Embedding Artificial Intelligence into Constrained Devices

PhD Student: *Andrea Agiollo*[*]
Supervisor: Andrea Omicini[*]

[*]Dipartimento di Informatica – Scienza e Ingegneria (DISI)
Alma Mater Studiorum – Università di Bologna
andrea.agiollo@unibo.it

PhD First Year Report,
20th October 2021, Bologna

Outline

Context

- AI proven successful for most diverse tasks and applications
- AI requires high computational capabilities
- Application of AI on restricted devices (e.g. IoT) open issue:
    - Minimize costs
    - Poor performances
    - Real-time results
- AI in IoT requested for industrial applications

Research Focus

Goal

Resource-friendly Artificial Intelligence

$\Downarrow$

Parallel approaches

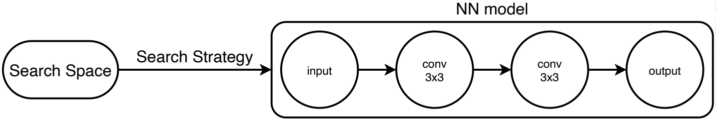
1. Identify small, yet powerful, Neural Network models
2. Combine symbolic and sub-symbolic AI techniques

Searching Powerful NNs - SOTA

- Neural Networks are the most popular AI technique
- NN performance heavily depends on NN architecture (VGG [7], ResNet [5], MobileNet [6], etc.)
- Identification of powerful NN architectures is cumbersome

$$\Downarrow$$

Iterative searching approaches called Neural Architecture Search (NAS) [4]

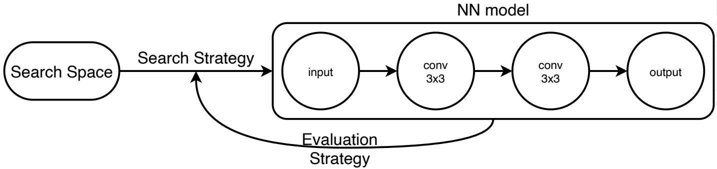


Searching Powerful NNs - SOTA

- Neural Networks are the most popular AI technique
- NN performance heavily depends on NN architecture (VGG [7], ResNet [5], MobileNet [6], etc.)
- Identification of powerful NN architectures is cumbersome

$\Downarrow$

Iterative searching approaches called Neural Architecture Search (NAS) [4]

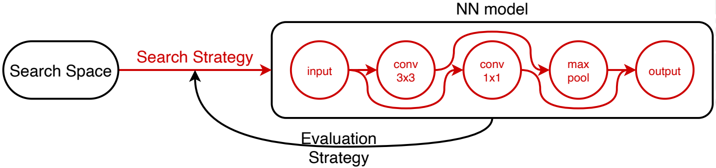


Searching Powerful NNs - SOTA

- Neural Networks are the most popular AI technique
- NN performance heavily depends on NN architecture (VGG [7], ResNet [5], MobileNet [6], etc.)
- Identification of powerful NN architectures is cumbersome

$\Downarrow$

Iterative searching approaches called Neural Architecture Search (NAS) [4]



Searching Powerful NNs - Our work (1/2)

- Analysis of most common approaches to NAS task
- Common NAS focus on raw performance, ignoring NN size/footprint
- NN obtained from NAS are not applicable to IoT
- Propose iterative search mechanism to limit NN footprint

Paper

A. Agiollo, G. Ciatto, A. Omicini: **Shallow2Deep: Restraining Neural Networks Opacity Through Neural Architecture Search**. In *International Workshop on Explainable, Transparent Autonomous Agents and Multi-Agent Systems (2021)* [2]

Searching Powerful NNs - Our work (2/2)

- Common NAS iteratively explore a search space
- Learning how to explore against properly learning construction criteria
- NAS are overly complex (400 GPU hours) and do not generalize
- Graph Neural Networks proven to learn graph structures' characteristics
- Generative GNN to build powerful NN architectures
- Learning construction criteria $\rightarrow$ true meta-learning
- *Draft ongoing*

Combining symbolic and sub-symbolic AI

- Logical information complicated to extract, elaborate, treat with NNs
- Symbolic techniques better suited for logical information
- NN complex to interpret and understand $\rightarrow$ eXplainable AI (XAI)
- Sub-symbolic benefit from symbolic integration in complexity and explainability
- Focus leveraging GNNs to link symbolic and sub-symbolic

Paper

A. Agiollo, G. Ciatto, A. Omicini: **Graph Neural Networks as the Copula Mundi between Logic and Machine Learning: A Roadmap**. In *WOA 2021 – 22nd Workshop "From Objects to Agents"* [1]

Other works

- AI applied to IoT cybersecurity
- Model available attacks against RPL
- Propose AI-based Intrusion Detection System (IDS) to identify most attacks

Paper

A. Agiollo, M. Conti, P. Kaliyar, T.N. Lin, L. Pajola: **DETONAR: Detection of routing attacks in RPL-based IoT**. In *IEEE Transaction on Network Service Management (2021)* [3]

Industrial applications

- Results of research applied to Electrolux Professional appliances
- Focus on visual tasks (e.g. image classification)
- Load recognition in dishwashing machine
- Analysis of possible extensions to other appliances

Courses with exams (1/2)

- Emanuele Rodolà (University Sapienza of Rome): **Geometric Deep Learning**. *Hours*: 10. *CFUs*: 2. *Dates*: 12/2/2020 - 12/11/2020
- Daniela Loreti (University of Bologna): **Programming Paradigms for High Performance Computing**. *Hours*: 10. *CFUs*: 2. *Dates*: 12/9/2020 - 12/16/2020
- Tullio Vardanega (University of Padova) and Andrea Zanella (University of Padova): **Scenarios of IoT**. *Hours*: 20. *CFUs*: 4. *Dates*: 01/19/2021 - 02/26/2021

Courses with exams (2/2)

- Gianluca Campana (University of Padova) and Lamberto Ballan (University of Padova): **Human and Machine Vision**. *Hours*: 12,5. *CFUs*: 3. *Dates*: 04/19/2021 - 04/29/2021
- Mirco Musolesi (University College London): **Advanced Topics in Reinforcement Learning**. *Hours*: 10. *CFUs*: 2. *Dates*: 04/13/2021 - 06/01/2021
- Diego Valsesia (Politecnico of Turin): **Adversarial Training of Neural Networks**. *Hours*: 15. *CFUs*: 3. *Dates*: 03/31/2021 - 05/12/2021

Courses without exams

- Maria Pia Torricelli, Rosalia Miceli (Library of Engineering and Architecture, University of Bologna): **Risorse bibliografiche per l'ingegneria e l'architettura**. *Hours*: 18. *CFUs*: 4. *Dates*: 02/01/2021 - 02/16/2021
- Gian Antonio Susto (University of Padova): **Explainable Machine Learning**. *Hours*: 6. *CFUs*: 1. *Dates*: 03/15/2021 - 03/17/2021
- Antonio Rodà (University of Padova): **Principles of Computational Creativity**. *Hours*: 6. *CFUs*: 1. *Dates*: 04/14/2021 - 04/15/2021
- Davide Bresolin (University of Padova): **Temporal Logic in Artificial Intelligence**. *Hours*: 6. *CFUs*: 1. *Dates*: 05/04/2021 - 05/11/2021

Embedding Artificial Intelligence into Constrained Devices

PhD Student: *Andrea Agiollo**
Supervisor: Andrea Omicini*

*Dipartimento di Informatica – Scienza e Ingegneria (DISI)
Alma Mater Studiorum – Università di Bologna
andrea.agiollo@unibo.it

PhD First Year Report,
20^{th} October 2021, Bologna

References I

[1] Andrea Agiollo, Giovanni Ciatto, and Andrea Omicini.
Graph neural networks as the copula mundi between logic and machine learning: A roadmap.
In Roberta Calegari, Giovanni Ciatto, Enrico Denti, Andrea Omicini, and Giovanni Sartor, editors, *WOA 2021 – 22nd Workshop "From Objects to Agents"*, volume 2963 of *CEUR Workshop Proceedings*, pages 98–115. Sun SITE Central Europe, RWTH Aachen University, October 2021.
22nd Workshop "From Objects to Agents" (WOA 2021), Bologna, Italy, 1–3 September 2021. Proceedings.

References II

[2] Andrea Agiollo, Giovanni Ciatto, and Andrea Omicini.
Shallow2Deep: Restraining neural networks opacity through neural architecture search.
In Davide Calvaresi, Amro Najjar, Michael Winikoff, and Kary Främling, editors, *Explainable and Transparent AI and Multi-Agent Systems. Third International Workshop, EXTRAAMAS 2021, Virtual Event, May 3–7, 2021, Revised Selected Papers*, volume 12688 of *Lecture Notes in Computer Science*, pages 63–82. Springer Nature, Basel, Switzerland, 2021.

[3] Andrea Agiollo, Mauro Conti, Pallavi Kaliyar, Tsung-Nan Lin, and Luca Pajola.
DETONAR: detection of routing attacks in rpl-based iot.
IEEE Trans. Netw. Serv. Manag., 18(2):1178–1190, 2021.

[4] Thomas Elsken, Jan Hendrik Metzen, and Frank Hutter.
Neural architecture search: A survey.
J. Mach. Learn. Res., 20:55:1–55:21, 2019.

References III

[5] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun.
Deep residual learning for image recognition.
In *2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016*, pages 770–778. IEEE Computer Society, 2016.

[6] Andrew G. Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam.
Mobilenets: Efficient convolutional neural networks for mobile vision applications.
CoRR, abs/1704.04861, 2017.

[7] Karen Simonyan and Andrew Zisserman.
Very deep convolutional networks for large-scale image recognition.
In Yoshua Bengio and Yann LeCun, editors, *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*, 2015.