Stability of DCNNs under deformations

MaLGa MACHINE LEARNING GENOA CENTER

Fabio Nicola & S. Ivan Trapasso - arXiv:2104.11977

AFOSR AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

A motivating example

(MNIST) handwritten digits classification

Intra-class variance modelled by **deformation operators**

Signal	$f:\mathbb{R}^d \to \mathbb{R}$
Distortion field	$\tau:\mathbb{R}^d \to \mathbb{R}^d$
Deformation operator	$F_\tau f(x) = f(x-\tau(x))$

DCNN feature extractor

$$\Phi : L^2(\mathbb{R}^d)\cap C(\mathbb{R}^d) \to (\mathcal{B}, \|\!|\cdot|\!\|)$$

The classifier is expected to be **stable under natural deformations**

τ is small
w.r.t. some metric

$\Downarrow$

$\|\!|\Phi(F_\tau f) - \Phi(f)|\!\|$ is small
($\propto$ deformation size)
for a reasonably large class of signals

Some natural questions

Stability estimates for regular, small-size distortions (at least $C^1(\mathbb{R}^d;\mathbb{R}^d)$ with $\|\tau\|_{L^\infty}$ or $\|\nabla\tau\|_{L^\infty}$ small enough)

- Mallat (2012) (**wavelet scattering transform**)
- Bölcskei & Wiatowski (2015-18) (**generalized scatt. net.**)

- What about **general distortions** $\tau \in L^\infty(\mathbb{R}^d;\mathbb{R}^d)$ without any additional regularity assumption?
- What about the interplay between **signal complexity** and the structure of the network?
- What about **general DCNNs** that are only assumed to satisfy a Lipschitz property?

Robustness to irregular deformations

Fix a suitable filter ϕ and a scale $s>0$.

The associated **approximation space** is

$$U_s := \overline{\mathrm{span}\{\phi_{s,n}\}_{n\in\mathbb{Z}^d}}, \quad \phi_{s,n}(x) := \frac{1}{s^{d/2}}\phi\left(\frac{x-ns}{s}\right)$$

(e.g., band-limited functions, polynomial splines).

There exists a constant $C>0$ such that

$$\|F_\tau f - f\|_{L^2} \le C \begin{cases} (\|\tau\|_{L^\infty}/s)\|f\|_{L^2} & (\|\tau\|_{L^\infty}/s \le 1) \\ (\|\tau\|_{L^\infty}/s)^{d/2}\|f\|_{L^2} & (\|\tau\|_{L^\infty}/s \ge 1) \end{cases}$$

for every $\tau \in L^\infty(\mathbb{R}^d;\mathbb{R}^d)$ and $f\in U_s$.

Hence, **for any Lipschitz DCNN** Φ:

$$\|\!|\Phi(F_\tau f) - \Phi(f)|\!\| = O(\|\tau\|_{L^\infty}) \ \text{ as } \ \|\tau\|_{L^\infty}\to 0$$

Random deformations

Let τ be a measurable **random field** with identically distributed variables $|\tau(x)|$.

Stability estimates (e.g., $f\in U_s$, $d=2$):

$$\mathbb{E}\|\!|\Phi(F_\tau f) - \Phi(f)|\!\|^2 \le C\,\mathrm{Lip}(\Phi)^2 \times \mathbb{E}[(|\tau|/s)^2]\|f\|^2_{L^2}$$

The field $\tau(x)$ is no longer assumed to be bounded!

Additional comments

- Stability in the regime $\|\tau\|_{L^\infty}/s \ll 1$ ($\sim$ uncertainty principle)
- The bounds are **sharp** for wavelet scattering networks
- Heavy role of **harmonic analysis** (e.g., Wiener amalgam spaces are optimal for L^∞ deformations)
- More general time-frequency def. and signal classes (Besov spaces)

S. Ivan Trapasso
Università di Genova
salvatoreivan.trapasso@unige.it