

Topológiai ritka reprezentációk segítségével

Miért kell topológia? Hogyan? Működik?

Csató Lehel

¹Matematika és Informatika Kar, Babeş–Bolyai Tudományegyetem, Kolozsvár

²Informatika Kar, Eötvös Loránd Tudományegyetem, Budapest

2021 június 10



Tartalom

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

- 1 Motiváció
- 2 Közelítés ritka reprezentáció segítségével
- 3 Topologikus kiterjesztések
- 4 Terv



Tartalom

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

- 1 Motiváció
- 2 Közelítés ritka reprezentáció segítségével
- 3 Topologikus kiterjesztések
- 4 Terv



Mély-Tanulás (Deep Learning, DNN)

- Biológiai alapozottságú, paraméterezett architektúra, **ahol**
- A rendszer paramétereit egy hiba – vagy energiafüggvény – optimalizációjával találjuk meg;
- Az optimalizáció eszköze a sztochasztikus gradiens algoritmus;

Mélytanuló algoritmusok limitációi

- A **hibafelület komplex** $\Rightarrow$ az optimum-pont nem egyedi;
- A paraméterek a száma **hatalmas** $\Rightarrow$ az adatmennyiség **mindig** kevés;
- Bonyolult energiafelület $\Rightarrow$ nincs **egyedi** a megoldás, nem konvergens;



Mély-Tanulás (Deep Learning, DNN)

- Biológiai alapozottságú, paraméterezett architektúra, **ahol**
- A rendszer paramétereit egy hiba – vagy energiafüggvény – optimalizációjával találjuk meg;
- Az optimalizáció eszköze a sztochasztikus gradiens algoritmus;

Mélytanuló algoritmusok limitációi (folyt)

- A **hibafelület komplex** $\Rightarrow$ nincs egyedi optimum-pont;
- The number of parameters is extremely high $\Rightarrow$ data is always insufficient;
- A **lokális minimumok** miatt a kapott rendszer **nem robusztus**.

(1) A DNN hiba-gradiensek nem konvergálnak

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

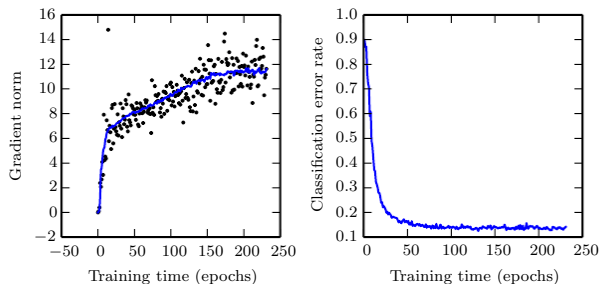
Ritka reprezentáció

Topológia

Terv

A mélytanuló algoritmusok **gradiens tanulási folyamata** ellentmond a numerikus algoritmusok módszertana által nyújtott intuíciónak.

A gradiens-vektorok abszolút értéke **nő** a tanulás folyamata alatt; azonban a tanulási hiba csökken.



Deep Learning Book, 283.o

Megjegyzés: Tekintettel a nagy paramétertérre, ez egy korábbi technika, az „**early stopping**” megvalósulása!

(2) A robusztusság hiánya rendszerszinten kihasználható

Topológiai ritka
reprezentációkon

Csató Lehel

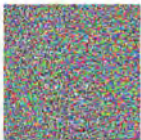
Motiváció

Ritka reprezentáció

Topológia

Terv

DNN-ek nem elég robusztusak (pillangó-hatás):

	$+ .007 \times$		$=$	
x		$\text{sign}(\nabla_x J(\theta, x, y))$		$x + \epsilon \text{sign}(\nabla_x J(\theta, x, y))$
$y = \text{"panda"}$		"nematode"		"gibbon"
w/ 57.7%		w/ 8.2%		w/ 99.3 %
confidence		confidence		confidence

Ellenséges „beavatkozások”

<https://arxiv.org/pdf/1605.07277.pdf>

Id:

„... could be used to target online classifiers trained and hosted by Amazon and Google, without any knowledge of the model design or parameters, but instead simply by making label queries for 800 inputs. The attack successfully forces these classifiers to mis-classify 96.19% and 88.94% of their inputs.”

(3) Információ-elméleti vizsgálatok

Topológiák ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

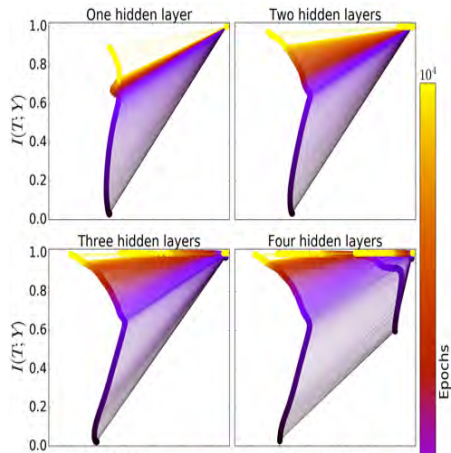
A DNN-ek előrecsatolt jellege a kimenet- és bemeneti rétegek között információátvitel valósul meg.

A kimeneti címke információja visszaterjed

Az első rejtett réteg „mindent tud” a kimenetről.

Forrás:

Ravid S.-Z., Tishby N. (2017) Opening the black box of deep neural networks via information, arXiv preprint arXiv:1703.00810



Megjegyzés: Szükség egy teljesen kapcsolt hálóban több, mint egy réteg?

Javasolt válasz: **NEM BIZTOS...**



Tartalom

Topológiák ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

- 1 Motiváció
- 2 Közelítés ritka reprezentáció segítségével
- 3 Topologikus kiterjesztések
- 4 Terv



Közelítés ritka reprezentáció segítségével I

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

Cybenko tétele

(általánosította Hornik, 1991)

Minden folytonos függvény megközelíthető **egy rejtett réteget** tartalmazó neurális hálóval, ahol a $g()$ monoton és korlátolt aktivációs függvény:

$$\mathcal{F} = \left\{ \sum_i^K v_i g \left(b_i + \sum_j^d x_j w_{ij} \right) \mid K \in \mathbb{N}, v, b \in \mathbb{R}^K, W \in \mathbb{R}^{K \times d} \right\}$$

Következtetések

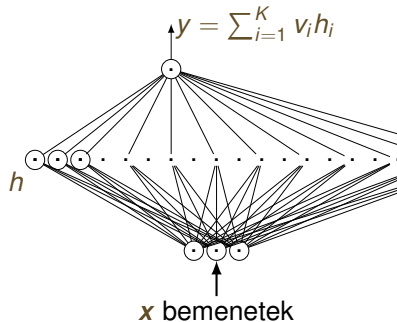
- A neurális hálók univerzális approximátorok (tetszőleges hibafüggvényre);
- Egy rejtett paraméter a K , mely **kellően nagy**, – bonyolult a közelítés.
- Egy rejtett réteg elégséges – azonban **lehet több is**.

- A neuronok felcserélhetőek $\Rightarrow$
 $K!$ – lehetőség a paraméterterben.

- **Értelmezés:** a rejtett neuronok egy-egy jellemző – feature – jelenlétét kódolják:

$$h_i \stackrel{\text{def}}{=} g\left(\sum_j w_{ij} x_j\right) \stackrel{\text{def}}{=} \phi_i(\mathbf{x}) \quad \forall i = 1, K$$

ahol $\phi_i(\mathbf{x})$ egy **jellemező-detektáló** függvény.



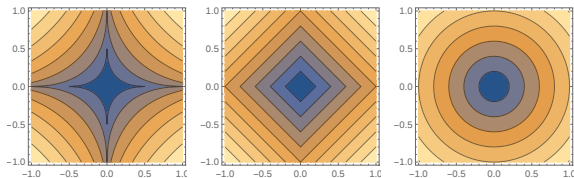
Ritka közelítések

- Kis-számú jellemző-függvényt használnak, ezeket a **bemenetek fölött** értelmezik;
- Ezeket a „**szótár-függvényeket**” (dictionary) $\phi_j(\cdot)$ **kiválasszuk**;
- **Valós esetekben** egy kis halmaz elégséges a jó teljesítményhez.

Miért kell a ritka reprezentáció a robusztussághoz

Ritka reprezentációk: azon paraméter-értékek, melyeknél **a paraméterek nagy része nulla.**

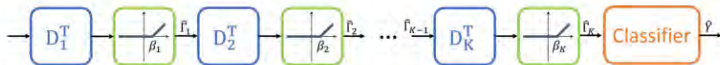
Az optimalizáció eszköze egy **ritkító-regularizáció**, pl. $L_{1/2}$



Ritkító-regularizáció

Az alapértelmezett „hibafüggvény mellett” használja a ritkító penalizálást:

$$E_q(\boldsymbol{\theta} \mid \mathcal{D}) = E(\boldsymbol{\theta} \mid \mathcal{D}) + \lambda L_q(\boldsymbol{\theta})$$



(a) The Layered-Thresholding classifier (L-THR), corresponding to a CNN - a feed-forward convolutional neural network.

Egyrétegű rendszerek kiterjesztése alapján vizsgálják a robusztusságot.

Eredményeik, hogy a rendszerek „robusztusabbak” (ellenállóbbak).

Kérdések: A ReLU függvényt használják; a **csak** pozitív rejtett-kimenet kapcsolat növeli a stabilitást.

Forrás:

Romano Y, Aberdam A, Sulam J, Elad M. (2020) Adversarial Noise Attacks of Deep Learning Architectures: Stability Analysis via Sparse-Modeled Signals, *Journal of Mathematical Imaging and Vision*, Vol.62-4, pp. 313–327, 10.1007/s10851-019-00913-z

Elad M (2010) *Sparse and Redundant Representations*, Springer Verlag

Papayan V, Romano Y, Elad M (2017) Convolutional Neural Networks Analyzed via Convolutional Sparse Coding, *Journal of Machine Learning Research*, JMLR.org, 18/1, 1532–4435



Tartalom

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

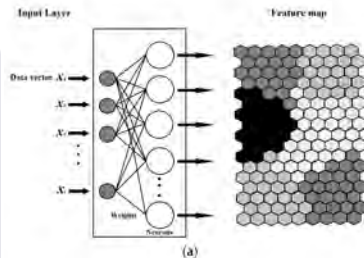
Terv

- 1 Motiváció
- 2 Közelítés ritka reprezentáció segítségével
- 3 Topologikus kiterjesztések**
- 4 Terv

Topológia – informálisan

A topológia egy **neurális réteg** kimeneteinek a vizsgálatára használjuk.

Esetünkben neurális rétegek **szomszédsági kapcsolatait** írja le, hasonlóan a **Kohonen-hálókhoz**.



Forrás: <https://www.mdpi.com/1420-3049/24/10/2006/html>

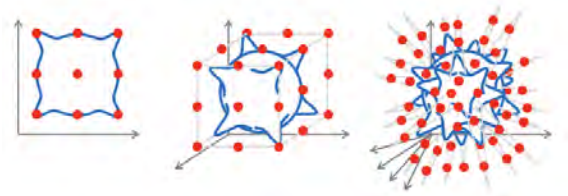
A topológia segít a robusztusságban, ha:

- Csak tanulás alatti minták **környezetére** szorítkozik a rendszer;
- A környezetet adat- és doménium-specifikusan definiáljuk;
- A „jellemzők” hiányát is lehessen kvantálni

— Csak pozitív súlyok?

„Jellemzők” kivonása:

- A bemeneti tér „effektív dimenziója” nem ismert egyszerűsíteni kell.
- Képek esetén **kitűnően** működnek a konvolúciós algoritmusok, más adatoknál ez nem igaz.



Forrás: <https://towardsdatascience.com/geometric-foundations-of-deep-learning-94cdd45b451d>

Topológiák definiálása (Konv + RELU esetben):

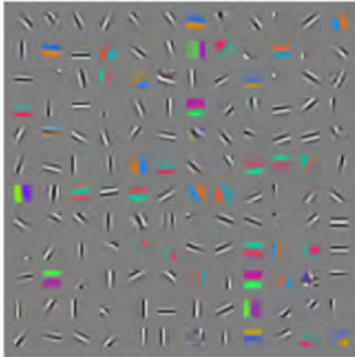
- Két „feature”-függvényt – dictionary – távolságának a meghatározása.
- A távolságok kvantálásánál a tanuló adatokat is figyelembe kellene venni.

Forrás:

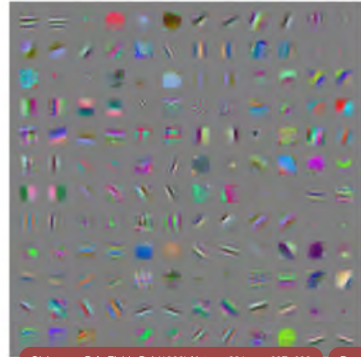
Bronstein M.M, Bruna J, Cohen T, Velicković P (2021) Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges, *CoRR*, <https://arxiv.org/abs/2104.13478>

Arjovsky M, Chintala S, Bottou L (2017), Wasserstein Generative Adversarial Networks, *Proceedings of the 34th International Conference on Machine Learning*, Vol. 70, pp. 214–223

Példa „jellemző”-függvényekre:



Olshausen-Field receptív mezők:



Olshausen B.A, Fields D.J (1996) Nature, 381, pp. 607–609

Deep Learning Book, 371.o

Kérdések:

- Hogyan mérjük két „mező” közötti távolságot?
- Tudunk algoritmust mondani, mely hasonló függvényeket „tanul”?



Tartalom

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

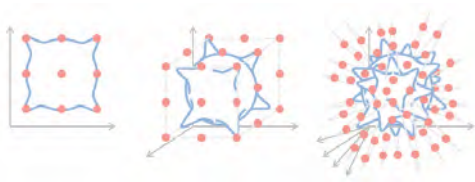
Topológia

Terv

- 1 Motiváció
- 2 Közelítés ritka reprezentáció segítségével
- 3 Topologikus kiterjesztések
- 4 Terv

Kérdések:

- Teszteljük a pozitivitás-hipotézist
A pozitívan korlátolt rendszerek képesek-e **megtanulni az osztályozást**;
- Teszteljük a „jellemző” előállítás módszertanát – hogyan generáljunk „hasznos” feature-függvényeket;
- Egy / Több-rétegű architektúrák.
- Lehetséges **létező** modellek ritkítása?



Adathalmazok:

- **Fashion-MNIST** – változatosabb adathalmaz – az osztályok heterogének;
- „Reverse game of life” – az ismert életjáték inverze egy **25x25**-ös táblán;
- HubMap projekt: „Mapping the kidney” – **szegmentálási** feladat;



Köszönet

Topológiai ritka
reprezentációkon

Csató Lehel

Motiváció

Ritka reprezentáció

Topológia

Terv

Köszönöm a figyelmet!

Kérdések?