

Don't trust neural networks? Me neither, but here's how I use them anyway

COSMO21 conference, Chania, Crete, Greece

Florent Leclercq

www.florent-leclercq.eu



Institut d'Astrophysique de Paris CNRS & Sorbonne Université





In collaboration with: Deaglan Bartlett (IAP), Marco Chiarenza (IAP), Ludvig Doeser (Stockholm University)

and the Aquila Consortium
www.aquila-consortium.org

21 MAY 2024



Neural networks and their reliability (or lack thereof)

Large language models (and their limitations...)

1568 x 9762 = **15306816**

- ChatGPT 3.5
 - Florent Leclercq What is 1568 times 9762?
- ChatGPT 1568 times 9762 equals 15,316,416.
- Florent Leclercq Now what is the correct result?
- ChatGPT Apologies for the error. Let me recalculate that for you.

1568 times 9762 equals 15,322,016.

- Florent Leclercq No, that's still wrong!
- ChatGPT My apologies for the mistake. Let me calculate it again.

1568 times 9762 equals 15,318,816.

ChatGPT 4

- Florent Leclercq What is 1568 times 9762?
- ChatGPT The result of multiplying 1568 by 9762 is 15,306,816. 1



The **A** Register[®]

Gentoo Linux tells Al-generated code contributions to fork off

Tue 16 Apr 2024 // 18:30 UTC

AI-generated and assisted code contributions are no longer allowed in the Gentoo Linux distribution.

AI hallucinates software packages and devs download them – even if potentially poisoned with malware

Simply look out for libraries imagined by ML and make them real, with actual malicious code. No wait, don't do that

Thu 28 Mar 2024 // 07:01 UTC

Florent Leclercq



Safe uses of machine learning

- <u>Safe use</u>: applying machine learning (ML) in particular neural networks (NNs) in a way that ensures the results are either <u>correct by construction</u> or, at worst, <u>suboptimal</u>.
- Safe uses of ML include:
 - Ensuring <u>certifiability</u> of the model used for parameter inference and model comparison.
 - Eliminating the requirement for <u>explainability</u>.
- Examples: denoising autoencoders (DAE) to build summaries, information-maximising neural networks (IMNN) for simulation-based inference (SBI).



<u>Charnock et al., 1802.03537, Makinen et al., 2107.07405</u>

Florent Leclercq COmoving Computer Acceleration (COCA)

Comparative growth of models and methods

- Amdahl's law: latency kills the gains of parallelisation.
- Machine learning (ML) has caught up with the largest cosmological simulations!



Amdahl 1967, doi:10.1145/1465482.1465560

Emulation of N-body simulations



- Pleasantly fast, but what about the accuracy?
- There remains an emulation error [up to $\mathcal{O}(10\%)$] that we cannot ever correct for.
- Using these emulators as forward models does not qualify as a safe use of NNs.

He et al., 1811.06533, Lucie-Smith et al., 1802.04271, Jamieson et al., 2206.04594, Conceição et al., 2304.06099, Doeser et al., 2312.09271

The tCOLA framework: (temporal) COmoving Lagrangian Acceleration

 $x \left[\mathrm{Mpc}/h \right]$

res

PM

• Idea behind tCOLA: we can make use of the analytical solution at large scales and early times: Lagrangian perturbation theory (LPT).

 $\partial_a^2 \Psi = - \boldsymbol{\nabla}_{\mathbf{x}} \Phi$

Ο

Write the displacement vector as: $\Psi = \Psi_{\text{LPT}} + \Psi_{\text{res}}^{\text{COLA}}$ $(\mathbf{x} = \mathbf{q} + \mathbf{\Psi})$ Tassev & Zaldarriaga, 1203.5785 Equation of motion (omitted Analytical constants and Hubble expansion): _______solutions! $\partial_a^2 \Psi_{\rm res}^{\rm COLA} = \partial_a^2 (\Psi - \Psi_{\rm LPT}) = -\nabla_{\bf x} \Phi - \partial_a^2 \Psi_{\rm LPT}$ 2LPTGADGET COLA ~ 3 timesteps 10 timesteps 2000 timesteps 50 Mpc/I

Tassev, Zaldarriaga & Einsenstein, 1301.0322

 $x \left[\mathrm{Mpc}/h \right]$

Florent Leclercq COmoving Computer Acceleration (COCA)

21/05/2024

 $x \left[\text{Mpc}/h \right]$

The tCOCA framework: (temporal) COmoving Computer Acceleration

• The idea behind tCOCA: the easiest simulation to run is the one where nothing moves!



- Write the displacement vector as:
 - $\Psi = \Psi_{LPT} + \Psi_{ML} + \Psi_{res}^{COCA} \quad (\mathbf{x} = \mathbf{q} + \Psi)$
- Equation of motion (omitted constants and Hubble expansion):

$$\partial_a^2 \Psi_{\rm res}^{\rm COCA} = -\nabla_{\bf x} \Phi - \partial_a^2 \Psi_{\rm LPT} - \partial_a^2 \Psi_{\rm ML}$$
$$\implies \partial_a^2 \Psi = -\nabla_{\bf x} \Phi$$

- With COCA:
 - Any emulation error will be corrected by solving the <u>correct physical equation of motion</u>.
 - Any ML algorithm can do the job!
 - Building a data model is a <u>safe use</u> of ML.

Bartlett, Chiarenza, Doeser & FL, in prep.

Florent Leclercq COmoving Computer Acceleration (COCA)

Time stepping and force calculations in COCA

https://simbelmyne.florent-leclercq.eu — Bitbucket:florent-leclercq/simbelmyne

- Learning the new frame of reference means emulating the COLA residual momenta at every time step: $\mathbf{p}_{\mathrm{res}}^{\mathrm{COLA}} = \mathbf{p} \mathbf{p}_{\mathrm{LPT}}$.
- When the emulation error is small ($\mathbf{p}_{\mathrm{ML}} \approx \mathbf{p}_{\mathrm{res}}^{\mathrm{COLA}}$), particles are already at rest in the COCA frame of reference, so it is <u>unnecessary to compute forces at every step</u>.



• A good frame-of-reference emulator therefore makes COCA cheaper than COLA.

Training a frame-of-reference emulator for COCA

- We trained a styled V-net with initial density field and scale factor as inputs; frame of reference (particles' residual momenta) as output.
- We used 100 training COLA simulations with L=128 Mpc/h, N=64³ particles, and 200 epochs.
- We can predict the frame of reference to run test COCA simulations:



Milletari, Navab & Ahmadi, 1606.04797



Results: COCA density field



Florent Leclercq COmoving Computer Acceleration (COCA)

11

Results: COCA two-point statistics



Results: COCA three-point statistics



Florent Leclercq COmoving Computer Acceleration (COCA)





Conclusions

- <u>Safe uses</u> of neural networks exist, where:
 - The answer is <u>correct by construction</u> or <u>suboptimal</u>,
 - Use for physics (parameter inference, model comparison) is <u>certifiably</u> robust,
 - Explainability is not needed.
- <u>tCOCA</u> reimagines the use of neural networks for emulating *N*-body simulations:
 - It generalises the idea of tCOLA: running simulations in a <u>new frame of</u> reference,
 - It solves the correct equations of motion, so it is a <u>safe use</u> of neural networks,
 - It makes simulations cheaper by skipping unnecessary force evaluations.
- The large-scale ML solution can also be used to decouple subvolumes, in the same spirit as sCOLA: the <u>sCOCA</u> framework!

Acknowledgements, credits, contacts



References:

- Simbelmynë: Leclercq, Jasche & Wandelt 2014, 1403.1260, Bayesian analysis of the dynamic cosmic web in the SDSS galaxy survey — https://simbelmyne.florent-leclercq.eu
- sCOLA: Leclercq et al. 2020, 2003.04925, Perfectly parallel cosmological simulations using spatial comoving Lagrangian acceleration
- **COCA**: Bartlett, Chiarenza, Doeser & Leclercq, in prep.

www.florent-leclercq.eu

www.aquila-consortium.org



The author acknowledges the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-23-CE46-0006 (project INFOCW). The author does not acknowledge any support from a famous American soda company.