David A. R. ROBIN

PhD in Mathematics from INRIA / ENS Paris

+33 7 78 21 59 51
david.a.r.robin@gmail.com
www.robindar.com

Education

2021 - 2025 **PhD in Mathematics**, *INRIA / École Normale Supérieure*, Paris,
Advised by Marc Lelarge & Kevin Scaman.
Construction and convergence of provably-correct neural networks.

2020 - 2021 **Diplôme de l'ENS (Info - Maths)**, *École Normale Supérieure*, Paris.
Additional advanced courses on stochastic processes and algebraic geometry.

2018 - 2020 **M. Sc. Computer Science (MVA)**, *ENS Paris & ENS Paris-Saclay / Cachan.*
Relevant coursework includes: Category theory, Parallel programming, Computer vision, Convex optimization, Statistical learning, Differential geometry, Reinforcement learning, Natural language processing, Optimal Transport.

2017 - 2018 **B. Sc. Computer Science**, *École Normale Supérieure*, Paris.
Relevant coursework includes: Randomized data structures and algorithms, Formal languages, Compilation, Algebra, Mathematical Logic, Semantics and Verification, Operating Systems, Information Theory, Cryptography, Databases.

2015 - 2017 **CPGE MP***, *Lycée Louis-le-Grand*, Paris.
Two-year post-secondary program in advanced maths and physics.

Publications (Machine Learning)

Dec 2025 NeurIPS **Noise-Adaptivity in Smooth Optimization with Stability Ratios**, *San Diego (CA)*, Neural Information Processing Systems 2025.
Constructed an algorithm adaptive to noise levels in stochastic gradient descent by automatically computing a scheduler to shrink the step-size along the trajectory. Proved adaptivity and rates matching nearly all best rates of SGD with noise-tuned schedulers.

May 2024 ICLR **Random Sparse Lifts: convergence of finite sparse networks**, *Vienna*, International Conference on Learning Representations 2024.
Proved convergence of multi-layer networks to arbitrarily low loss values by gradient flow, for large families of MLP and derivative architectures at initialization. Showed that probable-approximate-correctness is a type of structural guarantee that is achievable for large neural networks of essentially arbitrary architectures.

Nov 2022 NeurIPS **Convergence beyond the over-parameterized regime with Rayleigh quotients**, *New Orleans (LA)*, Neural Information Processing Systems 2022.
Presented a proof that two-layer networks trained by gradient flow are probably approximately correct, without over-parameterization assumptions, extending to cases with infinite data, by leveraging a structural inequality (Separable Kurdyka-Łojasiewicz).

Nov 2022 NeurIPS **Periodic Signal Recovery with Regularized Sine-Networks**, *New Orleans (LA)*, NeurReps workshop at NeurIPS 2022.
Showed failure of neural networks to learned periodic functions, identified obstructions, and presented a more diverse initialization and non-convex regularization enabling sinusoidal two-layer networks to perfectly recover a periodic signal far outside the training interval.

Publications (Cybersecurity)

Jun 2025 Euro S&P — **Attacking and Fixing the Android Protected Confirmation Protocol**, *Venice*, IEEE European Symposium on Security and Privacy 2025.
Identified two vulnerabilities in Android's Trusted Execution Environment (TEE) registration and user validation protocols leading to a bypass of user consent. Demonstrated attacks on Google's Pixel, and proved that a fixed protocol does achieve the intended APC trusted user-consent guarantees in the Universal Composability (UC) framework.

Oct 2020 Asia CCS — **Return-oriented programming on RISC-V**, *Taipei Taiwan*, ACM Asia Conference on Computer and Communications Security 2020.
Demonstrated a vulnerability in prefix-code machine instructions exploited by crafting sequences of long (32-bit) instructions whose last 16 bits are either a valid instruction or a valid prefix that can be chained into an overlapping sequence of instructions fooling current ROP gadget detectors, with a corresponding tree-based detection method.

Experience

Apr - Oct 2024 — **Quantitative Researcher**, *Qube Research & Technology (QRT)*, Paris.
Developed automated derivatives-trading algorithms exploiting statistical arbitrages.

Oct 2020 - Jun 2021 — **Research Internship**, *Laboratoire de Mathématiques LMO*, Orsay.
Research internship with Lénaïc Chizat (CNRS) on the implicit bias of gradient descent on two-layer neural networks. Characterized the limit point as the Bregman projection for hyperbolic-entropy of initialization to the zero-loss set with linear convergence speed.

Feb - Aug 2020 — **Research Internship**, *Upstride SAS*, Station F - Paris.
Research internship with Wilder Lopes exploring computational efficiency of variational auto-encoders defined over Clifford algebras. Demonstrated experimentally superior reconstruction performance of models leveraging higher-dimensional algebras on images.

Feb - Aug 2019 — **Research Internship**, *Technicolor AI Research*, San Francisco (CA).
Research Internship with Swayambhoo Jain on compression of neural networks, by iterative reconstruction of activations, re-cast as a sequence of convex problems.

Jun - Aug 2018 — **Research Internship**, *Massachussets Institute of Technology*, Boston (MA).
Summer internship with Philippe Rigollet (MIT) on reconstruction of cellular trajectories in gene expression space, between single-cell RNA sequencings of populations of cells at various stages of development, through optimal transport methods.