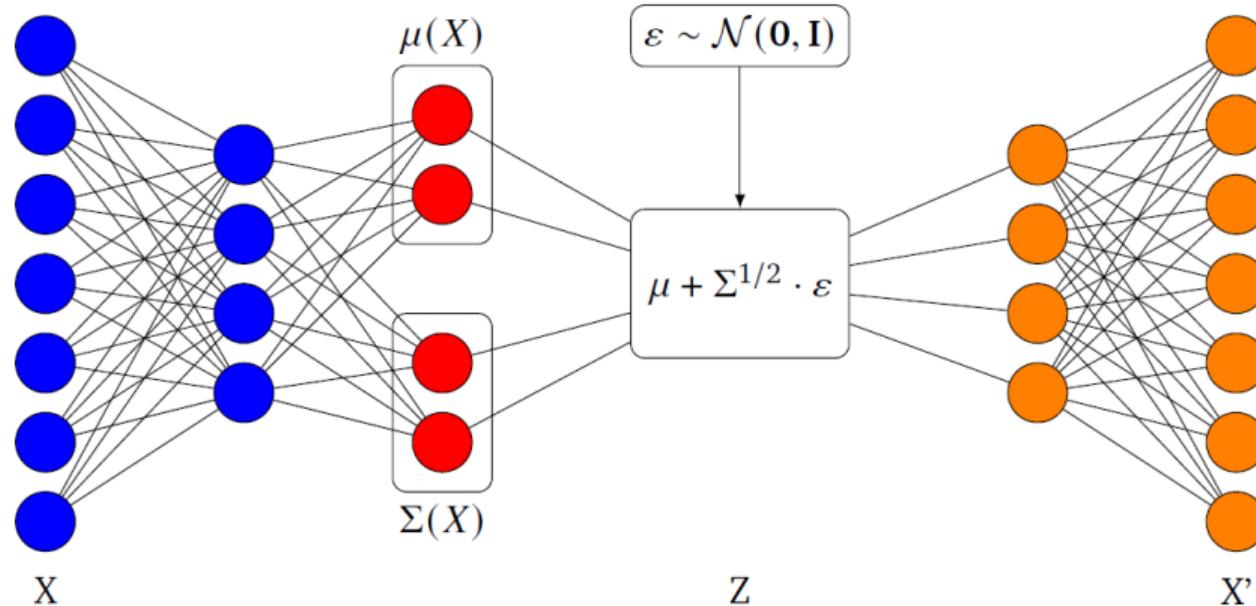
Co s natréovaným modelem?

Problém nastává ve chvíli, kdy chceme do modelu přidat nově získaná data. Jaké jsou naše možnosti?

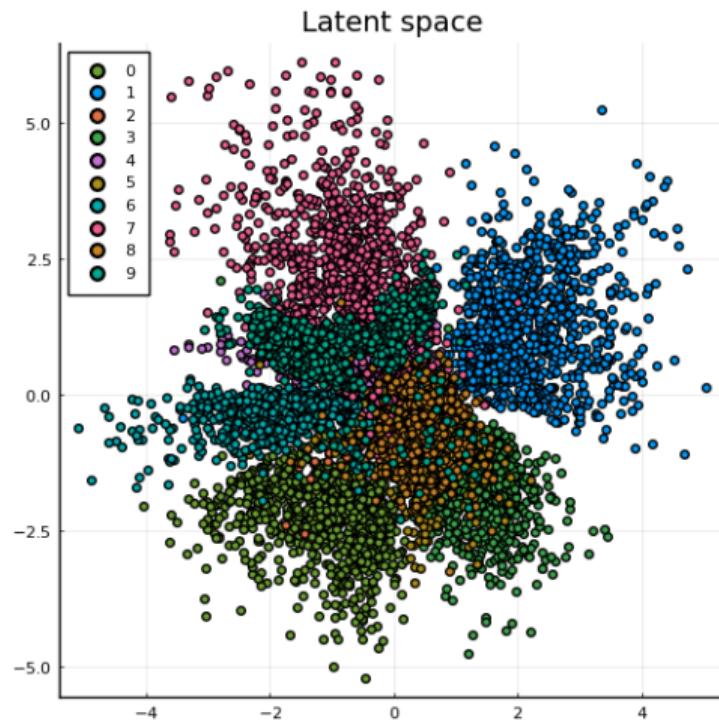
- přetrénovat celý model od začátku na všech datech,
- přetrénovat model pouze na nových datech,
- ?

Variační autoencoder

Ukážeme si příklad na variačním autoencoderu, který se umí naučit pravděpodobnostní distribuci trénovacích dat $p(X|Z)$.

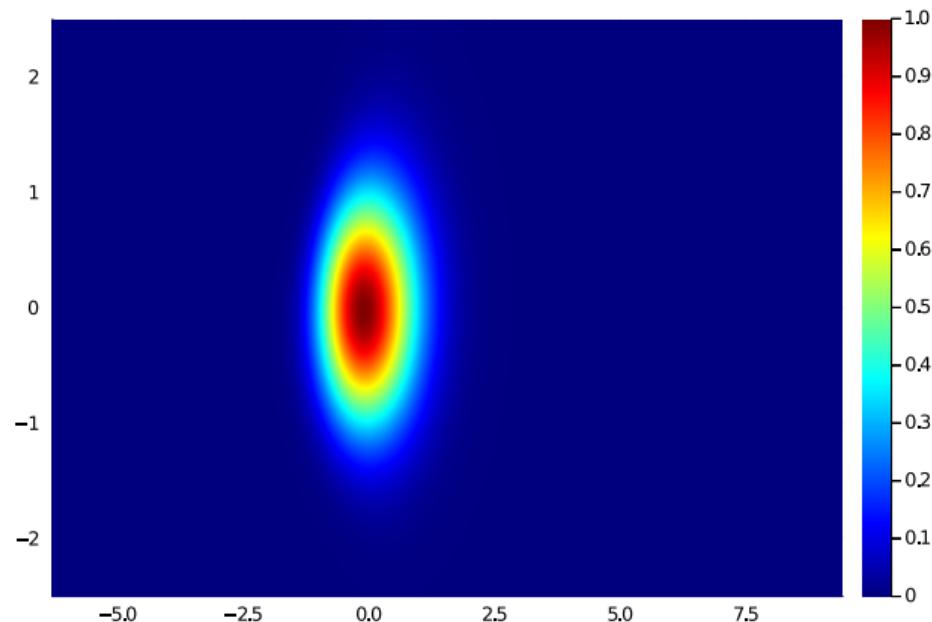


VAE - latentní prostor



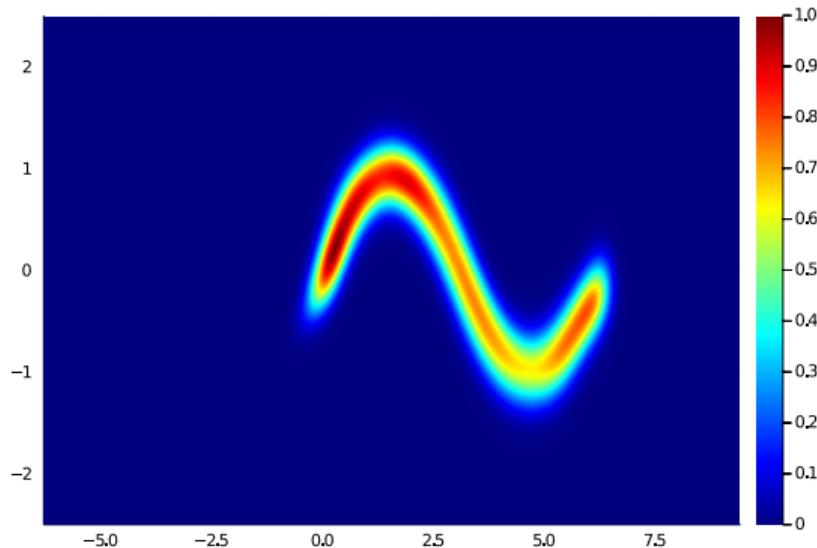
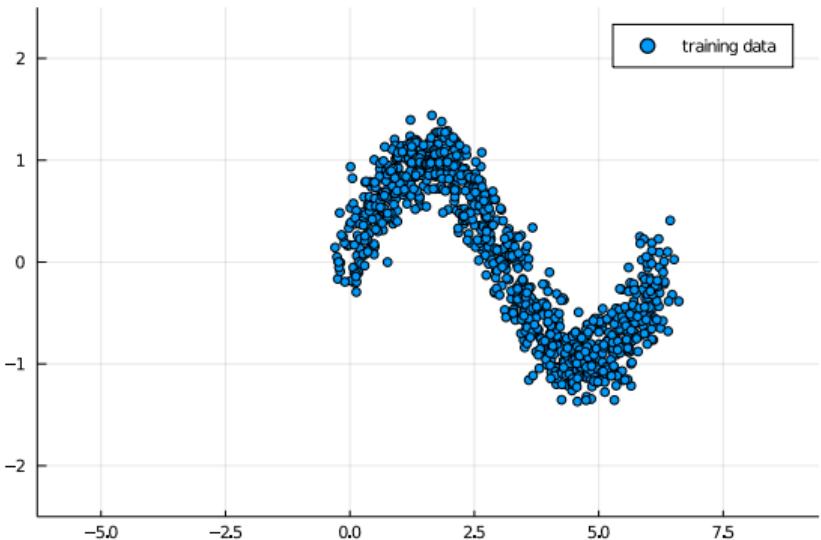
VAE - natrénovaná distribuce

Distribuce dat $p(X)$ před trénováním:



VAE - natrénovaná distribuce

První natrénovaný model:



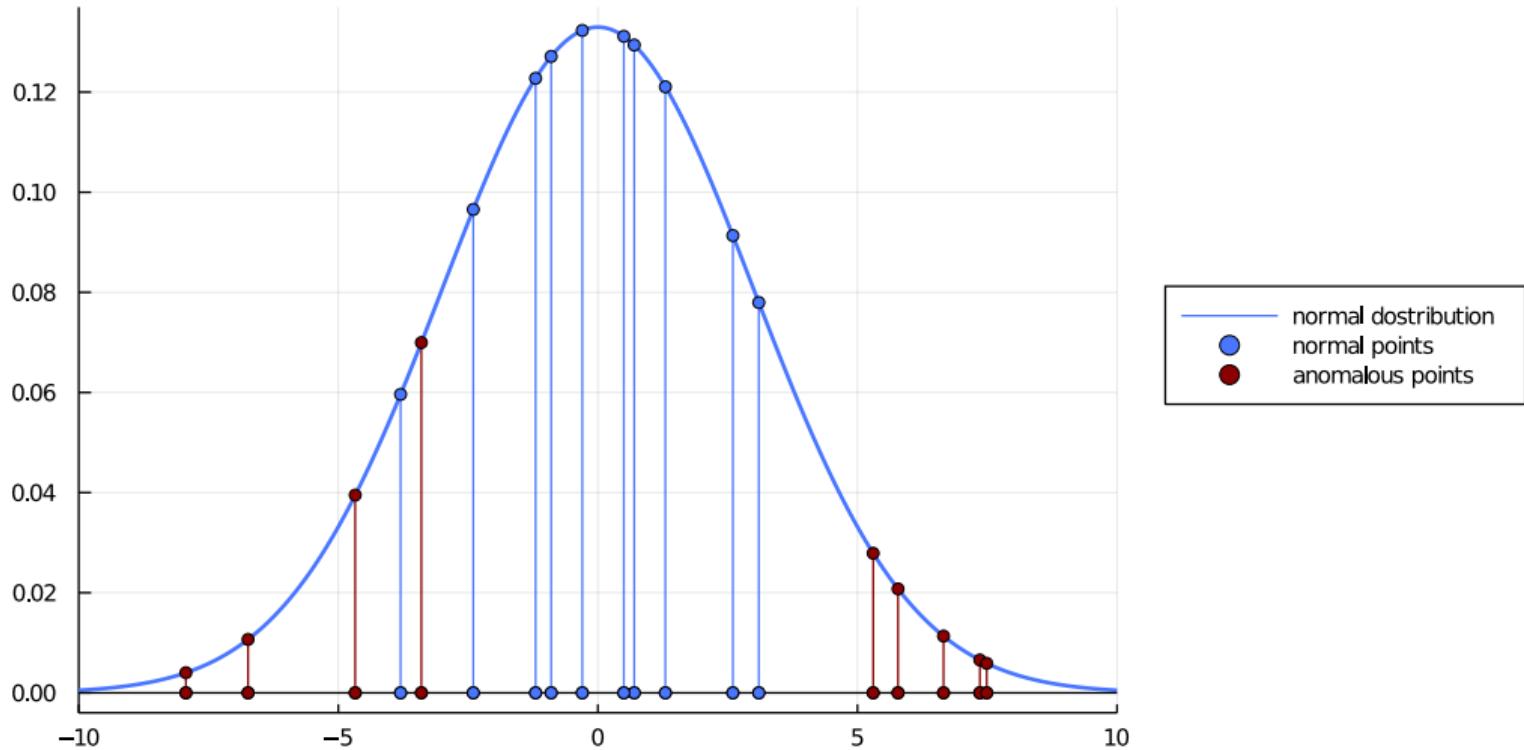
VAE & Detekce anomálií

Variační autoencoder lze použít na detekci anomálií.

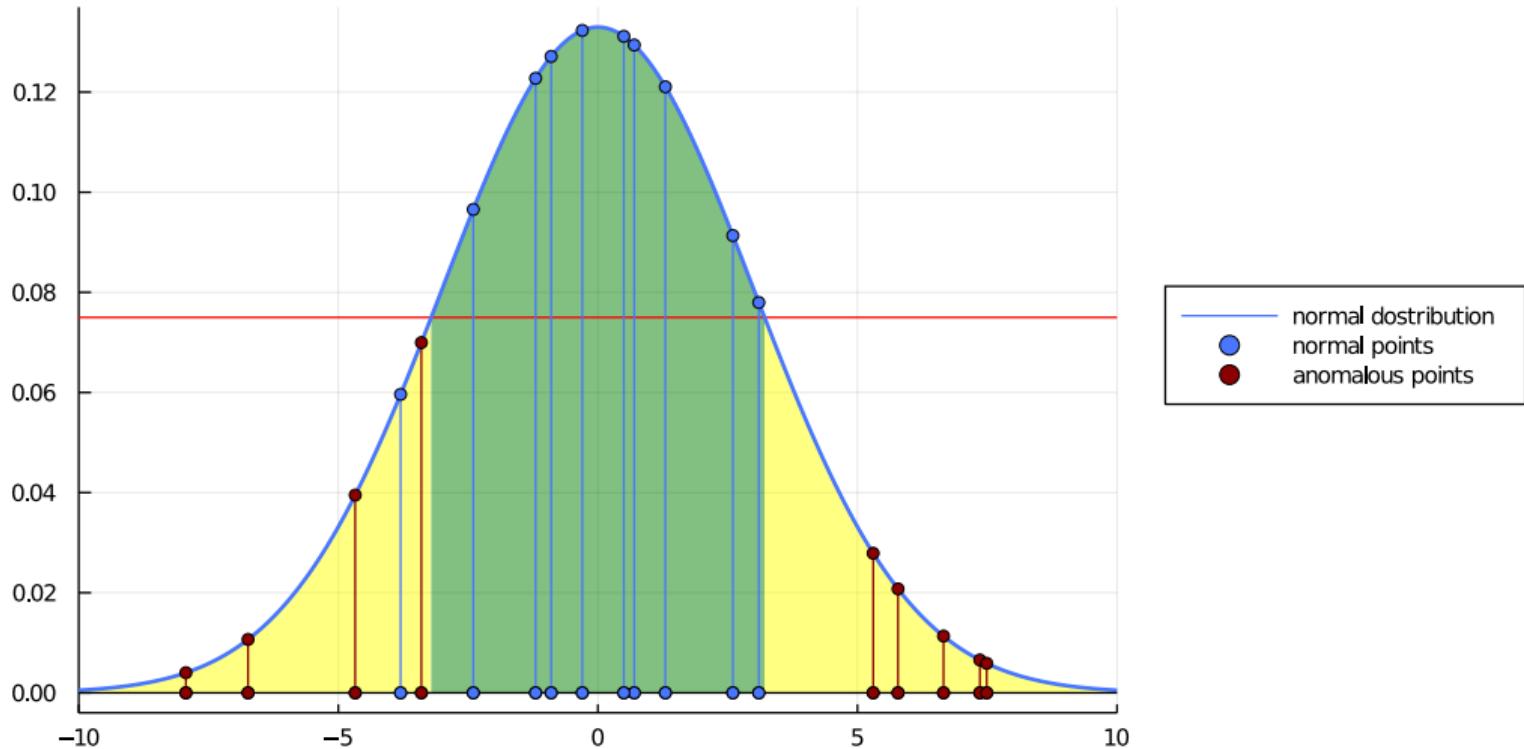
Myšlenka je jednoduchá:

- přepokládáme, že normální a anomální data pochází z jiných distribucí,
- naučíme model pouze na normálních datech,
- pravděpodobnost, že anomální data pochází z pravděpodobnostního rozdělení normálních dat by měla být nižší.

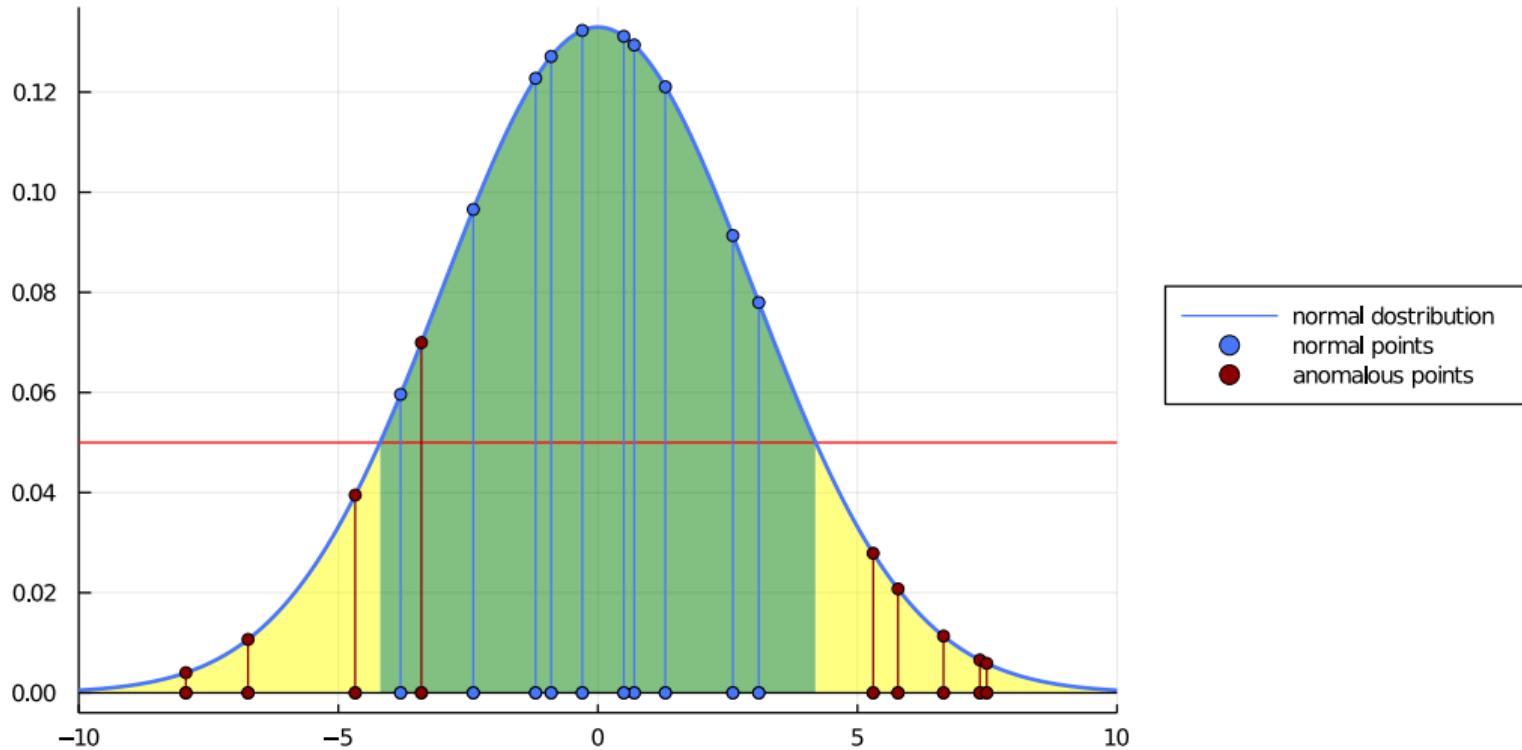
VAE & Detekce anomálií - ilustrační příklad



VAE & Detekce anomálií - ilustrační příklad



VAE & Detekce anomálií - ilustrační příklad



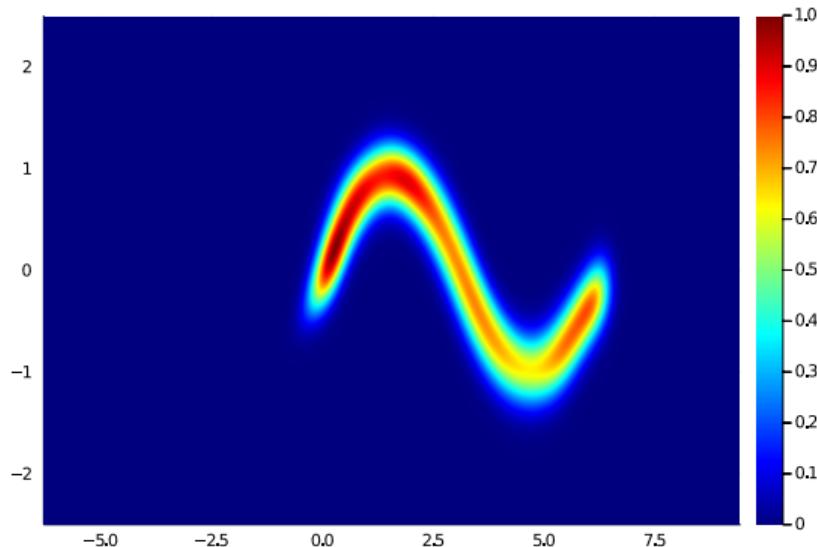
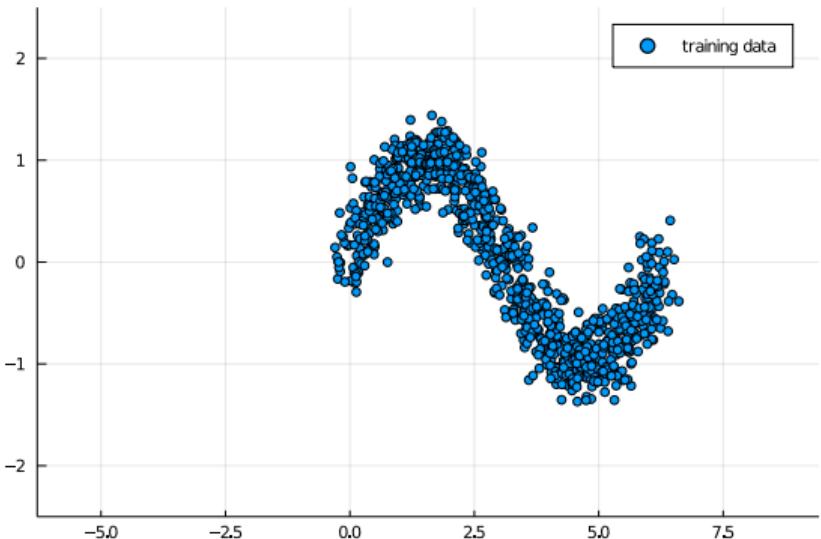
VAE & Detekce anomálií

!

Kontinuální učení je v detekci anomálií velmi důležité, jelikož s časem získáváme více dat a chceme zpřesňovat detekci.

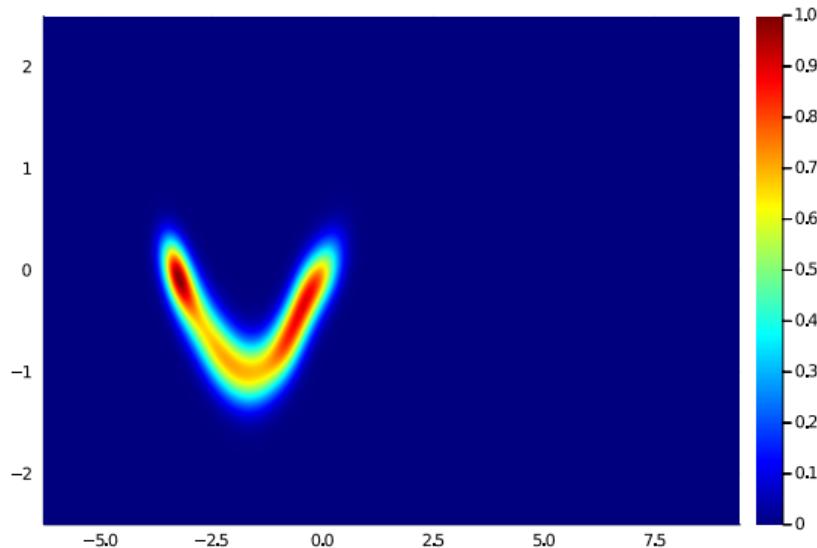
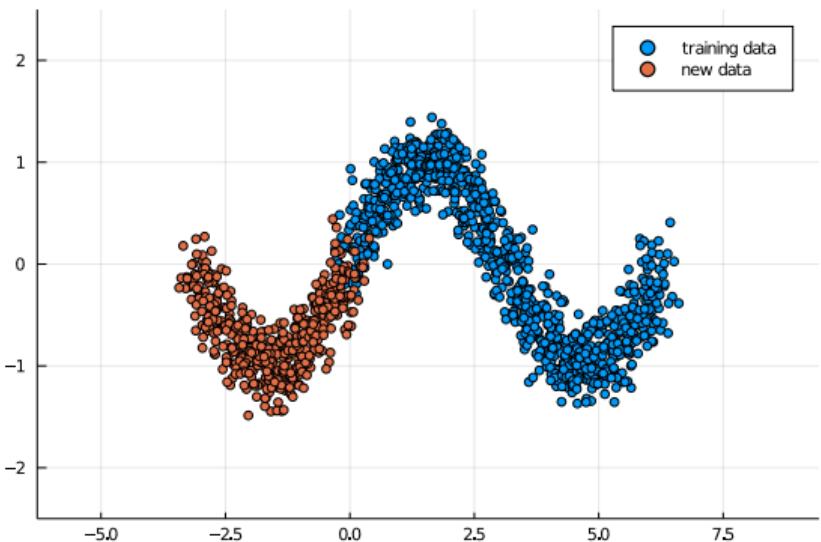
Zpět k příkladu...

První natrénovaný model:



Zpět k příkladu...

Model přetrénovaný pouze na nových datech:



Co s tím?

Naše hlavní otázka:

Jak doučit model, aniž bychom ho museli učit celý od začátku na všech datech, a přitom neztratili původní informaci z natrénovaného modelu?

Deep Generative Replay

Máme data $D = \{D_1, D_2, \dots\}$. Generative Replay má dvě složky:

- solver (například binární klasifikátor),
- generátor (GAN, VAE, AE, ...).

Postup:

- Solver i generátor jsou natrénovány na prvním subsetu dat D_1 ,
- nová data D_2 jsou namixována s daty generovanými generátorem D'_1 s nějakými mixovacími váhami $\mathbf{w} = (w_1, w_2)$, které určují poměr počtu nových a starých dat,
- solver i generátor jsou přetrénovány na novém datasetu.

VAE & Generative Replay

Pro kontinuální učení s VAE může být natrénovaný VAE **zároveň solver i generátor**.

Navíc nepotřebujeme ukládat původní normální data! Pro generaci zcela nového vektoru podobného původním datům stačí použít funkci

```
function generate_new( model :: VAE, n=100)
    z = rand(model.prior, n)
    rand(model.decoder, z)
end
```

Stačí nám tedy uložit pouze daný model (dekodér).

Algoritmus

Algoritmus kontinuálního učení pak vypadá následovně:

- natrénovat model na D_1
- pro všechny datasety D_i , $i = 2, \dots, n$:
 - uložit kopii natrénovaného modelu `generator = copy(model)`
 - zvolit váhy w_{prev}, w_{new} a tím příslušná n_{prev}, n_{new}
 - přetrénovat model tak, že v každé epoše
 - vytvořit nový batch `batch_old = generate_new(generator, n_prev)`
 - vybrat batch z nových dat `batch_new` o velikosti n_{new}
 - update modelu `model` na batchi `cat(batch_old, batch_new)`

Rozhodovací úlohy

V detekci anomálií s kontinuálním učením se pak řeší dvě hlavní rozhodovací úlohy

- volba vah w_{prev}, w_{new} ,
- optimalizace hraniční pravděpodobnosti (threshold).

Rozhodovací úlohy

Možností, jak váhy volit, je mnoho, měli bychom se řídit podle důležitosti nových dat vůči starým:

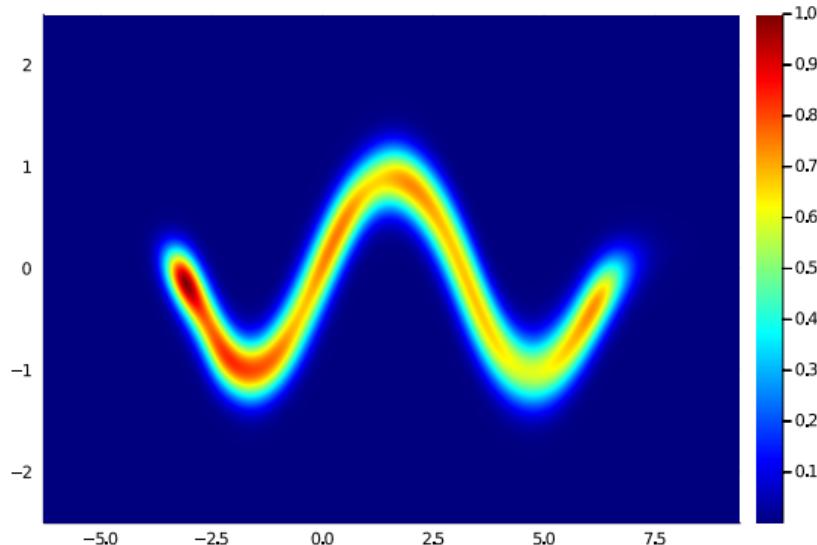
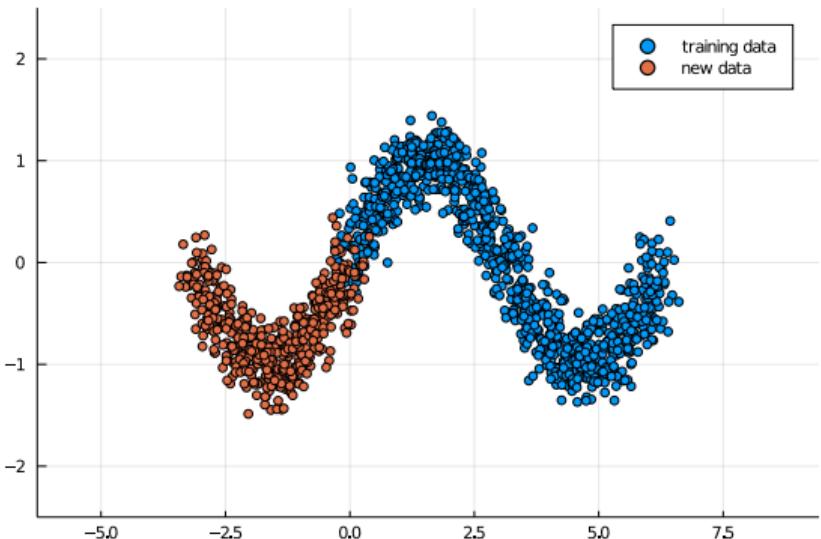
- stejná důležitost původních a nových dat → $\mathbf{w} = (0.5, 0.5)$
- důležitost podle počtu dat v jednotlivých sadách $D_1, D_2 \rightarrow \mathbf{w} = \left(\frac{n_1}{n}, \frac{n_2}{n}\right)$
- chceme zapomínat původní informaci a dávat vždy větší váhu novým datům → $w_1 < w_2$

Poznámka

Pokud mají nová data větší váhu, dochází k **zapomínání**.

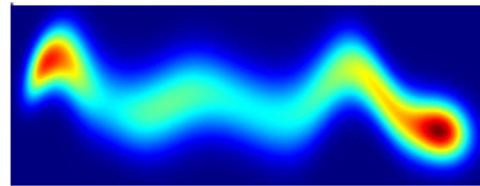
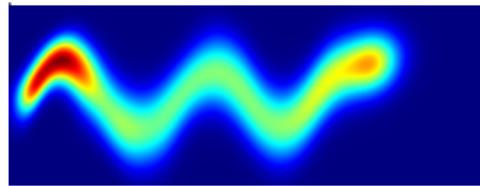
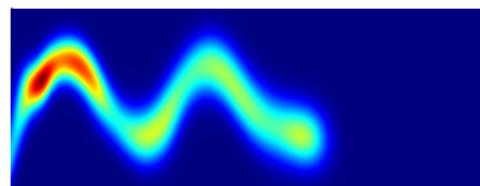
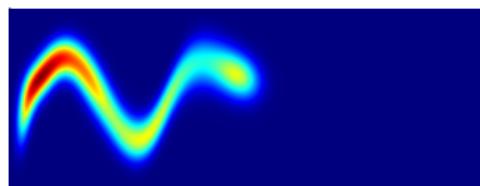
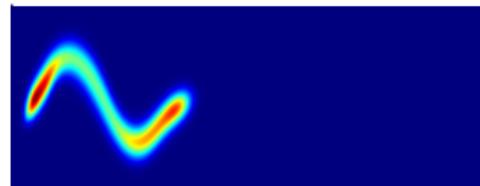
Zpět k příkladu podruhé...

Model natrénovaný pomocí Generative Replay (poměr 1:1):



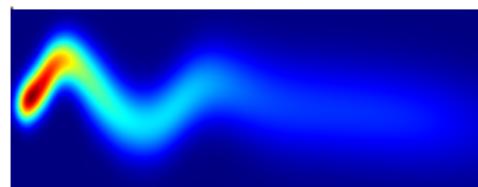
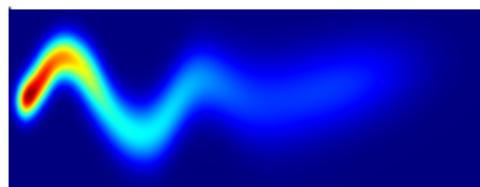
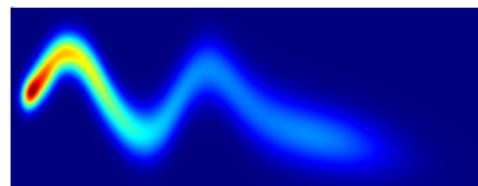
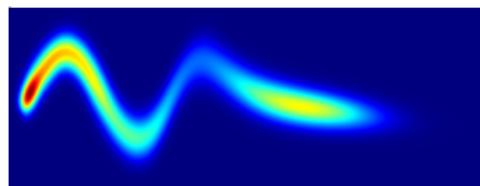
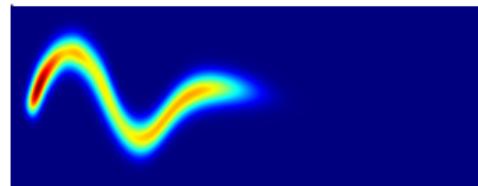
Kontinuální učení sinusoidy

Ukázka pro $w = (0.5, 0.5)$.



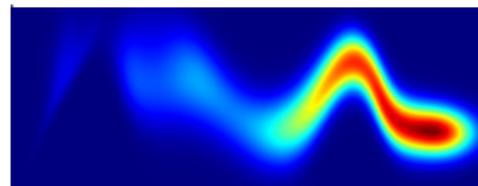
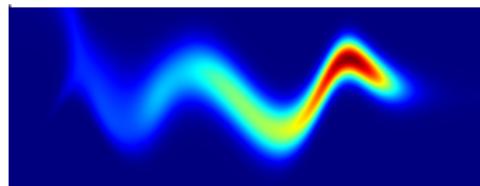
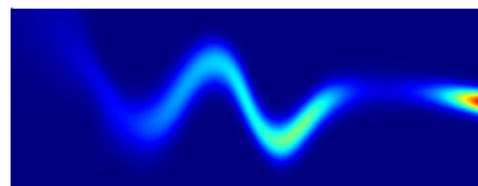
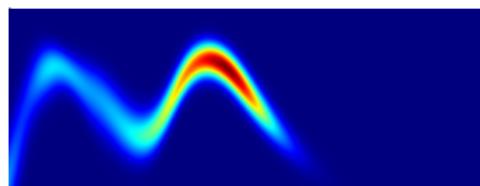
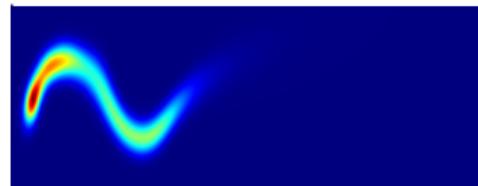
Kontinuální učení sinusoidy

Ukázka pro $w = \left(\frac{n_1}{n}, \frac{n_2}{n} \right)$.



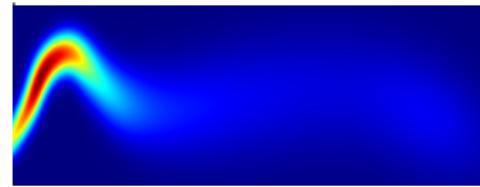
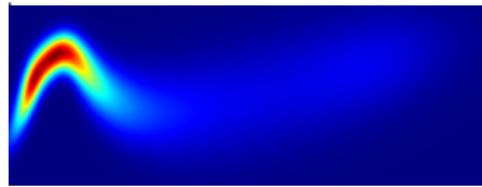
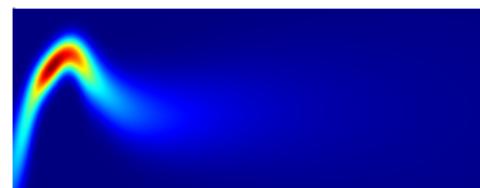
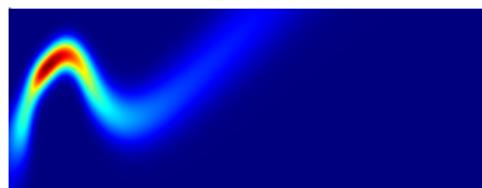
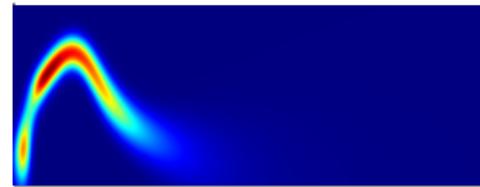
Kontinuální učení sinusoidy

Ukázka pro $w = (0.2, 0.8)$.



Kontinuální učení sinusoidy

Ukázka pro $w = (0.8, 0.2)$.



Zdroje

-  F. Wiewel and B. Yang (2019)
Continual Learning for Anomaly Detection with Variational Autoencoder
IEEE International Conference on Acoustics, Speech and Signal Processing, pages 3837-3841.
-  Hanul Shin and Jung Kwon Lee and Jaehong Kim and Jiwon Kim (2017)
Continual Learning with Deep Generative Replay
ArXiv, 1705.08690.

Otázky?