

# Fail Fast, Run Faster: Shape Safe Deep Learning in Rust on Apple Silicon

Taylor Tam  
Stanford University  
450 Jane Stanford Way, Stanford CA  
taylor52@stanford.edu

Jai Agarwal  
Stanford University  
450 Jane Stanford Way

## Abstract

*Shape errors are among the most common and frustrating failures in deep-learning code, usually surfacing at runtime after long training jobs. We tackle this reliability issue by building a complete MNIST digit-classification pipeline entirely in Rust, encoding every tensor dimension as a const-generic type parameter so that illegal operations are rejected at compile-time.*

*Situated at the intersection of shape-safe languages and hardware-centric compilers, our approach extends prior work on dependent-type arrays and MLIR-style kernel generation while targeting Apple-Silicon GPUs that are inaccessible to CUDA-centric toolchains. The system ingests the canonical MNIST dataset, normalizes and batches it in Rust, and then trains a CNN whose layers are backed metal performance shaders. These shaders sustain  $\approx 850$  GFLOP  $s^{-1}$  ( $\approx 16\%$  of an M1 Pro’s FP32 peak) by fusing GEMM, bias-add, and ReLU in a single pass, and they are monomorphized at compile time, eliminating all runtime shape checks, JITs, and Python overhead.*

*End-to-end, the resulting model reaches 99% test accuracy and delivers batch inference in 8.2ms, within  $\Delta \approx 5\%$  of PyTorch-MPS throughput while guaranteeing that every linear-algebra operation is dimensionally correct before the program can even be linked. Micro-benchmarks, energy profiles, and a set of 50 deliberately malformed tensor programs confirm that compile-time shape algebra, auto-specialized Metal kernels, and unified-memory optimization can coexist without sacrificing performance.*

*Ultimately, we argue that const-generic Rust coupled with low-level GPU control offers a compelling foundation for future safe, high-performance ML systems.*

## 1. Introduction

Deep learning is dominated by Python frameworks like PyTorch and JAX, whose dynamic graphs and execution times enable rapid prototyping but defer most error detection to runtime. A single shape mismatch—such as adding a  $[128 \times 256]$  tensor to a  $[128 \times 255]$  tensor or wiring layers of inconsistent sizes—can crash hours into

training. Moreover, the Python interpreter, the Global Interpreter Lock, and heavyweight dependencies complicate deployment on edge devices or safety-critical systems where reliability and binary size matter.

Rust offers a compelling alternative: zero-cost abstractions, strong memory safety, and a type system capable of encoding invariants at compile-time. It only recently did Rust’s nightly channel introduce const-generic expressions, unlocking the ability to compute with type-level integers inside generic parameters. Because of this novelty, Rust ML projects have not yet leveraged compile-time shape checking in concert with GPU acceleration, nor have they targeted Apple Silicon’s rapidly proliferating hardware.

Meanwhile, Apple’s M-Series chips integrate a high-bandwidth unified memory GPU accessible only through Metal, leaving CUDA-centric toolchains unable to exploit Apple Silicon’s hardware.

In this paper, we investigate whether compile-time safety checks and hardware-level performance can coexist by implementing a complete, convolutional neural network that:

1. Tracks every tensor dimension in the type system. Operations that violate linear algebra rules fail to compile, ensuring shape correctness by construction.
2. Accelerates training and inference on Apple Silicon GPUs. A tile-based GEMM kernel written in Metal Performance Shaders sustains  $>16\%$  of theoretical peak throughput, and element-wise activations are fused to minimize memory traffic. Metal Performance Shaders (MPS) API appeared in 2023 and remains untapped by mainstream numerical frameworks such as JAX, NumPy, and the standard PyTorch wheels, which are tied to CUDA. Consequently, a large portion of Apple Silicon compute is currently idle.
3. Matches PyTorch accuracy and approaches its speed while producing a self-contained binary free of Python, dynamic linking, or runtime graph machinery.

The input to our system is a  $28 \times 28$  grayscale image, and the output is a one-hot vector over ten-digit classes (0–9).

We begin by situating our approach within shape-safe languages, deep-learning compilers, and Apple-Silicon optimization literature. Then, we describe data handling, tensor layout, compile-time generics, and GPU-kernel design. Micro-benchmarks quantify matrix-multiplication performance; end-to-end MNIST results and energy profiles follow. Finally, we discuss trade-offs—developer ergonomics, compile times, and future convolutional extensions—and argue that Rust’s fail-at-compile-time philosophy, coupled with low-level Metal control, provides a promising foundation for safer, high-performance machine-learning system.

## 2. Related Work

In systems-oriented deep learning research, the central objective is to combine correctness guarantees with high hardware utilization. Ideally, a model developer writes tensor code that is probably shape-safe yet still runs at near peak FLOPs on modern GPUs. Over the past decade, researchers have explored a spectrum of approaches to reach this goal: statically typed array languages that encode dimensions in the type system, graph compilers that fuse and schedule kernels for NVIDIA/AMD GPUs, and more recent efforts to exploit Apple Silicon’s unified memory. Below, we situate our Rust-to-Metal pipeline within these threads—shape-safe programming languages, deep learning compilers, and on-device Apple Silicon inference—highlighting where these methods fall short and how our work unifies their strengths.

### 2.1. Shape Safe Programming Languages

Early attempts at guaranteeing tensor correctness were made inside arrays DSLs such as Dex (“getting to the point”) which encodes index sets and dependent types so that illegal shapes are rejected by the compiler [3]. In the ML community, Swift for TensorFlow embedded automatic differentiation and compile-time tensor checking in the Swift language, but these features were discontinued before any widespread adoption [4]. Our work brings similar safety using Rust, relying on its const-generic types to make shape mismatches a compile-time error while retaining a zero-cost abstraction model.

### 2.2. Deep Learning Compilers

Multi-level intermediate representations—such as MLIR—provide reusable passes that unify graph and kernel level optimization across domains [1]. On top of MLIR, TVM demonstrated auto-tuned tensor scheduling that rivals handwritten CUDA code, while XLA performs ahead-of-time linear algebra fusion for Tensorflow/JAX workloads [2, 9]. Dynamic shape networks prompted new compilers: Nimble introduced a dynamic type system and VM runtime to handle control flow and jagged tensors [5]; DISC extended MLIR with fully dynamic shape IR and

achieved up to 3.3x speedups over mainstream networks [6]. Unlike these systems—which still surface shape errors at runtime—our Rust pipeline proves shape compatibility at compile time and can offload computation to a Metal GPU backend.

### 2.3. Apple and On-Device Accelerations

Apple’s M-Series have only recently gained academic attention. Hübner et al. quantified FP32 throughput, unified memory bandwidth and energy efficiency across M1-M4 SKUs, showing that GPUs can exceed 200 GFLOPW [7]. Feng et al. profiled training performance for large language models and highlighted kernel-launch latency and page-fault overheads unique to the unified-memory design [8]. For inference, Tang et al. introduced ML Drift, an engine that scales generative models up two orders of magnitude larger than previous mobile deployments, with an Apple Silicon evaluation in its cross-platform study [10].

Our work complements prior analyses by presenting a from-scratch Metal GEMM that sustains  $\approx 16\%$  of an M1 Pro’s theoretical FP32 peak while preserving full compile-time shape safety. Crucially, it demonstrates practical use of Metal Performance Shaders (MPS) for machine-learning workloads—an approach rarely adopted in mainstream frameworks such as NumPy, JAX, or the default PyTorch builds.

### 2.4. Our Approach

Where prior compilers trade static safety for performance (TVM, Nimble) or focus on NVIDIA/AMD backends, we demonstrate that compile-time tensor guarantees and near state-of-the-art throughput are simultaneously possible on Apple Silicon.

Inspired by Dex’s dependent-type arrays and DFDX’s const-generic tensors, we encode  $M \times N$  sizes in Rust types and propagate them into MLIR-style code-generation macros. The same compiler-time constants parameterize our Metal shaders so that the GPU kernel is fully specialized for each layer and can’t be invoked with a badly shaped tensor.

We additionally adopt TVM’s tile-size auto search heuristic to pick  $\langle \text{TILEm}, \text{TILEn}, \text{TILEk} \rangle$  that maximize occupancy on the M-series shader cores, then hardwire those choices into the generated kernel—eliminating the runtime JIT layer NIMBLE and DISC require for dynamic shapes.

Finally, we build on Nimble’s operator-fusion insight, collapsing bias-add, activation, and dropout into a single thread block pass that exploits the M-Series GPU’s 128-bit vector units and avoids redundant trips through unified memory, delivering up to 1.4x or more GFLOPs-l than PyTorch MPS or mid-sized GEMMs.

These steps retain compile-time tensor shape guarantees while matching—or exceeding—PyTorch’s MPS throughput on an MNIST workload, demonstrating that static safety does not need to preclude aggressive GPU optimization even on non-CUDA hardware.

### 3. Data

#### 3.1. Dataset Description

We evaluate on the canonical MNIST handwritten digit corpus (70,000 grayscale images, 28x28px, 10 classes) introduced by LeCun et al. (1998). The data is split into 60,000 images for training and 10,000 for testing, where each image is provided as an unsigned 8-bit pixel matrix with an intensity range of [0, 255]. Although MNIST is already considered “solved,” its small size and well-established baselines make it ideal for isolating the systems-level questions of compile-time safety and Apple Silicon optimization that are addressed in this paper.

#### 3.2. Preprocessing Pipeline

Each 8-bit pixel is first cast to f32 and divided by 255 to obtain values in [0, 1]; we intentionally omit augmentations such as crops or rotations so that any accuracy or speed differences isolate systems effects rather than data-level regularization. The normalized images are then reshaped into `Tensor3<f32, 1, 28, 28>`, encoding channel, height, and width as const-generic parameters, and stacked into `Tensor4<f32, B, 1, 28, 28>` mini-batches—where the compile-time-fixed feature axes coexist with a loader-supplied batch size  $B$  to preserve static safety without sacrificing flexibility. Finally, label bytes are converted in a single SIMD pass (for the CPU backend) or a `MPSMatrixMultiplication` (on the MetalGPU backend) to one-hot `Tensor2<f32, B, 10>` vectors, and an epoch-wise PRNG shuffle of index arrays yields statistically independent mini-batches without extra copies.

#### 3.3. I/O Pipeline

All four IDX blobs (train/test images and labels) are memory-mapped at launch. Apple Silicon’s unified address space lets CPU and GPU access the same pages, eliminating host-to-device copies. A sequential scan of the full 60 000-image training set completes in  $\approx 250$  ms on an M1 Pro, leaving data loading comfortably off the critical path.

While the GPU processes the current mini-batch, pre-fetches the next 128 samples, endian-flips, normalises, and packs them into a contiguous `Tensor4`. This overlap sustains  $> 3 \text{ GB s}^{-1}$  of effective throughput—orders of magnitude above the  $\sim 55 \text{ kB}$  footprint of a single batch a dedicated Rayon worker thread—and keeps CPU

utilisation below 2 %. Because the tensor already resides in unified memory, the MetalBackend consumes it with zero-copy, ensuring that Section 5’s throughput and energy numbers measure kernel execution alone.

Our data pipeline therefore maintains compile-time shape safety, saturates the memory bus, and introduces no measurable latency between epochs—establishing a clean baseline for evaluating the GPU kernels described next.

### 4. Methods

#### 4.1 Const-Generic Shapes: Enforcing Operation Boundaries at Compile-Time

We encode every tensor dimension as a const-generic parameter so the Rust type checker can reason about shapes before any instructions are executed. Each dimension is a compile-time `usize`; the compiler can perform arithmetic on these constants exactly as it does on literals, then erases them at monomorphization—no runtime metadata remains.

GEMM is also expressed as a shape-constrained trait. If a tensor’s inner  $K$  dimension disagrees, no `MatMul` impl exists and the compiler triggers a shape error. This mechanism holds for up to rank-4 tensors: `Tensor4<N, C, H, W>` will only multiply with `Tensor4<C, W, P, Q>` only if dimension  $W$  matches.

Scalar and tensor-wise operators use the same idea. Scalar tensor addition delegates to a backend kernel that receives a compile-time length  $N = R * C$  for a constant  $C$  and a tensor of dimensions `Tensor2<T, R, C, B>`. Because the array is a const-generic type, Rust’s borrow checker verifies that kernel authors cannot read or write past bounds—mis-sized buffers would fail to compile.

Tensor-Tensor addition implements `ElemAdd` which only exists when both operands share the identical compile time product  $R * C$ . Mismatched shapes would again trigger trait-resolution failure.

Convolutions are parameterized by an input tensor—`Tensor<N, C_in, H, W>`, `Kernel<C_out, C_in, K_h, K_w>`, `stride<S_h, S_w>`, `Padding<P_h, P_w>`, `Dilation<D_h, D_w>`—all of which are const generics. The trait is implemented only when the derived output height and width evaluate to positive integers with zero remainder. If the stride, padding, or dilation choices would yield a fractional result—or if the kernel channels do not match  $C_{in}$ —no `Conv2` implementation is found and compilation halts. Because the output shape is computed at the type level, every downstream operator sees `Tensor4<N, C_out, O_H, O_W>` whose spatial extents are already verified. Kernel authors therefore write inner loops that are provably stride-aligned and bounds-safe; mis-configured convolutions manifest as compiler errors instead of runtime faults.

Our macro system is central to making this scale across a growing library of tensor operations. Instead of hand-writing trait implementations for every rank and shape

combination, we generate consistent, type-safe boilerplate using declarative macros. These macros abstract over dimension arity and operator traits, allowing the same safety guarantees to be extended from Tensor2 (matrices) to Tensor3 (e.g., image stacks) and Tensor4 (e.g., NCHW batches). Each generated implementation preserves the same shape-checking logic while remaining zero-cost at runtime, thanks to LLVM’s constant folding and inlining optimizations.

We supply compile-time safe kernels for matrix multiplication, constant addition, constant multiplication, element addition, element multiplication, element subtraction, logs, and exponents, each with broadcasts where mathematically valid. All these invariants are enforced before linking, guaranteeing that if the code compiles, every `matmul`, `add`, `sub`, or `mul` (known at compile-time) is dimensionally correct.

The const expressions (`R*C`, `R*W`, etc.) are folded by LLVM. Generated code passes raw pointers and integer literals to the backend, so there is no measurable overhead compared to a handwritten C loop. This compile-time gatekeeping forms the foundation upon which our Metal-accelerated pipeline builds, combining static correctness with hardware-class speed.

#### 4.2 Stack Allocated Tensors With Const Generics

By using Rust’s const generics, our tensor types (e.g., `Tensor2<f32, R, C, NaiveCpu>`) encode shapes directly in the type system. For small tensors, this allows full stack allocation via the `HasStorage` trait, which maps to a fixed-size array `[T; N]` in the `NaiveCpu` backend. As a result, tensors incur no heap allocation, no runtime shape metadata, and benefit from fully inlined accessors and static bounds checks—all optimized away by LLVM.

This approach is ideal for constants, small batches, and intermediate values, ensuring low-latency execution with compile-time shape safety. If an operation has incompatible dimensions (e.g., mismatched matrix multiplication), it fails at compile time. This enforces correctness while achieving performance on par with hand-optimized C code.

By abstracting storage behind the `HasStorage` trait, the same tensor API supports both stack-based backends like `NaiveCpu` and GPU-accelerated memory layouts in Metal, preserving flexibility without sacrificing speed or safety.

#### 4.3 Backend Trait Allows Hot Swappable Backends

To achieve modularity and extensibility in our tensor computation framework, we introduce a generic backend trait that abstracts the execution environment for tensor operations. This trait encapsulates backend specific functionalities like memory allocation, kernel execution, and numerical precision handling. Each backend (ex. `NaiveCpu`, `Metal`) implements this trait, ensuring that

swapping backends only requires a build-time change rather than any modifications to the core tensor API.

By leveraging compile-time polymorphism, we enable backend hot-swapping at build time without incurring any runtime overhead. This approach facilitates backend-specific optimizations while maintaining a clean and consistent core tensor API. Developers can instantiate tensor objects parameterized over the desired backend, for example, `Tensor2<f32, R, C, Metal>` and rely on the type system to dispatch calls to the appropriate implementation. This design makes it possible to use shape-specialized kernels (e.g., a `16x16` matrix multiplication routine) and have them inlined or optimized aggressively, since the compiler knows the exact backend and tensor dimensions at compile time.

Because our trait covers all essential operations—memory allocation, data transfers, kernel invocation, and precision handling—adding support for new execution environments (CPUs, GPUs, or specialized accelerators) is straightforward: simply implement the trait for the new target, and the same tensor API works. This approach preserves a single, consistent tensor interface while allowing each backend to apply its own low-level optimizations and scheduling policies. Rust’s trait system lets each backend implement only the operations it can accelerate, inheriting safe fall-backs for the rest. This means developers can start with minimal, shape safe backends and incrementally optimize the performance-critical kernels without breaking the unified tensor API.

#### 4.4 Metal Performance Shaders Used for Optimization on MacOS

A naive route for Apple-Silicon acceleration would be to hand-craft Metal Shading Language (MSL) kernels or to wrap a cross-platform layer such as `WebGPU/Vulkan`. Both options sacrifice performance: handwritten MSL requires per-SKU retuning to track Apple’s rapidly iterating micro-architectures, while `WebGPU/Vulkan` targets a lowest-common-denominator ISA that cannot exploit proprietary instructions, cache hints, or register-tiling schemes unique to the M-series. Instead, we invoke Metal Performance Shaders (MPS)—Apple’s vendor-supplied library whose GEMM, convolution, activation, and pooling kernels are co-designed with the silicon floorplan. MPS kernels benefit from privileged compiler passes and internal APIs (e.g., fused half-precision accumulation, hidden tile pre-fetch units) that are simply unreachable from user-authored MSL; empirical profiling shows a 1.3-1.6x throughput advantage over our best hand-tuned shaders.

All compute is orchestrated from Rust. We bridge the language boundary via `objc2`, `objc2-metal`, and `objc2-metal-performance-shaders`—three auto-generated crates that surface every MPS\* class as a lifetime-safe Rust handle. This Foreign-Function Interface eliminates raw

pointers and manual retain/release pairs, guaranteeing memory safety without sprinkling unsafe blocks throughout the training loop. It also slashes maintenance effort: when Apple releases new MPS symbols, we regenerate bindings with bindgen rather than touching a single line of shader code.

Batching follows a “batch-per-command-buffer” policy. For each mini-batch (250 samples) we instantiate or recycle MPSMatrix/MPSVector objects, enqueue every layer’s GEMM, bias-add, and ReLU into the same command buffer, commit the buffer once, and call `wait_until_completed()` exactly once per batch. Because MPS overlaps DMA and ALU work internally, this schedule sustains high occupancy with near-zero host-side overhead. The result is a shape-safe, ahead-of-time binary that reaches  $\approx 16\%$  of the M1 Pro’s FP32 roofline—all without writing or tuning a single shader, and with portability guarantees that extend to forthcoming M-series devices.

## 5. Evaluation

We evaluate our system across three axes: (1) end-to-end accuracy on MNIST, (2) matrix multiplication throughput under varying shapes and batch sizes, and (3) compile-time safety and binary portability. Comparisons are made against PyTorch with MPS backend and a naive CPU implementation, using an M1 Pro 10-core MacBook Pro (2021, 16GB unified memory) running MacOS 14.0.

### 5.1 Accuracy and End-to-End Runtime

Our model achieves 99% accuracy on MNIST after 15 epochs, matching PyTorch baselines trained under identical conditions (batch size 250, learning rate 0.001, ReLU activations, softmax cross-entropy loss). Training takes 52 seconds end-to-end on the GPU, including preprocessing and evaluation, compared to 34 seconds in PyTorch/MPS and 127 seconds on our naive CPU backend.

Inference latency for a single batch (250 images) is 8.2ms on the GPU, yielding 25,230 images/sec sustained throughput. While PyTorch MPS reaches slightly higher throughput (30,800 images/sec), our pipeline achieves this without dynamic graph machinery, global interpreters, or Python overhead. Critically, our binary remains under 1.2MB and doesn’t require any external dependencies—making it suitable for edge deployment.

### 5.2 Matrix Multiplication Throughput

To isolate the GEMM kernel’s performance, we benchmark square and rectangular matrix multiplications across a range of sizes (64-1024). Results are reported in GFLOP/s and averaged over 100 runs with warmup.

Our kernel peaks at 850 GFLOP/s (16% of the M1 Pro’s theoretical peak of  $\sim 10.4$ TFLOP/s [7]), with performance tapering slightly for large matrices due to tile

underutilization and increased cache pressure. Compared to PyTorch MPS, our kernel performs competitively—often faster for mid-sized batches common in edge ML workloads.

Matrix Size (MxK x KxN)	Rust MPS (GF/s)	PyTorch MPS (GF/s)	Naive CPU (GF/s)
128 x 128 x 128	147.90	174.0	58.1
256 x 256 x 256	548.6	645.4	73.5
512 x 512 x 512	1714.7	2017.3	142.3

### 5.3 Impact of Fusion and Memory Traffic Reduction

Fusing bias-add and ReLU into the GEMM shader yields a consistent 1.35x speedup versus nonfused execution, verified by toggling a compile time feature flag. Energy measurements from powermetrics show a 17% reduction in average GPU power draw when fusion is enabled, attributed to fewer unified memory reads and improved cache locality.

### 5.4 Compile-Time Guarantees and Developer Ergonomics

To validate compile-time shape enforcement, we attempt to compile 50 incorrect tensor operations (e.g., mismatched GEMMs, invalid broadcasts, shape-violating additions). All 50 result in compiler errors with descriptive messages indicating the violated constraints—none silently pass or require runtime checks. Compared to PyTorch or JAX, which may raise shape errors only at runtime or during model execution, our system eliminates entire classes of shape bugs before the binary is built.

Build time remains manageable. A complete rebuild of the project takes 10.4 seconds in release mode. Hot reloads during development (e.g. changing layer weights or activation functions) compile in under 0.1 seconds with Cargo’s incremental build system.

Our compiled binary is 1.2MB in release mode with no dynamic linking, interpreters, or runtime dependency resolution. By contrast, the same MNIST model in PyTorch with Python, NumPy, and MPS dependencies requires over 500MB of installed packages and system libraries. Our binary is self-contained and reproducible in rustc alone, making it suitable for constrained deployment targets.

## 6. Conclusion

Our results demonstrate that it is feasible and beneficial to design machine learning systems that enforce shape correctness at compile time without sacrificing hardware level performance. By combining Rust’s const generic type system with Metal compute shaders, we produce a model that is competitive with PyTorch in accuracy and

throughput, yet offers stronger correctness guarantees and a dramatically smaller, dependency-free deployment.

The 99% accuracy achieved on MNIST confirms that our compile time guarantees do not impede learning dynamics, optimizer behavior, or model expressiveness. Further, our throughput benchmarks shows that our MPS approach and tensor system can match or exceed the performance of PyTorch’s CPU backend while delivering on-par performance with PyTorch’s MPS backend on medium sized inference workloads with the safety benefits of Rust. Our stack allocated tensors also reduce energy consumption by avoiding redundant memory traffic, a crucial optimization on unified memory architectures like Apple Silicon.

However, our system has important limitations—both in terms of model expressiveness and developer workflow. At the architectural level, our pipeline currently supports only a limited number of operations and up to rank-4 tensors. While sufficient to validate our safety and performance claims, more complex architectures require support for more tensor ranks. These components would significantly increase the size and complexity of the shape-type system, and may require compile-time shape inference or higher-kinded generics—features Rust does not yet support directly.

Our system leverages Rust’s const-generics to encode many tensor dimensions at compile time, but a future approach could make it so not all dimensions are not required to be statically known. This would allow for features like dynamic batch sizes, support for variable-sized user input, etc. Currently, The system lacks support for fully dynamic shapes along feature axes, which limits applications involving variable-length sequences (e.g., in NLP) or inputs with nonuniform spatial resolution (e.g., real-time video). While frameworks like PyTorch and JAX allow such shapes to propagate through the computational graph dynamically, our system would require either pre-padding or shape-specialized implementations. Expanding support for richer forms of dynamic shape reasoning—potentially through trait-based runtime assertions or shape-polymorphic types—remains a promising direction for future work.

There are also practical limitations stemming from Rust’s position in the current ML ecosystem. Most machine learning researchers and practitioners rely heavily on Python, and the majority of tools in the stack—such as TensorBoard, Hugging Face Transformers, scikit-learn pipelines, or ONNX export—are not readily interoperable with Rust projects. Our system, while safe and efficient, cannot currently import pre-trained models from other frameworks, nor can it export its weights in a widely supported format. Moreover, common visualization, logging, and checkpointing libraries require custom implementations or language bindings. These limitations create friction for adoption in real-world workflows,

especially for researchers accustomed to the Python-first tooling culture. While crates like `burn` and `candle` are beginning to bridge these gaps, Rust remains several years behind in terms of ecosystem maturity for applied ML.

Our choice of hyperparameters—batch size 250, learning rate  $1e-3$  with the Adam optimizer—was informed by a small grid search on a held-out validation set. Although we did not observe signs of overfitting (validation accuracy stabilized within 0.5% of training accuracy), we employed early stopping to avoid excessive specialization. No explicit regularization (e.g., dropout, weight decay) was necessary, likely due to the simplicity of the dataset. Scaling to more complex tasks will require more robust optimization pipelines and may necessitate compile-time-safe abstractions for regularization operators.

In sum, while our system proves that compile-time tensor correctness and near-peak GPU utilization can coexist, important work remains to bridge the gap between this shape-safe foundation and the flexible, expressive workflows expected in modern ML pipelines. Balancing safety, performance, and usability remains an open challenge—but one that Rust’s type system, with careful design, is well-positioned to tackle.

## References

- [1] C. Lattner, M. Amini, U. Bondhugula, A. Cohen, A. Davis, J. Pienaar, R. Riddle, T. Shpeisman, N. Vasilache, and O. Zinenko. MLIR: A Compiler Infrastructure for the End of Moore’s Law. In *Proceedings of the IEEE/ACM Int. Symp. Code Generation and Optimization (CGO)*, pp. 2-14, 2021.
- [2] T. Chen, T. Moreau, Z. Jiang, L. Zheng, E. Q. Yan, H. Shen, M. Cowan, L. Wang, Y. Hu, L. Ceze, C. Guestrin, and A. Krishnamurthy. TVM: An Automated End-to-End Optimizing Compiler for Deep Learning. In *Proc. USENIX Symp. Operating Systems Design and Implementation (OSDI)*, pp. 578-594, 2018.
- [3] A. Paszke, D. Johnson, D. Duvenaud, D. Vytiniotis, A. Radul, M. J. Johnson, J. Ragan-Kelley, and D. Maclaurin. Getting to the Point: Index Sets and Parallelism-Preserving Autodiff for Pointful Array Programming. *Proc. ACM Program. Lang.* 5(ICFP): 1-29, 2021.
- [4] B. Saeta, D. Shabalin, M. Rasi, B. Larson, X. Wu, P. Schuh, M. Casbon, D. Zheng, S. Abdurassool, A. Efremov, D. Abrahams, C. Lattner, and R. Wei. Swift for TensorFlow: A Portable, Flexible Platform for Deep Learning. In *Proc. Mach. Learn. and Systems (MLSys)*, pp. 803-815, 2021.
- [5] H. Shen, J. Roesch, Z. Chen, W. Chen, Y. Wu, M. Li, V. Sharma, Z. Tatlock, and Y. Wang. Nimble: Efficiently Compiling Dynamic Neural Networks for Model Inference. In *Proc. Mach. Learn. and Systems (MLSys)*, pp. 208-222, 2021.
- [6] K. Zhu, W. Zhao, Z. Zheng, T. Guo, P. Zhao, J. Bai, J. Yang, X. Liu, L. Diao, and W. Lin. DISC: A Dynamic Shape Compiler for Machine Learning Workloads. *arXiv preprint arXiv:2103.05288*, 2021.

- [7] P. Hübner, A. Hu, I. Peng, and S. Markidis. Apple vs. Oranges: Evaluating the Apple Silicon M-Series SoCs for HPC Performance and Efficiency. arXiv preprint arXiv:2502.05317, 2025.
- [8] D. Feng, Z. Xu, R. Wang, and F. X. Lin. Profiling Apple Silicon Performance for ML Training. arXiv preprint arXiv:2501.14925, 2025. arxiv.org
- [9] OpenXLA Team. XLA: Optimizing Compiler for Machine Learning. White Paper, 2024.
- [10] J. Tang, R. Sarokin, E. Ignasheva, G. Jensen, L. Chen, J. Lee, A. Kulik, and M. Grundmann. Scaling On-Device GPU Inference for Large Generative Models. arXiv preprint arXiv:2505.00232, 2025.